

Succession

SN07 OSS Guide (IP)

Advance Feature Guide

SN07 Standard 01.04 December 2004

Succession

SN07 OSS Guide (IP)

Advance Feature Guide

Publication number: PLN-07IP-OSS

Product release: SN07

Document release: Standard 01.04

Date: December 2004

Copyright © 2004 Nortel Networks,
All Rights Reserved

United States of America

NORTEL NETWORKS CONFIDENTIAL: The information contained herein is the property of Nortel Networks and is strictly confidential. Except as expressly authorized in writing by Nortel Networks, the holder shall keep all information contained herein confidential, shall disclose the information only to its employees with a need to know, and shall protect the information, in whole or in part, from disclosure and dissemination to third parties with the same degree of care it uses to protect its own confidential information, but with no less than reasonable care. Except as expressly authorized in writing by Nortel Networks, the holder is granted no rights to use the information contained herein.

Nortel Networks, the Nortel Networks logo, the Globemark, How the World Shares Ideas, and Unified Networks are trademarks of Nortel Networks.



Publication History

December 2004

Re-release of the Standard version of this document for SN07 for the FVS release.

August 2004

Re-release of the Standard version of this document for SN07 due to churn.

July 2004

Standard release of this document for SN07.

May 2004

Preliminary release of this document for SN07. The following sections are updated for this release:

- Mapping tables (ACTID-to-solutions; ACTID-to-OAM&P impacts)
- New or changed per release
- Feature deltas by product/network element
- Baseline information for Logs/Faults
- Baseline information for OMs/PMs
- Appendices

Table of Contents

SN07 Feature Mapping Tables 13

Table: Network elements-to-ACTID-to-documentation elements mapping 14

Table: Network elements-to-ACTID-to-solution mapping 18

New or changed per release

23

Logs/faults changes overview 23

Data Schema/MIBs changes overview 45

Commands and User Interface changes overview 61

Servord changes overview 72

Office Parameter changes overview 74

OM/PM changes overview 78

AMA/Billing changes overview 84

Software Optionality Control (SOC) changes overview 84

SN07 Feature Deltas 89

Product = AIN 89

A00001990 -- CAIN via CIC Route PEP Sourcing (Succession on DMS) 89

A00002016 -- AINDENY CUSTSTN increase from 10 to 15 (Succession on DMS) 95

A00004500--IN TCAP Messaging on IP (Succession on DMS) 103

Product = Carrier Hosted Services 128

A00006495 -- H.323 Flexible Carriers (MMBS) 128

A00006496 -- H.323 Multiple D Channels (MMBS) 130

A00006741 -- H.323 Gatekeeper to CS2K Gatekeeper Interoperability (MMBS) 134

A00007063 -- H.323 Gateway Profile Changes (MMBS) 145

A00007211 -- SN07 H.323 GWC600 Log Changes (MMBS) 152

Product = CS 2000 153

A00001319 -- Device activity & RMID-PWID restoration tool & Panther enhancements (PT-AAL1, Succession on DMS) 153

A00001649 -- SBA Robustness: End-to-end Integrity (Succession on DMS) 166

A00001650 -- SBA Patch Size Reduction (Succession on DMS) 175

A00001743 -- SYSLOG Consolidation for Succession (PT-IP, UA-IP, IAW, IAC) 178

A00002008 -- CBM Introduction (Succession on DMS) 194

A00002009 -- Enhance display on PEPSET (Succession on DMS) 203

A00002011 -- Virtual Office Worker (Succession on DMS) 219

A00002012 -- HIOP-CMIC/RTIF development (Succession on DMS) 283

A00002013--Intelligent Network T1 Timer Expiry Message Suppression (Succession on DMS) 334

A00002047 -- SPM Backplane (Succession on DMS) 344

A00002133 -- CBM SDM SW Installation & Commissioning (Succession on DMS) 352

A00002155 -- SSH Core File Transfer (SCFT) for CBM and SDM (Succession on DMS) 371

A00002186 -- IOM DDU Capacity Enhancement (Succession on DMS) 374
A00002196 -- Do Not Disturb - Residential Market (Succession on DMS) 376
A00002281 -- AMAPRT Expansion (Succession on DMS) 403
A00002340 -- Add Extension Registers for CDR OMS (Succession on DMS) 405
A00002431 -- LX82BA capacity delivery (Succession on DMS) 415
A00002432 -- SPM Enhanced Overload OMs and Logs (Succession on DMS) 435
A00002433 -- XA-Core Baseline Control (Succession on DMS) 452
A00002499 -- Store Audit for XA-CORE (Succession on DMS) 478
A00002505--Universal Signaling Point Interface Client - GUI (PT-IP, UA-IP, IAC) 483
A00002510 -- LANCOMM IP over IRM (Succession on DMS) 489
A00002538 -- Performance Measurement Tools (Succession on DMS) 494
A00002549 -- CSP20 CALLP Robustness (Succession on DMS) 499
A00002555 -- SERVORD manipulation of the GND option
(Succession on DMS, UA-IP) 506
A00002585 -- TMM Development for PTS Trunk (PT-IP) 515
A00002741 -- Supernode Billing Application Base Real Time Billing Robustness
(Succession on DMS) 535
A00002744 -- SBA: Automatic Recovery File Closure (Succession on DMS) 538
A00002757 -- NSDM Fault Management HA (Succession on DMS) 541
A00002766 -- Add Extension Registers for AMA OMs (Succession on DMS) 547
A00002822 -- UI Manager (Succession on DMS) 551
A00002858 -- SYSB Carrier (Succession on DMS) 569
A00002901 -- Meet-Me Conference Enhancement (Succession on DMS) 588
A00002960 -- Originator Identification Screening (Succession on DMS) 609
A00002966 -- Base Re-architecture Phase 2 (Succession on DMS) 619
A00002979 -- Panther Electronic Software Delivery (Succession on DMS) 622
A00003073 -- SimRing Deny Redirection (SRDR) (Succession on DMS) 631
A00003273 -- NGSS Application Maintenance (PT-IP) 644
A00003277 -- SP2000 Logs, Alarms, OMs, Subsystem (PT-IP) 644
A00003279 -- Load Balancing (PT-IP) 644
A00003371 -- SESM Common Inventory Data Consolidation
(PT-IP, UA-IP, IAW, IAC) 644
A00003454 -- Secure and Firewall Compatible CS2M and UE9KEM Client
GUI Communication (PT-IP, UA-IP, IAW, IAC) 654
A00003459 -- GWC Lifecycle: SSC & Application Datasync Support (UA-IP) 668
A00003485--ISUP 200,000 Ports Trunk Support (PT-IP) 681
A00003486 -- Gateway Location information (UA-IP) 685
A00003487 -- Tri-modal Provisioning, Logs and OMs (UA-IP) 703
A00003489 -- ABI SMS Support (UA-IP) 927
A00003490 -- Network Change Upgrade Tools (UA-AAL1) 936
A00003506 -- H.248 Per Trunk Signaling Development (PT-IP) 984
A00003562 -- SAM21 Element Manager support for CICM (UA-IP) 1030
A00003568 -- CICM ECS Location Identification (UA-IP, IAC, IAW) 1042

A00003576 -- Trunk Security (IAC) 1079
A00003613 -- SSPFS: CBM Configuration Parameters (PT-IP) 1080
A00003617 -- AlarmD Integration (PT-IP) 1090
A00003618--SSPFS: High Availability Enhancements (PT-IP, AAL2) 1104
A00003630 -- TGCP for the Cable Market (IAC) 1112
A00003667 -- SESM NB Alarm Interface Changes required for OSS (UA-IP) 1155
A00003698 -- Razor Gateway Requirements for Trunking (PT-IP) 1163
A00003711 -- CS2000 SUPPPORT FOR GateWay Inter Machine Trunk (GWIMT)
ON Passport Voice Gateway (UA-IP) 1167
A00003767 -- IP ABI PPVM Robustness & Msg Loss Alarms (UA-IP) 1347
A00003789 -- INTRA IMT CAUSE Enhancements (Succession on DMS, AAL2) 1367
A00003905 -- DIRP Enhancements for Billing (Succession on DMS) 1380
A00003933 -- Succession Communication Server (SCS) 2000 - Session Server
Manager: SCS 2000 - SIP Gateway application (PT-IP) 1399
A00003971 -- SPM Log Robustness (Succession on DMS) 1537
A00003995 -- SESM: H323 GW Change Capability (UA-IP) 1570
A00004005 -- NCGL Support for SAM XTS and SP2000 (PT-IP) 1603
A00004020 -- USP Java GUI Introduction to Succession (PT-IP) 1645
A00004036 -- AIN Update Message Query, Response Enhancement
(Succession on DMS) 1652
A00004037 -- USNBD CALEA CMR Interaction Enhancements
(Succession on DMS) 1720
A00004045 -- Calling Line Identification Directory Number (CLIDN) for
DMS-250 (Succession on DMS, AAL2) 1725
A00004046 -- ECAN for Trimodal, 9K-IP-IPIW to Legacy (UA-IP) 1739
A00004271 -- SIP App Server SOC (PT-IP) 1753
A00004391 -- ACD Agent Expansion from 9,999 to 30,000 Agents
(Succession on DMS) 1763
A00004414 -- SIP Call Server SOC (PT-IP) 1792
A00004422--Enhanced 911 Dynamic Packet Trunks Session Initiation
Protocol-Telephony Call Trace (Succession on DMS) 1806
A00004554--SDM FX System Backup Enhancements (Succession on DMS) 1817
A00004713--1+1 Speedometer Support (Succession on DMS) 1820
A00004868--FTP Proxy for SDM and CBM (Succession on DMS) 1823
A00004872 -- MIDCALL Tones /Services for CS2K (UA-IP, IAW) 1825
A00004922-4923 -- DMS-250 N449 PRI Enhancements (PT-IP) 1833
A00005007--Cause Indicators parameter support for DTAG AMA Enhancement
(PT-IP) 1842
A00005073--SBA Outbound Connection Security (Succession on DMS) 1850
A00005074--OMDD: Outbound Connection Security (Succession on DMS) 1858
A00005190--nSDM (Takoma) OC3 Node and Link Maintenance
(Succession on DMS) 1864
A00005192--CBM 800 OC3 BRISC connectivity and OC3 node and link maintenance

(Succession on DMS) 1873
A00005193 -- 9+1 Performance Measurements Tools Support (Succession on DMS) 1882
A00005363--CAIN and CDR Support for GNS Personal Toll Free Service
(Succession on DMS) 1885
A00005268 -- SBA: Multi-volume Support for Core Backup (Succession on DMS) 1898
A00005485 -- SAM21 Platform Installation on SSPFS (PT-IP, UA-IP, IAC, IAW) 1902
A00005734 -- Multiple Time Zone (MTZ) support for CICM lines (IAW) 1902
A00005758 -- ESUP over Telnet support (Succession on DMS) 1910
A00005986 -- EM integration with PAM+ proxy (IAW) 1913
A00005988 -- XPe OS Evolution and platform boot (IAW) 1919
A00006405 -- Multi Point Code Expansion (Succession on DMS, AAL2) 1929
A00006483 -- Audio Server Node Announcement Capacity Increase to 1280
(PT-IP, AAL2) 1929
A00006693 -- XA-Core IO Capacity Monitoring Toolset (Succession on DMS) 1935
A00008902 -- SAM21 Log Changes (PT-IP, UA-IP) 1963
A59039138 -- (Visual) Message Waiting Indicator (V)MWI/CFX (IAC) 1967
Product = CS 2000 Core Manager 1979
A00002920 -- Support of Passport 8600 logs on SDM (Succession on DMS) 1979
Product = Centrex IP Client Manager (CICM) 1985
A00003717 -- OSSGate - Centrex IP Flow-through Provisioning (IAW) 1985
A00003718 & A00003719 -- Alarms, Logs & Performance for Centrex IP
Client Manager (IAW) 2000
Product = MG 4000 2019
A00003650 -- MG4K-IP Logs (PT-IP, UA-IP) 2019
A00003669 -- Media Gateway 4000 - Internet Protocol (MG4K-IP) (PT-IP) 2030
A00003672 -- GEM NTLZ20CA Core Definition (PT-IP) 2044
A00003773--OM for TRKQOS for MG4K IP (PT-IP) 2048
Product = MG9000 2055
A00001893 and A00001894--MG9K Imaging (UA-IP) 2055
A00003074 -- MG9000 Manager Capacity Increase (UA-IP) 2085
A00003531 -- MG9K EM - Frame location enhancements (UA-IP) 2092
A00003567 -- MG9000 Manager - ABI ESA Support (UA-IP) 2115
A00003571 -- MG9000 Manager - New MG9000 Card Support (UA-IP) 2130
A00003591--MG9000 OC3 Channelization support from EM (UA-IP) 2137
A00003737--LCI Remote Access, Enhancements and MG9000 Security (UA-IP) 2157
A00004109--MG9K Hardware Upgrade and Call Processing Changes (UA-IP) 2166
A00005016 -- VMG Out of Service Alarms (UA-IP) 2170
A00005375 -- New Shelf Discovery Alarms (UA-IP) 2187
A00006639--MG9K Overload OM pegs (UA-IP) 2209
CD003593--MG9000 Aggregation on Passport 15000 and PVG (UA-IP) 2214
Product = MediaServer 2000 2219
A00004873--MS2000 CLUI Enhancements (UA-IP, IAW) 2219
Product = Network Patch Manager 2227

A00003560 -- Patching SSPFS, CBM, and IEMS via the NPM (UA-IP) 2227
Product = SAM21 Element Manager 2238
A00003562--New Cards Support in SAM21 EM (UA-IP) 2238
Product = TOPS 2253
A00002740 -- TOPS International DA Call Completion (Succession on DMS) 2253
A00002765 -- Station Paid Routing (Succession on DMS) 2264
A00003687 -- Integration (Succession on DMS) 2278
A00003704 -- OSSAIN Enhancements for SN07 (Succession on DMS) 2354
A00005160--OSSAIN XA-Core Data Messaging Capacity Enhancements
(Succession on DMS) 2363

Succession baseline information**2411****Logs/Faults information 2411**

Audio Codes Media Server (AMS)--available logs/faults for Succession 2417
Audio Provisioning Server (APS)--available logs/faults for Succession 2418
Compact Call Agent (CCA) --available logs/faults for Succession 2418
CS2K Management Tools (CMT)--available logs/faults for Succession 2420
SAM21--available logs/faults for Succession 2421
CS2000 XA-Core--available logs/faults for Succession 2427
GWC--available logs/faults for Succession 2439
SPM--available logs/faults for Succession 2442
Stormia (STM)-available logs/faults for Succession 2450
MG4000-available logs/faults for Succession 2450
MG9000--available logs/faults for Succession 2451
NPM--available logs/faults for Succession 2462
CS2000 Core Manager--available logs/faults for Succession 2464
Passport 8600--available traps/faults for Succession 2468
PVG Logs/Faults in Succession 2472
Preside Multiservice Data Manager logs/faults 2472
QCA Logs/Faults in Succession 2472
UAS--available logs/faults for Succession 2474
USP Logs/Faults in Succession 2484

Operational measurements/performance measurements 2485

OM collection and delivery 2485
PM collection and delivery 2485
Performance Monitoring Poller data collection output 2485
AMS Performance Measurements 2488

Available OMs/ PMs in Succession 2489

AudioCodes media servers PMs in Succession 2489
SAM21 OMs/PMs in Succession 2495
CS 2000 XA-Core OMs/PMs in Succession 2496
DPT-SPM OMs/PMs in Succession 2500
IW-SPM OMs in Succession 2503

GWC OMs/PMs in Succession 2504
MG9000 OMs/PMs in Succession 2507
PVG/Media Gateway 15000 OMs/PMs in Succession and Passport
15000/Multiservice Switch OMs/PMs 2508
Statistics collection and data flow 2509
Line Provisioning OMs/PMs in Succession 2511
TOPS OMs/PMs in Succession 2512
UAS OMs/PMs in Succession 2515
USP OMs/PMs in Succession 2517
OM Export interface on USP 2518

SN07 IEMS Functionality 2523

IEMS Northbound Interfaces 2523
General Information 2523
New or changed in SN07 2523
IEMS Northbound Fault Interface 2524
IEMS Northbound Fault Specifications 2529
Northbound Performance Interface 2568
Common Performance Record Comma Separated Values (CSV) format 2585
Inventory/Topology Interface 2591
IEMS Supported Devices 2596
Call Agent Core 2598
GUI/CLUI Documentation for Call Agent Core 2601
Call Agent Platform 2602
GUI/CLUI Documentation for Call Agent Platform 2604
Centrex IP Call Manager (CICM) 2604
GUI/CLUI Documentation for CICM 2612
Passport 8600 2613
Gateway Controller (GWC) 2622
Media Application Server (MAS) 2626
Multimedia Communication Server (MCS) 2633
Media Gateway 9000 (MG9000) 2636
MultiService Switch 7400, 15000, 20000 2639
MS2000 Series Node 2645
Session Server Manager 2656
SAM21 Shelf Controller 2664
Storage Manager (STORM) 2666
Universal Audio Server (UAS) 2674
Universal Signaling Point (USP) 2677
XACore 2681
SDM Platform 2690
Succession Server Platform Foundation Software (SSPFS) 2692
CS2000 Core Manager 2695

Centrex IP Call Manager (CICM Manager)	2698
GUI/CLUI Documentation for CICM Manager	2708
GWC Manager	2708
Integrated Element Management System (IEMS)	2711
MG9000 Manager	2713
Multi-Service Data Manager (MDM)	2716
SAM21 Element Manager	2721
Audio Provisioning Server (APS)	2724
Line Maintenance Manager (LMM)	2726
Network Patch Manager (NPM)	2727
OSSGate	2729
QoS Collector Application (QCA)	2730
Trunk Maintenance Manager (TMM)	2733
Non-Topology Elements	2735
Data Audit System	2735
IW-SPM IP	2737
MG9000 Manager Mid-Tier	2740
OM Collector	2742
V5.2 Data Audit	2744
References	2749
IEMS Appendix 1: Northbound OSS Configurations	2751
IEMS Appendix 2: Nortel Alarm Extension MIB	2755
Appendix A: Passport 8600 Performance Metrics	
Appendix B: MG9000 OMs	
Appendix C: Passport 15000 and MDM Alarm Logs Summary	
Appendix D: USP OMs	
Appendix E: MG9000 Alarms, Event Logs, Audit Logs	
Appendix F: CICM Logs	



About this document

When to use this document

This document supports the SN07 release of Succession Solutions. It provides SN07 design documents that contain Operations Support Systems (OSS) information. It also provides information on what is new and changed in SN07, related to the following areas:

- Logs/faults
- Data schema tables/MIBs
- Commands/User Interface
- Service Orders
- Office Parameters
- Operational/performance measurements (OMs/PMs)
- AMA/billing
- Software optionality control (SOC)

In addition, it provides a baseline of the Logs/Alarms and Operational Measurements (OMs)/Performance Measurements (PMs) that are available in Succession, organized by network element.

Information in this document is believed to be accurate at the time of publication, but it is subject to change. Use of this document should be restricted to resource planning and estimating for SN0&. **Do not use this document to make changes to existing software.**

How this document is organized

This document is divided into the following sections:

- Mapping tables
 - Mapping network elements to ACTIDs to solutions
 - Mapping network elements to ACTIDs to OAM&P documentation elements
- New/changed information for SN07
 - Logs and faults
 - Data Schema/MIBs
 - Commands/User Interface
 - Service Order
 - Office Parameters
 - Operational Measurements/Performance Measurements
 - AMA/Billing
 - Software Optionality Control (SOC)
- SN07 features, organized by network element
- Succession Baseline information
 - Logs/faults available in Succession, organized by network element
 - OMs/PMs available in Succession, organized by network element
- Appendix A: Network Data Provisioning
- Appendix B: SAM21 Logs and Alarms
- Appendix C: MG9000 MIB OMs/PMs
- Appendix D: USP logs/faults and OMs/PMs
- Appendix E: UAS Logs

Audience

This document is intended for Nortel Networks personnel, third-party OSS vendors, and customers who need to plan resources and estimate network impacts for this release.

How to check the version and issue of this document

The document release information on the title page and the footers of this document indicate the version and issue, for example, 01.01.

The first two digits indicate the version. The version number increases each time the document is updated to support a new software release. For example,

the first release of a document is 01.01. In the next software release cycle, the first release of the same document is 02.01.

The second two digits indicate the issue. The issue number increases each time a document is revised but re-released in the same software release cycle. For example, the second release of a document in the same software release cycle would be 01.02.

Writing conventions

Descriptions of commands, parameters, and responses in this document use the following conventions:

Input prompt

An input prompt (> or #) indicates that the information that follows is a command:

>LIST

Commands and fixed parameters

Commands and fixed parameters that are entered at the MAP terminal are shown in uppercase letters:

>LIST ALL

Variables

Variables that are entered at a MAP terminal are shown in lowercase letters:

>TABLE table_name

References in this document

This document refers to the following Nortel Networks publications:

- 297-8001-840, *NA DMS-100 Log Report Reference Manual*
- 297-2621-840, *DMS-250 Logs Reference Manual*
- 297-5051-840, *SDM Log Report Reference Manual*
- NN10021-111, *cCS 2000 Product and Technology Fundamentals*
- NN10025-111, *SAM21 Product and Technology Fundamentals*
- NN10089-911, *SAM21 Fault Management*
- NN10083-911, *CS 2000 Fault Management*
- NN10090-911, *GWC Fault Management*
- NN10012-111, *SPM Product and Technology Fundamentals*
- NN10075-911, *SPM Fault Management*

- NN10079-911, *DPT-SPM (IP) Fault Management*
- NN10078-911, *IW-SPM (IP) Fault Management*
- NN10073-911, *UAS Fault Management*
- NN10085-911, *cCS 2000 Fault Management*
- NN10082-911, *CS 2000 Core Manager Fault Management*
- NN10300-100, *CS 2000 Management Tools IP Solutions Basics*
- NN10325-900, *CS 2000 Management Tools ATM/IP Fault Management*
- NN10276-500, *CS 2000 Management Tools ATM/IP Configuration Management*
- NN10149-711, *CS 2000 Performance*
- NN10145-711, *DPT-SPM (IP) Performance*
- NN10144-711, *IW-SPM (IP) Performance*
- NN10137-711, *USP Performance*

In order to find information about the Preside Multiserver Data Manager (MDM), refer to the following documents:

- 241-6001-011, *Preside MDM Fault Management User Guide*
- 241-6001-501, *Preside MDM Proxy Alarms Reference Guide*
- 241-6001-801, *Preside MDM Overview*



SN07 Feature Mapping Tables

Introduction

This document contains advance information about differences in operations, administration, maintenance, and provisioning (OAM&P) for Succession Networks Release 7 (SN07). The purpose of this document is to provide early information about new, modified or deleted items related to the following areas:

- Faults, including logs and alarms
- Data schema tables
- Office parameters
- User interface/human-machine interface
- Operational/performance measurements
- Software optionality control (SOC)
- Service orders
- AMA/billing

SN07 product information

Table: Network elements-to-ACTID-to-documentation elements mapping

This table illustrates mapping from the network elements to their related ACTIDs to documentation elements (logs/faults, data schema, office parameters, servord, alarms, user interface/HMI, OMs/PMs, AMA/billing, and SOC (Software Optionality Control).

SN07 Solutions		Documentation Elements							
PRODUCT	ACTID	Logs/Faults	Data Schema	Office Params	Service Orders	Commands/User Interf/HMI	OMs/PMs	AMA/Billing	Optionality
AIN	A00001990	X	X						X
AIN	A00002016		X		X	X			X
AIN	A00004500		X				X		X
Carrier Hosted Svcs	A00006495					X			
Carrier Hosted Svcs	A00006496					X			
Carrier Hosted Svcs	A00006741					X			
Carrier Hosted Svcs	A00007063					X			
Carrier Hosted Svcs	A00007211	X							
CS 2000	A00001319	X				X			
CS 2000	A00001649	X				X			
CS 2000	A00001650					X			
CS 2000	A00001743	X				X			
CS 2000	A00002008							X	
CS 2000	A00002009		X		X				X
CS 2000	A00002011								X
CS 2000	A00002012	X				X			
CS 2000	A00002013	X		X					X
CS 2000	A00002047		X			X			
CS 2000	A00002133					X			
CS 2000	A00002155					X			
CS 2000	A00002186								X
CS 2000	A00002196		X		X				X
CS 2000	A00002281		X						
CS 2000	A00002340						X		
CS 2000	A00002431		X						X
CS 2000	A00002432						X		
CS 2000	A00002433	X	X			X			
CS 2000	A00002499	X							
CS 2000	A00002505					X			

SN07 Solutions		Documentation Elements							
PRODUCT	ACTID	Logs/Faults	Data Schema	Office Parns	Service Orders	Commands/User Interf/HMI	OMS/PMs	AMA/Billing	Optionality
CS 2000	A00002510	X							
CS 2000	A00002538	X					X		
CS 2000	A00002549	X							
CS 2000	A00002555				X				
CS 2000	A00002585					X			
CS 2000	A00002741					X			
CS 2000	A00002744					X			
CS 2000	A00002757	X							
CS 2000	A00002766						X		
CS 2000	A00002822					X			
CS 2000	A00002858	X		X		X			
CS 2000	A00002901		X						
CS 2000	A00002960		X						X
CS 2000	A00002966					X			
CS 2000	A00002979					X			
CS 2000	A00003073		X		X	X			
CS 2000	A00003371	X							
CS 2000	A00003454					X			
CS 2000	A00003459	X	X	X		X			
CS 2000	A00003485		X			X			
CS 2000	A00003486		X			X			
CS 2000	A00003487	X	X	X		X	X		
CS 2000	A00003489					X			
CS 2000	A00003490		X			X			
CS 2000	A00003506		X						
CS 2000	A00003562					X			
CS 2000	A00003568		X			X			
CS 2000	A00003576					X			
CS 2000	A00003613					X			
CS 2000	A00003617	X				X			
CS 2000	A00003618					X			
CS 2000	A00003630		X			X			
CS 2000	A00003667	X				X			
CS 2000	A00003698					X			
CS 2000	A00003711		X	X					

SN07 Solutions		Documentation Elements							
PRODUCT	ACTID	Logs/Faults	Data Schema	Office Params	Service Orders	Commands/User Interf/HMI	OMs/PMs	AMA/Billing	Optionality
CS 2000	A00003767	X	X			X			
CS 2000	A00003789		X	X					X
CS 2000	A00003905		X						X
CS 2000	A00003933	X	X			X			
CS 2000	A00003971	X				X			
CS 2000	A00003995					X			
CS 2000	A00004005	X				X	X		
CS 2000	A00004020					X			
CS 2000	A00004036							X	X
CS 2000	A00004037	X				X			
CS 2000	A00004045	X	X						X
CS 2000	A00004046			X					
CS 2000	A00004271	X					X		
CS 2000	A00004391		X	X	X	X			X
CS 2000	A00004414								X
CS 2000	A00004422					X			
CS 2000	A00004554					X			
CS 2000	A00004713			X					
CS 2000	A00004868					X			
CS 2000	A00004872		X						
CS 2000	A00004922-23								
CS 2000	A00005007			X					
CS 2000	A00005073	X				X			
CS 2000	A00005074					X			
CS 2000	A00005190		X			X			
CS 2000	A00005192	X							
CS 2000	A00005193		X						
CS 2000	A00005363	X	X						X
CS 2000	A00005268	X				X			
CS 2000	A00005485					X			
CS 2000	A00005734		X		X				
CS 2000	A00005758					X			
CS 2000	A00005986	X							
CS 2000	A00005988					X			
CS 2000	A00006405								

SN07 Solutions		Documentation Elements							
PRODUCT	ACTID	Logs/Faults	Data Schema	Office Params	Service Orders	Commands/User Interf/HMI	OMs/PMs	AMA/Billing	Optionality
CS 2000	A00006483		X						
CS 2000	A00006693			X		X	X		
CS 2000	A00008902	X							
CS 2000	A59039138			X	X				
CS 2000 Core Mgr.	A00002920					X			
Centrex IP	A00003717			X	X				
Centrex IP	A00003718-19	X							
MG 4000	A00003650	X	X						
MG 4000	A00003669		X						
MG 4000	A00003672		X						
MG 4000	A00003773			X			X		
MG 9000	A00001893-94					X			
MG 9000	A00003074	X				X			
MG 9000	A00003531					X			
MG 9000	A00003567	X				X			
MG 9000	A00003571	X				X			
MG 9000	A00003591	X				X			
MG 9000	A00003737		X			X			
MG 9000	A00004109	X							
MG 9000	A00005016	X	X			X			
MG 9000	A00005375	X							
MG 9000	A00006639						X		
MG 9000	CD003593					X			
Media Server 2000	A00004873					X			
Network Patch Mgr.	A00003560					X			
SAM21 Element Mgr.	A00003562					X			
TOPS	A00002740		X						X
TOPS	A00002765		X						
TOPS	A00003687	X	X	X			X		
TOPS	A00003704		X						
TOPS	A00005160		X			X	X		

Table: Network elements-to-ACTID-to-solution mapping

This table illustrates mapping connections between the network elements, their related ACTIDs, and the applicable solutions.

SN07 Solutions							
PRODUCT or APPLICATION	ACTID	PT-IP	UA-IP	IAW	IAC	Succ on DMS	MMBS
AIN	A00001990					X	
AIN	A00002016					X	
AIN	A00004500					X	
Carrier Hosted Svcs	A00006495						X
Carrier Hosted Svcs	A00006496						X
Carrier Hosted Svcs	A00006741						X
Carrier Hosted Svcs	A00007063						X
Carrier Hosted Svcs	A00007211						X
CS 2000	A00001319					X	
CS 2000	A00001649					X	
CS 2000	A00001650					X	
CS 2000	A00001743	X	X	X	X		
CS 2000	A00002008					X	
CS 2000	A00002009					X	
CS 2000	A00002011					X	
CS 2000	A00002012					X	
CS 2000	A00002013					X	
CS 2000	A00002047					X	
CS 2000	A00002133					X	
CS 2000	A00002155					X	
CS 2000	A00002186					X	
CS 2000	A00002196					X	
CS 2000	A00002281					X	
CS 2000	A00002340					X	
CS 2000	A00002431					X	
CS 2000	A00002432					X	
CS 2000	A00002433					X	
CS 2000	A00002499					X	
CS 2000	A00002510					X	
CS 2000	A00002538					X	
CS 2000	A00002549					X	
CS 2000	A00002555		X			X	
CS 2000	A00002556					X	
CS 2000	A00002585	X				X	
CS 2000	A00002741					X	
CS 2000	A00002744					X	
CS 2000	A00002757					X	

SN07 Solutions								
PRODUCT or APPLICATION	ACTID	PT-IP	UA-IP	IAW	IAC	Succ on DMS	MMB S	AAL2
CS 2000	A00002766					X		
CS 2000	A00002822					X		
CS 2000	A00002858					X		
CS 2000	A00002901					X		
CS 2000	A00002960					X		
CS 2000	A00002966					X		
CS 2000	A00002979					X		
CS 2000	A00003073					X		
CS 2000	A00003371	X	X	X	X			
CS 2000	A00003454	X	X	X	X			
CS 2000	A00003459		X					
CS 2000	A00003485	X						
CS 2000	A00003486		X					
CS 2000	A00003487		X					
CS 2000	A00003489							
CS 2000	A00003490		X					
CS 2000	A00003506	X						
CS 2000	A00003562		X					
CS 2000	A00003568		X	X	X			
CS 2000	A00003576				X			
CS 2000	A00003613	X						
CS 2000	A00003617	X						
CS 2000	A00003618	X						X
CS 2000	A00003630				X			
CS 2000	A00003667		X					
CS 2000	A00003698	X						
CS 2000	A00003711	X						
CS 2000	A00003767		X					
CS 2000	A00003789					X		X
CS 2000	A00003905					X		
CS 2000	A00003933	X						
CS 2000	A00003971					X		
CS 2000	A00003995		X					
CS 2000	A00004005	X						
CS 2000	A00004020	X						
CS 2000	A00004036					X		
CS 2000	A00004037					X		
CS 2000	A00004045					X		X
CS 2000	A00004046		X					
CS 2000	A00004271	X						

SN07 Solutions								
PRODUCT or APPLICATION	ACTID	PT-IP	UA-IP	IAW	IAC	Succ on DMS	MMB S	AAL2
CS 2000	A00004391					X		
CS 2000	A00004414	X						
CS 2000	A00004422					X		
CS 2000	A00004554					X		
CS 2000	A00004713					X		
CS 2000	A00004868					X		
CS 2000	A00004872		X	X				
CS 2000	A00004922-23							
CS 2000	A00005007	X						
CS 2000	A00005073					X		
CS 2000	A00005074					X		
CS 2000	A00005190					X		
CS 2000	A00005192					X		
CS 2000	A00005193					X		
CS 2000	A00005363					X		X
CS 2000	A00005268					X		
CS 2000	A00005485	X	X	X	X			
CS 2000	A00005734			X				
CS 2000	A00005758					X		
CS 2000	A00005986			X				
CS 2000	A00005988			X				
CS 2000	A00006405					X		X
CS 2000	A00006483	X						X
CS 2000	A00006693					X		
CS 2000	A00008902	X	X					
CS 2000	A59039138				X			
CS 2000 Core Manager	A00002920					X		
Centrex IP	A00003717			X				
Centrex IP	A00003718-19							
MG 4000	A00003650	X	X					
MG 4000	A00003669	X						
MG 4000	A00003672	X						
MG 4000	A00003773	X						
MG 9000	A00001893-94		X					
MG 9000	A00003074		X					
MG 9000	A00003531		X					
MG 9000	A00003567		X					
MG 9000	A00003571		X					
MG 9000	A00003591	X						
MG 9000	A00003737		X					

SN07 Solutions								
PRODUCT or APPLICATION	ACTID	PT-IP	UA-IP	IAW	IAC	Succ on DMS	MMBS	AAL2
MG 9000	A00004109		X					
MG 9000	A00005016	X						
MG 9000	A00005375		X					
MG 9000	A00006639		X					
MG 9000	CD003593		X					
Media Server 2000	A00004873		X	X				
Network Patch Mgr.	A00003560	X	X		X			
SAM21 Element Mgr	A00003562		X					
TOPS	A00002740					X		
TOPS	A00002765					X		
TOPS	A00003687					X		
TOPS	A00003704					X		
TOPS	A00005160					X		



New or changed per release

New or changed for SN07

This section of the document describes the feature-based changes occurring in the SN07 release for the following categories:

- Logs/alarms
- Data Schema and MIBs
- Commands
- Service order
- Office parameters
- Operational measurements (OMs) and performance measurements (PMs)
- AMA/Billing
- Software Optionality Control (SOC)

SSH Compatibility statement

Access to some functions requires the use of SSH compatible client software for access to secure telnet and ftp services (via the SSH standard). SSH clients are supplied bundled with some operating systems, but may need to be obtained separately. Sources for SSH clients include (but are not limited to):

- PUTTY - freeware
- OpenSSH - freeware
- SSH Inc. - commercial
- Secure CRT - commercial
- WinSCP - freeware

Nortel does not supply or recommend a particular supplier.

Logs/faults changes overview

The following logs/faults are new or changed for SN07. They also appear in the logs-by-product tables in the Baseline section of this document with descriptions/cause for generation. This section also offer general log changes.

Additional information is available in the Feature Deltas section of this document.

Summary of new or changed Logs/Faults for SN07

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
Product = Carrier_AIN		
CAIN log (changed)	CAIN902	Feature A00001990 (Succession on DMS) updates log CAIN902. CAIN902 shows the subscription method and other pertinent details when a call subscribes to Carrier Advanced Intelligent Network (CAIN), not when the query is sent to the Service Control Point (SCP). The METHOD field of the log indicates the subscription type (for example, ANI or OFFICE) and the precedence level. The CAIN902 log will indicate a METHOD of CICROUTE and precedence level of six when appropriate. CAIN902 is also generated when table CICROUTE does not have a CAINGRP option for the ALTERNATECARRIER and the carrier subscription is undone. Feature A00001990 updates the logs that indicate the subscription method to display the CIC information.
VAMP log (changed)	VAMP902	Feature A00001990 (Succession on DMS) updates log VAMP902. VAMP902 logs are output when the VPTrace CI tool is enabled and an outbound message is sent through the VAMP framework to the SCP. The VAMP902 log might display the subscription type through the SUBINFO field. Feature A00001990 modifies this field to include CARRIER as a possible value. Feature A00001990 updates the logs that indicate the subscription method to display the CIC information.
Product = Carrier Hosted Services (CHS)		
GWC log (changed)	GWC600	Feature A00007211 (MMBS) modifies the existing H.323 GWC600 log format to follow a generic OSS log framework to adhere to OSS requirements. Both the header and body are changed.
Product = CS 2000		
SPM log	SPM605 (new)	Feature A00001319 (PT-AAL1, Succession on DMS) creates new Info log SPM605 to indicate that a particular resource RM protection group is excluded by the SPMRESALIGN tool, without align RMID-PWID values.
SBA backup alarms (changed)	BAK50 BAK70 BAK90 NOBAK	Feature A00001649 (Succession on DMS) changes the priority of the backup alarms so that they take precedence over the NOCOM alarm.

Summary of new or changed Logs/Faults for SN07

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
Feature A00001743 (PT-IP; UA-IP; IAC; and Succession on DMS) provides a host of log-related modifications. This activity provides a new custlog format GenCustLog version 2. The feature also implements an initial phase of a lost log detection of non-CM logs. It also enhances the lost indication mechanism for CM logs. Feature A00001743 also enhances log delivery to support STD, SCC2, STD-OLD and SCC2-OLD format with ECORE node id enabling and Dual Sequence Numbering. It also ensures that new functionality does not adversely affect log delivery performance and also ensures that the application conforms to specified limits.		
XAC logs (changed)	XAC312 XAC610	Feature A00002012 (Succession on DMS) modifies XAC information and action logs related to the Core to MS InterConnect (CMIC) to display the new CMIC port device and CMIC packets and links. This feature also modifies XAC information and action logs related to the Reset Terminal InterFace (RTIF) to display the new RTIF device and the RTIF packets and ports. This activity also modifies the impact statement of existing XAC logs for the new CMIC/RTIF HIOP card. The affected logs include XAC610 and XAC312.
MScomm alarm (changed)		While feature A00002012 does not add or remove any existing XA-Core System alarms displayed under the XAC heading, it does introduce a new situation that raises this alarm. The alarm is indirectly raised if the system is unable to bring a misconfigured CMIC link in-service. An MScomm MAJOR alarm is raised if a CMIC link between the XA-Core and the Message Switch (MS) is in-service but not configured properly. An MScomm MAJOR alarm also occurs after a misconfigured CMIC link is newly provisioned by the system and the system brings the misconfigured CMIC link in-service. This alarm also occurs if the CMIC links are out of service.

Summary of new or changed Logs/Faults for SN07

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
GAME logs (new)	GAME101 GAME102	Feature A00002013 (Succession on DMS) creates two new logs. - GAME101 is created if the RSPTMOUT OM count is greater than zero. The log is created during the RSPTMOUT OM transfer period and records the RSPTMOUT OM count value. - GAME102 is created if RSPTMOUT OM count becomes equal to the office parm T1_TIMER_EXPIRY_MSG_SUPPRESS threshold value. The log is created when this feature suppresses a 'T1 Timer Expiry' message. When a GAME102 log is created it raises an external minor alarm. The alarm must be cleared before another log entry is created.
SPM log (new)	SPM399	Feature A00002432 (Succession on DMS) creates this new log, generated whenever an SPM enters or leaves an overload condition.
System alarm (new)	Baseln	Per feature A00002433 (Succession on DMS) the "Baseln" alarm is raised whenever any XA-Core Field Replaceable Unit (FRU) installed in the shelf is not at Hardware (HW) or Firmware (FW) baseline. Only the Major level is used. Associated with log XAC337.
XAC logs (new)	XAC337 XAC637 XAC415 (changed)	Per feature A00002433 (Succession on DMS) XAC337 is raised when the Baseln alarm is first raised, or the Baseln alarm is still raised and the non-baseline component list changes. XAC637 is raised when the Baseln alarm is cleared, due to an empty list of non-baseline components. XAC415 adds "not at baseline" as a reason for not running the SREx test.

Summary of new or changed Logs/Faults for SN07

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
STOR logs (new)	STOR605 STOR606 STOR607	Feature A00002499 (Succession on DMS) creates three new logs to flag the detection of faults by the XA-Core Store Audit. - STOR605 (critical) is output when the Store Audit has detected a corruption in the Bstree structures containing the information about the data address space STOR is responsible for. - STOR606 indicates that the Store Audit has found a corruption in the allocation information for data store which is dumped (such as DSPROT) and it is very likely that a attempt to perform a dump while in this state would fail. - STOR607 is generated when the Store Audit detects a mismatch between the Store Allocator's internal setting of an address' blocking attribute and the actual setting of the attribute in memory hardware. The attribute is either blocking or write-blocking. An incorrect value could mislead the Store Allocator's initialization routines and cause traps.
ITN log (new)	ITN307	Feature A00002510 (Succession on DMS) creates this INFO log to indicate that IP transmit failed.
CAP logs (changed)	CAP100 CAP101	Feature A00002538 (Succession on DMS) removes the complexity measurement from these capacity summary and capacity logs since the complexity measurement is not valid on an XA-Core (multiple-processing) switch.
XAUD logs (changed)	(various)	Feature A00002549 (Succession on DMS) extends and re-numbers the XAUD logs to match the numbers of the AUD logs for simplicity. Consult the FM section of this feature for a mapping table that shows both the old and new names.

Summary of new or changed Logs/Faults for SN07

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
Alarm Database logs (new)	Report Alarm Log Clear Alarm Log Alarm Summary Log	Feature A00002757 (Succession on DMS) provides functionality to an SSPFS Platform for the aggregation of Alarms into one database. Logs will be generated by the reporting entity when using the <i>Reporting API</i> to enter/update/clear alarms in the database. The Report Alarm Log is sent when requested by the entity that is reporting an alarm. The Clear Alarm Log is generated when a client clears an existing alarm in the alarms database managed by Alarmd. The Alarm Summary Log is sent periodically by Alarmd to summarize the Alarms in the database managed by Alarmd.
SPM log (changed)	SPM300	Feature A00002858 (Succession on DMS) modifies SPM300 with a new text reason showing that it is generated when a STS3L carrier experiences an RFI alarm.
Database logs (new)	DB600 DB601 DB602 DB603 DB604	Feature A00003371 (UA-IP) creates five new logs: - DB600 is generated when an attempt to allocate a database connection encounters an I/O error. These errors can occur when the database has been stopped momentarily for administrative purposes. - DB601 is generated when an attempt to allocate a database connection encounters detects that the connection is already closed. These errors can occur when the database has been stopped momentarily and then again started. - DB602 is generated when an attempt to allocate a database connection encounters an invalid password error. These errors can occur when the database log in password for a database user is changed. - DB603 is generated when an attempt to allocate a database connection encounters maximum database sessions exceeded error. These errors can occur when an unusual event has occurred that caused sustained high levels of system activity.

Summary of new or changed Logs/Faults for SN07

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
(continued) Database logs (new)	DB604	(continued) Feature A00003371 (UA-IP) creates five new logs: DB604 is generated when an attempt to allocate a database connection encounters maximum database processes exceeded error. These errors can occur when an unusual event has occurred that caused sustained high levels of system activity.
IWBM logs (new)	IWBM800 IWBM801 IWBM802 IWBM803	Feature A00003487 (UA-IP) creates four new Interworking Bridge Manager Pool Logs. - IWBM800 indicates that the number of available IW bridges exceeds the first threshold (70%) when attempting to retrieve an IW-bridge ID from the IW bridge manager. - IWBM801 indicates that the number of available IW bridges falls to less than 65% of bridges in the pool in use. This log always occurs after IWBM800 - IWBM802 indicates that the number of available IW bridges exceeds the second threshold (90%) when attempting to retrieve an IW-bridge ID from the IW bridge manager. - IWBM803 indicates that the number of available IW bridges falls to less than 85% of bridges in the pool in use. This log always occurs after IWBM802.
XNET logs (new)	XNET605 XNET606 XNET607	Feature A00003487 (UA-IP) creates three new external packet network bearer connection logs. - XNET605 indicates that the bearer networks of the two parties in a connection attempt are not permitted to inter-connect, based on datafill in table NET2NET. - XNET606 indicates a software or provisioning problem in the switch, in that an appropriate bearer network could not be determined through provisioned data for a particular party in a connection attempt. - XNET607 indicates that an IW SPM interworking bridge was not available for the connection request, either because of a bridge exhaust condition, or a bridge is not available.

Summary of new or changed Logs/Faults for SN07

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
GWC log (new)	GWC314	Feature A00003568 (UA-IP, IAC, IAW) creates new log GWC314, raised in connection with a Location Id Reporting connection failure alarm.
SPFS logs (new)	SPFS310 SPFS350	Feature A00003617 (PT-IP) creates two new logs. SPFS310 is generated for the following reasons: - when the CPU load Average threshold is exceeded, or when the related Major or Minor alarm is cleared. - when the Swap Space usage threshold is exceeded, or when the related Critical or Major alarm is cleared. - when the Memory usage threshold is exceeded, or when the related Major or Minor alarm is cleared. SPFS350 is generated for the following reasons: - when the File System is not mounted, the File System usage threshold is exceeded, a File System read/write failed, or when the related Critical, Major or Minor alarm is cleared.
CMT logs (new)	CMT500 CMT501 CMT502 CMT302 (with alarm)	Feature A00003667 (UA-IP) creates four new logs. - CMT500 is generated by the SESM alarm system to indicate the system is initializing. - CMT501 is generated by the SESM alarm system upon shutdown. - CMT502 is generated by the SESM alarm system to inform northbound alarm clients that alarm notifications cannot be generated. This log will be sent via the SSPFS syslog feed to the customer log. - CMT302 (major alarm) replaces the critical GWC398 and/or UAS398. The alarm and log are raised when the SNMP poller cannot communicate to the network device due to an SNMP timeout.
SESM syslog generation (changed)		A00003667(UA-IP) describes for customers who use IEMS in SN07 how to manually turn off syslog generation to avoid duplication of alarm logs.
PM log (changed)	PM181	Feature A00003767 (UA-IP) modifies PM181 to generate when an ABI messaging alarm is set or cleared.

Summary of new or changed Logs/Faults for SN07

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
ABI messaging alarms (new)	Links down	Feature A00003767 (UA-IP) creates three new alarms that affect the DMS alarm banner, show up as an InService Trouble (ISTB) reason for the applicable ABI XPM, and generate a log message. - ABI external messaging alarm Links Down - Alarm Set (or Alarm cleared) - ABI external messaging alarm Severely Degraded - Alarm Set (or Alarm cleared) - ABI external messaging alarm Degraded - Alarm Set (or Alarm cleared)
	Severely Degraded	
	Degraded	
SIPC logs (new)	SIPC310	Feature A00003933 (UA-IP) creates new logs related to SIP Gateway application call processing. - SIPC310, "SIP CallP No Database Connection" is associated with the generation of the Critical alarm due to a loss of connectivity between the database and the CallP application. The same log number is used for "SIP CallP Database Connection Established" when the connection that caused the first SIPC 310 log is re-established and the alarm is cleared. - SIPC650 is an informational log that is generated when the CallP application goes to get data from the database for a particular table and no data is found. - SIPC301 is a critical log that is generated when the SIP Gateway Call Processing Application will not receive any incoming SIP messages due to Access Control List being enabled and no valid entries in the Remote SIP server or ACL list. - SIPC750 is generated when the SIP Gateway Call Processing Application drops incoming SIP messages due to Access Control List restrictions. A Minor, Major, or Critical log is generated based on the number of SIP messages dropped in the last 15 minutes. - SIPGW700 is an INFO log that contains one of 34 possible log messages related to SIP call processing.
	SIPC650	
	SIPC301	
	SIPC750	
	SIPGW700	

Summary of new or changed Logs/Faults for SN07

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
SIP Gateway Application CallP Alarms (new)	Database Access Alarm	Feature A00003933 (UA-IP) creates new alarms: SIP Gateway CallP Database Access Alarm (critical) occurs when the CallP application tries to access the database and it fails due to a loss of connectivity between the database and the CallP application. Correlates with the SIPC310 log. SIP Gateway CallP ACL Trouble Alarm is raised when incoming SIP messages are dropped due to Access Control List enforcements. The severity of the alarm is based on the number of packets dropped in last 15-minute time interval. Correlates with the SIPC750 log.
	ACL Trouble Alarm	
SIP Gateway Application Maintenance Alarms (new)	SIP Gateway Maintenance Trouble Alarm	Feature A00003933 (UA-IP) creates new alarms: SIP Gateway Maintenance Trouble Alarm (critical) occurs when the SIP Gateway Application transitions to a state that indicates it should be in-service, but is not, and the Session Server unit the application is running on is in an enabled operational state. SIPM301 logs are generated when this alarm is raised or lowered. SIP Gateway CallP ACL Trouble Alarm is raised when the Session Server the SIP Gateway Application is running on is in a duplex configurations with both units in an enabled operational state, and the SIP Gateway application state becomes out of sync between the two Session Server units. SIPM302 logs are generated when this alarm is raised or lowered.
	SIP Gateway Maintenance Sync Trouble Alarm	

Summary of new or changed Logs/Faults for SN07

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
SIPM logs (new)	SIPM300 SIPM301 SIPM302 SIPM500	Feature A00003933 (UA-IP) creates two new logs related to SIP Gateway application maintenance. - SIPM300 is a Trouble log which is generated any time the SIP Gateway Application Maintenance software encounters an unexpected condition. - SIPM301 is a Trouble log which is generated any time the SIP Gateway Maintenance Trouble Alarm is raised or lowered. - SIPM302 is a Trouble log which is generated any time the SIP Gateway Maintenance Sync Trouble Alarm is raised or lowered. This occurs when the SIP Gateway application state gets out of sync, or gets back in sync in a duplex Session Server configuration. - SIPM500 is an INFO log which is generated any time the SIP Gateway Application maintenance state changes.
SIP Gateway Application Maintenance Alarms (new)	Maintenance Trouble Alarm Maintenance Sync Trouble Alarm	Feature A00003933 (UA-IP) creates new alarms: SIP Gateway Maintenance Trouble Alarm (critical) is raised when the SIP Gateway Application transitions to a state that indicates it should be in-service, but is not, and the Session Server unit the application is running on is in an enabled operational state. Correlates with the SIPM301 log. SIP Gateway Maintenance Sync Trouble Alarm (major) is raised when the Session Server the SIP Gateway Application is running on is in a duplex configurations with both units in an enabled operational state, and the SIP Gateway application state becomes out of sync between the two Session Server units. Correlates with the SIPM302 log.
Session Server Provisioning Log (new)	DBSE300	Feature A00003933 (UA-IP) creates a new Session Server Provisioning log. DBSE300 is a Trouble (TBL) log which is generated any time a change in database connectivity is detected. It reports 'No Solid DB Connection' when database connectivity is lost. It reports 'Solid DB Connection Restored' when database connectivity is reestablished. Correlates to the critical alarm "No Database Connection" raised when a loss of connectivity to the database is detected.

Summary of new or changed Logs/Faults for SN07

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
SPM logs and NODE log (new)	SPM682 SPM683 NODE602	Feature A00003971 (Succession on DMS) creates three new logs. SPM682 indicates CEM manual reset. SPM683 indicates the reason for CEM swact. NODE602 indicates the reason for CEM state transition, generated only when the CEM state transitions from Insv to Istb or Insv to Sysb.
SPM logs and NODE logs (changed)	Various; see details in next column	Feature A00003971 (Succession on DMS) performs multiple changes on multiple logs. The following logs are enhanced by adding the activity/status of the unit/device: SPM300, SPM500, SPM650, SPM651, SPM 684, SPM301, NODE302, NODE303, NODE326, NODE600, NODE601. The following logs are enhanced by adding the TaskName and the taskID: SPM311, SPM312. Log SPM331 is enhanced by adding new field "Reason" to provide a reason for protection switch failure.
Various	Various	Feature A00004005 (PT-IP) describes and illustrates the user interface for the Session Server. An application on the Session Server, such as the SIP Gateway application, has the ability to generate Alarms, Logs, and Operational Measurements (OMs). The alarms that are raised on the Session Server are reported to the SNMP Trap destination server, if one is provisioned.
UNB error and secret logs (changed)	UNB306 and others	Feature A00004037 (Succession on DMS) modifies existing UNB error and secret logs to report problems specific to Switched Remote CDCs during administration or audits. UNB306 logs are output if the PIC or LATA fields are deleted.
TRK log (changed)	TRK605	Feature A00004045 (Succession on DMS, AAL2) modifies existing TRK605 log. This log is generated when the SOC UTRS0012 is ON and the called number is data filled in table CLIDN in a DMS-250 toll switch. The TRK605 log is used in a toll switch to identify the origination number when the called number is being traced.

Summary of new or changed Logs/Faults for SN07

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
NGSS logs (new)	NGSS700 NGSS701	Feature A00004271 (PT-IP) creates NGSS700 to indicate when a SIPT CS2CS call is rejected because it would exceed the LIMIT setting of the CS2B0008 SOC. The SIPT call is not allowed to complete through the NGSS. The CS2CSOV register in OM group NGSSOM is pegged. NGSS701 is generated when a CS2AS call is rejected because it would exceed the LIMIT setting of the CS2B0009 SOC. The SIPT call is not allowed to complete through the NGSS. The CS2ASOV register in OM group NGSSOM is pegged.
SDM log (new)	SDM739	Feature A00004868 (Succession on DMS) creates SDM739 to indicate file transfers between the FTP Client and the CORE and to show user log-ons to the CORE.
SDMB log (changed)	SDMB375	Feature A00005073 (Succession on DMS) modifies SPMB375 so that it is generated when an error occurs in SBA secure file transfer.
SDM logs (new)	SDM267 SDM314	Feature A00005190 (Succession on DMS) creates two new logs. - SDM267 indicates a change in the condition of a CBM link. - SDM314 indicates two SDM links connections are physically crossed.

Summary of new or changed Logs/Faults for SN07

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
SDM logs (new)	SDM314 SDM334 SDM335 SDM336 SDM633 SDM634 SDM635 SDM636	Feature A00005192 (Succession on DMS) creates the following new logs. - SDM314 indicates that two link connections are physically crossed. Associated with Major alarm Crossed Link. - SDM334 indicates that the signal on receive/transmit fibre to the OC3 card is faulty or not present. - SDM335 indicates a probable link equipment malfunction. Associated with Minor alarm Minor Link Fault. - SDM336 indicates that a response to CBM 800 heartbeat is not received from the core. Associated with major alarm Core Heartbeat. - SDM633 is a CBM info log that indicates a change in the condition of a CBM link. - SDM634 indicates that the OC3 Card Fault alarm raised with SDM334 has been cleared. - SDM635 indicates that the Minor Link Fault alarm raised with SDM335 has been cleared. - SDM636 indicates that the heartbeat alarm raised with SDM336 has been cleared.
SDMB logs (changed)	SDMB531 SDMB820	Feature A00005268 (Succession on DMS) modifies logs SDMB531 and SDMB820 to reflect the increased backup storage capacity for SBA on the CM from 2 volumes per stream up to 69 volumes per stream.
VAMP log (changed)	VAMP901	Feature A00005363 (Succession on DMS) modifies VAMP901 to display the new Business Customer ID parameter, and to make possible an additional value in the Digits Type subfield of the AMA Digits parameter. This log is intended for lab use only and is not suitable for live switches.
PAM logs (changed)		Feature A00005986 (IAW) logs the following events on IEMS: - User successfully authenticated through PAM - User authentication through PAM failed. - Request Timeout on PAM proxy

Summary of new or changed Logs/Faults for SN07

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
SAM21 logs (changed)	SCUxxx IPOAxxx SM21xxx	Feature A00008902 (PT-IP) modifies SAM21 logs to add two lines for alarm detail. The 3 digits of the alarm ID use the first digit for the alarm category and the last two digits for the alarm's cause. Using a mapping table, the items of Category and Cause are added to the end of the alarm detail.
SDMB logs (changed)	SDMB690 SDMB691	CR Q00664538 (Succession on DMS) creates the following logs: • SDMB690 indicates that an SBAIF alarm and the fault that caused it have cleared. • SDMB691 generates when a problem occurs with the scheduled transfer of billing files and when that fault clears. It also generates when a file transfer schedule is manually deactivated or deleted.
Product = Centrex IP Client Manager (CICM)		

Summary of new or changed Logs/Faults for SN07

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
Logs and alarms (changed)	Various	Feature A00003718 and 3719 (IAW) revisits the existing fault generation, logging and performance management capability of the CICM system. A new Integrated Element Manager System (IEMS) interface manages the output used by external OSSs to monitor the network element and, for example, detect alarm conditions. The IEMS can be accessed using a Graphical User Interface which will give access to the alarms and logs for a network element. This will also interact with the Element Manager GUI. This feature ensures that alarms and logs are in a format IEMS can read. The CICM alarm manger is modified by having separate buffers for each severity of alarm. This will enable the critical alarms to be sent immediately and for major, minor and warning alarms to be prioritized in order that they are sent within the required time periods, but at a controllable rate. The rate of alarms being raised is configured in the CICM registry MIB. CICM log delivery is enhanced to use three log streams to send logs to up to three different syslog daemons on the IEMS. The CICM will send logs to custlog, audit log, and security log streams. Each log must be formatted correctly for that particular stream.
Product = MG 4000		
MG4I logs (new)	MG4I 501 MG4I 502 MG4I 300 MG4I 301 MG4I 320	Feature A00003650 (PT-IP, UA-IP) introduces the log series MG4I, including the following: • MG4I 501, SCTP Core Connection State Change • MG4I 502, SCTP Peer Connection State Change • MG4I 300, Media Integrity Failure • MG4I 301, GigE Audit Failure • MG4I 320, counter overflow in the Operational Measurement pegs
Product = MG 9000		

Summary of new or changed Logs/Faults for SN07

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
MGEM log NE log	MGEM714 (new) NE609 (new)	Feature A00001893-94 (UA-IP) creates this new audit log MGEM714, generated whenever a user attempts to image an MG9K device, and new software image log NE609, generated whenever a user executes an image request.
Download alarm (new)	nnESADownloadFault (Critical)	Feature A00003567 (UA-IP) introduces this new alarm to indicate a failure to download ESA data to a given VMG. This alarm will only be generated for autonomous download attempts. This was indicated by a log in previous releases.
MGEM and VMG logs (new)	MGEM704 MGEM705 VMG600 VMG601	Feature A00003074 (UA-IP) creates 4 new INFO logs to inform users when data has not been saved in the database: • MGEM704 indicates that an attempt to correct the database has failed. • MGEM705 indicates that the Database is unavailable and correction failed. • VMG600 indicates that termination data was successfully provisioned in all appropriate areas except for the database. • VMG601 indicates that an attempt to correct termination data in the database has passed.
ESA alarm and ESA log (new)	nnESADownloadFault ESA302	Feature A00003567 (UA-IP) adds new alarm "nnESADownloadFault" to indicate a failure to download ESA data to given VMG. This alarm will only be generated for autonomous download attempts. This was indicated by a log in previous releases. The ESA302 log (Critical) is generated when the EM is unable to download ESA data to a VMG.

Summary of new or changed Logs/Faults for SN07

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
OVLD logs (new)	OVLD808	Feature A00003571 (Succession on DMS) introduces new alarms and corresponding logs. OVLD808 (Critical) indicates that an external messaging link has closed and cannot send/receive message.
	OVLD809	OVLD809 (Major) indicates that the message loss is high enough such that the message link is in a degraded service state. For ABI, this would mean that some calls are failing and perhaps maintenance actions are failing (e.g. static data download, etc.).
	OVLD810	OVLD810 (Minor) indicates message retransmissions are high enough that system is starting to see performance degradation. Potentially, this could mean increased latency, reduced messaging through the system, buffer overflows and perhaps heading toward congestion.
DS3 alarms and Logs (new)	ds3ais with MGCA333	Feature A00003591 (UA-IP) adds the following alarms and logs: - AlarmIndicationSignal (ds3ais) generates log MGCA333 when a AlarmIndicationSignal fault is received from the Gateway. - LossofFrame (ds3lof) generates log MGCA334 when a LossOfFrame fault is received from the Gateway. - RemoteAlarmIndication (ds3rai) generates log MGCA335 when a RemoteAlarmIndication fault is received from the Gateway.
	ds3lof with MGCA334	
	ds3rai with MGCA335	
HW Mismatch alarm and Log (new)	Hardware Fault	Feature A00004109 (UA-IP) adds a new Hardware Mismatch alarm to indicate an incorrect replacement card has been installed. The NE301 log (Critical) is generated when such an equipment malfunction occurs.
	NE301	

Summary of new or changed Logs/Faults for SN07

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
VMG Out of Service faults (new)	VMG Admin State is OOS	Feature A00005016 (UA-IP) adds the following VMG Out of Service faults and enhances the information available in log VMG300:
	VMG Initializing	VMG Admin State is OOS is generated when a vMGAdminStatusOutOfService fault is received from the MG9kEM server (Warning). Relates to log VMG322.
	VMG OOS-card locked	VMG Initializing is generated when a cardInitializing fault is received from the MG9kEM server (Warning). Relates to log VMG325.
	VMG OOS-card disabled	VMG OOS-card locked is generated when a cardLocked fault is received from the MG9kEM server (Warning). Relates to log VMG323.
	VMG OOS-Line Maintenance is not Ready	VMG OOS-card disabled is generated when a cardDisabled fault is received from the MG9kEM server (Warning). Relates to log VMG324.
	VMG OOS-Megaco Maintenance is not Ready	VMG OOS- Line Maintenance is not Ready is generated when a lineMtceNotReady fault is received from the MG9kEM server (Critical). Relates to log VMG328.
	VMG OOS-GWC is not reachable	VMG OOS- Megaco Maintenance is not Ready is generated when a MegacoMtceNotReady fault is received from the MG9kEM server (Critical). Relates to log VMG329.
	VMG OOS- no reply from GWC	VMG OOS- GWC is not reachable is generated when a GWCUnreachable fault is received from the MG9kEM server (Critical). Relates to log VMG373.
	VMG OOS-AAL1 bearer subsystem not ready	VMG OOS- no reply from GWC is generated when a noReplyFromGWC fault is received from the MG9kEM server. Relates to log VMG374.
	VMG OOS- IP bearer subsystem not ready	- VMG OOS- AAL1 bearer subsystem not ready is generated when an aal1BearerSubsystem OnPairNotReady fault is received from the MG9kEM server. Relates to log VMG376. - VMG OOS- IP bearer subsystem not ready is generated when an ipBearerSubsystem OnPairNotReady fault is received from the MG9kEM server. Relates to log VMG377.

Summary of new or changed Logs/Faults for SN07

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
Shelf Logs (new)	SHLF392 SHLF393	Feature A00005375 (UA-IP) adds new faults to provide the reason when shelf discovery failed due to a particular card or due to an incompatible card. SHLF392 is generated when a shelfCompatibility fault is received from the MG9kEM server. SHLF393 is generated when a cardDiscovery fault is received from the MG9kEM server.
Product = TOPS		
TOPS log (changed)	TOPS131	Feature A00003687 (Succession on DMS) modifies TOPS131 by adding additional text reasons to the Reason field and by adding a new field, Wireless type, which indicates whether the log was generated on an IS-41 or GSM call.
OAIN logs (changed)	OAIN606 OAIN607	Feature A00005160 (Succession on DMS) modifies the values that can appear in the existing OAIN606 and OAIN607 logs. OAIN 606 adds reason field "Msg Received at Unexpected Destination Address." OAIN 607 adds reason field "XAETHR Transmit Failure."
Product = CR Changes		
SDM log (changed)	SDM325	CR Q00970381 fixes the problem of SDM325 having a blank line in the middle of the log (after the header). Available in an SN07 patch.
SDM log (changed)	SDM610	CR Q00972933 fixes the problem of SDM610 having a blank line in the middle of the log (after the header). Available in an SN07 patch.
SDM logs (changed)	SDM327, SDM627	CR Q01001000 fixes the problem of these two logs having a different format in CBM than what was produced for SDM. Resolution of this issue will be to align the CBM log format of the logs with that of the older SDM version again. Fix will be available in an SN07 patch.

Summary of new or changed Logs/Faults for SN07

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
SDM/CBM logs (changed)		CR Q00970344 fixes an Equipment Identifier field problem in the header. The Equipment Identifier field in an NT STD/SCC2 log header is the last field in a header and is optional in that only some core logs make use of it. (CARR and PM logs do.) The CS2000 has a log formatting "rule" where if the header length exceeds 65 characters, the Equipment Identifier field (if present in the log) should be "wrapped" to a new line, i.e. an end-of-line string is added after Event Label, and the Equipment Identifier is moved to line 2 of the log with regular indentation. SN07 code churn in SDM's Log Delivery Service application resulted in the calculation of where 65th character position of the header being sometimes different than how the CS2000 calculated it. The end result of this was that some of the logs coming out of the SDM no longer looked as exactly like they would on the CS2000 because they'd possibly have 1 extra row in them if Equipment Identifier was used. To address this issue and make the CS2000 logs look the same on the SDM, the resolution of this CR will be patched back to SN07.
MG9K logs (changed)		CR Q00973875 fixes the problem that MG9K alarm logs sent to the OSS through IEMS had a tab character indenting the 2 Site information rows and sometimes a blank would be found after the Description row. Resolution of these issues is available in an SN07 patch.
MG9K logs (changed)		CR Q00987360/Q00987380 fixes the problem that MG9000 alarm logs were being duplicated in the northbound OSS log stream from IEMS. Resolution of this issue will be available in an SN07 patch.
GWC logs (changed)	GWC3XX	CR Q00976754 fixes the problem that sometimes some of the GWC3XX logs for GWC had differing formats of the Component Id field. Resolution of this issue is available in an SN07 patch.

Summary of new or changed Logs/Faults for SN07

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
IEMS logs (changed)	IEMS606	CR Q00989603 fixes the problem that when the number of log events received by IEMS reached a certain threshold, an IEMS606 log was generated with a severity and later cleared when the threshold was no longer crossed. An SN07 patch will for this CR will change the nature of IEMS606 to be an INFO log with no severity. One will be generated when the threshold is crossed. Another will be generated when an automatic old event cleanup will have completed.
IEMS logs (changed)	IEMS607	CR Q00992391 fixes the problem that when IEMS did a re-sync of its alarm list with a managed component it would create a clear log for when alarms were found to have gone away. These "explicit" clears used the log name/number of the original alarm and did not look like the regular clear logs. It was decided in these situations to instead create a new IEMS607 log for "explicit" clears for all managed components supporting re-sync. This log would contain all the information normally needed from a regular clear log. This new log will be introduced in an SN07 patch.

Data Schema/MIBs changes overview

The following Data Schema tables or MIBs are new or changed for SN07. More complete descriptions will appear in the Feature Deltas section of this document.

Summary of new/changed Data Schema/MIBs information for SN07

Table or MIB name	New or changed	Description
Product = AIN		
CICROUTE	Changed	Per feature A00001990 (Succession on DMS), there is a new subscription point in this table. Currently, Carrier Advanced Intelligent Network (CAIN) subscription can be achieved through tables TRKGRP, AINSCUSP, UNIPROF, AUTHCODU, AUTHCDX, and STDPRTCT. The sourcing of this patch will allow CAIN subscriptions to be added to table CICROUTE enabling subscription on a per Carrier Identification Code (CIC)-basis. This new subscription point will allow carriers to use the SCP to route calls based on their CIC. The new subscription point will be created by adding the CAINGRP option tuples of table CICROUTE, just as in other CAIN subscription tables.
TRKOPTS	Changed	Per feature A00002016 (Succession on DMS), creation of the new option AINDENY option in table TRKOPTS provides the ability to deny AIN prefix triggers (Specified_Carrier, One_Plus_Prefix, International, Operator Services). The AINDENY option in table TRKOPTS will also allow AINDENY to be associated with specific trunk groups as datafilled in table TRKGRP. (Only AIN-capable trunks will be allowed AINDENY options in table TRKOPTS.) The new option will function in a similar manner to the line and customer group options except that it will only block prefix triggers. It will not be capable of holding SFC, PFC, or Office-Wide PFC triggers. It will allow 15 DENYs or RESTOREs just as the line and customer group options.

Summary of new/changed Data Schema/MIBs information for SN07

Table or MIB name	New or changed	Description
CUSTSTN	Changed	Feature A00002016 (Succession on DMS) will - enlarge the storage capacity of the CUSTSTN AINDENY option to 15 elements. - allow the CUSTSTN, line and the TRKOPTS AINDENY to hold the four prefix triggers and block their triggering at the Info_Analyzed TDP.
TRIGITM	Changed	Feature A00002016 requires addition of one or more prefix triggers to table TRIGITM. With feature A00002016, individual agents need to subscribe to the prefix triggers. Accomplishment of this task is possible in tables OFCTIID, CUSTIID, TRKAIN or through Servord.
TRIGITM TRIGINFO	Changed	Feature A00004500 (Succession on DMS) modifies these tables by adding SCTP as a valid AIN transport entry to the AIN_TRANSPORT field.
IPAPPL	New	Feature A00004500 (Succession on DMS) creates table IPAPPL which defines the IP Application instance that data will be transmitted over for a given service.
Product = Call Server 2000		
DNROUTE VOWINV	Changed	Feature A00002011 (Succession on DMS) modifies table DNROUTE to add VOWDNIDX field information. It also modifies table VOWINV to add VOWDNDN field information (for VOWKEY = VOWDN).
MNSHELF and MNCKTPAK	Changed	Feature A00002047 (Succession on DMS) modifies tables MNSHELF and MNCKTPAK to enforce specific restrictions with respect to the double density Spectrum backplane.
STDPRTCT	Changed	Feature A00002281 (Succession on DMS) expands the maximum value of this table to allow for 32000 entries. This modification allows the customer to datafill significantly more AMA options.
IPNETWRK	Changed	Per feature A00002281 (Succession on DMS) field name PARM in table IPNETWRK has been refined, a new value IRM_INTERFACE is added. This new value has an impact to the dump and restore table transfer order. Table CMIPADDR needs to be transferred before IPNETWRK.

Summary of new/changed Data Schema/MIBs information for SN07

Table or MIB name	New or changed	Description
PXRTE	Changed	Feature A00002319 (Succession on DMS) enhances the CNDSEL of the CND route selector with a VMI CND route condition. The CND_RTE_CONDITION type is extended with VMI value.
MNNODE and MNCKTPAK	Changed	Feature A00002431 (Succession on DMS) modifies tables MNNODE and table MNCKTPAK. It adds a new field <i>capindx</i> to table MNNODE, only for DMNCP class of SPMs to provision this capacity. Feature A00002431 introduces new error and success messages to table MNCKTPAK. For additional information, refer to the configuration section for this feature in the "Features Deltas" section of this document.
PECINV FWINV	Changed New	Per feature A00002433 (Succession on DMS) PECINV increases the maximum number of tuples from 200 to 256, and the default datafill is updated. New table FWINV is intended to maintain the FW baseline for a PEC and allows from 0 to 4 exception versions.
XAFWLOAD	Changed	Feature A00002433 (Succession on DMS) will provide a warning to display if an user tries to provision a non-baseline firmware loadname.
EMMCDATA	New	Feature A00002901 (Succession on DMS) creates new table EMMCDATA, used to provision Enhanced Meet-Me Conferencing.
SCAISSRV	Changed	Feature A00002904 (Succession on DMS) adds new field TOGGCALL under categories TPCC and SCAI3WC. It also adds new parameter HDUHDLEG under category SCAICC for functions CALLHELD and CALLUNHELD.
TRKOPTS	Changed	Feature A00002960 (Succession on DMS) adds new trunk group option ORIGIDSCR for ISUP EANT trunks only. This allows the customer to specify which ISUP EANT trunks perform originator identification screening.

Summary of new/changed Data Schema/MIBs information for SN07

Table or MIB name	New or changed	Description
IBNFEAT KSETFEAT	Changed	Feature A00003073 (Succession on DMS) adds a Redirection subfield to the SimRing line option. When this option has a value of Not_allowed on a SimRing pilot DN then the resultant NPMDN legs are not allowed to call forward. The same case applies to table KSETFEAT.
C7TRKMEM	Changed	Feature A00003485 (PT-IP) increases the limit on the size of table C7TRKMEM for a standalone SSP using the Universal Signaling Platform from 165,000 tuples to a maximum of 200,000 tuples.
LTCINV GATWYINV	Changed New	Feature A00003486 (UA-IP) modifies these tables as follows: - LTCINV modifies field OPTATTR by adding 1 new subfield for the EXTDS512 refinement and deleting 4 existing subfields for the EXTDS512 refinement. - Table Gateway Inventory (GATWYINV) is where gateway configuration information is provisioned. Provisioning gateways in this table does not allocate IOUI nodes of any kind. For this release, this table contains configuration information only (no nodes) involving gateways. The term "gateway" could either mean a physical gateway or logical gateway, it depends on the actual "gateway" in question.
MNNODE SERVRINV SERVSINV	Changed	Feature A00003487 (UA-IP) modifies eleven existing tables, as follows: - MNNODE added the new BEARNETS field (and related subfields) to IW DPT_ONLY and SMG4 nodes to indicate the bearer network associated with the node. It also added the BRDGCLLI field to IW BRDG_ONLY nodes to indicate the bridge groups the particular SPM node contributes to. - SERVRINV added the new BEARNETS field (and related subfields) to indicate the bearer networks of the packet nodes it controls. For SN07, there will be a limit of one bearer network per gateway controller, and it will be the default. - SERVSINV added provisioning consistency checks for use during an ONP.

Summary of new/changed Data Schema/MIBs information for SN07

Table or MIB name	New or changed	Description
(continued)	Changed	(continued)
TRKOPTS		Feature A00003487 (UA-IP) modifies eleven existing tables, as follows: - TRKOPTS removes DPT from the APPLICATION field under the DYNAMIC option and adds DPT as a new OPTION. NGSS is added as a new selector field under the SIPT protocol. - OFRT, OFR2, OFR3, OFR4 changed the name of the PKT conditional selector to FABRIC, and increased the allowable FABRIC range from {ENET} to {ENET, AAL1, AAL2, IP}. It also added the new CND/NOT selector condition of BEARNET to allow conditional routing based on the originator's bearer network. - IBNRTE, IBNRTE2, IBNRTE3, IBNRTE4 changed the name of the CND/NOT PKT conditional selector to FABRIC and enhanced it to support AAL1, AAL2 and IP fabrics. It also added the new CND/NOT selector condition of BEARNET to allow conditional routing based on the originator's bearer network. - HNPACONT:RTEREF and FNPACONT:RTEREF have the same changes found in the routing tables as described in the previous bullet. - GWCNode adds three new fields: Network_Instance to indicate the network instance, Network_Fabric_Type to indicate the bearer network fabric type, and Network_Codec_Profile_Id to indicate the associated network codec profile. - GATEWAYPROFILE adds new field Bearer_Fabric_Restriction_List used to support the fabric type check when customer associate gateway to GWC node.
OFRn		
IBNRTE		
HNPACONT:RTEREF		
FNPACONT:RTEREF		
GWCNode		
GATEWAYPROFILE		

Summary of new/changed Data Schema/MIBs information for SN07

Table or MIB name	New or changed	Description
MNNODE	Changed	Feature A00003487 (UA-IP) modifies eleven existing tables, as follows: - MNNODE added the new BEARNETS field (and related subfields) to IW DPT_ONLY and SMG4 nodes to indicate the bearer network associated with the node. It also added the BRDGCLLI field to IW BRDG_ONLY nodes to indicate the bridge groups the particular SPM node contributes to. - SERVIRNV added the new BEARNETS field (and related subfields) to indicate the bearer networks of the packet nodes it controls. For SN07, there will be a limit of one bearer network per gateway controller, and it will be the default. - SERVSINV added provisioning consistency checks for use during an ONP. - TRKOPTS removes DPT from the APPLICATION field under the DYNAMIC option and adds DPT as a new OPTION. NGSS is added as a new selector field under the SIPT protocol. - OFRT, OFR2, OFR3, OFR4 changed the name of the CND/NOT PKT conditional selector to CND/NOT FABRIC and enhanced it to support conditional routing for multiple bearer fabrics (e.g., AAL1, AAL2 or IP). It also added the new CND/NOT BEARNET selector to allow conditional routing based on the originator's bearer network. - IBNRTE, IBNR2, IBNR3, IBNR4 have the same changes found in the routing tables as described in the previous bullet on OFRx. - HNPACONT:RTEREF and FNPACONT:RTEREF have the same changes found in the routing tables as described in the previous bullet. - GWCNode adds three new fields: Network_Instance to indicate the network instance, Network_Fabric_Type to indicate the bearer network fabric type, and Network_Codec_Profile_Id to indicate the associated network codec profile.
SERVIRNV		
SERVSINV		
TRKOPTS		
OFRn		
IBNRn		
HNPACONT:RTEREF		
FNPACONT:RTEREF		
GWCNode		

Summary of new/changed Data Schema/MIBs information for SN07

Table or MIB name	New or changed	Description
(continued) GATEWAYPROFILE	(continued) Changed	Feature A00003487 modifies eleven existing tables, as follows: (continued) GATEWAYPROFILE adds new field Bearer_Fabric_Restriction_List used to support the fabric type check when customer associate gateway to GWC node.
BEARNETS NETBRDGE NETPATH NET2NET GWC_NETWORK_CODEC_PROFILE GWC_NETWORK_RECOMMENDED_CODEC_SETTING	New	Feature A00003487 (UA-IP) creates six new tables, as follows: - BEARNETS identifies the bearer networks supported by the server and the network options that apply to the packet networks. - NETBRDGE defines the network bridging resources for interconnecting networks. Bridges provide the ability to connect one network to another without regard to the call type. Bridges typically have two connectivity endpoints, one for each of the networks that it interconnects. - NETPATH identifies the list of bridging resource groups (the bridge path) that can be used to interconnect two networks. In SN07, two bridges are required to connect an AAL1 agent and an IP agent, so the path consists of a bridge resource from each of those NETBRDGEs. - NET2NET defines the allowable interconnections between networks, and the network path used to interconnect them. - GWC_NETWORK_CODEC_PROFILE stores network codec profiles that are created by the customer. The profiles will be used when the customer adds a GWC node. Changed in SN07 to support multiple bearer networks. - GWC_NETWORK_RECOMMENDED_CODEC_SETTING stores recommended network codec settings. When customers add/change network codec profile, this information will help the customers to datafill the codec profile with the recommended codec setting. Changed in SN07 to support multiple bearer networks.

Summary of new/changed Data Schema/MIBs information for SN07

Table or MIB name	New or changed	Description
LTCINV	Changed	Feature A00003490 (UA-IP) modifies LTCINV as follows: - EXTDS512 OPT_ATTR is now allowed for the SMS peripheral type. “\$” should be entered in the CSLNKTAB field for external XPMs (the C-side link information will be generated automatically).
SERVINV TRKGRP TRKSGRP TRKOPTS TRKMEM	Changed	Feature A00003506 (PT-IP) modifies these tables as follows: - SERVINV adds three new exec line-ups, GWCEX, GWCFX, and GWC250 for GWC node types. The new exec line-ups are specific to Per-Trunk Signaling (PTS) trunk types that are configured on a GWC node type. - TRKGRP adds new provisioning restrictions for PTS trunks groups configured on a GWC. The restrictions apply when the trunk group is assigned the GWCPTSTK option in table TRKOPTS and when a PTS group tuple is changed in table TRKGRP. - TRKSGRP adds new provisioning restrictions for PTS trunks groups configured on a GWC. The restrictions apply when the trunk group is assigned the GWCPTSTK option in table TRKOPTS and when adding or changing the GWC PTS trunk subgroup tuples in table TRKSGRP. - TRKOPTS adds the new trunk group option, GWCPTSTK, that identifies PTS trunk groups configured on a GWC that provide connectivity between the packet network and the PSTN. - TRKMEM adds new provisioning restrictions for PTS trunks groups configured on a GWC.
GateWay Controller Location Change Reporting MIB	New	Per feature A00003568 (UA-IP, IAC, IAW), this MIB defines information about the Location Change Reporting data provisioning supported by the GateWay Controller (GWC). The MIB uses a boolean value indicating whether Location Change Reporting is enabled or disabled on a per GWC base. By default, Location Change Reporting is disabled.

Summary of new/changed Data Schema/MIBs information for SN07

Table or MIB name	New or changed	Description
NORTEL-GWC-COMMON-TC	Changed	Feature A00003630 (IAC) modifies these tables as follows:
SERVINV		- NORTEL-GWC-COMMON-TC is the MIB used for defining all the supported gateway protocols. This feature adds a new protocol "TGCPPTOCOL" in the supported protocol list for the field "GWCDeviceProtocol." - SERVINV adds a new exec line-up, GWCEX, for GWC node types. The new exec line-up is specific to Succession End Office and Tandem Per Trunk Signaling (PTS) trunk types configured on a GWC node type. - TRKGRP adds new provisioning restrictions for MF OP and ES trunks groups configured on a GWC. The restrictions apply when the trunk group is assigned the GWCPTSTK option in table TRKOPTS and the trunk group tuple is changed in table TRKGRP. - TRKSGRP adds new provisioning restrictions for MF OP and ES trunks groups configured on a GWC. The restrictions apply when the trunk group is assigned the GWCPTSTK option in table TRKOPTS and adding or changing the trunk subgroup tuples in table TRKSGRP - TRKOPTS adds the new trunk group option, GWCPTSTK, that identifies PTS trunk groups configured on a GWC that provide connectivity between the packet network and the PSTN. It also adds a sub-option, PRELOADANI, to the GWCPTSTK trunk group option. PRELOADANI sub-option identifies PTS trunks which support a call model that allows the ANI digits to be sent from the Core to the GWC prior to receiving any ANI request from the far-end. - TRKMEM adds new provisioning restrictions for MF OP and ES trunks groups configured on a GWC.
TRKGRP		
TRKSGRP		
TRKOPTS		
TRKMEM		
CPCSCRN	New	Feature A00003711 (PT-IP) creates two tables:
CCTABLE		- CPCSCRN. - CCTABLE.

Summary of new/changed Data Schema/MIBs information for SN07

Table or MIB name	New or changed	Description
CPCSCRN CCTABLE	Changed	Feature A00003711 (PT-IP) modifies the following tables: • TRKGRP. • TRKSCR. • STDPRTCT. • RTEATTR. • CSEMAP. • TMTMAP.
NORTEL-UEM G-RELMMSGIN G-MIB	New	Feature A00003767 (UA-IP) creates new MIB "Nortel-UEMG-ReliableMessaging-MIB" with four sections: • Association general info, including some thresholds for alarms. • Current OMs provide counts for the sample of OM data which is currently being collected. • Interval OMs provide historical samples of the OMs that have been collected. • Alarms - If a threshold is crossed or the association fails/recovers an alarm will be raised or cleared. The MIB contains the data which will be contained in the alarm.
DIRPPPOOL DIRPOOL2	Changed New	Feature A00003905 (Succession on DMS) modifies DIRPPPOOL and creates new table DIRPOOL2. • DIRPPPOOL is modified to increase the number of volumes from 24 to 72 which requires 3X the memory store. Each individual volume field in table DIRPPPOOL is now replaced with a field that contains three volume names. • DIRPOOL2 provides information needed to consolidate linked pools when moving to a load that now has 72 volumes per pool in table DIRPPPOOL. The table is created at IPL. Its data is transferred during DART (if applicable). The table data is used during POSTSWACT to consolidate volumes in DIRPPPOOL, after which table DIRPOOL2 is deleted from the switch.

Summary of new/changed Data Schema/MIBs information for SN07

Table or MIB name	New or changed	Description
SIPLINK	New	Feature A00003933 (PT-IP) creates new table SIPLINK that creates an association between CS 2000 agents (e.g., ISUP trunks) and a SIP link name. The SIPLINK table is downloaded to GWCs datafilled as DPT SIPT in table SERVINV.
UEMG Megaco Enterprise MIB	Changed	Feature A00003933 (PT-IP) modifies this MIB definition to allow for multiple types.
CLIDN	Changed	Feature A00004045 (Succession on DMS, AAL2) modifies table CLIDN for DMS-250 functionality, supporting originations and terminations on the following DMS-250 trunk types: EANT (PTS and SS7), PRI, DAL, ONAL, ONAT and IMT (PTS and SS7).
ACDLOGIN	Changed	Feature A00004391 (Succession on DMS) expands ADCLOGIN to support up to 30000 tuples. The LOGINID field is expanded from 4 to 5 digits.
ACDENLOG	Changed	Feature A00004391 (Succession on DMS) expands ADCENLOG to support up to 30000 tuples. The LOGINID field is expanded from 4 to 5 digits.
ACDGRP	Changed	Feature A00004391 (Succession on DMS) adds new field IDSIZE to specify the number of login digits to be used by all agents in the group.
KSETLINE KSETFEAT IBNFEAT	Changed	Feature A00004391 (Succession on DMS) expands the POSID field for certain tuples in these three tables from 4 digits to 5 digits. Existing 4 digit POSIDs will be padded with a leading 0 during ONP.
STN	Changed	Feature A00004872 (UA-IP, IAW) modifies STN so that special tones are still provisioned via Table STN for Legacy lines, but this is no longer a requirement for packet lines. Also, the "typical" tone characteristics can be stated, but if the tone is played by the GW, these characteristics are a product of the GW providing the tone.
SDMINV	Changed	Feature A00005190 (Succession on DMS) modifies SDMINV to add new PEC NTRX51LS for a simplex CBM which is OC3 connected.

Summary of new/changed Data Schema/MIBs information for SN07

Table or MIB name	New or changed	Description
CAINRESP CAINREXT CDRTMPLT	Changed	Feature A00005363 (Succession on DMS) for CAINRESP adds new entry AMABUSCISTID (AMA Business Customer ID) to subfield CAIN_PARM_VALUE. It also adds a new digits id type of 300 to the AMA_DIGS_TYPE subfield. For CAINREXT, this feature adds a new digits id type (300) to the AMADIGS parameter. For CDRTMPLT, this feature adds 3 new parameters to the FIELDS and REORIGCP subfields: BUSCUSTID, SLPID1ST and AMADGSWC
MULTITM	Changed	Feature A00005734 (Succession on DMS) requires datafill in MULTITM with any relevant time zones to enable the feature. See also changes in Servord.
C7NETWRK	Changed	Feature A00006405 (Succession on DMS, AAL2) expands the number of Point Codes (PC) that can be defined in an SSP office in table C7NETWRK from 16 to 31.
SERVSINV	Changed	Feature A00006483 (PT-IP, AAL2) modifies subfield ANNTERMS under the ANNC option in the OPTIONS field. The value for number of announcement terminals is increased from a maximum 300 up to the new maximum of 1280.
IBNFEAT	Changed	Feature A59039138 (IAC) adds new announcement field MWT_ANNOUNCEMENT to the MWT feature.
Product = Centrex IP Client Manager (CICM)		
Performance MIB	New	Feature A00003718-3719 (IAW) creates a new MIB as the key for this feature to integrate IEMS reporting with CICM performance measurements.
Product = DMS_Centrex_Res		
KSETFEAT	Changed	Per feature A00002009 (Succession on DMS), the name of up to 24 characters that this feature provides will be stored in table KSETFEAT.
LCCOPTS	Changed	Feature A00002009 also provides a list of compatible line class codes (LCCs) that will be specified in table LCCOPTS.

Summary of new/changed Data Schema/MIBs information for SN07

Table or MIB name	New or changed	Description
IBNXLA	Changed	Feature A00002196 (Succession on DMS) adds the following entries to the Result field: DNDACT and DNDDEACT.
RESFEAT	Changed	Feature A00002196 adds the following field to the table: DND_ONLY.
Product = MG 4000		
MNNODE MNIPPARM MNMGPIP	Changed	Feature A00003669 (PT-IP) changes these tables as follows: - MNNODE adds new field SGFABRIC for SMG4 (MG4K) class SPM. - MNIPPARM adds new fields DIFFSERV for the codepoints, and MEDIA_INTEG to indicate the state of media integrity on the GEM card.
(continued) MNMGPIP	Changed	(continued) Feature A00003669 (PT-IP) changes these tables as follows: MNMGPIP adds new fields GEMSIGIP for the signalling IP address, SIGSUBMASK for the signaling mask, BEARERVLAN for the signaling enabled status, SIGVLAN for the VLAN TCI for the signaling interface, and SIGIPENABLED for the VLAN TCI for the bearer interface.
MNCKTPAK	Changed	Feature A00003672 (PT-IP) adds new value NTLZ20CA to existing field PEC to support the new circuit pack for the GEM MG4K RM.
Product = MG 9000		
UEMG Megaco Enterprise MIB	Changed	Feature A00005016 (UA-IP) modifies the MIB definition by adding fault types to the nnMegacoFaultType where previously there was only one fault type.
Product = TOPS		

Summary of new/changed Data Schema/MIBs information for SN07

Table or MIB name	New or changed	Description
TDBDAOPT TOPSFTR TOPSPARM VROPT	Changed	Feature A00002740 (Succession on DMS) modifies the following tables: • MNIPPARM adds new fields DIFFSERV for the DIFFSERV codepoints, and MEDIA_INTEG for the Media Integrity Indicator. • TDBAOPT adds new option OVERSEAS to the ADACCSRV field. • TOPSFTR adds parameter International_DA_Call_Comp to enable international DACC. • TOPSPARM adds parameter International_DACC_Prefix to allow datafilling this tuple with the actual prefix digits (0-999).
(continued) VROPT	Changed	(continued) Feature A00002740 (Succession on DMS) modifies the following tables: • VROPT parameter DACC_Local_Toll_Activation modifies the TOLL and ALL setting to now include International requested numbers.
XLACCLASS XLABILL	New	Feature A00002765 (Succession on DMS) creates these two new tables. XLACCLASS allows XLAGRP refinements based on a range including coin, station, hotel, and restricted. XLABILL allows XLAGRP refinements based on a range including paid, collect, third, cards, special calling, special called.
TRKOPTS	Changed	Feature A00002960 (Succession on DMS) introduces new trunk group option ORIGIDSCR. It allows the customer to specify which ISUP EANT trunks perform originator identification screening.
LTCINV	Changed	Feature A00003490 (UA-IP) provides the ability to rehome an ABI XPM to a different GWC by performing a tuple change operation. This feature also makes modifications to the tuple change operation restrictions.

Summary of new/changed Data Schema/MIBs information for SN07

Table or MIB name	New or changed	Description
ISUPTRK TOPSFTR TOPSPARM TOPSTLDN TOPSTOPT	New	Feature A00003687 (Succession on DMS) modifies five tables as follows. • ISUPTRK adds value RLT_GSM in field RLT to accommodate WIN TOPS calls using GSM. For future use. • TOPSFTR adds value RLT_FOR_GSM to allow the customer to enable GSM TOPS ADACC with release. In order to activate the feature, the SOC option OSEA0104 must be on, and this tuple must be set to Y. For future use. • TOPSPARM adds two new parameters: SMS_LOG_FAILURE, and SMS_TIMEOUT. Enabling the first will limit the number of TOPS131 logs generated in SMS failure situations. Enabling the second permits control of how long TOPS waits before marking an SMS attempt as timed out. • TOPSTLDN is modified in SN07 to use a pool ID as the key field. • TOPSTOPT adds field WIRELESS to control whether TOPS can use wireless functions on a non-WIN (non-CAMEL) call.

Summary of new/changed Data Schema/MIBs information for SN07

Table or MIB name	New or changed	Description
MSCIDMAP TOPSMCDB	New	Feature A00003687 (Succession on DMS) creates two new tables. - Table Mobile Switching Center Identifier Mapping (MSCIDMAP) maps MSCIDs to TLDN pool identifiers from Table TOPSTLDN. This allows the customer to control TLDN allocation on a per-MSC basis. - Table TOPS Message Center Database (TOPSMCDB) provides datafill for a TOPS SMS SS7-based message center simulator. An operator position or automated node can send SMS messages using either IS-41 TCAP or GSM TCAP. When the simulator receives the SMS, it looks up the data stored against the SMS destination number to determine the disposition of the SMS. The simulator can successfully acknowledge the SMS, send back a failure message, or ignore the SMS so the TOPS SMS time-out code executes.
OAFUNDEF	Changed	Feature A00003704(Succession on DMS) modifies the TOPSAUTO option to include a DAS option. Since the DAS option will require a CT4Q and refinement option similar to TOPSOPER, the TOPSAUTO option is now broken into refinement areas for each automated system.
TRKOPTS	Changed	Feature A00003789 (Succession on DMS, AAL2) introduces new option INTRACSE with field RTE_ADV_CHOICE that must be datafilled to select the route advance capabilities of office parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT.
OANODINV, CMIPADDR, and QMSMIS	Changed	Feature A00005160 (Succession on DMS) modifies these tables as follows: In OANODINV, field NODEAREA has modified refinements. Also, if the entry in subfield ONPMTYPE is OSN, OSNM, or OSAC, 3 new fields are added. In CMIPADDR, a new cross check with table OANODINV is added, as is a new error message if an attempt is made to delete or change a CMHOST tuple whose active IP address is datafilled in OANODINV. In QMSMIS, cross checks are added to enforce that an OSSAIN QMS MIS server cannot be datafilled in table OANODINV with data path XAETHR.

Commands and User Interface changes overview

The following Commands and/or User Interface are new or changed for SN07. More complete descriptions appear in the Feature Deltas section of this document.

Affected Area	Command/User Interface Description
Product = AIN	
Regarding feature A00002016 (Succession on DMS), the Traver tool will display information regarding subscriptions to AIN triggers and will display the criteria associated with those triggers. The tool also respects the AINDENY line and customer group options and will tell the user if the SCP query was blocked due to AINDENY. Traver will be enhanced to consider AINDENY for prefix triggers and trunk origination.	
AIN TSTQUERY	Feature A00004500 (Succession on DMS) enhances this command to support SCTPIP as a valid transport.
Product = Carrier Hosted Services (CHS)	
Feature A00006495 (MMBS) permits a craftsperson to allocate an H.323 virtual carrier with as few as 4 endpoints/TIDs, up to a maximum of 672 endpoints/TIDs. Only 254 D channels can be defined on a H.323 GWC after this feature is delivered.	
Feature A00006496 (MMBS) enables the support of mapping multiple D channels to a single H.323 gateway such that it can be mapped to the full capacity of a SN07 H.323 GWC (1024 for International/1032 for North American).	
The H.323 maintenance model will be changed by this feature. A H.323 D channel will come into service once a H.323 gateway successfully registers with a H.323 GWC. If a H.323 gateway has multiple D channels, all the D channels will be brought into service once a H.323 gateway successfully registers. If at least one D channel comes into service the registration process will be successful.	
Feature A00006741 (MMBS) enables H.323 Gatekeepers in an external network (private, enterprise, other carriers, etc.) to interoperate with a CS2K H.323 Gatekeeper on a carrier network. In general, the Acme Session Director (SD), acting as an H.323 Proxy, will register Gateway instances with the CS2K that represent Gatekeepers on the external network. This is the basic mechanism for supporting H.323 Gatekeeper to CS2K Gatekeeper Interoperability (GK-GK Interop).	
Feature A00007063 (MMBS) enables setting the maximum reserved termination values for all the H.323 gateway profiles to the maximum capacity of a H.323 GWC. Customers will be able to configure the number of desired endpoints against H.323 gateways.	
Product = CS 2000	
CI tool SPMRESALIGN (new)	Feature A00001319 (PT-AAL1, Succession on DMS) creates a new CI tool 'SPMRESALIGN' implemented as a new CI directory which ensures the following: • The RMID-PWID values of the Resource RMs (DSP & VSP RMs) are aligned. • The activity of DSP & VSP RMs are aligned as per the table MNCKTPAK datafill.

Affected Area	Command/User Interface Description
CLLI command in SBA RMS subsystem (new)	Feature A00001649 (Succession on DMS) adds new CLLI command to retrieve the CLLI name from the BILLMTC interface. The “cli” command is not available either as a numbered command or as a menu command, unlike other commands in BILLMTC interface. The user has to directly enter the command “cli” at the BILLMTC interface from any level to retrieve the CLLI name.
	Feature A00001743 (PT-IP; UA-IP; IAC; and Succession on DMS) modifies existing screens to enable an user to access and modify the existing information more easily. This feature also adds new menus and screens to make the Logroute Command Line User Interface (Logroute CLUI).
	The following list details how feature A00002012 (Succession on DMS) updates various MAP levels and two MAP commands:
	Feature A00002012 allows the IO MAP level to display of a middle packet with use of HIOP; it currently displays only the CMIC and RTIF functionalities in the lower and upper positions.
	This feature also provides a new CMIC MAP that shows the CMIC functionality hosted on either a CMIC packet on a IOP card or CMIC/RTIF HIOP.
	With the CMIC port/link separation on the CMIC/RTIF HIOP, the new CMIC port0 and CMIC port1 will appear in the CMIC MAP level.
	Furthermore, A00002012 allows the two Time of Day (TOD) devices to appear for the CMIC/RTIF HIOP card, instead of one: TOD0 and TOD1.
	Furthermore, the <i>uneq</i> command will be used for deprovisioning a CMIC packet on an IOP card or CMIC link on CMIC/RTIF HIOP card.
	The feature also allows use of the <i>trns/</i> command with the new HIOP card; the feature does not change the functionality of the command. The <i>trns/</i> command is also a command for use on the CMIC MAP level to obtain the specific MS port numbers to be busied.
	With introduction of the new CMIC/RTIP HIOP, the new RTIF MAP will display the functionality hosted by either an RTIP packet on an IOP card or an CMIC/RTIP HIOP card. Furthermore, with the RTIP port/link separation on the CMIC/RTIF HIOP, the new RTIP link0 and link1 will appear on the RTIF MAP level. The RTIF local port will be changed to Link0, and the RTIF remote port will be changed to Link1. Port 0 and Port 1 will be left blank.
	With introduction of the new CMIC/RTIP HIOP card, the RTIF packets will have to be migrated to the new card. Thus, the <i>uneq</i> command will be used for deprovisioning an RTIP packet on an IOP card or an RTIF link on a CMIC/RTIF HIOP card.
	Feature A00002047 (Succession on DMS) truncates the SPM shelf level and CEM/RM protection level MAP displays to display only the one card shelf.

Affected Area	Command/User Interface Description
	Per feature A00002133 (Succession on DMS), the “cbm_setup” tool is an installation interface that is command line driven. It provides an interface to initiate, complete and provide status feedback for installation. The SWIM level of the “cbmmtce” interface is used to install applications. It also provides a transaction history. These logs are maintained on the system and rotated weekly or as disk space requires. There is also a SWIM capability that will allow users to view logs. The suite of patching tools built into the SSPFS provide user interfaces to apply and remove patches and query and audit software. Another new mechanism for the Nortel Networks Core and Billing Manager (CBM) product provides verification of the integrity of patches as they are received. This feature will also provide a CBM capability to override embedded patching handling with a more cautious handling procedure. The root password is not required to control patching. Maintenance users (maint group or emsadm group) will have access to run the “patchctrl” tool. There are four tools are patching: patchconfig, patchctrl, queryloads, and patchfilter.
QUERYCARD and QUERYSHELF (changed)	Feature A00002433 (Succession on DMS) enhances these commands to show if the field replaceable unit (FRU) is HW and FW/DLL baseline compatible. This feature enhances ONP precheck steps to detect a non-baseline FRU on the active image. It also provides a new pre-SWACT check to request/ receive the new side PECINV (hardware baseline) data.
	Feature A00002505 (PT-IP, UA-IP, IAC, AAL2) expands upon the functionality and usability of the USP GUI. This new GUI replaces the GUI distributed with the previous software releases.
	Feature A00002585 (PT-IP) modifies the TMM web-based GUI by adding a new “Mtc by Carrier” link which supports six commands. The feature also adds a new link for online Help.
RMI (BILLMTC) (changed)	Feature A00002741 (Succession on DMS) enhances RMI (BILLMTC) by allowing the user to configure the location of the downstream test files and to configure the location of the partial file that renames the functionality. It also allows the user to turn the auto-recovery option ON or OFF.
CBM User Interface (UI) (new)	Feature A00002822 (Succession on DMS) creates a User Interface Manager for local CBM maintenance and system administration. Functions include access and control over the CBM application software, CBM configuration, and package installation/removal.
QUERYPM FLT REASON (changed)	Feature A00002858 (Succession on DMS) adds new ISTb reasons to the output of the QUERYPM FLT REASON Command: “Check SysB Carrier” and “Check Carrier on OC3 (or STM) RM” and “Check RFI Alarm on STS3L (or STM1M) Carrier.” This feature will only work on TDM (legacy) SPM nodes (i.e. SPM and STM1).

Affected Area	Command/User Interface Description
	Feature A00002966 (Succession on DMS) is expected to port the following major functions from the SDM to the Core and Billing Manager (CBM): Passthru users using SSH/telnet; restriction of shell for maint class users; and cbmgather tool. The feature is also expected to add the following enhancements: addition of query subcommand; querytape; dat0 and dat1; new option to <i>platgather</i> and <i>cbmgather</i> to specify number of days' logs to be collected in order to accommodate a special need; capability for passthru users to change their own passwords for the SDM and CBM; listing, addition and modification of passthru users through the command line tool - passthru.
PMUPGRADE directory (changed)	Feature A00002979 (Succession on DMS) modifies the LOADDISTRIB and PATCHDISTRIB options of the SET command, extending them to support electronic software delivery via FTP.
SimRing group commands (changed)	Feature A00003073 (Succession on DMS) adds a new option "Redirection" prompt to commands ADO, CHF, and EST.
QSIMR (changed)	Feature A00003073 (Succession on DMS) modifies the display of QSIMR. It adds an indication that Redirection is allowed/not allowed on the SimRing group.
CLI (changed)	Feature A00003454 (Succession on DMS) modifies the CLI command to configure this feature.
SERVMAN (new)	Feature A00003454 (Succession on DMS) introduces this command to start, stop, and query the status of the SOCKS server.
EPUTIL (new)	Feature A00003485 (PT-IP) makes this tool field ready (previously a lab-only tool). EPUTIL is a CI tool in the CM (type EPUTIL on the CI prompt for access) tool which allows a user to capture and display maintenance messages sent from the GWCs to the CM.
QUERYPM (changed)	Feature A00003486 (UA-IP) modifies the legacy QUERYPM command by displaying an additional screen to the default QUERYPM command (without arguments) which reflects the ABI MG9K. Note: New output only occurs if the posted XPM is an ABI XPM.
TRAVER TR (changed)	Feature A00003487 (UA-IP) modifies this command to allow specifying the originator's bearer fabric or bearer network using the new optional TRKMEM or BEARNET parameters such that when encountering a CND/NOT FABRIC or CND/NOT BEARNET selector in the translations route, the parameters are used to determine how to interpret the CND/NOT route selector.

Affected Area	Command/User Interface Description
GWC-EM GUI (changed)	Feature A00003487 (PT-IP) modifies the GUI to include a new MIB table: GET_NETWORK_CODEC_PROFILE. It adds functionality to support the provisioning of multiple network codec profiles, and to support the specification of a bearer network fabric instance and a network codec profile for each GWC. Refer to the Feature Deltas section for screen shots.
Updated displays for MAPCI;MTC;PM (changed)	Feature A00003489 (UA-IP) modifies the displays at the PM level to support certain maintenance functions and states for the ABI host XPMs. When an ABI peripheral (LTC, LTCI, LGC, LGCI, SMA2, or SMS) subtending a GWC is posted, the display looks just like it did for the same peripheral posted as a direct HOST peripheral (legacy).
ABIREHOME (changed)	Feature A00003490 (PT-IP) adds 3 rehome query commands and 6 INVASIVE rehome commands to the ABIREHOME tool: • QUERY_IMPACTED_NODES/QIN: This command is used to display all the nodes currently marked as impacted. • FIND_AFFECTED_NODES/FAN: This command is used to display all the nodes impacted by rehome of given XPM node. • SHOW_NODE_STATUS / SNS: This command displays the current status, through ABI rehome, of a specified node, or all rehomeing nodes. • SET_AFFECTED_NODES/SAN: This command is used to set the protected rehome bit for each node impacted by rehomeing the given XPM. • CLEAR_AFFECTED_NODES/CAN: This command is used to clear the protected rehome bit for each node impacted by rehomeing the given XPM. • MARK_DS512_LINK_VERIFIED/VER512: This command sets the DS512 Link Verified bit for the specified node. • ADJUST_FRAME_SYNC/AFS - This command is used to adjust the frame sync on the ABI cards to sync to the inactive XPM unit. • SEND_GWC_STATIC_DATA/GWCSD - This command is used to send a limited static data update request to GWCs with new or deleted ABI XPMs. • ABORT_GWC_STATIC_DATA/ABORT_GWCSD - This command is used to send a limited static data update request to UNDO the recent GWC static data updates.

Affected Area	Command/User Interface Description
	Feature A00003506 (PT-IP) adds new restrictions for PTS trunk groups that are provisioned on a GWC, affecting the following levels of the MAP: TTP, MANUAL, MONITOR, and DATATTP.
	Feature A00003562 (UA-IP) defines new provisioning panels for the new CICM and CICM-EM service.
	Feature A00003568 (UA-IP, IAC, IAW) modifies the CICM soft client (M6350) to provide the user with an interface to specify their civil location description when logging in, and to allow the user to specify automatic server selection. The user log-in process has been changed so that the user is prompted to enter a location description. A new option in the 'Server Settings' window allows the user to choose 'automatic server selection'. The GWC Element Manager GUI has been modified to make equivalent changes.
IPSec provisioning GUI (changed)	Feature A00003576 (IAC) modifies the IPSecurity provisioning GUI as follows: • in the "IPSec Profile" panel, the "SA renew thresh" field (which was previously expressed as a percentage of SA lifetime) is changed to "Grace Period (seconds)". • a "Comment" field is added to the "Connection Policy" panel. When a connection policy is added, the user can enter descriptive comments in the "Comment" field. These descriptive comments provide an extra level of detail or history regarding that specific connection policy. • the option to enter the Kerberos service key in hexadecimal format, as well as the currently supported PEM format. • showing (1) the Kerberos panel and (2) the "KERBEROS" option in the "IPSec Profile" panel "Key Negotiation" field, only if the Kerberos capability is included for that GWC profile.
Parameters added to CLI in SSPFS (changed)	Feature A00003613 (PT-IP) adds three configuration parameters to the existing SSPFS configuration, which will be configured via the existing "cli" tool: • <i>CM Internet Protocol (IP) Address</i>: The address by which the CM may be reached. This address should be reachable by the SSPFS through VLAN's, which are defined in the network topology. • <i>Login Greeting</i>: A string that will be displayed to remote telnet users before they attempt to login. • <i>System Location</i>: A string defining the physical location of the SSPFS Server.

Affected Area	Command/User Interface Description
CLI to query all system faults (new)	Feature A00003617 (PT-IP) creates a command line interface to query all the faults on a system (an aggregate view of the system). It also provides interfaces to turn on, turn off and query alarm lights on Netra 1400 and N240 platforms. It also provides an interface to turn ON or OFF local logging.
SSPFS CLI menu tool (changed)	Feature A00003618 (PT-IP, AAL2) modifies the following commands: • conf_test command is removed and replaced by UpLink. The UpLink configuration is completely automated. • config_ip command allows the user to configure the public IP addresses on both simplex and HA cluster systems. • disable_failover command allows the user to disable a cluster failover. It must be run from the active node in the cluster. • req_failover command allows the user to perform/initiate a cluster failover. It must be run from the active node in the cluster.
Feature A00003630 (IAC) changes the “Associate Gateway” GUI so that when adding a TGCP gateway, the TGCP gateway profile should be selected from the provided profile list. It also changes the “Add GWC” GUI so that when PTS functionality is provided, TRUNKNA needs to be selected when adding a GWC, and when PTS functionality is provided, EXEC type needs to include ABTRK. Feature A00003630 also adds new restrictions for MF OP and ES trunk groups that are provisioned on a GWC, affecting the following levels of the MAP: TTP, MANUAL, MONITOR, and DATATTP	
SESM Alarm Manager GUI (changed)	Feature A00003667 (UA-IP) modifies the Alarm Manager GUI because of the addition of IEMS capability. The alarm acknowledgment feature is removed because it is no longer required at this level.
SESM Alarm History GUI (changed)	Feature A00003667 (UA-IP) modifies the Alarm History GUI because of the addition of IEMS capability. The check box to filter on acknowledged alarms is removed to avoid confusion.
Feature A00003698 (PT-IP) provides an extension to the existing CALLTRAK/TRMTRACE functionality found on the Core. The Session Server and the Core will now be able to track and initiate the Trmtrace on a SIP call for both incoming and outgoing SIP trunks. The user will only need to know the trunk group CLLI for that SIP trunk (or Access Link) in order to capture the GWC Trmtrace from the beginning. The Session Server will also capture (locally) the SIP messages and GCP messages used in the life of the traced call.	

Affected Area	Command/User Interface Description
	Feature A00003767 (PT-IP) adds three new text strings to QUERYPM FLTS which may appear for HOST ABI XPMs: • External Pkt Ntwk Msg Link(s) Problems - CRITICAL links down • External Pkt Ntwk Msg Link(s) Problems - Major severe message loss • External Pkt Ntwk Msg Link(s) Problems - Minor degraded
GateWay Status Configuration tab (changed)	Feature A00003933 (PT-IP) adds new field "Fault Status" inside this tab, which is under the Switched Line Services screen. The field shows what alarms have been raised against the VMG.
MANUAL FORCE RTS (changed)	Feature A00003971 (Succession on DMS) modifies at the CEM PROT level the responses from command MANUAL FORCE to show reasons for the failure or refusal of the command. Also, one failure response to the RTS command has been changed for improved clarity.
Feature A00003995 (UA-IP) adds, changes, and/or deletes multiple GUIs to support H.323 provisioning, as follows (details in the Feature Deltas section): • Associate Media Gateway changes functionality in SN07. • GWC Provisioning Panel Endpoint Group Component is deleted in SN07. • Add Carrier is new for H.323 in SN07. • GWC Provisioning Panel Carrier Component is new for H.323 in SN07. • Trunks Associated with EPG Dialog is new for H.323 in SN07. • Change Gateway changed in SN06.2 and is propped into SN07. • Change Gateway IP and Port Dialog was new in SN06.2 and is propped into SN07. • Change Gateway Capacity Dialog is new for H.323 in SN07. • Disassociate Gateway changes functionality in SN07. • Delete Carrier is new for H.323 in SN07.	
Feature A00004005 (PT-IP) describes and illustrates the user interface for the Session Server. The SIP Gateway application is the initial application for the Session Server platform, with the intention to provide a reusable infrastructure that can support additional applications. Refer to A00003933 for details on the SIP Gateway application.	
Replacement for USP GUI (changed)	Feature A00004020 (PT-IP) describes the new thin Java compiled client GUI which will include the ability to connect to the USP via a TELNET or SSH proxy. For Succession solutions a SSH proxy function will be used on the SSPFS that will eliminate the need for the "Reach Through" PC in the solution.

Affected Area	Command/User Interface Description
USNBD CDC and AGENCY commands (changed)	Feature A00004037 (Succession on DMS) modifies these commands to allow a new type of transport protocol, SR (switched remote) for FSK CDC over trunks. The Agency commands ADD and LIST will be enhanced to add the PIC and LATA fields.
ACDDEBUG ACDSHOW (changed)	Feature A00004391 (Succession on DMS) modifies these Command Interface tools to handle a 5-digit position ID so that indexing using these IDs will work properly.
SIPTRACE (new)	Feature A00004422 (Succession on DMS) introduces new command SIPTRACE to identify which SIP-T DPT (originating and/or terminating) is associated with an active call within the call server by means of SIP-T DPT callid. This new CI command utility is at the top level of CI.
SDM Menu enhancements	Feature A00004554 (Succession on DMS) implements scheduling of the system image backup to both SDM tape drives and the capability to configure the "Backup Required Alarm."
Ability to configure secure file transfer	Feature A00005073 (Succession on DMS) provides optional secure outbound file transfer using OpenSSH sftp client. The SBA user can configure the secure file transfer by adding or changing an existing schedule tuple in billmtc.
OM Data Delivery (OMDD) enhancements	Feature A00005074 (Succession on DMS) modifies the OMDD User Interface (OMUI) by allowing the user to select either "Standard" or "Secure" file transfer for the destination in addition to the already existing parameters.
MAPCI modified to support an OC3-connected CBM	Feature A00005190 (Succession on DMS) modifies the MAPCI to support an OC3-connected CBM. Refer to the configuration section of this feature for the differences between the OC3 environment and the DS512 environment.
MAPCI modified at SDMBIL level	Feature A00005268 (Succession on DMS) introduces new MAPCI commands to allow the user the add (ADDVOL) or remove (RMEVOL) more than one volume at a time per stream. The CONF command is modified to reflect this new capability.
CICM Element Manager view (changed)	Feature A00005988 (IAW) modifies this GUI so that when viewing a CICM running on the CPN5385 chassis on the CICM Element Manager, the card status overview is no longer provided. This is as a result of being able to have multiple CICM pairs within one SAM21 shelf, and so a graphical representation of the status of the whole shelf would provide potentially misleading information.

Affected Area	Command/User Interface Description
IOCAP MAPCI level (new)	Feature A00006693 (Succession on DMS) modifies the CAPACITY MAPCI level to provide a new IOCAP MAPCI level in XA-Core only. The new IOCAP level will provide IO utilization and IO messaging throughput information for HCMIC and HIOP IO cards. New commands at this level include IOCAP, QUIT, IOMAX, IOAVG, DISP, and STATUS.
Product = Media Server	
Feature A00004873 (UA-IP, IAW) describes the following enhancements to the MS2000 Series Node CLUI: Ability to configure MS2020 device Force Lock of a Device Ability to change the SNMP Community Strings	
Product = MG 9000	
Feature A00001893-94 (UA-IP) changes the MG9K Element Manager Graphical User Interface (GUI) at the card level by adding an item named <i>Software Image</i> to the <i>Actions</i> menu. It also asks the user to provide additional information at start up time for the MG9K EM Server. Also, the NPM will offer the ability to image an MG9K device via a new maintenance command <i>SmartImage</i>.	
SPMCPCAP	Feature A00002431 (Succession on DMS) introduces this new CI tool to display the capacity information of SPM. This tool enables the user to list the SPM and their capacities based on the variant type or list the SPMs based on the capacities. There is also a provision to find out capacity for a given SPM number. Remarks field in this tool displays if CEM(s) are not datafilled in table MNCKTPAK.
MG9000EM GUI (changed)	Feature A00003074 (UA-IP) removes the menu tab for ExportNE because it is no longer needed. It creates a new status icon that appears when an EM has an MG9K provisioned but is no longer managing that MG9K. It also creates a new GUI error message if a database error is encountered during MG9000 EM GUI actions.
Feature A00003531 (UA-IP) changes the following MG9K GUIs: - MG9K-EM Frame-view--Frames are displayed without a gap; the master frame is shown on the far left and all subtending frames to the right. - MG9K-EM "Provision a Virtual Media Gateway" GUI--Internal frame number is hard-coded to zero in VMG name, while provisioning VMG. - MG9K-EM Alarm browser GUI--the Description field changes so that once Frame location information is provisioned, for new alarms, Frame location detail is appended to the data which is shown in this field in SN06.2. If Frame location information is not provisioned, default fillers F's are appended to the data which is shown in this field in SN06.2.	

Affected Area	Command/User Interface Description
Feature A00003567 (UA-IP) modifies the ESA Config view from within the MG9000 Element View to support ABI ESA for enhanced ESA only. The subnet view is changed to show the DMS icon and subtending nodes.	
OC3STS1PortView GUI (new) Performance browser (changed)	Feature A00003591 (UA-IP) creates the OC3STS1PortView GUI and modifies the Performance Browser: • If the carrier is channelized, the Carrier Configuration display, OC3STS1PortView, will display OC3 Section/Line and three STS1 path information. • If the carrier is in channelized mode, the Channelized Carrier Performance parameter, performance browser, will display the OC3 Section/Line, STS1 path performance parameters and DS3 path information (if DS3 payload is selected).
Feature A00003737 (UA-IP) creates the following new MG9K GUIs: • ESA Query Tool (LCI)--to inform the node owner whether a MG9K that has lost its communication with the Element Manager is in ESA and still processing calls. • Ethernet Provisioning (LCI)--to allow the user to provision the ethernet ports to a specified IP address so customers can gain remote access to the ethernet port for FTP and LCI management. • SNMP Alarm Log (LCI)--to allow the user to query and display the SNMP alarm from the active DCC, providing a history of all the major events that have occurred on a node. • Password Change (LCI)--to allow the customer with a means for changing the default password that all MG9ks are shipped with. This password is used for LCI and SSH FTP authentication.	
GW Status Config Tab under the Switched Line Services screen	Feature A00005016 (UA-IP) adds a new field to the Gateway Status Configuration tab to show what alarms have been raised against the VMG. If there are no faults, then this field will be empty.
SAM21 Platform Installation Tool (changed)	Feature A00005485 (PT-IP) enhances the tool to allow the user to extract the SAM21 Platform Package from CD where it is stored in a "RPM" format.
Product = SAM21 Element Manager	
Feature A00003562 (UA-IP) provides new card support. The user can now provision the following: CICM on a given MCPN5385 card, CICM-EM on a given MCPN5385 card, and GWC on a given Force695 card. New provisioning screens are provided for these purposes.	

Affected Area	Command/User Interface Description
Product = TOPS	
QUERYPM in OAINPMDIR directory; BUFSTATS in OSSAINCI directory	Feature A00005160 (Succession on DMS) makes the following changes: For QUERYPM, changes the output that is displayed when the QUERYPM command is issued with no arguments in the OAINPMDIR directory. The new BUFSTATS command allows the user to view information about the queues and buffer pools that are used for processing messages incoming to OSSAIN via an XA-Core Ethernet interface. It also allows the user to reset the low water marks associated with the free queues.

Servord changes overview

The following Service Order items are new or changed for SN07. More complete descriptions will appear in the Feature Deltas section of this document.

Area	New or changed	ServOrd Description
Product = AIN		
With feature A00002016 (Succession on DMS), the AINDENY option in table TRKOPTS will also allow AINDENY to be associated with specific trunk groups as datafilled in table TRKGRP. (Only AIN-capable trunks will be allowed AINDENY options in table TRKOPTS.) The new option will function in a similar manner to the line and customer group options except that it will only block prefix triggers. It will not be capable of holding SFC, PFC, or Office-Wide PFC triggers. It will allow 15 DENYs or RESTOREs just as the line and customer group options. With feature A00002016, individual agents need to subscribe to the prefix triggers. Accomplishment of this task is possible in tables OFCTIID, CUSTIID, TRKAIN or through Servord.		
Product = CS 2000		
OPTION	New prompt	Per feature A00002009 (Succession on DMS), NAME24 can be assigned to KSET via Servord ADO command. It can also be added to a line with NEW and COPYSET commands.
VOW Options	Changed	Feature A00002011 (Succession on DMS) updates the list of incompatible options for VOW and VOWDN and removed the table that documented extra prompts for adding and deleting VOWDN option. These prompts are no longer valid or relevant.

Area	New or changed	ServOrd Description
ADO, DEO, and CLN	Changed	Feature A00002555 (Succession on DMS) allows the ADO, DEO and CLN Servord commands to manipulate the GND Bool in table LNINV for these supported line cards: 3A06BA, 7A25AA, SCD271, RDTCON, and RDTLSG. Other line cards that support GND are not affected by this feature.
ADO, CHF, EST	New prompts	Feature A00003073 (Succession on DMS) adds a new option "REDIRECTION" to the existing SimRing group commands. The "Redirection" prompt affects NPMDNs with active call forwarding (CAF, CFD, CFB).
POSID	New prompts	Feature A00004391 (Succession on DMS) changes the acceptable value of POSID to be a 5-digit value in the range of 00000 to 30000. This change affects command prompting for NEW, ADO, NEWACD, and CHF commands.
New line option MTZ MWT_ANNO UNCEMENT	New	Feature A00005734 (IAW) adds new line option MYZ, used on any line that is physically located in a different time zone to the controlling CM. When the user activates other time related features (Such as Wake Up Call Request), the time will be converted to their local time, rather than the CM time.
MWT_ANNO UNCEMENT	New	Feature a59039138 (IAC) adds this new prompt to allow the user to enable the CLASS Message Waiting Indicator, adding an announcement as an optional replacement for the stuttered dial tone indicator.
Product = Centrex IP		
USERID PASSWD	New	Feature A00003717 (IAW) adds two new Centrex IP-specific line options to the SERVORD+ options list. The options added by this activity are specific to the OSSGATE/Lines Provisioning / CICM EM system and are not provisionable on the core and are not sent by Lines Provisioning to the core.
Product = DMS_Centrex_Res		
OPTION	New prompt	Per feature A00002009 (Succession on DMS), NAME24 can be assigned to KSET via Servord ADO command. It can also be added to a line with NEW and COPYSET commands.
SCA option	new field	Feature A00002196 (Succession on DMS) introduces a new field, DND_ONLY, for the SCA option.
CFDVT option	New prompt	CRs Q000707607 and Q00935523 (Succession on DMS) add new prompt RINGCTRL when provisioning the CFDVT option. The default should be FIXRING. This fix also allows IBN, MBS, and ISDN lines to now be provisioned with CFDVT PRGRING.

Office Parameter changes overview

The following office parameters are new or changed for SN07. More complete descriptions will appear in the Feature Deltas section of this document.

Summary of new/changed Office Parameters for SN07

Status	Name	Description
Product = CS 2000		
New	T1_TIMER_EXPIRY_MSG_SUPPRESS	Feature A00002013 (Succession on DMS) creates this parameter in Table OFCVAR to provide optionality control for the feature in conjunction with SOC INW00001.
New	SPM_NODE_ISTB_FOR_CARRIER_OUTAGE	Feature A00002858 (Succession on DMS) creates this parameter in Table OFCENG. The parm name means SPM Node ISTb under PM Map banner for carrier outage. When the parameter is enabled ("Y"), any SPM carrier outage will cause an indicator under the PM banner that a SPM node has gone ISTb. When the parameter is disabled ("N"), carrier outages will never cause a SPM node to go ISTb. The parameter is only supported on TDM Legacy nodes (SPM and STM-1), and has no impact on Succession nodes (MG4K, LSA, IW, STS-1).
New	MULTINET_DISPLAY_ACTIVE	Feature A00003487 (UA-IP) creates two new parameters. MULTINET_DISPLAY_ACTIVE (OFCVAR) activates the new and changed OMs and logs. It enables the display of certain OM groups (such as TRK2NET1/TRK2NET2) and information displayed in certain logs such as IWBm. This office parameter cannot be turned on unless NETWORK_ACTIVE = EXTENET.

Summary of new/changed Office Parameters for SN07

Status	Name	Description
(continued) New	(continued) PRE_SN07_DUMPSIDE_PACKET_FABRIC	(continued) Feature A00003487 (UA-IP) creates two new parameters. PRE_SN07_DUMPSIDE_PACKET_FABRIC (OFCENG)--This office parameter is set by the Nortel engineering team in an office parm changes flat file prior to the night of ONP. It is to be applied after the transfer of the office parameters and prior to the TABXFER. The parameter identifies the FABRIC type of the single packet fabric supported on the from side prior to the upgrade, in order for the proper network tuples to be created in tables BEARNETS, CLLI, NETBRIDGE, NETPATH, and NET2NET, as well as allow the new network related fields in tables MNODE, TRKOPTS, and SERVIRNV to be assigned the proper default values.
Changed	NETWORK_ACTIVE	Feature A00003487 (UA-IP) expands the value EXTENET to include the ability to support multiple packet networks.
New	OFC_SERVING_CC	Feature A00003711 (PT-IP) creates this office parameter in OFCVAR to
New	RTE_ADVANCE_FOR_INTRA_IMT_NCRT	Feature A00003789 (Succession on DMS, AAL2) creates this office parameter in OFCVAR to control the route advance behavior of CAUSE 34 in conjunction with the INTRACSE TRKOPTS option. The functionality of this parameter does not affect the route advance capability of cause values 42, 47 and 51.
Changed	ECAN_EDGE_STRATEGY	Per feature A00004046 (UA-IP), ECAN_EDGE_STRATEGY in table OFCENG in SN07 and beyond will only apply to AAL1 bearer networks. All other packet network type such as IP will assume the edge ECAN strategy.

Summary of new/changed Office Parameters for SN07

Status	Name	Description
Changed	MAX_NUM_ACD_AGENT S_PER_SWITCH	Feature A00004391 (Succession on DMS) modifies this parameter in Table OFCOPT by increasing the maximum value from 9999 to 30000. The actual value of this parameter can no longer be changed by the end user. In order to change the value of the parameter, the SOC usage limit must be changed.
Changed	RATED_POWER	Feature A00004713 (Succession on DMS) modifies this parameter in Table OFCENG to allow the users to change the value of Rated Power to as small as 1. Previously the lowest possible value was 2.
New	REPORT_ISUP_CI_TO_CM	Feature A00005007 (PT-IP) creates this parameter in Table OFCENG to enable sending of supervision to GWC for reporting of the cause indicator of Release message to CM. The cause indicator will be attached to the Clear Forward or Clear Back Message.
Changed	RATED_POWER	Feature A00005193 (Succession on DMS) modifies this parameter in Table OFCENG to allow the users to change the value of Rated Power to as large as 9. Previously the largest possible value was 7.
Changed	LSCM_SYNC_BURST LSCM_SYNC_DELAY	Feature A59039138 (IAC) modifies these parameters in Table OFCENG to allow the users to datafill values related to refreshing the visual indicator of call waiting on customer premises equipment.
New	IO_WARNING_THRESHOLD	Feature A00006693 (Succession on DMS) creates this new parameter in table OFCENG to define a utilization warning threshold for all IO service types (CMIC, ETHR, AMDI) in the system. The IOCAP monitoring toolset uses the value of this parameter to peg the IOTHRESH register of the IOCAP OM whenever the IO utilization level of any IO service has exceeded this threshold on the switch.

Summary of new/changed Office Parameters for SN07

Status	Name	Description
Product = Centrex IP		
New	sub-network parameters: cicm.em.primary.url cicm.em.backup.url	Feature A00003717 (IAW) introduces two new SESM sub-network parameters required for Centrex IP flow-through provisioning. The <i>cicm.em.primary.url</i> parameter stores the URL of the primary CICM EM node. The <i>cicm.em.primary.url</i> parameter stores the URL of the primary CICM EM node. The URL is comprised of the communications protocol (HTTPS), the IP address of the CICM EM node, the HTTPS port and web server file. Only the IP address is provisionable - the other URL components are fixed. It is required to allow the flow-through provisioning enabled Lines Provisioning application to establish a secure communications session with the CICM EM in order to send it Centrex IP provisioning data (e.g., KSET key features). The <i>cicm.em.backup.url</i> parameter functions the same as the primary described above, except it applies to the optional, backup Element Manager IP address. Both of these parameters are provisioned using the "Configure" tool.
Product = MG 4000		
Changed	PACKET_QOS_OM_THR ESHOLDS	Feature A00003773 (PT-IP) adapts this existing office parameter in OFCVAR to support MG4K. The same QOS OM threshold values defined in table OFCVAR will be applied to all MG4K-IP nodes datafilled on the Call Server.
Product = TOPS		

Summary of new/changed Office Parameters for SN07

Status	Name	Description
New	NUM_OF_WIN_TOPS_EXT_BLKs	Feature A00003687 (Succession on DMS) creates this new parameter in OFCAUT to control how many extension blocks are allocated for use by Wireless Intelligent Network (WIN) TOPS calls.
Deleted	NUM_OF_IS41TOPS_EXT_BLKs	Feature A00003687 (Succession on DMS) deletes this parameter from OFCENG. It is replaced by NUM_OF_WIN_TOPS_EXT_BLKs in OFCAUT.

OM/PM changes overview

The following OMs/PMs are new or changed for SN07. They also appear in the OMs/PMs-by-product tables later in this document with lists of registers and descriptions.

Summary of new or changed OMs/PMs for SN07

OM Group or PM name	New or Changed	Description
Product = AIN		
INSCTP	New	Feature A00004500 (Succession on DMS) creates this new OM group for AIN transports. The group consists of the following eight registers: MSGOUT MSGIN SENDFAIL DATAERR MSG2BIG BMSFAIL DATARCVD NOTREADY
Product = Call Server 2000		

Summary of new or changed OMs/PMs for SN07

OM Group or PM name	New or Changed	Description
XACORE	Changed	Feature A00002012 (Succession on DMS) extends the existing CMIC and RTIF OM to distinguish between packet and device (port or link) state changes to give a more refined count of the CMIC and RTIF component state changes. This feature also changes the OM related to the AMDI functionality to provide a consistent OM structure for components with port and link devices in the XA-Core system. Four registers are deleted, seven new registers are added, and one register is changed. Refer to the Performance section of this feature for details.
FCDRTM1E FCDRTM2E FCDRALG2	New	Feature A00002340 (Succession on DMS) provides the following new OM groups: FCDRTM1E. The group FCDRTM1E is used for register overflows from the OM group FCDRTMP1. FCDRTM2E. The group FCDRTM2E only applies to DMS. This group is used for register overflows from the OM group FCDRTMP2. FCDRALG2. This group is used for register overflows from the OM group FCDRALGR.
SPMACT SPMOVLD	Changed New	Feature A00002432 (Succession on DMS) adds new register CAPINDEX to display the capacity level at which the SPM is running. The capacity index is a numeric value, with possible values of 0, 1, or 2, corresponding to regular, enhanced and premium capacity, respectively. New SPMOVLD group will have 18 OM registers that give metrics on the SPM flow control system and the system overload control component.
XASTAT	Changed	Feature A00002538 (Succession on DMS) modifies OM group XASTAT to remove register XASCMPLX since this measurement is not valid in XA-Core.
ATTAMA2	New	Feature A00002766 (Succession on DMS) creates new OM group ATTAMA2 which provides overflow for registers for AMANS and AMUNANS from OM group ATTAMA. ATTAMA2 is enabled/disabled with SOC BAS000023.

Summary of new or changed OMs/PMs for SN07

OM Group or PM name	New or Changed	Description
SCAISRV4	Changed	Feature A00002904 (Succession on DMS) creates two new registers to peg any application-specific outgoing SCAI messages. • TOGCLLRR - pegged when the switch sends out a RR in response to a valid DV_TOGGLE_CALL message request being received and processed. • TOGCLLRE - pegged when the switch sends out a RE in response to an invalid DV_TOGGLE_CALL message request being received.
DPTNODE IWB	Changed	Feature A00003487 (UA-IP) modifies these two OM groups. • DPTNODE adds additional information to the OM tuples. If the DPT Node is a GWC, then the associated DPT protocol (i.e., BICC or SIP-T) is added to the information. If the DPT Node is an SPM (i.e., either MG4K or DTP SPM), then the associated bearer network, DPT protocol and SPM node type is added to the information. • IWB is modified to collect data per each of the bridge pools defined in table NETBRIDGE.

Summary of new or changed OMs/PMs for SN07

OM Group or PM name	New or Changed	Description
DPTOFCP OFZ2NET1	Changed	Feature A00003487 (UA-IP) adds five new OM groups. • DPTOFCP measures the performance of the supported dynamic packet trunk protocols for the office. The two supported protocols are BICC and SIP-T. • OFZ2NET1 provides information for traffic analysis per bearer network. It pegs calls for the intended destination, not the destination where the call terminates. • OFZ2NET2 provides information for traffic analysis per bearer network. The OFZ2NET2 OM group counts calls that the system routes to generalized no circuit treatment (GNCT). The system routes a call to GNCT when a trunk group is the last route in the route list and all trunks are busy. • TRK2NET1 provides information for per-trunk group traffic analysis per bearer network with information on trunk traffic for each trunk group. • TRK2NET2 provides information for per trunk group traffic analysis per bearer network. It contains extension registers for registers found in OM Group TRK2NET1.

Summary of new or changed OMs/PMs for SN07

OM Group or PM name	New or Changed	Description
SIPGW_CALLP	Changed	Feature A00003933 (PT-IP) adds three new OM groups supported on the Session Server (not related to OMs on the core). - SIPGW_CALLP measures call processing activity with 6 registers that provide totals for incoming call attempts, outgoing call attempts, calls answered, calls abandoned, calls rejected, and calls redirected. - SIPGW_SERVICES measures services activity with 10 registers that provide totals for incoming refer attempts, successful refers, incoming DTMF subscribes, outgoing DTMF subscribes, incoming DTMF notifies, outgoing DTMF notifies, incoming fax subscribes, outgoing fax subscribes, incoming fax notifies, and outgoing fax notifies. - SIPGW_MISC measures miscellaneous activity with 5 registers that provide totals for TCP calls, UDP calls, SIP Msg Send Failures, incompatible SDPs received from remote SIP services, and incompatible SIPs received from local gateways.
SIPGW_SERVICES		
SIPGW_MISC		
Various	Various	Feature A00004005 (PT-IP) describes and illustrates the user interface for the Session Server. An application on the Session Server, such as the SIP Gateway application, has the ability to generate Alarms, Logs, and Operational Measurements (OMs). The alarms that are raised on the Session Server are reported to the SNMP Trap destination server, if one is provisioned.
NGSSOM	New	Feature A00004271 (PT-IP) creates this OM group to provide information on the maximum number of simultaneous calls that utilize the NGSS platform as well as indication of the number of times the limit settings of the CS2B0008 and CS2B0009 usage SOC's have been exceeded.
IOCAP	New	A00006693 (Succession on DMS) creates this new OM group to provide information on IO capacity such as utilization and utilization high watermark and IO throughput information on a per IO service type (CMIC, ETHR and AMDI). The group consists of 7 registers. This OM group provides one tuple for each IO service type. There are 3 possible IO service types (CMIC, ETHR, AMDI) displayed as a 4-digit string.

Summary of new or changed OMs/PMs for SN07

OM Group or PM name	New or Changed	Description
Product = MG 4000		
TRKQOSOM	Changed	Feature A00003773(PT-IP) adapts this existing OM group to support MG4K to record instances in which QOS threshold values have been exceeded for calls handled by MG4K-IP based TDM trunk group. The QOS statistics that are included in the OM for each MG4K-IP and GWC trunk group are packet loss, jitter, and delay (latency).
Product = MG 9000		
GWOVLOM	New	Feature A00006639 (UA-IP) creates this OM group to count the number of denied call connection requests due to an overload condition on the MG9K node.
Product = TOPS		
IS41TOPS	Deleted	Feature A00003687 (Succession on DMS) deletes this OM group, replacing it with three others as described in the following table entry.
SMSTOPS WINTOPS TC7WRLSS	New	Feature A00003687 (Succession on DMS) creates three new OM groups. - SMSTOPS records application-level events for the TOPS short message service. - WINTOPS records application-level events for wireless ADACC with release. This group uses WIN in the name since wireless intelligent network capabilities are used to provide ADACC with release for both IS-41 and GSM. - TC7WRLSS records transport-level events such as types of TCAP messages sent and received, SS7 errors, etc. on TOPS wireless calls (SMS and WIN, as well as IS-41 and GSM).
TDGTHRU	New	Feature A00005160 (Succession on DMS) creates new OM group TOPS Datagram Throughput can be used in analyzing messaging throughput of TOPS applications that send and receive UDP datagrams. The 28 registers each count the number of messages in a particular size range that a TOPS application sent or received during the reporting period. The numbers in the register names indicate the size ranges or "buckets."

AMA/Billing changes overview

The following AMA/Billing information is new or changed for SN07. More complete descriptions appear in the Feature Deltas section of this document.

Summary of new or changed AMA/billing

AMA/billing item	New or Changed	Description
Product = CS 2000		
Backing up billing data	New	Feature A00002008 (Succession on DMS) provides a manual procedure for backing up billing data from the CBM to a DVD, both with and without a script.
Multiple	Changed	Feature A00004036 (Succession on DMS) appends a Service Logic Identification Module (module code 039) to the current record as an AMASlpid is included in the corresponding update request. Refer to the Accounting section of this feature for additional details for each group.

Software Optionality Control (SOC) changes overview

The following SOC information is new or changed for SN07. More complete descriptions appear in the Feature Deltas section of this document.

Summary of new or changed SOC information for SN07

SOC code	New or Changed	Description
Product = AIN		
CAIN0612	New	A State SOC will control feature A00001990 (Succession on DMS) -- state is either IDLE or ON. Functionality of this activity depends on a number of basic CAIN SOC's that are provided in the functional description (FN) for this activity.
With feature A00002016 (Succession on DMS), the SOCS relevant to the detected triggers need to be activated. See the functional description of this activity in this document for a list of the SOC order codes for VSC and prefix triggers.		
INW00003	New	Feature A00004500 (Succession on DMS) creates this SOC to control the allocation of IN SCTP links in table IPAPPL. If the limit has not been met, the user will be allowed to add entries to table IPAPPL.

Summary of new or changed SOC information for SN07

SOC code	New or Changed	Description
CAIN0202	New	Feature A0005363 (Succession on DMS) adds a new SOC to enable new CAIN message processing. • Support for a new parameter, AMABusiness CustomerId in some incoming messages. • Support for a digits id (300) for an existing parameter, AMADigitsDialedWC • Support for recording all the digits for a currently supported digits id (301) for the existing CAIN parameter AMADigitsDialedWC • Support for retaining the first occurrence of an existing parameter, AMASlpID. Currently, only the last occurrence of this parameter is retained. • Support for 4 new parameters in the CDRTMPLT table: SLPID1ST, BUSCSTID, DGI300 and DGI301. This feature does not create a new predefined template. The customer must either modify their existing template or create a new template which includes the 4 new parameters.
Product = CS 2000		
MDC00075	New	Feature A00002009 (Succession on DMS) introduces a SOC to control NAME24 line option processing, and it also controls the display when NAME24 does not apply to the originator.
TBD	New	For non-MSL customer, standard SOC control will regulate feature A00002011 (Succession on DMS). VOWs and VOWDNs can be datafilled but will not be permitted to log in unless the feature is activated in SOC. If the SOC is turned off, attempts to log in by VOW user will be routed to FNAL treatment. In loads built for the MSL market, the SOC should always be turned on.
INW00001	New	Feature A00002013 (Succession on DMS) controls the functionality of T1 Timer Expiry Message Suppression. When enabled, T1 Timer Expiry messages are not generated. Suppressing the 'T1 Timer Expiry' messages from being generated will prevent the messages from flooding the network should an SCP go down.

Summary of new or changed SOC information for SN07

SOC code	New or Changed	Description
BASE0015	New	Per feature A00002186 (Succession on DMS) when BASE0015 is ON, IOM DDU capacity increases from 1G to 4G. The status must be ON before the additional capacity is visible.
SPMS0020 SPMS0028	New	Feature A00002431 (Succession on DMS) introduced two new USAGE SOC's under the existing SPMS group for DMSCP class of SPMs. The SOC option SPMS0020 corresponds to the SPMs with Enhanced capacity; the SOC option SPMS0028 corresponds to the SPMs with Premium capacity.
ICM00079	Changed	Feature A00002904 (Succession on DMS) adds a warning message when the CTI Toggle Transfer SOC ICM00079 is toggled from ON to IDLE state. The warning message indicates that state transition disables the associated dv_Toggle_Call functionality.
UTRS0011	New	Per feature A00002960 (Succession on DMS), when UTRS0011 is IDLE calls will not be blocked on any ISUP EANT trunks when the CPN or CN is not present. The new ORIGIDSCR option in Table TRKOPTS can be datafilled when SOC is IDLE. When UTRS0011 is ON certain calls can be blocked.
NSER0005	New	Per feature A00003789 (Succession on DMS, AAL2), when NSER0005 is IDLE, CAUSE handling behavior is unchanged for calls with INTRA IMT originators. The new TRKOPTS option INTRACSE can be data filled when the SOC state is IDLE or ON. This SOC depends on SOC NSER003, Inter/Intra IMT, for the described functionality to be active.
BASE0014	New	Per feature A00003905 (Succession on DMS), when BASE0014 is IDLE, it limits the number of provisionable volumes per pool in table DIRPPool to 24. SOC state ON increases the total number of volumes per pool to 72.

Summary of new or changed SOC information for SN07

SOC code	New or Changed	Description
CS2B0008 CS2B0009	New	Feature A00003933 (PT-IP) creates the following SOCS. (The combined total limits of these two SOCs should not exceed the limit of the base DPT SOC option, CS2B0005.) - CS2B0008, "Call Server to Call Server SOC" - CS2B0009, "Call Server to Application Server SOC" Without one or both of the new SOC options, no call processing can take place using the Session Server Manager.
AIN00321 AIN00322 AIN00323 AIN00324 AIN00325 AIN00326 AIN00327	New	Feature A00004036 (Succession on DMS) creates seven new SOC options, as follows: - AIN00321 SVC MGR Basic handles all group 1 and 2 features except MWI, and Visual MWI. These features include ACB, AR, CWT, LDSA, CSMI, ACRJ and MSB in group 1. And PRN in group 2. - AIN00322 SVC MGR List Editing handles all group 3 and 5 features. These features include DRCW and SCRJ in group 3. It also includes SCA and SCF in group 5. - AIN00323 SVC MGR Speed Call handles all group 9 features. These features include SCS, SC1/SC2/SC3, SCL and SCU. - AIN00324 SVC MGR Call Forward handles all group 4 and group 6 features. These features include CFUIF/CFW, CFDA/CFD and CFBL/CFB in group 4. And CFDDVT in group 6. - AIN00325 SVC MGR Privacy Control handles all group 7 features. These features include CNMB and CNNB. - AIN00326 SVC MGR COT and CCW handles all group 8 features. These features include COT and CCW. - AIN00327 SVC MGR SIMRING handles the SIMRING feature.
UTRS0012	New	Per A00004045 (Succession on DMS, AAL2) when UTRS0012 is ON, call attempts on a supported incoming trunk to a called number marked for tracing in table CLIDN will generate a TRK605 log.

Summary of new or changed SOC information for SN07

SOC code	New or Changed	Description
ACD00101	New	A00004391 (Succession on DMS) creates a new SOC option to control the maximum number of ACD agents in the switch. Office parameter MAX_NUM_ACD_AGENTS_PER_SWITCH will automatically be updated to match the SOC usage limit.
CS2B0008	New	Feature A00004414 (PT-IP) implements a usage SOC to control the maximum number of SIPT calls that utilize the Next Generation Session Server (NGSS) platform when the far end is another CS2K.
Product = DMS_Centrex_Res		
RES00102	New	There is a new SOC option order code for feature A00002196 (Succession on DMS). The SOC option name is Enh Do not Disturb.
Product = MG 9000		
SPMS0020	New	Feature A00002431(Succession on DMS) creates two new USAGE SOC's under the existing SPMS group for DMSCP class of SPMs. The SOC option SPMS0020 corresponds to the SPMs with Enhanced capacity and the SOC option SPMS0028 corresponds to the SPMs with Premium capacity.
SPMS0028	New	
Product = TOPS		
ENSV0108	New	Feature A00002740 (Succession on DMS) introduces this SOC to enable International DACC. ENSV0108 requires ENSV0101, OSB00101, OSDA0101, and OSDA0102.



SN07 Feature Deltas

Product = AIN

A00001990 -- CAIN via CIC Route PEP Sourcing (Succession on DMS)

Functional Description

Currently, CAIN subscriptions can be achieved through tables TRKGRP, AINSCUSP, UNIPROF, AUTHCODU, AUTHCDX and STDPRTCT. The sourcing of this patch will allow CAIN subscriptions to be added to table CICROUTE enabling subscription on a per CIC (Carrier Identification Code) basis. This new subscription point will allow carriers to use the SCP to route calls based on their CIC.

This functionality was originally patched into the UCS12 load. That patch has been propagated to more recent UCS loads. This activity will source the patching into the SN07 load and put it under SOC (Software Optionality Control) control.

The new subscription point will be created by adding the CAINGRP option to tuples of table CICROUTE, just as in other CAIN subscription tables. The CAINGRP option takes one argument, the service name, as defined in table CAINGRP. In the example below, CIC 333 is subscribed service SRVC1.

CICROUTE Example with CAIN Subscription

KEY	NATLTS	INTLTS	MLTCSID	OPCHIDX	PRTNM	IDPRTNM	ADIN	CICDELVL	OPTIONS
3331	611	212	0	2	CIC	EAPT	3	ALWAYS	CAINGRP SRVC1

CAIN precedence levels determine the order in which specific subscription types are checked for applicability at a particular TDP. The new CICROUTE subscription point will have a new precedence level of CARRIER which will fit in the current order as below:

Precedence Level Between Subscription Types

Order	Subscription Type	Subscription Tables
1	SCP	Requested by SCP
2	Address	subtable STDPRT of STDPRTCT
3	Authorization Code	AUTHCODU, AUTHCDU*
4	ANI	ANICUSP, ANIVAL, UNIPROF
5	Agent	TRKGRP, CALLATTR, TRKFEAT
6	Carrier	CICROUTE
7	Office-wide	CAINPARM

Subscribing to CAIN via table CICROUTE

The originating agent types supported by this feature are PTS FGD, SS7 FGD, and SS7 Inter IMT.

All originating trunks wishing to use the CAIN functions must have the CAIN option defined in table TRKGRP, CALLATTR, or TRKFEAT. The CICRTE option also needs to be included in TRKGRP so translations will use table CICROUTE and encounter the new subscription point.

A service and its associated triggers must be added to table CAINGRP and the triggers must have their criteria defined in the relevant subscription tables.

Once the above datafill is in place, the CAINGRP option can be added to individual tuples in table CICROUTE. The CAINGRP option takes the name of a service defined in table CAINGRP.

More general information on CAIN datafill can be found in NTPs 297-2621-370*, the UCS DMS-250 NetworkBuilder Application Guides.

CallP Behavior

When a specific TDP (Trigger Detection Point) is encountered during call processing (see NTP 297-261-370 Network Builder Application Guide, Vol. 2), each subscription method is checked in the precedence order defined above. If a subscription to a CAIN service is defined via the CAINGRP option, and the service includes a trigger of this TDP, and the trigger's criteria is met, then the trigger will have its action performed.

Adding a new subscription point to CAIN does not affect the procedure described above. A service subscribed via table CICROUTE will have its triggers evaluated at the proper TDPs.

Traver

The traver tool simulates a call from the user specified originating trunk to the user specified address. Traver displays the following CAIN-specific information at each TDP encountered:

- 1 The name of the TDP encountered (e.g. ORIGATT)
- 2 The CAIN subscription method, if any (e.g. CARRIER)
- 3 The tuple from table CAINGRP detailing the subscribed to service
- 4 The tuple from the trigger table detailing the criteria being evaluated
- 5 The action, if any, taken if the trigger's criteria is met

Traver will be enhanced to display the subscription method of CARRIER, the CAINGRP data and the trigger table data if a call subscribes to CAIN via CICROUTE.

The following traver snippet shows the SCP being queried when it is determined that the call is subscribed to the SPECGRP service via table CICROUTE. This example was run via

```
> UVTSTS 611; traver tr dal221twdtls 2201234 t
```

Example Traver Output

--> ENTER TDP INFOANLZ <--
+++ CAIN SUBSCRIPTION VIA CARRIER +++
TABLE CAINGRP
SPECGRP 7 CAIN02 TCAP_SCCP (ANLZINFO INFOANLZ SPECDIG) \$ \$ (ADIN) (CAINGRP) (ORGTINFO) \$
TABLE SPECDIG
SPECGRP ADDR 2201234 2201234 QUERY SDS_ADDR ROUTE \$
UserID: DAL221TWDTLS 11
BearerCapability: SPEECH
CalledPartyID: 2201234
TriggerCriteriaType: SDS_ADDR
CallingPartyID: 214
+++ TRAVER: SUCCESSFUL CALL TRACE +++

Log Changes

Logs that indicate the subscription method will be updated to display the CIC information.

CAIN902 Logs

CAIN902 logs show the subscription method and other relevant details when a call subscribes to CAIN (not when the query is sent to the SCP). The METHOD field of the log indicates the subscription type (e.g. ANI, OFFICE) and the precedence level. CAIN902 logs will indicate a METHOD of CICROUTE and a precedence level of 6 when appropriate.

VAMP902 Logs

VAMP902 logs are output when the VPTrace CI tool is enabled and an outbound message is sent through the VAMP framework to the SCP.

The VAMP902 log may display the subscription type via the SUBINFO field. The SUBINFO field will be enhanced by this activity to include CARRIER as a possible value.

SOC Control

This feature will be controlled by a State SOC (State is either IDLE or ON). The SOC id will be CAIN0612. Using the SOC CI command to activate or deactivate a order code is covered in NTP 297-8991-901.

Datafilling a CAINGRP option will be allowed regardless of the state of SOC CAIN0612. However, if the SOC is IDLE, the CAIN software will not recognize subscriptions via CICROUTE either during CallP or in the Traver Tool.

ONP

Reformat procs will be written as part of this feature to guarantee the validity of CICROUTE tuples whether the switch has patch HIJ00 activated or not.

Hardware Requirements or Dependencies

N/A.

Software Requirements or Dependencies

No new dependencies are introduced by this work beyond the new SOC order code detail above. However, using the functionality of this activity depends on a number of basic CAIN SOC's detailed below.

CAIN SOC Codes of Note

Order Code	Function
CAIN0100	Usage Option for all CAIN msgs to SCP
CAIN0200	Extension Parameters
CAIN050*	SOCs to enable Specific Trigger

CAIN SOC Codes of Note

Order Code	Function
CAIN0600	Conversational Digit Collection
CAIN0601	SCP Trigger Subscription
CAIN0602	EDPs Enabled
CAIN604	Inter IMT Support

Limitations and restrictions

Originating trunk types supported by this feature are PTS-FGD, SS7-FGD and SS7 Inter IMT. Other trunk types are incapable of passing the CIC information.

Interactions**Normal CIC Routing Suspended**

If a CAINGRP is datafilled against a CICROUTE CIC, normal CIC routing will be suspended and CAIN processing will begin. For example, if the DEFCIC option is datafilled against a trunk in table TRKGRP that is supported by table CICROUTE with the DFCICRTE sub-option set (when this field is Y, the DEFCIC can be used as an index into table CICROUTE), call processing will exit and the CIC routing feature will begin CAIN processing. If a CAIN “no action” or continue response is encountered, normal CICROUTE call processing will continue.

CAINCIC Not Affected

The functionality of table TRKGRP option DEFCIC, sub-option CAINCIC will not be affected by this activity.

No Affect on CAIN Standard Routing

Standard routing parameters CARRIER, ALTERNATECARRIER and SECONDALTERNATECARRIER will continue to be used to identify a route by obtaining an STS value through table CICROUTE.

However, if the following scenario occurs, an extra CAIN902 log will be generated.

An Analyze_Route message containing CARRIER and ALTERNATECARRIER is received. Table CICROUTE is accessed for the CARRIER and a CAINGRP is picked up. The subsequent route selection results in a busy condition and the call route advances to the ALTERNATECARRIER. Table CICROUTE does not have a CAINGRP option for the ATLERNATECARRIER. Carrier subscription is undone and a CAIN902 log will be output to indicate this.

Applicable customer facing sections

Fault Management

Logs ☒ X ☐

Alarms ☐ N/A ☐

Configuration

Data Schema ☒ X ☐

User Interface ☐ N/A ☐

Element Management ☐ N/A ☐

Security ☒ X ☐

Service Order ☒ X ☐

Office Parameters ☒ X ☐

Accounting (includes AMA billing) ☐ N/A ☐

Performance (includes operational measurements) ☐

Indicate with an X if you are completing the sections of the DDOC listed below. Indicate with “N/A” if these sections do not apply to this functionality.

Realtime ☐ N/A ☐

Engineering Information ☐ N/A ☐

Glossary

Term	Description
CAIN	Carrier Advanced Intelligent Network
CIC	Carrier Identification Code
FGD	Feature Group D (Dial Plan for EANT trunks)
ONP	One Night Process (for software upgrade)
PEP	Product Enhancement Patch
PTS	Per-Trunk Signaling
SCP	Service Control Point
SOC	Software Optionality Control
SSP	Service Switching Point
UCS	Universal Carrier Software

Term	Description
VAMP	Variable AIN Messaging Platform

Product = AIN

A00002016 -- AINDENY CUSTSTN increase from 10 to 15 (Succession on DMS)

Functional Description

AINDENY currently exists as both a line and customer group option. Its purpose is to block the triggering of Vertical Service Code (VSC) triggers to lines and customer groups. The VSC triggers are Specific Feature Code (SFC), Public Feature Code (PFC) and Office-Wide PFC (OFCPFC). These triggers are all hit by the originator dialing a digit string starting with a * or #. The AINDENY line option blocks SFC, PFC and OFCPFC triggers. The CUSTSTN option only blocks OFCPFC triggers.

AINDENY options are lists of { ACTION, SCOPE } pairs where ACTION is either DENY or RESTORE and SCOPE specifies a specific tuple in table TRIGITM or a whole trigger-type. An AINDENY option of “AINDENY DENY TIID 4 OPFC3, DENY TIID 4 SFC2” will deny triggering to the triggers defined in table TRIGITM as “4 OPFC3” and “4 SFC2”. The option can block entire triggers types, e.g. “AINDENY DENY ALL SFC”. Furthermore, the option can specifically allow triggers that have been blocked by AINDENY. “AINDENY DENY ALL OFCPFC, RESTORE TIID 4 OFCPFC2” denies all Office-Wide PFC triggers except the “4 OFCPFC2” trigger.

Description

Customers have requested the ability to deny AIN Prefix triggers (Specified_Carrier, One_Plus_Prefix, International, Operator_Services) on a per trunk group basis. This can be accomplished by creating a new AINDENY option in table TRKOPTS. In addition, this activity will expand the CUSTSTN AINDENY option to hold 15 triggers to bring it in line with the AINDENY line option.

Enlarging the CUSTSTN AINDENY Option

Currently the AINDENY option of table CUSTSTN can only hold 10 elements; that is, only 10 DENY or RESTORE actions can be taken per customer group. The AINDENY line option can hold 15 elements. This activity will enlarge the storage capacity of the CUSTSTN AINDENY option to 15 elements.

Denying Prefix Triggers

The four Prefix triggers (Specified_Carrier, One_Plus_Prefix, International, Operator_Services) are all detected at the Info_Analyzed TDP. The AINDENY line and customer group options cannot currently block these trigger types. This activity will allow the CUSTSTN, line and the newly created TRKOPTS AINDENY options to hold the four Prefix triggers and block their triggering at the Info_Analyzed TDP.

Datafill for blocking Prefix triggers

The Prefix triggers are detected at the Info_Analyzed TDP (TDP 4). One or more Prefix triggers need to be added to table TRIGITM as shown here.

Example Datafill for the Prefix triggers in table TRIGITM

TDP	Name	Trigger	Criteria	State	Action	MSGSET	TRANSPRT	GTT
4	PRFXEX1	SPECARR	\$	ULK	EVENT	R02	SS7	AINPOP
4	PRFXEX2	ONEPLUS	\$	ULK	EVENT	R02	SS7	AINPOP
4	PRFXEX3	INTERNTL	\$	ULK	EVENT	R02	SS7	AINPOP
4	PRFXEX4	OPERSRV	\$	ULK	EVENT	R02	SS7	AINPOP

Secondly, individual agents need to subscribe to the Prefix triggers. This can be accomplished in tables OFCTIID, CUSTIID, TRKAIN or through Servord.

Subscribing Agents to AIN Prefix Triggers

Agent	Datafill
Office	table OFCTIID; add 4 PRFXEX1 ON
Customer Group	table CUSTIID; add RESGRP 4 PRFXEX1 ON
Line	servord; ado \$ 6213519 ain tiid 4 PRFXEX1 ON \$
Trunk	table TRKAIN; add CLI3 TIID 4 PRFXEX1 ON \$

Next, the AINDENY option can be added to the line, table CUSTSTN or table TRKOPTS.

Adding the AINDENY option

Agent	Datafill
Customer Group	table CUSTSTN; add RESGRP AINDENY AINDENY DENY TIID 4 PRFXEX1 \$
Line	servord; ado \$ 6213519 AINDENY DENY TIID 4 PRFXEX1 \$
Trunk	table TRKOPTS; add CLI3 AINDENY DENY TIID 4 PRFXEX1 \$

Finally, the SOC codes relevant to the trigger being detected need to be turned on. The following table details the SOC codes for PFC, SFC, OFCPFC, and the Prefix triggers.

SOC Order Codes for VSC and Prefix Triggers

Trigger	SOC
SFC	AIN00294
PFC	AIN00294
OFCPFC	AIN00309
SPECARR	AIN00252
ONEPLUS	AIN00251
INTERNL	AIN00253
OPERSRV	AIN00254

The New TRKOPTS AINDENY Option

Trunks can be subscribed to AIN triggers through table TRKAIN or through office-wide subscriptions. However, there is currently no way to block the triggering for specific trunk groups.

This activity will create a new AINDENY option in table TRKOPTS which will allow AINDENY to be associated with specific trunk groups (as datafilled in table TRKGRP). The new option will be functionally similar to the line and customer group options except that it will only block Prefix triggers. It will not be capable of holding SFC, PFC, or Office-Wide PFC triggers. It will allow 15 DENYs or RESTOREs just as the line and customer group options.

Datafilling AINDENY option in table TRKOPTS

Table TRKOPTS is indexed by a combination of trunk group and option name. To deny all Operator Services triggers, except trigger “4 OPSRV1” for trunk group ISUP2WITEA, add the tuple shown in the following table.

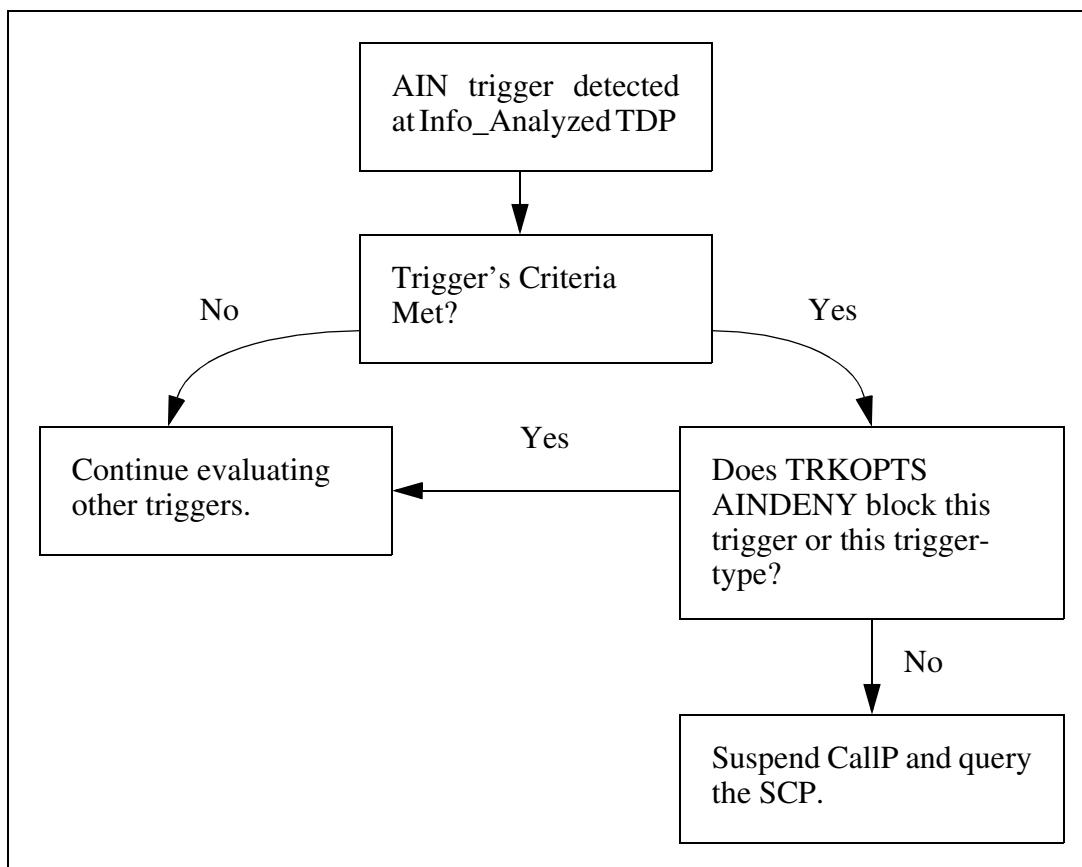
Example Datafill for an AINDENY Option in table TRKOPTS

OPTKEY	OPTINFO
ISUP2WITEA AINDENY	AINDENY (DENY ALL OPSERV) (RESTORE TIID 4 OPSRV1) \$

TRKOPTS AINDENY CallP Behavior

When an originating trunk encounters the INFO_ANALYZED TDP and is subscribed to any AIN triggers at this TDP, it will evaluate the criteria for each subscribed trigger. If the criteria are met, call processing will be suspended while the SCP is queried. If there is a TRKOPTS AINDENY option datafilled

against the originating trunk and the option specifies that the specific trigger or trigger-type is denied, the SCP will not be queried and AIN will continue evaluating any other subscribed triggers at this TDP. This behavior is summarized in the following flowchart.



Traver

The Traver tool simulates a call from the user specified originator with the user specified digits. Traver will display information regarding subscriptions to AIN triggers and will display the criteria associated with those triggers. The tool also respects the AINDENY line and customer group options and will tell the user if the SCP query was blocked due to AINDENY. Traver code will be enhanced to consider AINDENY for Prefix triggers and trunk origination.

Example of line being denied a One_Plus trigger by AINDENY line option:

```
>traver 1 6213512 16199451478 b
TABLE IBNLINES
HOST 01 0 00 23 0 DT STN RES 6213512 0 613_P621_0 L613_LATA1_0 613 (AR) $
TABLE LINEATTR
0 1FR NONE NT 0 10 NILSFC 0 NIL NIL 00 613_P621_0 L613_LATA1_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
613_P621_0 NSCR 613 P621 NONE Y RESGRP 0 0 $ $
TABLE RATEAREA
L613_LATA1_0 L613 NIL LATA1 $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE IBNFEAT
HOST 01 0 00 23 0 AIN AIN TIID (4 MKSFC ON) $
TABLE CUSTSTN
RESGRP AIN AIN TIID
TABLE OFCVAR
AIN_OFFICE_TRIGGRP TIID
AIN Orig Attempt TDP: no subscribed trigger.
TABLE NCOS
RESGRP 0 0 0 RES613 ( XLAS RESX613 STARXLA RES)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
RESGRP NXLA RESXLA STARXLA 0 RES
TABLE DIGCOL
RES specified: RES digit collection
TABLE IBNXLA: XLANAME RESX613
TUPLE NOT FOUND
Default from table XLANAME:
RESX613
      (NET N N 0 N RES N Y GEN ( LATTR 0 613_P621_0 L613_LATA1_0)
      (EA NILC Y 0) $ $)$ 9
TABLE DIGCOL
RES specified: RES digit collection
TABLE LINEATTR
0 1FR NONE NT 0 10 NILSFC 0 NIL NIL 00 613_P621_0 L613_LATA1_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
613_P621_0 NSCR 613 P621 NONE Y RESGRP 0 0 $ $
TABLE RATEAREA
L613_LATA1_0 L613 NIL LATA1 $
TABLE STDPRTCT
P621 ( 1) ( 0) 3
. SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING. CALL TYPE DEFAULT IS NP. PLEASE REFER TO
DOCUMENTATION.
```

Example of trunk being denied a One_Plus trigger by TRKOPTS AINDENY:

```
>traver tr priic 19199451478 b
TABLE TRKGRP
PRIIC PRA 0 PRAC NCRT DSEQ N (ISDN 501) $ $
TABLE LTCALLS
ISDN 501 PUB XLALEC 1 613_P621_1 L613_LATA1_0 $
. . TABLE TRKAIN
. . PRIIC TIID (4 MKONE ON) $
```

Hardware Requirements or Dependencies

No new hardware requirements are introduced by this feature.

Software Requirements or Dependencies

The basic AIN SOC options need to be in state ON for the AINDENY option to be encountered during CallP. However, no new software dependencies are introduced by this feature.

Limitations and restrictions

Only AIN-capable trunks will be allowed AINDENY options in table TRKOPTS.

Prefix triggers are detected only on ISUP, NTNA/NI, 4ESS/5ESS PRI incoming trunks only.

Interactions

N/A.

Applicable customer facing sections

Fault Management

Logs _N/A_

Alarms _N/A_

Configuration

Data Schema __X__

User Interface __X__

Element Management _N/A_

Security _N/A_

Service Order __X__

Office Parameters _N/A_

Accounting (includes AMA billing) _N/A_

Performance (includes operational measurements) _N/A_

Glossary

Term	Description
AIN	Advanced Intelligent Networks
AINDENY	A line option and an option in table CUSTSTN that blocks specific AIN triggers from querying the SCP.
PFC	Public Feature Code: an AIN trigger
Prefix Triggers	The Specified_Carrier, One_Plus_Prefix, International, and Operator_Services AIN triggers.
SCP	Service Control Point: the machine that the SSP queries with AIN TCAP messaging.
SFC	Specific Feature Code: an AIN trigger

Term	Description
SOC	Software Optionality Control
SSP	Service Switching Point: the DMS-100 in AIN speak.
VSC	Vertical Service Code: SFC, PFC and OFCPFC are VSC-detecting triggers. VSC codes are digit strings starting with * or #.

Product = AIN

A00004500--IN TCAP Messaging on IP (Succession on DMS)

Description

This document is a Functional Description for the support of the AIN TCAP (Transaction Capability Application Part) messaging in Open Standards Protocol. This activity is provided on the DMS / CS2K - CORE. It is intended to transport the IN messages via the IP fabric - using the Simple Control Transport Protocol¹ (SCTP). Control SOC INW0003 is used to control the IN Messaging over IP functionality.

With the converging of PSTN and IP networks, the existing transfer protocols (e.g.: TCP) has some major limitations. SCTP (Stream Control Transmission Protocol) is designed to overcome the limitations of TCP as well as supporting the extra requirements of PSTN signalling over IP networks.

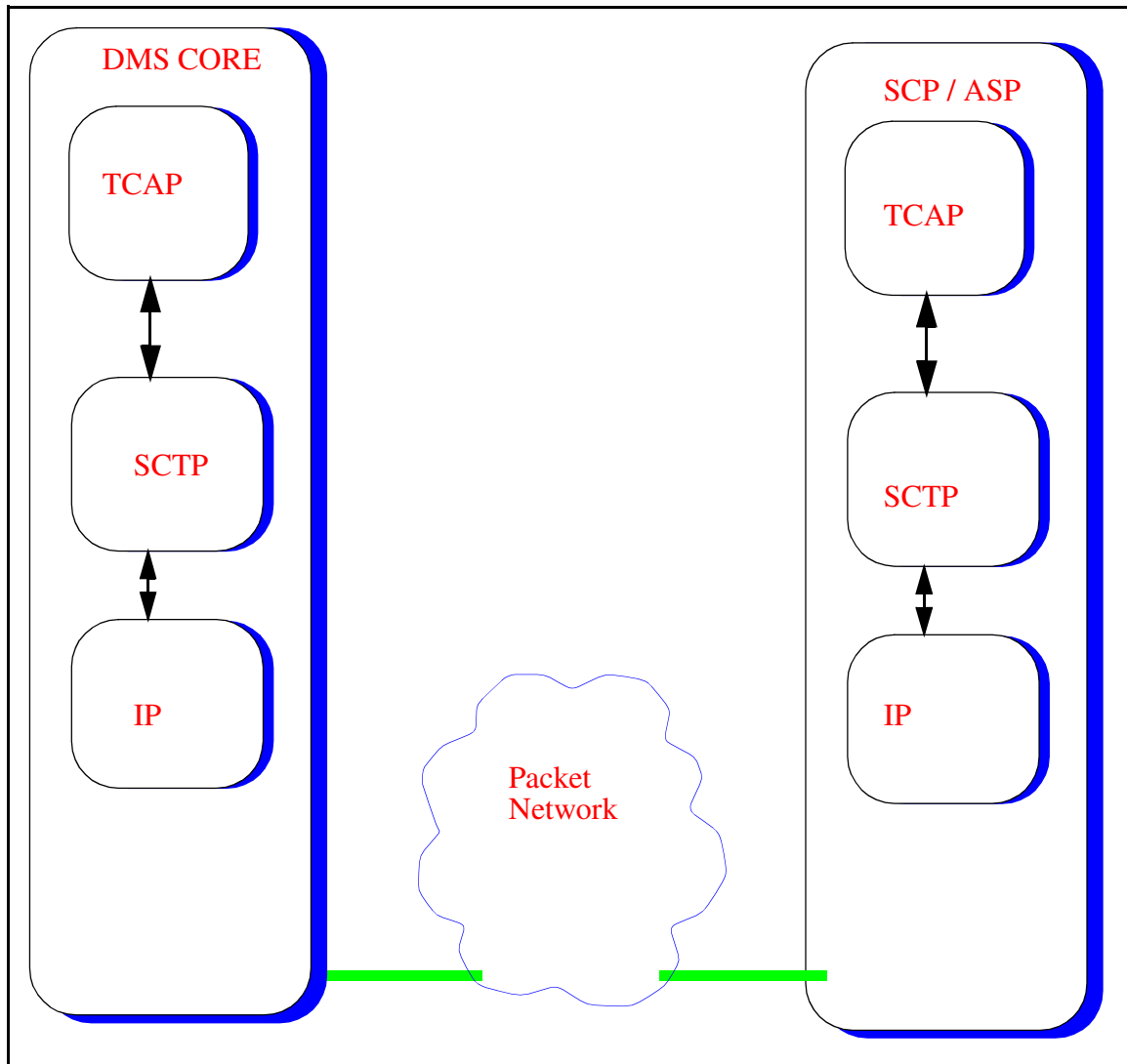
This activity provides the following functionality:

- Supporting AIN (IN) and LNP messages to / from the DMS / CS2K - CORE over SCTP / IP. Please note that the message sets supported for NA markets are only supported.

1. It should be noted that version 5 RFC is titled "Simple Control Transmission Protocol" and the original RFC2690 is titled "Stream Control Transmission Protocol". Throughout this document SCTP is "Stream Control Transmission Protocol".

Functional Behavior

Functional Behavior



The IN TCAP messages will use the Sctp as a transport layer over IP networks. The hardware at the DMS-Core / CS2K may be either EIU or HIOP depending upon the required bandwidth.

Note: HIOP card is available only over XA-CORE platform for high bandwidth IP access.

This feature provides an Interface to the IP network via Sctp, which enables an Advanced Intelligent Network (AIN) Application to access services offered by an Application Service Provider (ASP) located on an Offboard Processor

(OP) on an Ethernet / Local Area Network (LAN). The AIN Application uses the services of the Signalling System Number 7 (SS7) Transaction Capability Application Part (TCAP) Application Layer Protocol. This feature also provides the software to manage the SCTP association between the AIN Application in the Computing Module (CM) and the Application Service Provider in the Offboard Processor.

TCAP Background

Transaction Capability Application Part (TCAP) provides a common protocol for remote operations across the CCS7 network. The protocol consists of message formatting and contains rules and exchange procedures.

Transactions are functions which control non-circuit related information transfer between nodes in a CCS7 network. The TCAP protocol format is separated into two parts, the *Transaction and Component portions*.

The *Transaction Portion* provides a means of associating messages with a specific Application Process transaction. A transaction consists of one or more messages exchanged between Application Processes on the same or different Network Nodes.

The *Component Portion* ensures that Components are formatted and exchanged properly. A Component is a unit of information within a transaction. The Component Portion utilities provide all TCAP users with a common set of component encoding and decoding procedures. This eliminates the need for individual Applications that implement message formatting procedures thereby reducing development time and minimizing the risk of protocol errors.

A TCAP message consists of a Package containing a Transaction Portion plus one or more Components in any order.

TCAP enables the deployment of advanced intelligent network services by supporting non-circuit related information exchange between signaling points using the ***SCCP connectionless service***. An SSP uses TCAP to query an SCP to determine the routing number(s) associated with a dialed LNP, 800, 888, or 900 number. The SCP uses TCAP to return a response containing the routing number(s) (or an error or reject component) back to the SSP. Calling card calls are also validated using TCAP query and response messages.

In the CCS7 layered architecture, TCAP lies between the Application Processes using the CCS7 signalling network and the Signalling Connection Control Part (SCCP) which provides the message transfer capabilities.

Since IN TCAP messaging uses connectionless service, IN TCAP messages can be embedded in a transport layer function and transported across IP.

SCTP Background:

The limitations of TCP as a transport protocol for SS7 was the direct motivation for the using of SCTP as a new transport protocol. SCTP is a new IP transport protocol, which exists at an equivalent level with TCP and user datagram protocol (UDP) and which currently provides transport layer functions to many Internet-based applications. SCTP has been approved by the IETF as a proposed standard, and is specified in RFC 2960. Nortel Implementation of the SCTP transport protocol on the CORE was implemented by feature activity A59023997.

The SCTP transport service can be fragmented into several functionalities:

1. **Association Startup and Teardown** --An association is initiated by a request from the SCTP user. A cookie mechanism is employed during the initialization to provide protection against security attacks.
2. **Sequenced Delivery within Streams** --The SCTP user can specify at association startup time the number of streams to be supported by the association.
3. **User Data Fragmentation** --SCTP supports fragmentation and reassembly of user messages to ensure that the SCTP packet passed to the lower layer conforms to the path multiple-tenant unit (MTU).
4. **Acknowledgement and Congestion Avoidance** --SCTP assigns a transmission sequence number (TSN) to each user data message (fragment or unfragmented). The receiving end acknowledges all TSNs received, even if there are gaps in the sequence.
5. **Chunk Bundling** --The SCTP packet delivered to the lower layer consists of a common header followed by one or more chunks. The following table depicts the general structure of an SCTP packet:
6. **Packet Validation** --A mandatory verification tag field and a 32-bit checksum field are included in the SCTP common header.
7. **Path Management** --The SCTP path-management function chooses the destination transport address for each outgoing SCTP packet based on the SCTP user's instructions and the currently perceived reachability status of the eligible destination set.

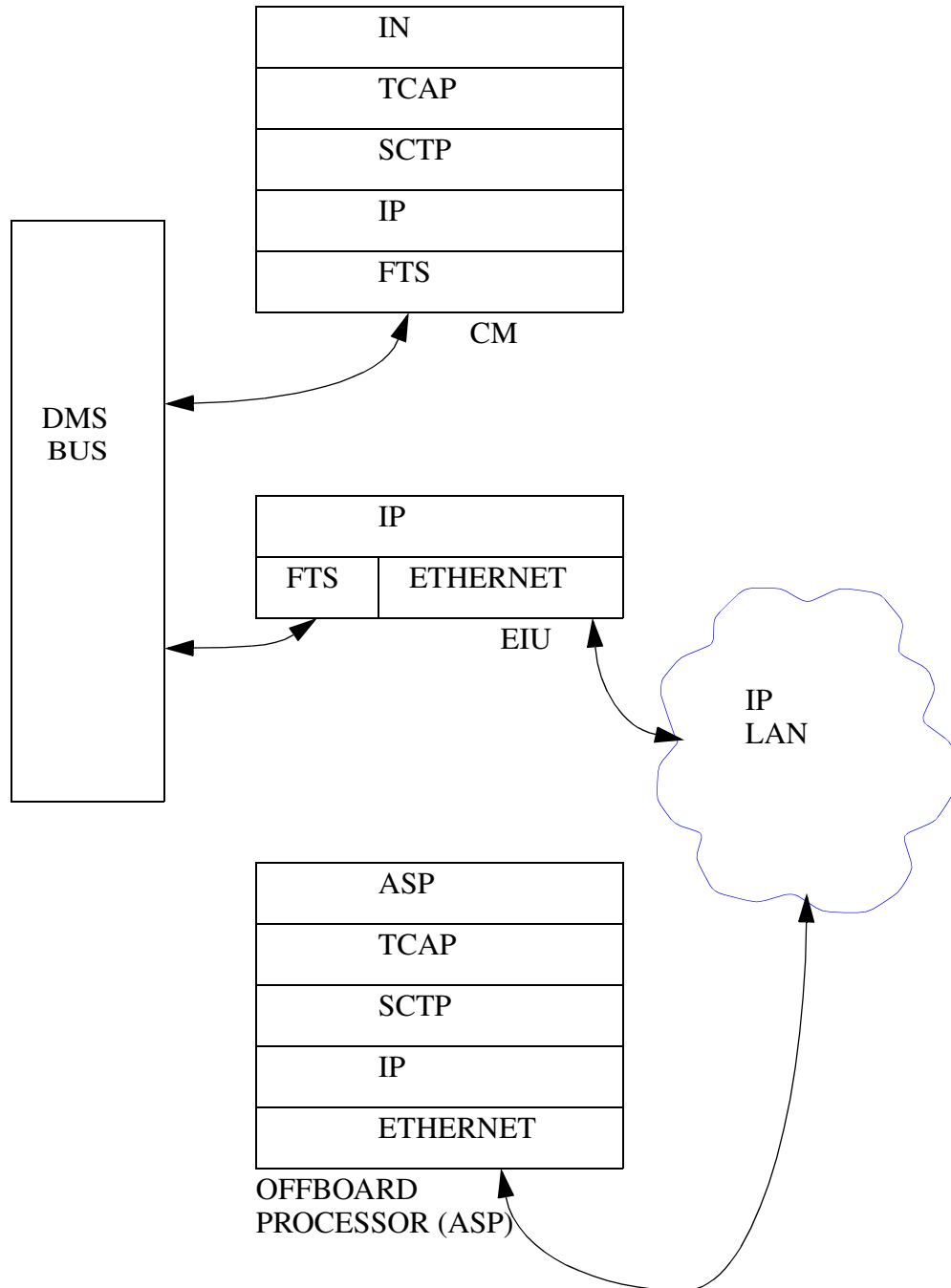
The feature activity that implemented the SCTP stack on the core provides the above SCTP advantages and a framework for developing an Application Program Interface.

System Flow

The following figure shows the message flow between the AIN Application (located in the CM) and the ASP (connected on an Ethernet LAN). An IN/TCAP message is encoded and passed to SCTP for delivery to the ASP.

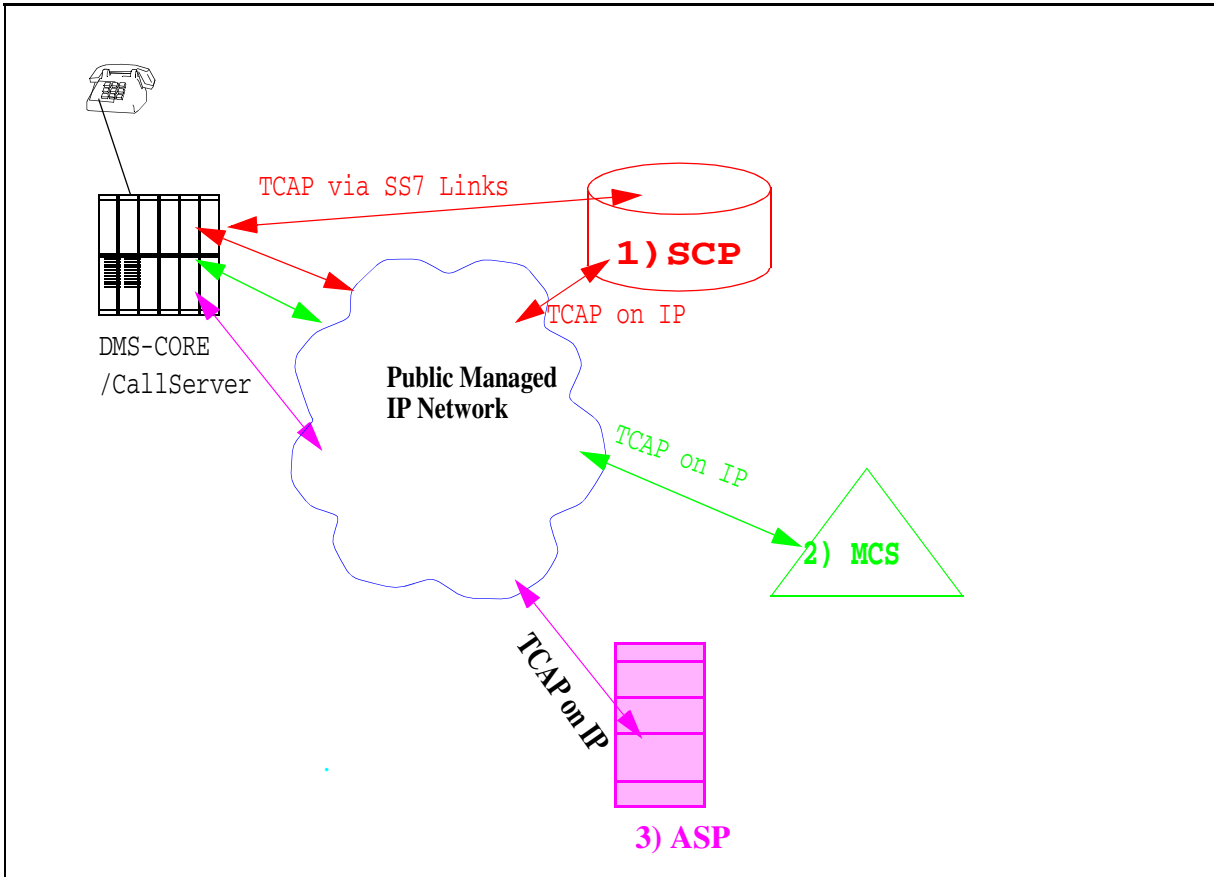
The SCTP transport hands over the TCAP Message to IP. IP forwards the Message to an Ethernet Interface Unit (EIU) through the Supernode Frame Transport System (FTS). In the EIU, the Message is received by FTS which passes it on to IP.

IP delivers the message to the Ethernet LAN which forwards it to the Appropriate Offboard Processor. On the ASP, the message is delivered to IP which passes it on SCTP transport which hands it over to the Application Service Provider. A Response Message from the ASP to the AIN Application follows the exact same path but in reverse order.

System Flow using EIU on DMS

Below is a diagrammatic representation of different nodes that could use the SCTP/IP interface.

Diagrammatic representation of Examples



Provisioning

Only the TRIGITM model of subscription supports IN messaging over IP. The TRIGGRP model of subscription is not supported by this activity. Following datafill is required to allow IN messages over IP.

Table IPAPPL**Table Control Changes****Table Trigitm Datafill**

TDP	TNAME	TRIGGER	TRIGDATA	CRITERIA	STATE	ACTION	SLHR	OPTIONS
4	ASDS3T1	SDS	(DG 408)	\$	ULK	EVENT	R02	SCTPIP 1\$
4	ASDS3L2	SDS	(DG 888)	\$	ULK	EVENT	R02	SS7 SCP1_GTT \$**
4	ASDS6T1	SDS	(DG 877)	\$	ULK	EVENT	R02	SCTPIP 2\$
4	ASDS10T1	SDS	(DG 4024574321)	\$	ULK	EVENT	R02	SCTPIP 3\$

Table IPAPPL: (new table)

InstKey	InstanceName	Transprt	IPDevice	IPAddr(s)	Port	OptList
1	SCPINST	SCTP	EIU	IPV4 47 142 160 173	\$	
	4900	(APPLICATION AIN R02)	(SETPRIM 1)	(MODE SERVER)	\$	
2	MCSINST	SCTP	EIU	IPV4 47 142 160 175	IPV4 47 142 160 176	\$
	4920	(APPLICATION AIN R02)	(SETPRIM 2)	(MODE SERVER)	\$	
3	PCMINST	SCTP	HIOP	IPV4 47 142 160 178	IPV4 47 142 160 178	
		IPV4 47 142 160 180	IPV4 47 142 160 181	\$ 4982	(APPLICATION AIN R02)	
		(SETPRIM 4)	(MODE SERVER)	\$		

** Note that SCP1_GTT points to the existing GTT for SS7 translations.

New **Table IPAPPL** datafill provides separation of various connections to the DMS. The use of SCTP transport requires that the application store the specific remote IP addresses and local Port number. Therefore table IPAPPL is datafilled in order to provide these details.

InstKey is datafilled in order to map this instance with an internally assigned instance number. This field is the unique key to the tuple. This field is used in the tuples in trigitm that uses SCTP as transport.

InstanceName is datafilled in order for the telco personnel to be able to distinguish one connection from the other.

Transprt is datafilled in order to classify the instance to which transport protocol be used. Currently the table will support SCTP functionality ONLY.

IPDevice is datafilled to indicate which IP interface hardware will be used. This table currently supports EIU and HIOP.

IP addresses (up to 4 addresses) are allowed in one instance tuple. This may be used to support multihoming. Please refer to Section “MultiHoming” on page 114. The first IP address in the list will be used as the primary address. IPV4 type IP addresses are supported.

Port Number is the local port number at which the DMS-Core will expect to receive messages from this instance. (Note that the remote port is received during the INIT message from the far-end). Valid range of Source port allowed to be configured on the CORE is from **4900 to 4982**.

The IN Messaging application using SCTP allows for multiple associations to an ASP on the same IP address, but using a different port number. Care must be taken to datafill a different portnumber in the source port field on the DMS Core. This method may be used by service providers that use the GTT or SSN in SS7 for translating to different applications.

OptList field may be datafilled with “**SETPRIME**” to set any of the IP address in an instance to be used as to set the primary destination address. The field is designed so as to support any future enhanced options. The setprime option is mandatory for AIN on SCTP.

This option has been used along with the position of the ipaddress as in above examples, (Please refer to “ Table Control Changes” on page 110.), where in the SCTPINST the ipaddress “47 142 160 173” is set as the primary IP address.

Optlist sub-field “**APPLICATION**” can be datafilled to specify the application e.g., AIN. This field is further augmented by **Msgset** e.g.: R01, R02. The application option is mandatory for AIN on SCTP.

Optlist sub-field “**mode**” is currently defaulted to the SERVER mode for AIN on SCTP. The IN TCAP messaging on IP requires the SCTP application runs in SERVER mode on the CORE.

Optlist sub-field “**multihoming**” is used to specify if the remote node supports multihoming. This option is currently only supported on the HIOP ipdevice.

Table Trigitim

In the trigitm model of AIN, the Trigitm table stores the trigger item definitions. Each trigger item also contains the Service Logic Host Route, which currently allows SS7 as transport and the datafill of a GTT per trigger item. The SLHR entry for each trigger specifies the ASP (Application Service Provider) destination (instance) to which this trigger query / messages will be sent.

When the transport mechanism is changed to SCTP, this entry needs to be changed for transport and GTT fields for each trigger item. It should be replaced with the transport as SCTP with an instance number.

Field **SLHR's** sub-field transport in table trigitm is modified to allow the following transports:

- TCP (Lab-only)

Software Requirements or Dependencies

Limit SOC INW0003 will be used with this functionality. The limit in SOC must be set to at least the number of tuples datafilled in the table IPAPPL. For more instances to be added in the table IPAPPL limit of this SOC must be increased by additional number of tuples.

Initial limit of this SOC will be zero. When limit is zero no tuples can be added to the IPAPPL table. Tuples can be added only when a non-zero limit is set. Maximum limit that can be set will be 32.

Adding, deleting and modifying do not impact the value of the SOC limit. The value of the current usage counter is however changed accordingly

If SOC limit is reduced after adding tuples, IN messaging on IP functionality will not be affected, but no further tuples will be allowed to be added to the table IPAPPL.

If the SOC limit set is less than or equal to the current number of tuples in table IPAPPL, no further tuples will be allowed to be added to the table IPAPPL. An attempt to add a tuple will result in the following message being displayed:

“SOC option INW0003: Usage limit exceeded”

“ERROR: Table IPAPPL is under SOC usage control.”

“ACTION: SOC Limit must be increased before adding further tuples.”

Limitations and restrictions

For Engineering Information on the

- bandwidth,
- Message Size,
- SCTP/IP Link Messaging Rate,
- Normal Throughput,
- Failure ThroughPut,
- Link Capacity as Call Attempts Per Hour, Messages Per Second and others,

Please refer to the EI section of this Document.

For EIU and HIOP being shared between various IP applications, For EIU configurations across subnets, etc. please refer to specific hardware guidelines as well as the EI documentation referring to the bandwidth allotted to application sharing the hardware.

MultiHoming

Multihoming is not supported for IN Messaging using the SCTP on EIU configuration. Multihoming is supported by SCTP on the HIOP configuration.

Simultaneous HIOP and EIU

Please refer to appropriate hardware procedures when operating with HIOP card as well as EIU peripheral on the CORE.

Sample EIU Configurations

Please refer to NTP 297-8991-910, DMS-100 Family Ethernet Interface Unit User Guide TELECOM12 Standard 03.01 August 1999, EIU documentation (LANCOMM) for recommended EIU configurations.

Interactions

Tools such as AINTRACE and TRAVER will be supported to be able to refer to SCTP instances for the transactions using this transport.

Applicable customer facing sections

Fault Management

Logs ☒

Alarms ☐

Configuration

Data Schema ☒

User Interface ☒

Element Management ☐

Security ☐

Service Order ☐

Office Parameters ☐

Accounting (includes AMA billing) ☐

Performance (includes operational measurements) ☒

Glossary

Term	Description
ASP	Application Service Provider
CS2K	Call Server 2000

Term	Description
SCP	Service Control Point
SCTP	Stream Control Transmission Protocol
TCP	Transmission Control Protocol
PSTN	Public Service Telephone Network
AIN	Advanced Intelligent Network
IP	Internet Protocol
IN	Intelligent Networks
CCS7	Common Channel Signalling 7
TCAP	Transaction Capabilities Application Part
SCCP	Service Connection Control Part
HIOP	High Performance I/O Peripheral
MCS	Multimedia Call Server
EIU	Ethernet Interface Unit
FTS	Frame Transport System

Configuration for A00004500

Hardware and Software Requirements

NONE

Initial Configuration

NONE

Office/Subnet parameters (OP/SP) (CM & SESM)

NONE

Upgrade Impact

NONE

Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

New table IPAPPL will be created to store data on each SCTP instance.

New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
IPAPPL	NEW	NEW
TRIGITM	Changed	NEW
TRIGINFO	Changed	NEW

Table/MIB/Remote Database Schema information

Name: IPAPPL - Internet Protocol Application

Functional description

Table IPAPPL defines the IP Application instance that data will be transmitted over for a given service. This table is being created for the AIN on SCTP/IP project but it is being designed so that it could be used by other applications (i.e., ACB/AR, NMS) that may want to use IP as a transport in the future. The table will contain the connection information for controlling the communications processes associated with the transport.

Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

IPAPPL

TRIGITM

OR

TRIGINFO

Tables TRIGITM and TRIGINFO use the INST (sctp instance) that is datafilled in table IPAPPL.

Size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
IPAPPL	0	64	Memory is automatically allocated for 64 Intelligent Network SCTP instances.

Fields/OIDs

The following table lists fields/OIDs for Table IPAPPL.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
INSTKEY	NEW	subfield	0-64	Defines the SCTP instance number.
INSTNAME	NEW	subfield	8 character vector	Defines the SCTP instance name.
TRANSPRT	NEW	subfield	SCTP	Defines the transport to be used by the application.
IPDEVICE	NEW	subfield	EIU/HIOP	Specifies the device that the instance will use.
IPADDRS	NEW	subfield	Vector of up to 4 IPV4 IP addresses	Specifies the remote IP addresses to be used for the instance.
IPPORT	NEW	subfield	UNSIGNED INT	Specifies the IP port to be used.
OPTLIST	NEW	subfield	VECTOR of IP_OPTION_LIST	Specifies optional data associated with the instance.
Application	NEW	refinement of optlist	Service {AIN}	Defines the service that is using the instance.
Multihoming	NEW	refinement of optlist		Specifies if the instance supports multihoming.
Mode	NEW	refinement of optlist	Client, Server	Specifies if the instance is a client or server.
Setprime	NEW	refinement of optlist	1 to 4	Specifies which of the IP address in the IPADDRS field is the primary.

Datafill example

The following example shows sample datafill for table IPAPPL

TABLE IPAPPL

INSTKEY INSTNAME TRANSPRT IPDEVICE IPADDRS IPORT
OPTLIST

0 SS SCTP EIU (IPV4 47 142 160 173) \$ 4977 (APPLICATION AIN R02)
(SETPRIME 1) (MODE SERVER) \$

Fields/OIDs

The following table lists fields/OIDs for Table TRIGITM/TRIGINFO.

Table field descriptions TRIGITM/TRIGINFO

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
AIN_TRANSPORT	Changed	refinement	SCTP INST {0 to 64}	Adding SCTP as a valid AIN transport.

Datafill example

The following example shows sample datafill for table TRIGITM and TRIGINFO.

TABLE TRIGITM

TDP TINAME TRIGGER TRIGDATA CRITERIA STATE ACTION SLHR
OPTIONS

20 SSTAT TERMATT \$ ULK EVENT R02 SCTPIP 0 \$

TABLE TRIGINFO

KEY ACTION OPTIONS

AININFO EVENT TCAP R02 SCTPIP 0 \$

Table release history update

NONE

Supplementary information

NONE

Translation verification other tools

The following example shows the output from TRAVER when it is used to verify TRIGITM.

```
>traver l 7502511 95505555 b
```

```
TABLE IBNLINES
```

```
HOST 00 0 00 22 0 DT STN IBN 7502511 CGA 0 0 909 (CDC) (CNDB) $
```

```
TABLE DNATTRS
```

```
909 750 2511
```

```
    (PUBLIC (NAME ASTN1CGA0) $)
```

```
    (PRIVATE (NAME PASTN1CGA0) $)$ $
```

```
TABLE DNGRPS
```

```
909 750 2511 2511
```

```
    (PUBLIC (NAME CGA) $)
```

```
    (PRIVATE (NAME PCGA) $)$
```

```
TABLE IBNFEAT
```

```
TUPLE NOT FOUND
```

```
TABLE CUSTSTN
```

```
TUPLE NOT FOUND
```

```
TABLE OFCVAR
```

```
AIN_OFFICE_TRIGGRP TIID
```

```
AIN Orig Attempt TDP: no subscribed trigger.
```

```
TABLE NCOS
```

```
CGA 0 0 0 CGA0 (IDDDARS N)$
```


TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA,
VACTRMT, AND DIGCOL

CGA CGAXLA CGXXLA STARXLA 1 CGXCOL

TABLE DIGCOL

CGXCOL 9 POTS Y

TABLE IBNXLA: XLANAME CGAXLA

CGAXLA 9 NET Y Y 1 Y POTS N N GEN (LATTR 42 909_EAEO_42
L909_LATA1_42) (EA C541 Y 0)\$ \$

TABLE DIGCOL

POTS specified: POTS digit collection

TABLE LINEATTR

42 1FR NONE NT 0 0 NILSFC 0 NIL NIL 00 909_EAEO_42
L909_LATA1_42 \$

LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE

TABLE XLAPLAN

909_EAEO_42 NSCR 909 EAEO RTE4 Y RGA 0 0 \$ \$

TABLE RATEAREA

L909_LATA1_42 L909 NIL LATA1 \$

TABLE STDPRTCT

EAEO (1) (1) 6

. SUBTABLE STDPRT

WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE

BILLING. CALL TYPE DEFAULT IS NP. PLEASE REFER TO

DOCUMENTATION.

. 550 5551211 N NP 0 NA

. SUBTABLE AMAPRT

. KEY NOT FOUND

. DEFAULT VALUE IS: NONE OVRNONE N

TABLE HPCPATTN

TUPLE NOT FOUND

TABLE HNPACONT

909 Y 949 8 (133) (1) (0) (0) 2 \$

. SUBTABLE HNPACODE

. 550 550 DN 909 550

TABLE TOFCNAME

909 550 \$

TABLE DNINV

909 550 5555 D BLDN

TABLE DNFEAT

TUPLE NOT FOUND

TABLE DNATTRS

TUPLE NOT FOUND

TABLE DNGRPS

TUPLE NOT FOUND

TABLE TMTCNTL

LNT (148)

. SUBTABLE TREAT

. BLDN Y S T120

LNP Info: Called DN is not resident.

LNP Info: HNPACONT results are used.

TABLE LCASCRCN

909 L909 (10) OPTL N N Y

. SUBTABLE LCASCR

. 550 551

TABLE PFXTREAT

OPTL NP Y NP UNDT

AIN Info Collected TDP: no subscribed trigger.

Checking AIN SDS Trigger Items as SDS is compatible with current call

. . TABLE OFCTIID

. . 4 SSSDS ON

. . TABLE TRIGITM

. . 4 SSSDS SDS (DG 9095505555) \$ ULK EVENT R02 SCTPIP 0 \$

AIN Info Analyzed TDP: trigger criteria met.

Querying the database would occur now.

Use the AINMQG option to save the query to a file for use in TstQuery.

Use the AINRES option for further information

+++ AIN TRAVER: SUCCESSFUL CALL TRACE +++

AIN Info Analyzed TDP: trigger criteria met.

Querying the database would occur now.

Use the AINMQG option to save the query to a file for use in TstQuery.

Use the AINRES option for further information

+++ AIN TRAVER: SUCCESSFUL CALL TRACE +++

Service Orders (SO) (CM & SESM)

Not impacted.

Software optionality control (SOC)

A new usage/limit SOC INW00003 will be created by this activity to control the allocation of IN SCTP links in table IPAPPL. If the limit has not been met then the user will be allowed to add entries to table IPAPPL.

SOC

SOC option name:	IN Messages Over IP
SOC option title:	Yes
SOC option control type:	usage
New SOC option?	Yes
SOC option order code	INW00003
Option defined in DRU:	SHR
Affected products:	All

Element Management

Not Impacted.

Command interface changes

Command: TSTQUERY

The AIN TSTQUERY command will be changed to support SCTPIP as a valid transport.

Command type: Listed MENU

The setrnsp MENU command will be modified to allow for SCTPIP prompting.

Command target: All

Command availability: RES

Command description

The setrnsp command is used to specify which AIN transport the TSTQUERY message should be sent over.

Command syntax

Help setrnsp

Command to set the Transport

Parms: <Transport> {SS7 <GttName> STRING

<GttSource> {DEFAULT,

CHARGE,

CALLED},

TCPIP <Application Instance Number> {0 TO 3},

SCTPIP <Application Instance Number> {0 TO 64}

Qualifications and warnings

NONE

Responses

NONE

Example

Setrnsp sctpip 0

Security

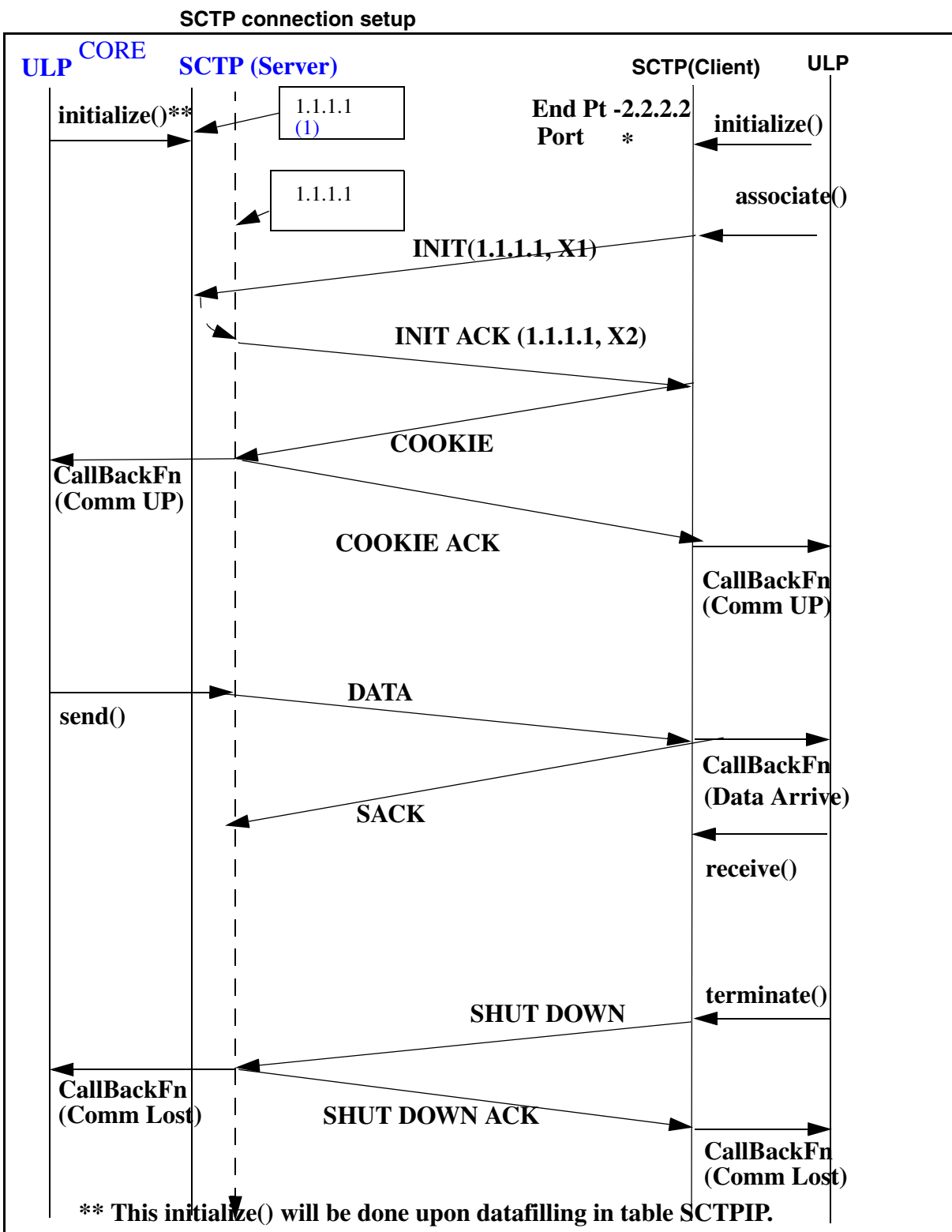
NONE

Configuration Walkthrough

NONE

Appendix A

Sample SCTP instance setup



Performance Management for A00004500

Performance management strategy

Not Applicable

Performance management tools and utilities

Not Applicable

Performance Measurements (PM), Operational Measurements (OM), and stats

This activity adds new OM registers in a new OM group. The new OM group is INSCTP OM for AIN transports. The following sections will outline in detail what OMs will be pegged.

New OM registers

MSGOUT - Pegs Outgoing IN messages using SCTP

MSGIN - Pegs Incoming IN messages using SCTP

SENDFAIL - Pegs IN messages using SCTP for which send failed

DATAERR - Pegs IN messages which encountered errors at application data

DATARCVD - Pegs for Incoming IN message decoding

MSG2BIG- Pegs IN Messages which failed due to message length

BMSFAIL - Pegs instances when buffer errors encountered while sending IN messages over SCTP

NOTREADY - Pegs when SCTP layer indicates that it is not ready to process the message. Please note that this register even though displayed part of the OM group INSCTP, is NOT used by this activity.

INSCTP Group Display

>omshow INSCTP active

INSCTP

CLASS: ACTIVE
START:2004/01/12 08:30:00 MON; STOP: 2004/01/12 09:55:39 MON;
SLOWSAMPLES: 5 ; FASTSAMPLES: 48 ;

MSGOUT MSGIN SENDFAIL DATAERR
MSG2BIG BMSFAIL DATARCVD NOTREADY

0				
	0	0	0	0
	0	0	0	0

MSGOUT

Register MSGOUT (IN SCTP MSG Out) will be pegged for every outgoing AIN message using the SCTP transport.

MSGIN

Register MSGIN (IN SCTP MSG In) will be pegged for every incoming AIN message using the SCTP transport.

SENDFAIL

Register SENDFAIL (IN SCTP SeND FAilure) will be pegged for every outgoing AIN message using the SCTP transport that failed.

DATAERR

Register DATAERR (IN SCTP Data ERRor) will be pegged for every Data Error that occurs which causes a messaging failure.

MSG2BIG

Register MSG2BIG (IN SCTP message too BIG) will be pegged for every outgoing message that failed to be send because of the message size being too BIG. (i.e beyond the maximum size) Please refer to the EI section for maximum message size allowed.

BMSFAIL

Register INSCTBMS (IN SCTP BMS buffer failure) will be pegged if any buffer failure results in send or recieve failure.

DATARCVD

Register DATARCVD will be pegged when the IN msg is received from SCTP stack and we are ready to decode the IN message.

NOTREADY

Register NOTREADY is used to indicate that the SCTP layer is not ready to send or receive a message. This Register is presently not used with the current functionality (but will be displayed on OMSHOW as one of the registers in the group).

Associated OM groups

Not Applicable

Associated logs

TBD

OM Group template (applies only to DMS)

Not Applicable

Register (applies only to DMS)

Not Applicable

Product = Carrier Hosted Services

A00006495 -- H.323 Flexible Carriers (MMBS)

Excerpts from the Design Description

Purpose

This SN07 activity enables the addition of H.323 virtual carriers with a size within the range of 4 to 672. The current implementation allocates H.323 virtual carriers in blocks of 24 or 32, based on the market. The new capability will only affect carriers that are defined as the type H.323.

The H.323 Flexible Carrier feature enables customers to allocate small and large groups of endpoints for H.323 gateways. By allowing variable size blocks of endpoints/TIDs (Terminal Identifiers), customers can manage the TID range of a H.323 GWC (Gateway Controller) more efficiently.

The new capability is targeted to customers who don't have OSS (Operations Support System) requirements to provision blocks of endpoints in (24 or 32) increments and support small H.323 systems.

Note: If a craftperson adds a H.323 virtual carrier and does not specify a size, the default number of endpoints/TIDs will be allocated (24 North American/32 International).

H.323 Capacities

The maximum number of gateways that will be supported on a H.323 GWC in SN07 is 254. The PRI data structures on the GWC currently support 168 D channels. Thus, the current maximum number of H.323 gateways is 168. This feature changes the PRI data structures on the GWC to support 254 D channels.

A craftperson can allocate (provision via SESM) 258 H.323 gateways (in the North American market) and virtual carriers with a minimum size of 4. A SN07 H.323 GWC in the North American market can be provisioned with 1032 endpoints/TIDs. A SN07 H.323 GWC in the International market can be provisioned with 1024 endpoints/TIDs. **Regardless of the number of gateways provisioned on a GWC, only 254 D channels can be defined on a H.323 GWC after this feature is delivered.** D channel provisioning is executed on the core. If an attempt is made to provision a 255th D channel on a H.323 GWC, an error is generated stating that the maximum number of D channels has been exceeded.

The smallest H.323 virtual carrier that can be allocated is 4 endpoints/TIDs. The largest H.323 virtual carrier that can be allocated is 672 endpoints/TIDs. The maximum size of a H.323 virtual carrier was based on the number of B channels that can be mapped to a PRI trunk group on the core in table TRKMEM (671 B channels maximum for a PRI trunk group). A H.323 virtual carrier can be any size within the range of 4 - 672.

H.323 GWC capacities

H.323 GWC Profile	Endpoint Capacity (maximum number of endpoints/TIDs per GWC)	Gateway Capacity (maximum number of gateways per GWC)
H.323_INTL	1024	1024/4 = 256
H.323_NA	1032	1032/4 = 258

H.323 Gateway Profile Changes

This feature delivers changes to the H.323 gateway profiles:

H.323 gateway maximum reserved terminations

H.323 Gateway Profile	SN06.2 Maximum Terminations	SN07 Maximum Terminations
NORTEL_BCM	64	consult the vendor documentation

H.323 gateway maximum reserved terminations

H.323 Gateway Profile	SN06.2 Maximum Terminations	SN07 Maximum Terminations
SUCCESSION_1000	480	consult the vendor documentation
CISCO_2600	96	consult the vendor documentation
CISCO_3600	384	consult the vendor documentation
CISCO_AS5300	384	consult the vendor documentation
WESTELL	64	consult the vendor documentation
CISCO_H323_IOS	N/A	consult the vendor documentation
H323_PROXY	N/A	consult the vendor documentation

Limitations and restrictions

The limitations of this activity include the following:

- The maximum number of gateways that will be supported on a H.323 GWC in SN07 is 254. A craftperson can allocate 258 H.323 gateways and virtual carriers with a minimum size of 4 but only 254 D channels can be defined on a H.323 GWC after this feature is delivered.
- The smallest H.323 virtual carrier that can be allocated is 4 endpoints/TIDs. The largest H.323 virtual carrier that can be allocated is 672 endpoints/TIDs.
- If H.323 virtual carriers are attempted to be provisioned on a pre-SN07 GWC load, an error is generated detailing that this functionality is not supported in previous releases.

Product = Carrier Hosted Services**A00006496 -- H.323 Multiple D Channels (MMBS)*****Excerpts from the Design Description***

Purpose

This SN07 activity will enable the support of mapping multiple D channels to a single H.323 gateway. The current H.323 implementation on the GWC makes the assumption that there is only *one* D channel mapped to a single H.323 gateway. The new capability will only affect H.323 gateways.

The multiple D channel feature provides the support to map more than one trunk group on the core to the allocated TIDs on the GWC. The current maximum number of endpoints supported on a single H.323 gateway by the CS2K is 672.

The new capability enables support of large H.323 systems such as the Succession 1000 H.323 gateway. Once this feature is delivered, a single H.323 gateway can be mapped to the full capacity of a SN07 H.323 GWC (1024 for International/1032 for North American).

H.323 Capacities

The maximum number of gateways that will be supported on a H.323 GWC in SN07 is 254. The PRI data structures on the GWC currently support 168 D channels. Thus, the current maximum number of H.323 gateways is 168. This feature changes the PRI data structures on the GWC to support 254 D channels.

A craftperson can allocate (provision via SESM) 258 H.323 gateways (in the North American market) and virtual carriers with a minimum size of 4. A SN07 H.323 GWC in the North American market can be provisioned with 1032 endpoints/TIDs. A SN07 H.323 GWC in the International market can be provisioned with 1024 endpoints/TIDs. *Regardless of the number of gateways provisioned on a GWC, only 254 D channels can be defined on a H.323 GWC after this feature is delivered. Thus the maximum number of H.323 gateways that can provide call processing is 254.* D channel provisioning is executed on the core. If an attempt is made to provision a 255th D channel on a H.323 GWC, an error is generated stating that the maximum number of D channels has been exceeded.

The smallest H.323 virtual carrier that can be allocated is 4 endpoints/TIDs. The largest H.323 virtual carrier that can be allocated is 672 endpoints/TIDs. The maximum size of a H.323 virtual carrier was based on the number of B channels that can be mapped to a PRI trunk group on the core in table TRKMEM (671 B channels maximum for a PRI trunk group). A H.323 virtual carrier can be any size within the range of 4 - 672.

H.323 GWC capacities

H.323 GWC Profile	Endpoint Capacity (maximum number of end-points/TIDs per GWC)	Gateway Capacity (maximum number of gateways per GWC)
H.323_INTL	1024	1024/4 = 256
H.323_NA	1032	1032/4 = 258

H.323 Gateway Profiles**H.323 gateway maximum reserved terminations**

H.323 Gateway Profile	SN06.2 Maximum Terminations	SN07 Maximum Terminations
NORTEL_BCM	64	consult the vendor documentation
SUCCESSION_1000	480	consult the vendor documentation
CISCO_2600	96	consult the vendor documentation
CISCO_3600	384	consult the vendor documentation
CISCO_AS5300	384	consult the vendor documentation
WESTELL	64	consult the vendor documentation
CISCO_H323_IOS	N/A	consult the vendor documentation
H323_PROXY	N/A	consult the vendor documentation

H.323. Maintenance Model

The H.323 maintenance model will be changed by this feature. A H.323 D channel will come into service once a H.323 gateway successfully registers with a H.323 GWC. If a H.323 gateway has multiple D channels, all the D channels will be brought into service once a H.323 gateway successfully

registers. If at least one D channel comes into service the registration process will be successful.

A craftperson must take all the D channels out of service to successfully “de-register” the H.323 gateway. If at least one D channel remains in service the gateway will not be “de-registered”.

Trunk Group Configuration

To support the mapping of multiple D channels or trunk groups to a single H.323 the configuration of the trunk groups must be identical. The translations, customer group, services, etc. must be provisioned on the core to be the same so there isn't any difference in services or terminations. Services and call routing via one trunk group or a different one mapped to the same H.323 gateway must be transparent to a user.

A H.323 gateway and the associated trunk group(s) must be mapped to only one GWC. A H.323 gateway can't be associated with two GWCs.

GWC Changes

The GWC software must be updated to support the Multiple D Channel feature. The changes focus on changing the D channel TID selection algorithm within the H.323 GWC application and the H.323 maintenance code on the GWC.

- Update the H.323 GWC maintenance application. The current H.323 GWC maintenance implementation assumes that there is only **one** D channel per H.323 gateway. The assigned TID range of the H.323 gateway must be traversed to capture all the mapped D channels.

The support of mapping multiple D channels to a single H.323 gateway changes the maintenance model. The changes include:

- Only **one** D channel is required to come into service for a H.323 gateway to successfully register.
- A H.323 gateway will be “unregistered” if **all** D channels are manually taken out of service. If a craftperson successfully executes the maintenance commands “BSY; BSY INB;” for all of the mapped D channels, the gateway will be unregistered. If any of mapped D channels do not reach an “INB” state, the gateway will not be unregistered.

Limitations and restrictions

The limitations of this activity include the following:

- The maximum number of gateways that will be supported on a H.323 GWC in SN07 is 254. A craftperson can allocate 258 H.323 gateways and virtual carriers with a minimum size of 4 but only 254 D channels can be defined on a H.323 GWC after this feature is delivered.
- A craftperson must post **all** the D channels when manually “unregistering” H.323 gateways with multiple D channels.
- Multiple commands must be executed to manually “unregister” a H.323 gateway with multiple D channels. A utility does not exist to BSY INB all D channels mapped to a single H.323 gateway.
- A craftperson must “keep track” or capture all the mapped D channels of a H.323 gateway to manually “unregister” the respective gateway. A craftperson can capture the D channel mappings by traversing table TRKSGRP on the core to determine the D channel(s) of a H.323 gateway. The TMM (Trunk Maintenance Manager) application can be used to provide the D channel mappings of a H.323 gateway and to “unregister” the gateway by executing the proper maintenance commands. The D channels are not explicitly listed when querying the endpoint data via TMM but the information is listed.

Product = Carrier Hosted Services

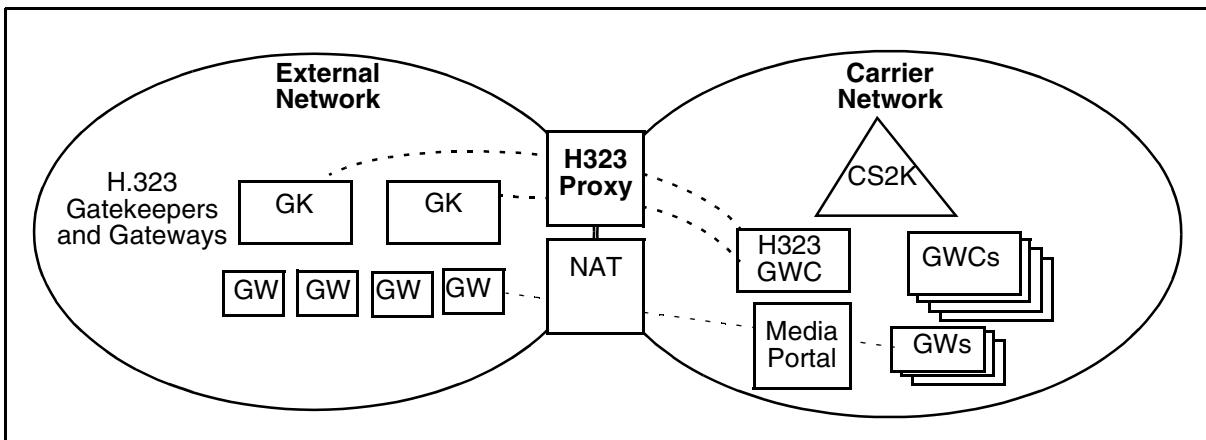
A00006741 -- H.323 Gatekeeper to CS2K Gatekeeper Interoperability (MMBS)

Description

This feature enables H.323 Gatekeepers in an external network (private, enterprise, other carriers, etc.) to interoperate with a CS2K H.323 Gatekeeper on a carrier network.

The solution uses an Acme Packet Session Director (SD) as an H323 Proxy which registers with H323 Gatekeepers on the external network and registers with the CS2K H.323 Gatekeeper on the Carrier Network. Maintenance and call processing messaging and events are proxied through the H323 Proxy.

Feature Overview



NOTE: Much of the configuration described herein reflects the current approach as described by Acme Packet. At the time of this writing, the software image from Acme Packet which supports this configuration has not been released. As such, the configuration described in here may change when the software is released, tested, and debugged.

Hardware Requirements or Dependencies

- H323 Proxy - Acme Packet Session Director (SD)
- NAT Router (for media between external network and Carrier Network or DMZ)
- Media Portal
- Succession Call Server

Summary of Customer Impacting Changes

In general, the Acme Session Director (SD), acting as an H.323 Proxy, will register Gateway instances with the CS2K that represent Gatekeepers on the external network. This is the basic mechanism for supporting H.323 Gatekeeper to CS2K Gatekeeper Interoperability (GK-GK Interop).

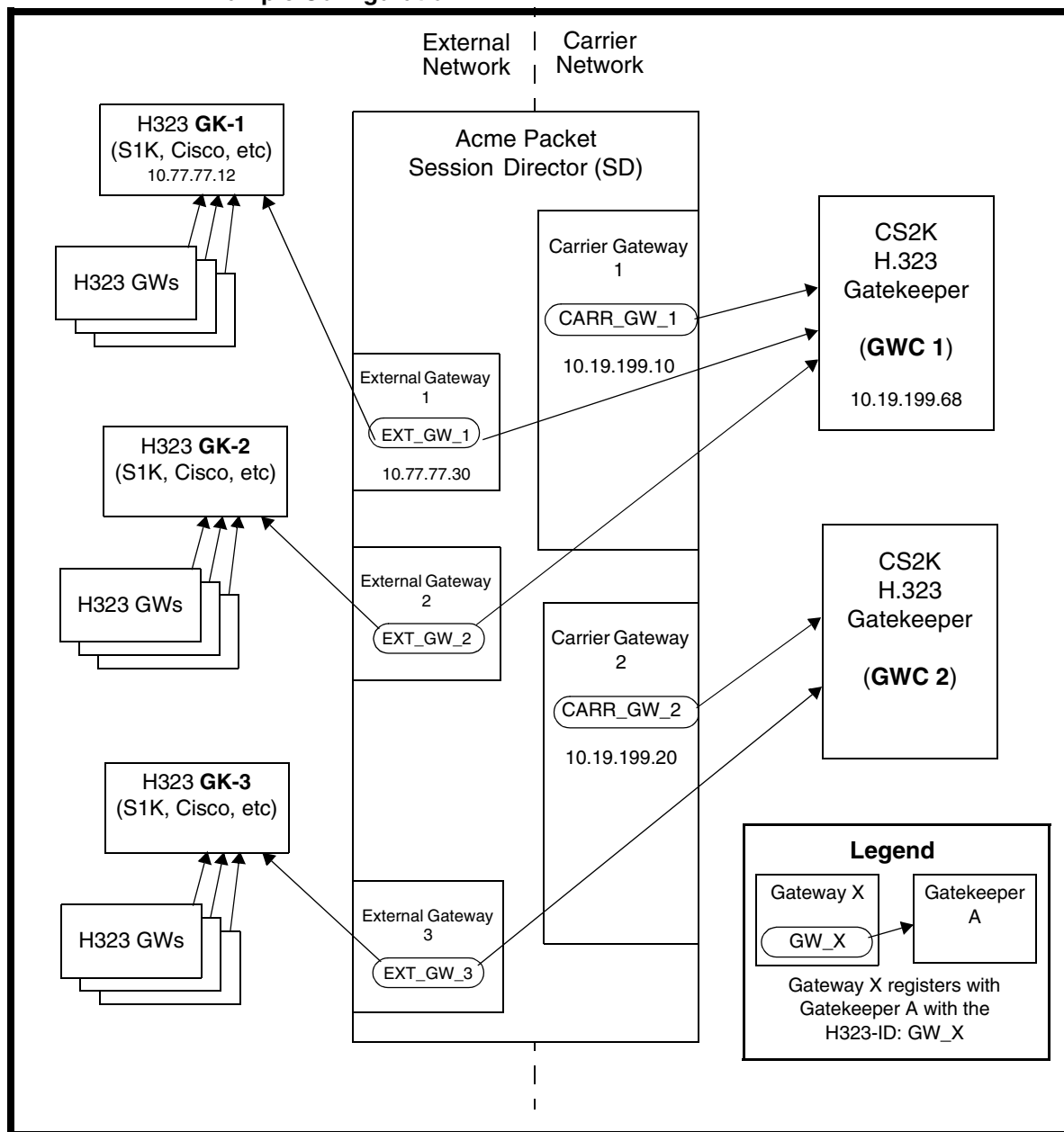
This solution involves a new configuration in which a single device (the Acme SD) registers multiple Gateways on both the carrier and external networks. Although the concept of multiple gateways residing on, and registering from, a single box is new to CS2K H.323, the only actual provisioning interface change is the introduction of a new Gateway Profile, `H323_PROXY`. This profile is used to provision Acme SD Gateways in SESM.

The Configuration section following discusses the GK-GK Interop configuration, and how to provision it, in detail. The new profile is discussed in this section as well.

Configuration

This section walks through the GK-GK Interop configuration through the use of the example configuration shown in the following figure.

Example Configuration



Configuration Overview

This example shows how one might configure interoperability between three Gatekeepers (GK-1, GK-2, and GK-3) on an *external network* (or networks)

and a CS2K on the *carrier network*. The gatekeepers may be on the same external network, or on different external networks.

In this example, there are a total of five Gateways residing on a single Acme SD. Gateways are configured as “stacks” in the Acme SD, so five stacks will be configured in the Acme Packet SD.

Carrier Gateways 1 and 2 (CARR_GW_1, CARR_GW_2) will register with the GWCs in order to provide a interface for the three external gateways (EXT_GW_1, EXT_GW_2, and EXT_GW_3) to send H.323 maintenance and call signalling messaging to and from the GWCs. These carrier gateways are necessary on the Acme SD in order to support this configuration, however they will not originate or terminate any calls. As such, they should be provisioned with one D-channel, no B-channels.

Each of the three external Gateways on the Acme SD (EXT_GW_1, EXT_GW_2, and EXT_GW_3) will register both with an external gatekeeper, and a GWC. Each of these three gateways represents, to the CS2K, one of the external gatekeepers. For example, EXT_GW_1, registered with both GK-1 and GWC-1, will proxy all calls from gateways registered with GK-1 and the CS2K. Any number and type of H.323 gateways may be registered with GK-1, however this is transparent to the CS2K. Any call originating from an H.323 Gateway registered with GK-1 that routes to the CS2K will appear to the GWC as if it is originating from an endpoint on EXT_GW_1 on the SD. The fact that the call actually originates on the external network from another H.323 gateway is transparent to the CS2K.

We can assume in this example that the engineering decision to register two of the external gateways (EXT_GW_1 and EXT_GW_2) with GWC 1 and the third external gateway (EXT_GW_3) with GWC 2 was made based on the maximum number of endpoints required for the external Gatekeepers (GK-1, GK-2, GK-3). Note that the maximum endpoints on a GWC is 1024 (North American) or 1032 (International).

Configuration Sequence

The general sequence of events for configuring the example shown is:

1. Carrier Gateway 1 and Carrier Gateway 2 are configured in SESM, SD, and core (no trunk members necessary, only a d-channel).
2. Carrier Gateway 1 and Carrier Gateway 2 successfully register with GWC 1 and GWC 2, respectively.
3. External Gateways 1, 2, and 3 are configured in SESM, SD, and core, with sufficient resources (reserved terminations in SESM, B-channels/trunk members in the core) provisioned to support the maximum number of calls each will support between the GWC and the external GK.
4. External Gateways 1, 2, and 3 are configured in the SD

5. If necessary, External Gateways 1, 2, and 3 are configured in the external Gatekeepers (GK-1, GK-2, and GK-3). This step is dependent on the type of external gatekeeper, and the desired configuration. For example, a Cisco Gatekeeper can be configured to allow registrations from any Gateway - no gateway configuration necessary in the Cisco GK. However, an S1000 requires that all registering gateways be explicitly provisioned in the S1000 Gatekeeper. Gateways that are not provisioned in the S1000 will not be permitted to register.
6. External Gateways 1, 2, and 3 successfully register with GK-1, GK-2, and GK-3, respectively.
7. Upon successfully registering with the external Gatekeepers, each External Gateway will then register with a GWC. The external gateway - GWC association is configured in the SD.

Configuring Acme SD *Carrier* Gateways

Carrier Gateways 1 and 2 (CARR_GW_1 and CARR_GW_2) will register with GWC 1 and GWC 2, respectively, on the CS2K. These gateways (stacks) can be considered “proxy gateways.” They will not originate or terminate calls, and as such do not require any endpoints or b-channels be provisioned against it in SESM or core datafill. They must be provisioned in SESM and each requires a single D-channel.

These gateways (stacks) are required by Acme to provide an interface through which the gateways (stacks) on the external side of the SD (External Gateways 1, 2 and 3 in this example) can proxy H.323 messages to and from the GWCs.

Carrier Gateway SESM Provisioning

The following figure shows example SESM provisioning for Carrier Gateway 1. The gateway will be associated against GWC 1. Carrier Gateway 2 would be similarly provisioned against GWC 2.

Example SESM Provisioning - Carrier Gateway 1

Associate Media Gateway

Gateway name: CARR_GW_1

Gateway IP address: 10.19.199.10

Gateway controller name: GWC-6

Gateway profile name: H323_PROXY

Reserved terminations: 4

Internet Transparency

☒ MG outside CS2K VPN, not behind NAT

IP-VPN / LBL Selection

☐ IP-VPNs ☐ LBLs

Adj ITRANS MiddleBox

Signal Protocol

Protocol type: H.323 (6)

Protocol port: 0

Protocol version: 4.0

OK Cancel

Fields that are significant to GK-GK interoperability include:

- **Gateway Profile name: H323_PROXY**
This **new profile** should be used for all Acme Packet SD Gateways (stacks).
- **Reserved terminations: 4**
This gateway (stack) should be provisioned with the minimum reserved terminations (4).
- **MG outside CS2K VPN, not behind NAT**
It is not necessary to associate a NAT for this gateway (stack)
- **Protocol port: 0**
H323_PROXY gateways should always be provisioned with a signalling protocol port of 0.

After the gateway is associated, a carrier must be added for this gateway in SESM. Provision the carrier just like any other H323 gateway - there are no carrier group changes specific to GK-GK interoperability.

Example SESM Provisioning - Add Carrier for Carrier Gateway 1

Fields that are significant to GK-GK interoperability:

- **Reserved terminations: 1**

Only one port is required for this gateway (the d-channel).

Carrier Gateway Session Director Configuration

Example configuration for Carrier Gateway 1 on the Acme SD is shown below:

```
h323-stack
  name CARR_GW_1
  state enabled
  isgateway enabled
  realm-id carrier_ntwk
  assoc-stack
  local-ip 10.19.199.10
  max-calls 1
  max-channels 2
  registration-ttl 50
  terminal-alias
  h323-ID=CARR_GW_1
  prefixes
  ras-port 1719
  auto-gk-discovery disabled
  multicast 0.0.0.0:0
  gatekeeper 10.19.199.68:1719
  gk-identifier
  q931-port 1720
  alternate-transport
  q931-max-calls 1000
  h245-tunneling enabled
  fs-in-first-msg disabled
  call-start-fast disabled
  call-start-slow disabled
  media-profiles
```

process-registration	disabled
options	maintenanceProxy
anonymous-connection	enabled
proxy-mode	H245
filename	
last-modified-date	2004-05-06 09:38:59

The **maintenanceProxy** option is important specifically to Carrier Gateway 1 and Carrier Gateway 2 because they tell the SD that these are the gateways that will be used to proxy H.323 maintenance and call processing messaging to the GWCs.

The **assoc-stack** (associated stack) field should be left blank for this gateway.

Carrier Gateway Core Provisioning

An H323 trunk group should be added to core datafill that maps to the gateway provisioned in SESM in section “Carrier Gateway SESM Provisioning” on page 138. There are no core datafill changes specific to this feature - the trunk should be datafilled just like any H323 trunk group. It is not necessary to provision any b-channels for Carrier Gateway 1 or Carrier Gateway 2.

Configuring Acme SD *External* Gateways

External Gateways 1, 2, and 3 (EXT_GW_1, EXT_GW_2, and EXT_GW_2) will register with GK-1, GK-2, and GK-3, respectively, on the external network(s), as well as with GWC-1 and GWC-2 on the carrier network. These gateways will proxy H.323 calls through the SD.

External Gateway SESM Provisioning

The following figure shows example SESM provisioning for External Gateway 1. The gateway will be associated against GWC 1. External Gateway 2 would also be provisioned against GWC 1, and External Gateway 3 would be provisioned against GWC 2.

Example SESM Provisioning - External Gateway 1

Associate Media Gateway

Gateway name:

Gateway IP address:

Gateway controller name:

Gateway profile name:

Reserved terminations:

Internet Transparency

☐ MG outside CS2K VPN, not behind NAT

IP-VPN / LBL Selection

☐ IP-VPNs ☐ LBLs

Adj ITRANS MiddleBox:

Signal Protocol

Protocol type:

Protocol port:

Protocol version:

OK Cancel

Fields that are significant to GK-GK interoperability include:

- **Gateway IP address: 10.19.199.10**
Messaging from the External Gateway to the GWC will be via the Carrier Gateway - thus we provision the Carrier Gateway's IP address here.
- **Gateway Profile name: H323_PROXY**
This **new profile** should be used for all Acme Packet SD Gateways (stacks).
- **Reserved terminations: 480**
This gateway (stack) should be provisioned with the minimum reserved terminations (480 in this example). This represents the maximum number of simultaneous calls between the CS2K and any/all gateways that are registered with GK-1 on the external network.
- **Adj ITRANS MiddleBox: NATA**
A NAT should be added for the external network that GK-1 resides in.

- **Protocol port: 0**

H323_PROXY gateways should always be provisioned with a signalling protocol port of 0.

After the gateway is associated, a carrier must be added for this gateway in SESM. Provision the carrier just like any other H323 gateway - there are no carrier group changes specific to GK-GK interoperability.

Example SESM Provisioning - Add Carrier for External Gateway 1

External Gateway Session Director Configuration

Example configuration for External Gateway 1 on the Acme SD is shown below:

```
h323-stack
  name                EXT_GW_1
  state               enabled
  isgateway           enabled
  realm-id            enterprise_z
  assoc-stack         CARR_GW_1
  local-ip            10.77.77.30
  max-calls           480
  max-channels        4
  registration-ttl    50
  terminal-alias      h323-ID=EXT_GW_1

  prefixes
  ras-port
  auto-gk-discovery   disabled
  multicast           0.0.0.0:0
  gatekeeper          10.77.77.12:1719
  gk-identifier
  q931-port           1720
  alternate-transport
  q931-max-calls      1000
  h245-tunneling      enabled
  fs-in-first-msg     disabled
  call-start-fast     disabled
  call-start-slow     disabled
  media-profiles
```


process-registration	disabled
anonymous-connection	enabled
proxy-mode	H245
filename	
last-modified-date	2004-05-06 09:38:59

The **assoc-stack** (associated stack) field should point to the stack on the carrier side that will proxy messaging for this gateway to the GWC. EXT_GW_1's associated stack is CARR_GW_1.

The **maintenanceProxy** is not added to this gateway.

External Gateway Core Provisioning

An H323 trunk group should be added to core datafill that maps to the gateway provisioned in SESM in section [“External Gateway SESM Provisioning” on page 141](#). There are no core datafill changes specific to this feature - the trunk should be datafilled just like any H323 trunk group. In this example, 480 trunk members (b-channels) should be added for EXT_GW_1.

Limitations and restrictions

Supported GK Devices

GK-GK interop is supported between the CS2K GK and the following GKs

- Cisco 36xx (IOS 12.2.24)
- Cisco 72xx (IOS 12.2.24)
- Nortel S1000 (Succession Rls 3)

Supported H323 Gateways

GK-GK interop is supported between the CS2K GK and the following GWs. That is, these Gateways can be registered with the Gatekeepers listed in section 2.6.1.

- Cisco 26xx (IOS 12.2.24)
- Cisco 36xx (IOS 12.2.24)
- Cisco 37xx (IOS 12.2.TBD)
- Nortel S1000 (Succession Rls 3)
- Nortel S1000M (Succession Rls 3)
- Nortel BCM (Version 3.6)

Supported CS2K Interoperability

Interoperability is supported between any combination of gateway and gatekeeper pairs listed in sections 2.6.1 and 2.6.3, and the following:

- Cisco 26xx (IOS 12.2.24)

- Cisco 36xx (IOS 12.2.24)
- Cisco 37xx (IOS 12.2.TBD)
- Nortel S1000 (Succession Rls 3)
- Nortel S1000M (Succession Rls 3)
- Nortel BCM (Version 3.6)

Non-H323 Gateways

- PVG
- Mediatix
- CICM
- UAS
- MG9000
- SIP-T (VRDN)
- SIP-T (NGSS)
- MCS

Acme Session Director Limitations

- Maximum BHCA: currently unknown/uncharacterized
- Maximum simultaneous calls: Tiered based on license
- Maximum number of provisionable stacks: approximately 100-200
- Maximum number of provisionable endpoints per stack: this is manually engineered based on the licensed number of simultaneous calls and the number of provisioned stacks. For example, if 100 stacks are configured and a license allows for 8,000 simultaneous calls, then the maximum number of endpoints per stack would be $8000/100 = 80$ (on average).
- Failover speed: depends on the outage type but anywhere from 40 ms to 300 ms should be expected

Product = Carrier Hosted Services

A00007063 -- H.323 Gateway Profile Changes (MMBS)

Description

The current design to limit the number of endpoints that can be assigned to a specific gateway via the CS2M (CS2K Management Tools) is to set a

maximum reserved terminations value in the respective gateway profile. The maximum reserved terminations value is set in the GWC EM (Gateway Controller Element Manager) database during initial installation and upgrades. The values are set per release and cannot be changed dynamically by a craftperson.

A better solution has been adopted to manage the number of endpoints a single H.323 gateway can have allocated towards it.

A single gateway cannot be assigned more endpoints/TIDs than the maximum reserved terminations value of the assigned gateway profile.

H.323 gateways are different than most supported Succession gateways from a capacity perspective. A number of H.323 gateways do not have physical limitations. H.323 gateways have many variables that determine the maximum number of simultaneous calls:

- What is the hardware platform the H.323 gateway application is running on?
- How much memory does it have?
- Which hardware version?
- Which software version?

Determining the proper maximum capacity for a H.323 gateway from release to release is inaccurate. Nortel's H.323 gateways' maximum reserved termination values are difficult to properly set during a given release. H.323 third party gateways are even more difficult.

The solution is to set the maximum reserved termination values for all the H.323 gateway profiles to the maximum capacity of a H.323 GWC. The maximum reserved terminations value for a H.323 gateway is now restricted by the GWC not the gateway profile maximum reserved termination setting. Instead of the design team trying to manage the capacities of Nortel and third party H.323 gateways, our customers will configure the number of desired endpoints against H.323 gateways. Nortel will no longer dictate the maximum capacity of a third party H.323 gateway supported by the CS2K.

Nortel documentation will direct our customers to the respective gateway vendor documentation for the maximum capacities of the supported H.323 gateways.

The maximum number of endpoints that can be assigned to a single H.323 gateway in SN07 will now be the capacity of a H.323 GWC. If an attempt is made to associate more endpoints/TIDs to a H.323 gateway than the capacity of a H.323 GWC, the request is rejected and an error message is generated.

H.323 Capacities

A SN07 H.323 GWC in the North American market can be provisioned with 1032 endpoints/TIDs. A SN07 H.323 GWC in the International market can be provisioned with 1024 endpoints/TIDs.

Note: The SN07 H.323 GWC capacities have not changed from SN06.2.

A H.323 virtual carrier can be any size within the range of 4 - 672.

H.323 SN07 GWC capacities

H.323 GWC Profile	Endpoint Capacity (maximum number of endpoints/TIDs per GWC)
H.323_INTL	1024
H.323_NA	1032

The H.323 gateway profiles have been consolidated and updated by setting the maximum reserved terminations values to the capacity of the H.323 GWC.

The updated SN07 H.323 gateway profiles are listed in the following table.

Note: The H.323 gateway profiles that are being removed are designated by the “*strike through*”.

H.323 gateway maximum reserved terminations

H.323 Gateway Profile	SN06.2 Maximum Terminations	SN07 Maximum Terminations
NORTEL_BCM	64	1032 for NA 1024 for INTL (please consult the vendor documentation for the recommended maximum)
~~NORTEL_BCM_NA~~	~~48~~	~~48~~
SUCCESSION_1000	480	1032 for NA 1024 for INTL (please consult the vendor documentation for the recommended maximum)

H.323 gateway maximum reserved terminations

H.323 Gateway Profile	SN06.2 Maximum Terminations	SN07 Maximum Terminations
CISCO_2600	96	1032 for NA 1024 for INTL (please consult the vendor documentation for the recommended maximum)
CISCO_3600	384	1032 for NA 1024 for INTL (please consult the vendor documentation for the recommended maximum)
CISCO_AS5300	384	1032 for NA 1024 for INTL (please consult the vendor documentation for the recommended maximum)
CISCO_H323_IOS	N/A	1032 for NA 1024 for INTL (please consult the vendor documentation for the recommended maximum)
WESTELL	64	1032 for NA 1024 for INTL (please consult the vendor documentation for the recommended maximum)
H323_PROXY	N/A	1032 for NA 1024 for INTL (please consult the vendor documentation for the recommended maximum)

Hardware Requirements or Dependencies

N/A

Software Requirements or Dependencies

N/A

Limitations and restrictions

N/A

Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema _____

User Interface _____X_____

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

Glossary

Acronym	Definition
ASPEN	Nortel proprietary GW control protocol (not an acronym).
BLM	Business Line Management
CLLI	Common Language Location Identifier
CM	Computing Module
CORBA	Common Object Request Broker Architecture
CPE	Customer Premises Equipment
CS2K	Call Server 2000
CS2M	Call Server 2000 Management Tools
DDMS	DMS Data Management System
DMS	Digital Multiplex System
DTC	Digital Trunk Controller

DTCI	ISDN Digital Trunk Controller
DTD	Document Type Definition
EPID	End Point Identifier
ETSI	European Telecommunications Standards Institute
GPS	Global Product Support
GUI	Graphical User Interface
GW	Gateway
GWC	Gateway Controller
GWC EM	Gateway Controller Element Manager
H.323	Industry protocol for GW/GK<->GW/GK communication (not an acronym).
HTML	HyperText Markup Language
IDL	Interface Definition Language
IP	Internet Protocol
ITA	Internet Transparency Agent
JAR	Java Archive
JDBC	Java Database Connectivity
JNLP	Java Network Launching Protocol
JWS	Java Web Start
LAN	Local Area Network
LTC	Line/Trunk Controller
MEGACO	H.248. Industry protocol for MG/MGC <->MG/MGC communication.
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIB	Management Information Block
MOP	Method of Procedure

MTC	Maintenance
NA	North American
NAT	Network Address Translator
NN	Node Number
NPM	Network Patch Manager
NTNA	Northern Telecom North American (proprietary PRI variant)
OAM&P	Operations, Administration, Maintenance and Provisioning
OSS	Operation Support System
OSSDI	OSS Data Interface
PRI	Primary Rate Interface
PLM	Product Line Management
PSTN	Public Switched Telephone Network
RMGC	Redirecting Media Gateway Controller
SDM	SuperNode Data Manager
SESM	Succession Element and Sub-Element Manager [system]
SNMP	Simple Network Management Protocol
SQL	Structured Query Language (for DBs)
SSPFS	Succession Solaris Platform Foundation Software
SS7	Signaling System 7
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TID	Terminal Identifier
TMM	Trunk Maintenance Manager
TN	Terminal Number

Product = Carrier Hosted Services

A00007211 -- SN07 H.323 GWC600 Log Changes (MMBS)

Purpose

Log report GWC600 indicates an Info Log for a H.323 failure with a failure reason that indicates specifically what happened.

The current GWC600 log does not adhere to the log formatting standards as described in IEMPG.AF01. Not adhering to the requirements often makes the log in question unsupportable or difficult to support in the OSS.

This SN07 activity will modify the existing H.323 GWC600 log format to follow a generic OSS log framework. These changes will impact both the NA and international versions of H.323.

GWC Changes

The H323 application will generate formatted GWC600 logs to adhere to the OSS requirements. The formatted logs are sent to the syslog customer log interface. The fields in the log body are defined and populated in the H323 application.

The header is changed from “H323 LOG MESSAGE” to something not H323 specific, but more function-indicating, like “Protocol Event”. So we won’t have to define GWC601 as “SCTP Event” and GWC602 as “TCP event”, and etc. The log body is modified as well.

After the changes for H323 the GWC600 log will look like:

RTPG GWC11 GWC600 MAY21 14:54:47 0895 INFO GWC Protocol Event
Category: Communication
Component Id: GWC=GWC-11-UNIT-0;LINK=BCM_RTPG
Specific Problem: H323 keepAlive RRQ rejected
Description: D-Channel Out Of Service

Logs for other applications will follow the same framework, and will look something like:

RTPG GWC11 GWC600 MAY21 14:54:47 0895 INFO GWC Protocol Event
Category: Communication
Component Id: GWC=GWC-11-UNIT-0;LINK=ABI_1_2_3
Specific Problem: SCTP packet NACK
Description: SCTP association re-established

and

RTPG GWC11 GWC600 MAY21 14:54:47 0895 INFO GWC Protocol Event
Category: Communication
Component Id: GWC=GWC-11-UNIT-0;LINK=CS2M_IP_ADDR
Specific Problem: SNMP ASN.1 format error
Description: Message from 47.142.108.100 dropped

Product = CS 2000

A00001319 -- Device activity & RMID-PWID restoration tool & Panther enhancements (PT-AAL1, Succession on DMS)

Functional Description

This activity provides two new functionalities:

- A new CI tool 'SPMRESALIGN' which ensures the following:
 - a. The RMID-PWID values of the Resource RMs (DSP & VSP RMs) are aligned.
 - b. The activity of DSP & VSP RMs are aligned as per the table MNCKTPAK datafill.
- A new automated task as a part of Panther Upgrade. When this new task is executed, it will align the RMID-PWID values of all the resource RMs of all the SPMs in the office.

New CI tool SPMRESALIGN

A new CI tool 'SPMRESALIGN' is introduced as a part of this feature. This tool aligns the RMID-PWID values of the DSP/VSP RMs of the all the SPMs in the office. Once the RMID-PWID values of a particular RM is aligned, the activity of that particular RM is aligned as per the table MNCKTPAK datafill. The tool is implemented as a new CI directory. The tool can be directly accessed from the CI prompt. The tool has the following commands:

- Align the RMID-PWID values of the resource RMs of all the SPMs in the office.

CI:
>SPMRESALIGN
SPMRESALIGN:
>align all

- Align the RMID-PWID values of the resource RMs based on the variant of SPMs

CI:
>SPMRESALIGN
SPMRESALIGN:
>align <variant>

where the variant can be DMSCP, SMG4 or IW-DPT.

- Align the RMID-PWID values of the resource RMs of a single SPM.

CI:
>SPMRESALIGN
SPMRESALIGN:
>align spm <no>

This command is applicable for all variants of SPMs.

- Align the RMID-PWID values of the resource RMs for a range of SPMs.

CI:
>SPMRESALIGN
SPMRESALIGN:
>align spm <from_no> <to_no>

This command is applicable for all variants of SPMs.

This tool is a single user tool. i.e. only one user can use the tool at a time. Also all the command in this tool are privclassed. For this, the command 'SPMRESALIGN; & 'align' will be added to the table CMDS.

Please refer to the Configuration section of this feature for more details on the CI tool.

Panther Enhancements

This feature enhances the planning phase of PMUPGRADE to create a default task. This new task is to align the RMID-PWID values of all the SPMs present in the entire office. The new task is appended to the upgrade plan and will be passed to the SWUPGRADE tool. The new task will be created only if there is at least one SPM is available in the upgrade plan.

In SWUPGRADE, the craft person can view this new task by issuing the command 'display steps'. An example is as shown in the following figure.

SWUPGRADE steps

```
>swupgrade pm
SWUPGRADE:
```

```
>display steps
```

```
SWUPGRADE steps for target PM:
```

1_A_SPM	Needed	Perm	Act	Proc
ALIGN_RMS	Needed	Perm	Act	Proc
UPGRADE_COMPLETE	Needed	Perm	Act	Proc

The default task created is ALIGN_RMS. This task is an automated task. i.e. it is automatically executed as soon as all the upgrade tasks are completed. As this step starts executing, it halts for a user confirmation to proceed or abort this step. The following warning message will be displayed on the Panther screen

****WARNING: This step ALIGN_RMS will align the RMID-PWID values of all the Resource RMs of the SPMs in the office. Do you wish to continue?**

Please confirm (“YES”, “Y”, “NO”, or “N”):

Once the craft person enters “YES”, Panther will start aligning the RMID-PWID values of the all the resource RMs in the office. If the craft person enters “NO”, it aborts this task.

Panther automatically triggers this alignment task only if all the other task in the plan is successfully completed without any failure. Also the user confirmation has to be turned off in the Panther planning phase. Otherwise Panther waits for a manual intervention after each task is completed, to trigger the next task.

On the other hand, the craft person can manually execute this alignment task by overriding all the other upgrade tasks. The craft person has to issue the following command:

```
>runstep ALIGN_RMS.
```

All the progress message that are part of the new CI tool will be printed on the Panther screen also. Please refer to section 13.9 in Configuration document to get more information on the progress messages.

Log generation

A new SPM log is introduced to make the craftperson aware that a particular resource RM protection group is excluded by the SPMRESALIGN tool, without align RMID-PWID values. A particular RM group will be excluded from the alignment due to three reasons:

- PWID duplication
- Any RM in invalid state.
- Sparing failure.

Under all these circumstances the new SPM log '**SPM605**' will be generated giving necessary information to the craftperson and what action to be taken. This is only an info log and there is no alarm associated with it. The fields of the SPM605 log are shown in the following figure.

SPM605 Log Format

a) PWID Duplication

```
SPM605 MAR25 05:06:48 3004 INFO RMID-PWID Alignment
Prot group : SPM 3 VSP
Prot grp id : 1
Result      : Not Aligned
Reason      : PWID duplication.
Action      : Rectify the duplication and execute SPMRESALIGN
```

b) Any RM in invalid state

```
SPM605 MAR25 05:06:48 3004 INFO RMID-PWID Alignment
Prot group : SPM 3 VSP
Prot grp id : 1
Result      : Not Aligned
Reason      : VSP 1 not in ISV/ISTB.
Action      : Bring this RM to INSV and execute SPMRESALIGN
```

c) Sparing failure

```
SPM605 MAR25 05:06:48 3004 INFO RMID-PWID Alignment
Prot group : SPM 3 VSP
Prot grp id : 1
Result      : Not Aligned
Reason      : Unsuccessfull sparing
Action      : Review the logs related to sparing
```

Hardware Requirements or Dependencies

None.

Software Requirements or Dependencies

None.

Limitations and restrictions

Following RM groups are excluded from the alignment process.

- If any RM in the group is having a PWID duplication.
- If there is no inactive RM in the group.
- If any RM in the group is in invalid state (offl, sysb, cbsy, manb).

No action is taken on these RM groups to align the RMID-PWID values. However, proper warning messages will be displayed. Please refer to the Configuration section of this feature for more information on the warning messages.

Interactions

When the office upgrade using Panther is in progress, the craftperson is restricted from executing the commands in the 'SPMRESALIGN' tool. Proper message will be displayed to the craftperson.

a) In a multiple window upgrade shift, after each days shift the craft can run the CI tool on the SPMs which finished the upgrade or.

b) The craftperson can run the automated task from panther. This will be run automatically after all the steps. Proper message will be displayed that it will align the RMID-PWID values of all the Resource RMs in the office.

Applicable customer facing sections

Fault Management

Logs	X
Alarms	N/A

Configuration

Data Schema	N/A
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A

Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A
Real-time	N/A
Engineering Information	N/A

Glossary

Term	Description
SPM	Spectrum Peripheral Module
RM	Resource Module
RMID	Resource Module ID
PWID	ProtWhom ID
DSP	Digital Signal Processor
VSP	Voice Signal Processor

Configuration for A00001319

Hardware and Software Requirements

None

Initial Configuration

None

Office/Subnet parameters (OP/SP) (CM & SESM)

None

Upgrade Impact

None

Data schema (DS) (CM, MIBS, RDB)

None

Service Orders (SO) (CM & SESM)

None

Software optionality control (SOC)

None

Element Management

None

Command interface changes**Directory: spmresalign****Directory description**

A new CI directory is created to enable the craftperson to access various commands to align the RMID-RWID values of the all the resource RMs (DSP/VSP/DLC) of a particular SPM or a set of SPMs or all the SPMs present in the office. This tool is a single user tool. i.e. only one user can use the tool at a time.

Accessing directory: spmresalign**Access to directory and return to CI**

To access spmresalign from the CI environment, enter **spmresalign**.

To return to the CI environment, enter **quit**.

Command: ALIGN**Command type: NON-MENU****Command target: All****Command availability: RES****Command description**

This command 'ALIGN' is used to align the RMID-PWID values of all the resource RMs of a single SPM, a set of SPMs or all the SPMs in the office.

Command syntax

The command syntax is as shown in the following figure.

: Syntax of align command

```

SYNTAX: align
Parms    : <OPTION> {ALL,
                      DMSCP,
                      SMG4,
                      IW_DPT,
                      SPM <FROM_NO>{0 TO 85}
                      [<TO_NO> {0 TO 85}]}}

```

Parameter Description:

- ALL** : This option aligns the RMID-PWID values of the resource RMs of all the SPMs in the office.
- DMSCP** : This option aligns the RMID-PWID values of the resource RMs of all the DMSCP SPMs present in the office.
- SMG4** : This option aligns the RMID-PWID values of the resource RMs of all the MG4K SPMs present in the office.
- IW_DPT** : This option aligns the RMID-PWID values of the resource RMs of all the DPT SPMs present in the office.
- SPM <FROM_NO> <TO_NO>**: This option aligns the RMID-PWID values of the resource RMs of all the SPMs specified within the range <FROM_NO> to <TO_NO>. If only <FROM_NO> is entered, the tool aligns the RMID-PWID values of that particular SPM only. This command is applicable to all variants of SPMs.

Qualifications and warnings

None

Responses**Wrong Input from the craftperson**

- a. If the tool is already in use, and if any other user try to access this tool a message will be displayed as shown:

SPMRESALIGN in use by <mapid>

- b. If the craftperson enters an SPM number which is not present in the office, a message will be displayed as shown:

>align spm 26
SPM 26 is not provisioned.

- c. If there are no dmSCP SPMs present in the office.

>align dmSCP
No DMSCP SPMs provisioned in the office.

- d. If there are no MG4K SPMs present in the office.

>align smg4

No MG4K SPMs provisioned in the office.

- e. If there are no DPT SPMs present in the office.

>align iw_dpt

No DPT SPMs provisioned in the office.

IW -Bridge only SPMs are not included in this.

- f. If <from_no> is greater than <to_no>

>align spm 30 2

Invalid tuple range.

Progress Message

After building the necessary information and initial screening of a particular RM protection group, the group will be subjected to alignment process. The craftperson will be notified with proper message as shown:

**SPM <no> <RM type> group < protection group id>: RMID-PWID
Alignment in progress.**

e.g., SPM 1 DSP group 1 : RMID-PWID Alignment in progress.

PWID duplication

If any of the RM in a particular RM protection group has a duplicate PWID, this particular group cannot be aligned. Hence the spmresalign tool will exclude this group, giving a proper message to the craftperson as shown:

*****Warning: SPM <no> <RM type><RM no> has a duplicate PWID.
The RMID-PWID values of this <RM type> group cannot be
aligned.**

e.g., ***Warning: SPM 1 DSP 1 has a duplicate PWID.
The RMID-PWID values of this DSP group cannot be
aligned.

RMID-PWIDs already aligned.

If all the RMs in a particular protection group is already aligned, no further action will be taken by the tool. The tool will exclude this particular group, giving a proper message to the craftperson as shown

**All the RMs in SPM <no> <RM type>group <protection group id> are
already aligned.**

e.g., All the RMs in SPM 1 DSP group 2 are already aligned.

No Inactive RM present in a protection group

If any of the RM protection group does not have an inactive RM, sparing cannot be performed on this group and the RMID-PWID values of this group cannot be aligned. The tool will exclude this particular group, giving a proper message to the craftperson as shown

*****Warning: SPM <no> <RM type>group <protection group id> does not have an inactive unit. The RMID-PWID values of this <RM type>group cannot be aligned.**

e.g., ***Warning: SPM 1 DSP group 1 does not have an inactive unit.
The RMID-PWID values of this DSP group cannot be aligned.

RM in invalid state

If any of the RM in a particular RM protection group is in invalid state (offl,sysb, cbsy, manb), the RMID-PWID values of this particular group cannot be aligned. Hence the spmresalign tool will exclude this group, giving a proper message to the craftperson as shown:

*****Warning: SPM <no> <RM type><RM no> is in invalid state. The RMID-PWID values of this <RM type> group cannot be aligned.**

e.g., ***Warning: SPM 1 DSP 2 is in invalid state.
The RMID-PWID values of this DSP group cannot be aligned.

RM sparing failure

If the sparing between two RMs for aligning the RMID-PWID values of a particular RM group fails, the RMID-PWID values of this particular group cannot be continued further. Hence the spmresalign tool will exclude this group, giving a proper message to the craftperson as shown:

*****Warning: SPM <no> <RM type><RM no> sparing failed. The RMID-PWID values this <RM type> group cannot be aligned.**

e.g., ***Warning: SPM 1 DSP 2 sparing failed.
The RMID-PWID values this DSP group cannot be aligned.

SPM REX in progress

If SPM REX is in progress on a particular SPM, that SPM is excluded from the alignment process. Proper message is displayed to the craftperson as shown:

*****Warning: SPM REX in progress on SPM <no>
Re-execute the tool on this SPM once REX is completed.**

Panther upgrade in progress

If the Panther upgrade is in progress, the craftperson will be restricted from issuing the 'align' command from the spmresalign tool. The craftperson will be notified about this with proper warning message:

Office upgrade in progress.

Please run the command after office upgrade is completed.

Alignment completed

Once the RMID-PWID values of all the RMs in a particular RM group is completely aligned by the tool, a message is displayed to the craftperson:

**SPM <no> <RM type> group < protection group id>: RMID-PWID
Alignment completed.**

e.g., SPM 1 DSP group 1 : RMID-PWID Alignment completed.

Final Summary

The spmresalign tool will give a final summary report of all the RM groups. This will help the craftperson to obtain a consolidated report.

Overall RMID-PWID Alignment Result:

SPM No	ProtGrp	GrpId	Result
SPM 1	DSP	1	Aligned
SPM 1	DSP	2	Aligned
SPM 1	VSP	1	Aligned
SPM 2	DSP	1	Not Aligned
SPM 2	DSP	2	Aligned
-----	----	--	-----
-----	----	--	-----

Example

The following table shows the output of align command.

Usage examples for align command

Description of task:	Align the RMID-PWID values of a set of SPMs or a single SPM or all the SPM.																								
Command:	spmresalign; align all																								
MAP response:	CI: >spmresalign spmresalign: >align all SPM 1 DSP group 1: RMID-PWID Alignment in progress. SPM 1: Manual Sparing from DSP 0 to DSP 1 SPM 1 DSP group 1: RMID-PWID Alignment completed. All the RMs in SPM 1 DSP group 2 are already aligned. SPM 2 DSP group 1: RMID-PWID Alignment in progress. ***Warning: SPM 2 DSP group 1 does not have an inactive unit.The RMID-PWID values of this DSP group cannot be aligned. SPM 2 VSP group 1: RMID-PWID Alignment in progress. ***Warning: SPM 2 VSP 1 Sparing failed. The RMID-PWID values of this VSP group cannot be aligned. Overall RMID-PWID Alignment Result ----- <table><tr><th>SPM No.</th><th>PrtGrp</th><th>GrpId</th><th>Result</th></tr><tr><td colspan="4">-----</td></tr><tr><td>SPM 1</td><td>DSP</td><td>1</td><td>Aligned</td></tr><tr><td>SPM 1</td><td>DSP</td><td>2</td><td>Aligned</td></tr><tr><td>SPM 2</td><td>DSP</td><td>1</td><td>Not Aligned</td></tr><tr><td>SPM 2</td><td>VSP</td><td>1</td><td>Not Aligned</td></tr></table>	SPM No.	PrtGrp	GrpId	Result	-----				SPM 1	DSP	1	Aligned	SPM 1	DSP	2	Aligned	SPM 2	DSP	1	Not Aligned	SPM 2	VSP	1	Not Aligned
SPM No.	PrtGrp	GrpId	Result																						

SPM 1	DSP	1	Aligned																						
SPM 1	DSP	2	Aligned																						
SPM 2	DSP	1	Not Aligned																						
SPM 2	VSP	1	Not Aligned																						

Usage examples for align command

Command:	spmresalign; align dmscp																								
MAP response:	Note: The dmscp SPMs present in office are SPM 21 & 24 Cl: >spmresalign spmresalign: >align dmscp SPM 21 DSP group 1: RMID-PWID Alignment in progress. SPM 21: Manual Sparing from DSP 0 to DSP 1 SPM 21 DSP group 1: RMID-PWID Alignment completed. SPM 21 VSP group 1: RMID-PWID Alignment in progress. SPM 21: Manual Sparing from VSP 0 to VSP 1 SPM 21 VSP group 1: RMID-PWID Alignment completed. All the RMs in SPM 24 DSP group 1 are already aligned. No RMs provisioned in SPM 24 VSP group 1. Overall RMID-PWID Alignment Result <table><tr><th colspan="4">-----</th></tr><tr><th>SPM No.</th><th>PrtGrp</th><th>GrpId</th><th>Result</th></tr><tr><th colspan="4">-----</th></tr><tr><td>SPM 21</td><td>DSP</td><td>1</td><td>Aligned</td></tr><tr><td>SPM 21</td><td>VSP</td><td>1</td><td>Aligned</td></tr><tr><td>SPM 24</td><td>DSP</td><td>1</td><td>Aligned</td></tr></table>	-----				SPM No.	PrtGrp	GrpId	Result	-----				SPM 21	DSP	1	Aligned	SPM 21	VSP	1	Aligned	SPM 24	DSP	1	Aligned

SPM No.	PrtGrp	GrpId	Result																						

SPM 21	DSP	1	Aligned																						
SPM 21	VSP	1	Aligned																						
SPM 24	DSP	1	Aligned																						

Usage examples for align command

Command:	spmresalign; align spm <no> <no>												
MAP response:	CI: >spmresalign spmresalign: >align spm 3 5 SPM 4 is not provisioned. SPM 3 DSP group 1: RMID-PWID Alignment in progress. SPM 3: Manual Sparing from DSP 0 to DSP 1 SPM 3 DSP group 1: RMID-PWID Alignment completed. SPM 5 DSP group 1: RMID-PWID Alignment in progress. SPM 5: Manual Sparing from DSP 0 to DSP 1 SPM 5: Manual Sparing from DSP 2 to DSP 0 SPM 5 DSP group 1: RMID-PWID Alignment completed. Overall RMID-PWID Alignment Result <table><tr><th>SPM No.</th><th>PrtGrp</th><th>GrpId</th><th>Result</th></tr><tr><td>SPM 3</td><td>DSP</td><td>1</td><td>Aligned</td></tr><tr><td>SPM 5</td><td>DSP</td><td>1</td><td>Aligned</td></tr></table>	SPM No.	PrtGrp	GrpId	Result	SPM 3	DSP	1	Aligned	SPM 5	DSP	1	Aligned
SPM No.	PrtGrp	GrpId	Result										
SPM 3	DSP	1	Aligned										
SPM 5	DSP	1	Aligned										
Command:	spmresalign; align spm all												
MAP response:	CI: >spmresalign spmresalign: >align spm all Office upgrade in progress. Please run the command after office upgrade is completed.												

Product = CS 2000**A00001649 -- SBA Robustness: End-to-end Integrity (Succession on DMS)****Description**

This feature has two parts:

1. SBA Backup Alarms Precedence
2. Add “cli” command to BILLMTC Interface.

The following sections give a brief description on SBA Backup Alarms Precedence and later a brief description of Add “cli” command to BILLMTC interface.

“SBA Backup Alarms Precedence”

This feature is to change the priority of the backup alarms so that these alarms take precedence over NOCOM alarm.

When the NOCOM alarm appears on the MAP at the SDBIL level, the streams on the CM go to backup mode. The billing records then generated will be written to backup files on backup volumes configured for the stream.

Eventually the backup space on core will start getting used up and backup alarms will start appearing on the SDBIL banner depending upon the amount of used space. When 50% of backup space has been used up, the BAK50 alarm will appear on the SDBIL banner on the MAP indicating that only 50% of the configured backup space is available for the stream.

Once 70% of the backup space is used, the BAK50 alarm will be changed to BAK70 alarm. Again when a situation is reached wherein only 10% of the free space is available, BAK70 alarm will be replaced by the BAK90 alarm. Eventually when the system runs out of backup space, NOBAK alarm will appear under the SDBIL banner replacing the BAK90 alarm.

Once the NOBAK alarm comes up for a stream, any further records generated would still persist in the buffer pool {buffer allocated to the stream}. Eventually if the situation continues the buffers would get depleted and a NOSTOR{Critical} alarm will appear under SDBIL level.

NOCOM alarm

Alarm condition : NOCOM occurs

APPL : SDM C

SDBIL : NOCOM C

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
AMDI	04SBPT	NODLOG	.	1 SPM	.	.	...	.	SDM
C				*C*					*C*
POST			OAMAP	ATMFW	SDM	SPMCP	SWMTC	SDBIL	TOPSIP
0 Quit			.	.	SysB	.	.	NOCOM	.
2 Post_					*C*			*C*	
3									


```

4          AMA :      Bkup Pri:      InSv Rec:      InSv
5          Bkup:      Bkup Comm:      InSv
6 TST
7 Bsy
8 RTS
9 Conf_
10         DispAL
11 DispAL    critical:ALL:NOCOM:Communication to SDM cannot be established.
12
13 Status    major: AMA: BAKUP: Backup time exceeds 10 minutes.
14 Query
15
16
17 Audit

```

NOCOM with BAK50

Alarm condition : Still in NOCOM, but we have just hit BAK50

APPL : SDM C

SDMBIL : BAK50 C

```

XAC      MS      IOD      Net      PM      CCS      Lns      Trks      Ext      APPL
AMDI      04SBPT  NODLOG      .      1 SPM      .      .      ...      .      SDM
*C*                                *C*                                *C*
POST                                SDM      SPMCP      SWMTC      SDMBIL      TOPSIP
0 Quit                                SysB      .      .      BAK50 .
2 Post_                                *C*                                *C*
3
4          AMA :      Bkup Pri:      InSv Rec:      InSv
5          Bkup:      Bkup Comm:      InSv
6 TST
7 Bsy
8 RTS
9 Conf_
10         DispAL
11 DispAL    critical:ALL:NOCOM:Communication to SDM cannot be established.
12         critical: AMA: BAK50: WARNING, less than 50% free space for Backup
13 Status    major: AMA: BAKUP: Backup time exceeds 10 minutes.
14 Query
15
16
17 Audit
18

```

NOCOM with BAK70

```
Alarm condition : Still in NOCOM, but we have just hit BAK70
APPL           : SDM      C
SDMBIL         : BAK70   C
```

```
XAC      MS      IOD      Net      PM      CCS      Lns      Trks      Ext      APPL
AMDI     04SBPT  NODLOG    .        1 SPM    .        .        ...      .        SDM
*C*                                           *C*                                           *C*
POST
0 Quit
2 Post_
3
4          AMA :      Bkup  Pri:      InSv  Rec:      InSv
5          Bkup:      Bkup  Comm:     InSv
6 TST
7 Bsy
8 RTS
9 Conf_
10
11 DispAL      DispAL
12 critical:ALL:NOCOM:Communication to SDM cannot be established.
13 critical: AMA: BAK70: WARNING, less than 30% free space for Backup
14 Status      major: AMA: BAKUP: Backup time exceeds 10 minutes.
15 Query
16
17 Audit
18
```

NOCOM with BAK90

```
Alarm condition :Still in NOCOM, but we have just hit BAK90
APPL           : SDM      C
SDMBIL         : BAK90   C
```

```
XAC      MS      IOD      Net      PM      CCS      Lns      Trks      Ext      APPL
AMDI     04SBPT  NODLOG    .        1 SPM    .        .        ...      .        SDM
*C*                                           *C*                                           *C*
POST
0 Quit
2 Post_
3
4          AMA :      Bkup  Pri:      InSv  Rec:      InSv
5          Bkup:      Bkup  Comm:     InSv
6 TST
7 Bsy
8 RTS
9 Conf_
```

```

10          DispAL
11 DispAL    critical:ALL:NOCOM:Communication to SDM cannot be established.
12          critical: AMA: BAK90: WARNING, less than 10% free space for Backup
13 Status    major: AMA: BAKUP: Backup time exceeds 10 minutes.
14 Query
15
16
17 Audit
18

```

NOCOM out of backup space

```

Alarm condition : Still in NOCOM, but we run out of backup space
APPL             : SDM      C
SDMBIL           : NOBAK    C

```

```

XAC      MS      IOD      Net      PM      CCS      Lns      Trks      Ext      APPL
AMDI      04SBPT  NODLOG      .      1 SPM      .      .      ...      .      SDM
*C*                               *C*                               *C*
POST
0 Quit      .      .      SysB      .      .      NOBAK .
2 Post_     *C*                               *C*
3
4          AMA :      Bkup  Pri:      InSv  Rec:      InSv
5          Bkup:      Bkup  Comm:      InSv
6 TST
7 Bsy
8 RTS
9 Conf_
10
11 DispAL    critical:ALL:NOCOM:Communication to SDM cannot be established.
12          critical: AMA: NOBAK: ERROR, no space on Backup volumes.
13 Status    major: AMA: BAKUP: Backup time exceeds 10 minutes.
14 Query
15
16
17 Audit
18

```

NOCOM out of buffers

```

Alarm condition : Still in NOCOM, but we run out of buffers .

```

```

APPL          : SDM      C
SDMBIL        : NOSTOR  C

```

```

XAC      MS      IOD      Net      PM      CCS      Lns      Trks      Ext      APPL
AMDI     04SBPT  NODLOG      .      1 SPM      .      .      ...      .      SDM
*C*                                     *C*                                     *C*
POST
0 Quit
2 Post_
3
4
5          AMA :          Bkup  Pri:          InSv  Rec:          InSv
6 TST
7 Bsy
8 RTS
9 Conf_
10
11 DispAL
12 critical:ALL:NOCOM:Communication to SDM cannot be established.
13 Status critical:AMA:NOBAK: ERROR, no space on Backup volumes.
14 Query  major: AMA: NOSTOR:No memory available to buffer records.
15
16
17 Audit
18

```

“Add “cli” command to BILLMTC Interface”

This feature will add a new functionality whereby a new command (“cli”) will be introduced under the SBA RMI subsystem to retrieve the CLI name from BILLMTC Interface.

This command is hidden and does not appear on the BILLMTC level. The command is available from all BILLMTC level as a non menu command. The user can run the “cli” command from any level of BILLMTC interface to get the CLI name.

“cli” command is not available either as a numbered command or as a menu command, unlike other commands in BILLMTC interface. The user has to directly enter the command ““cli”” at the BILLMTC interface from any level to retrieve the CLI name.

“cli” command

Command name: “cli”

Command description:

“cli” command displays the current information about the CLI connected with the sdm. The command should be used at BILLMTC level. The command is case in-sensitive.

The “cli” command response will be,

<Core CLI Name>

Command Format:

cli

Parameters

None

Response:

<Core CLI Name>

The “cli” command executed from BILLMTC level of BILLMTC interface

```
BILLMTC          MSH4_CALL_SERVER
0 Quit
2 Set
3
4 CONFSTRM

5
6
7
8 APPL
9 Query
10 Mib
11 DispAl
12 Displs
13 FILESYS
14 SCHEDULE
15 TOOLS
16 TAPE
17 Help
18 Refresh
root             > cli
Time 09:28
```

The “cli” command executed from BILLMTC; SCHEDULE level of BILLMTC interface.

```

SCHEDULE          MSH4_CALL_SERVER
0 Quit
2 Set
3
4
5
6
7 Add
8 Change
9 Delete
10 List
11 RTB
12
13
14
15
16
17 Help
18 Refresh
root              > clli

```

Help for clli

Help for “cli” command is available at all levels. To get the help for clli, enter the “help” without parameters at any billmtc level, help for “cli” command will be displayed along with the help for other commands.

The “help” command issued at BILLMTC interface

```

BILLMTC           The commands available at this level....
0 Quit            0 Quit      -> Quits the current level
2 Set             2 Set      -> Sets context
3
4 CONFSTRM        4 CONFSTRM -> Enters CONFSTRM level
5
6
7
8 APPL            8 APPL      -> Enters APPL level
9 Query           9 Query     -> Displays current state of streams
10 Mib            10 Mib      -> Sets and gets MIB objects
11 DispAl         11 DispAl   -> Displays all current SDM alarms
12 Displs         12 Displs   -> Displays logs not yet sent to CM
13 FILESYS        13 FILESYS  -> Enters FILESYS level
14 SCHEDULE        14 SCHEDULE -> Enters SCHEDULE level
15 TOOLS          15 TOOLS    -> Enters TOOLS level

```

```
16          16 TAPE      -> Enters TAPE level
17 Help      17 Help      -> Available commands with syntax
18 Refresh   18 Refresh   -> Refreshes the screen
    maint    MORE...
Time 12:16
```

Press enter to continue for the help for “cli”

```
BILLMTC      cli:  Displays core CLI
0 Quit
2 Set
3
4 CONFSTRM
5
6
7
8 APPL
9 Query
10 Mib
11 DispAl
12 Displogs
13 FILESYS
14 SCHEDULE
15 TOOLS
16
17 Help
18 Refresh
    maint    >
Time 12:17
```

Hardware requirements

None

Limitations and restrictions

“SBA Backup Alarms Precedence” will put the following limitations.

Any critical alarm raised by SBA under the SDBIL banner will be masked by the backup alarm if any. To see all the alarms (critical, major, minor) raised by SBA, the user will have to invoke the DispAl command to see the list of all SBA alarms.

“Add “cli” command to BILLMTC Interface“ will put the following limitations

The command is available only at BILLMTC level. The command can not be used at SDMRLOGIN level.

Interaction.

NA

Logs (LG)

Not Applicable

Data schema (DS)

Not Applicable

Alarms (AL)

Not Applicable

Command interface (BILLMTC)

New/modified commands

New command has been added through this “Add “cli” command to BILL-MTC interface.

New/Modified Commands

Command name	NEW, CHANGED OR DELETED	New name (if renamed)	Directory/ BILLMTC level name	MENU/NON-MENU /HIDDEN
cli	NEW	-	BILLMTC	HIDDEN

Product = CS 2000

A00001650 -- SBA Patch Size Reduction (Succession on DMS)

Description

SDM SBA application is delivered to Nortel’s customers as SDM_SBA.DMS500 and SDM_AFT.DMS500 filesets in the previous releases. The total size of the two filesets are greater than 160² MB (40MB +

120MB). When there is a change in SBA base code to fix issues, the whole 120 MB fileset must be packaged and delivered. In an extreme case, if a change is in base MIB functional component, the two filesets of 160MB will also be required if AFT is installed. In most of the cases, SBA base fix does not require the AFT fileset to be delivered to the customers.

In the past releases, SBA fix filesets were stored into 4Gg DAT tape and shipped to customer sites. However, Nortel's SDM fix delivery method have been migrating from shipping MNCL tape(s) to downloading the filesets (or packages) into the customer networks via IP protocols (i.e. electronic delivery).

In cases where customer only has 28.8K modem in the networks, the total download time would be more than 9 hours (120MB / 211Kbytes per minute³) for SBA SDM_SBA.DMS500 fileset and more than 3 hours for AFT fileset. If the customers has high speed cable connection, then the time for SBA and AFT would be 3 hours and 48 minutes; and 55 minutes respectively. Therefore, the "fix filesets" would not be downloaded completely before maintenance window had expired even though the customer has high speed connection.

This feature reduces SBA/AFT deliverable(s)⁴ size by de-coupling ACE and eighteen SBA base libraries code from SBA/AFT executable(s). The SBA base shared libraries will be packaged into the SBA fileset/package. The ACE library code will be packaged separately. The fileset/package for ACE is named as SDM_ACE.dist in AIX platform and SDM_ACE_5.3.0.0.pkg in Solaris platform.

Hardware Requirements or Dependencies

No new hardware required

Software Requirements or Dependencies

SBA and AFT requires ACE fileset and package in AIX and Solaris platforms respectively. The ACE fileset/package contains ACE shared libraries. This is the only copy of ACE library code. The filesets/packages must be installed in the following orders⁵:

1. ACE
2. SDM_SBA.DMS500
3. SDM_AFT.DMS500

2. The size information are taken from 19.72.0.0 NCL load. The SDM_SBA.DMS500-19.69.0.0.tape file is 120,287,232 bytes and the SDM_AFT.DMS500-19.69.0.0.tape file 40,079,360 bytes.

3. Data taken from "SDM Wellness Patching 3.1" presentation.

4. The deliverable(s) could be the whole SBA in a single fileset or a number of filesets of different sizes.

5. The installations follows the standard CBM and nSDM procedure

Similarly, the packages/filesets must be removed in the following orders.

1. SDM_AFT.DMS500
2. SDM_SBA.DMS500
3. ACE

In case ACE fileset is upgraded/patched, SBA and AFT fileset must be BSY/RTS after the new ACE fileset is installed otherwise SBA and AFT software will be running with the order version of ACE. This might lead to run time problems.

Limitations and restrictions

- SBA/AFT cannot be installed before ACE is installed.
- ACE cannot be removed before SBA/AFT are un-installed from the system. In CBM, the Solaris “pkgm” command does not prevent user from removing lower layer package that are needed by other upper layer package. In other words, there is nothing stopping user from removing ACE fileset even if SBA/AFT have not been un-installed. It is important to note that if a user removes ACE package from the system, SBA/AFT will not function.
- SBA/AFT must be BSY/RTS if ACE is upgraded on the system.

Interactions

None

Applicable customer facing sections

Fault Management

Logs __N/A__

Alarms __N/A__

Configuration

Data Schema __N/A__

User Interface __N/A__

Element Management __N/A__

Security __N/A__

Service Order __N/A__

Office Parameters __N/A__

Accounting (includes AMA billing) __N/A__

Performance (includes operational measurements) __N/A__

Glossary

Term	Description
ACE	The ADAPTIVE Communication Environment. "It freely available, open-source object-oriented (OO) framework that implements many core patterns for concurrent communication software"

Product = CS 2000

A00001743 -- SYSLOG Consolidation for Succession (PT-IP, UA-IP, IAW, IAC)

Functional Description

This activity uses the Log Delivery application to

- Provide a single consolidated northbound log feed for all the components in a succession node.
- Implement the initial phase of Lost Log detection for Non-CM logs.
- Enhance the Lost Log indication mechanism for CM logs.
- Enhance the Log Delivery application's capacity to handle bursty traffic of logs.
- Enhance Logroute tool to make it more user friendly and to remove redundant processing.

Functional Overview

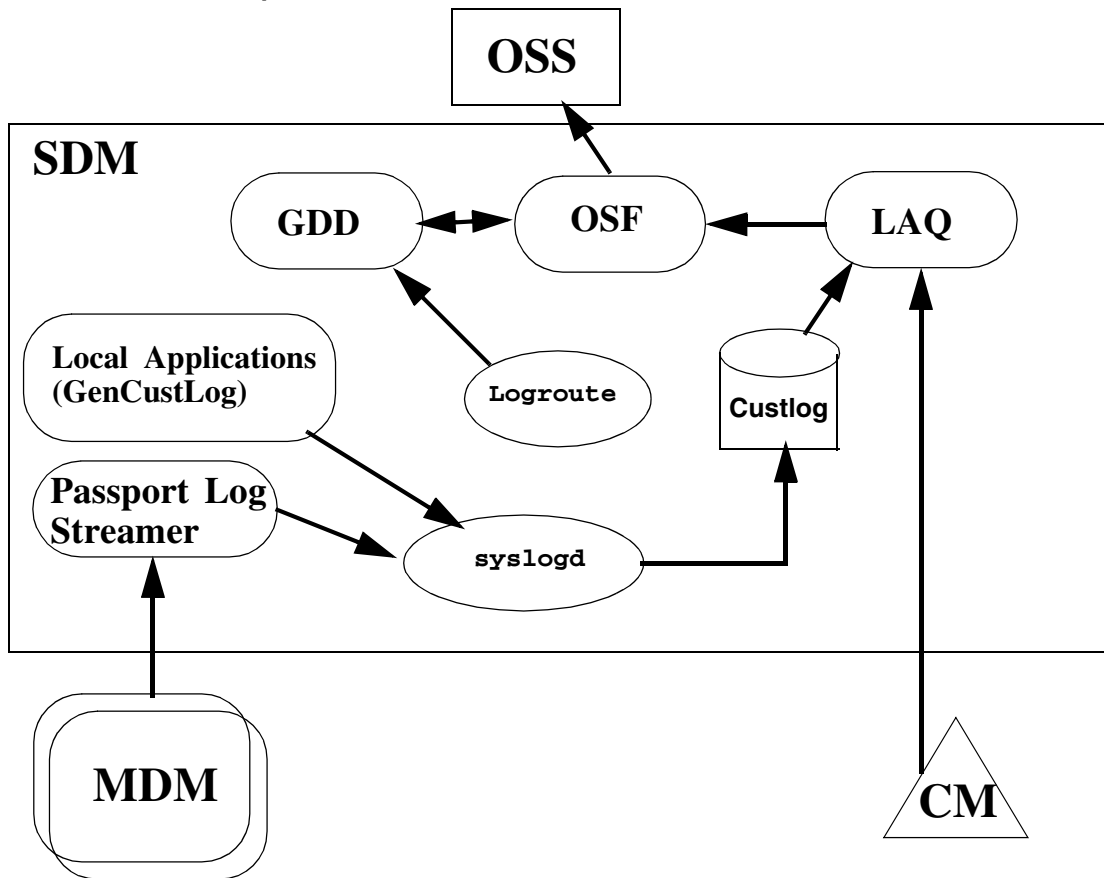
Introduction

The Log Delivery Application is used to collect CM logs and Customer logs, format them in either STD or SCC2 format and route them to remote (Telco) hosts, printers and/or UNIX files.

Log Delivery application has two components - **LAQ** and **OSF**. LAQ is the component which is used to receive the logs from the CM and custlog file, parse the logs and send them to OSF.

OSF receives these logs, formats the logs (into STD or SCC2 depending on the format configured for that device in Logroute) and sends the logs to the configured destination (that is, whether these logs need to be written to an UNIX file or sent to some remote destination).

The following figure shows the current design of the Log Delivery Application.

Interaction Between Component**Current Problem scenarios**

The Current Log Delivery application contains the following problem scenarios.

Logroute Command Line User Interface

The User Interface of Logroute is not very user-friendly currently. For example, consider the Main menu screen as shown in the following figure.

Logroute Main Menu screen.

Logroute Main Menu

1 - Device List
2 - Global Parameters
3 - CM Configuration File
4 - Gdd Configuration

c:change menu, q:quit, h:help, s:save changes

Enter command ==> **c**

Enter number of main menu option ==> **2**

The user has to first enter “c” and then the number of the main menu option to access any sub-menu. The same is the case for all sub-menu screens. This is a strenuous way to access the sub-menus and information in the logroute tool.

Lost Log Detection

The Log Delivery application currently does not have a mechanism to detect stoppage or any gap in the delivery of logs from a given Element Manager or a Network Element Application. Hence, the client is not notified regarding the loss of logs.

Conforming to Standards Specified

The Logroute tool is used to define the parameters of each individual OSS feed.

- Format: STD or SCC2
- Who originates connection: OSS (TCP), OSS (TCPIN)
- Port number used: <xxxxxx>
- Filtering rules (by log name and number):

OSF retrieves this information and based on the configured format, converts them into STD or SCC2 logs. The inconsistency of the OSF output for different formats can be noticed in the following figure.

Assuming that the LOG_OFFICE_ID (that identifies the switch generating the log) and Ecore_FORMAT (flag used to decided the display of the node name) in the DMS table OFCVAR have been set.

OSF outputs of the STD & SCC2 formats for CM and SDM logs.

LOG_OFFICE_ID=BRISC315BH
ECORE_FORMAT=TRUE

Ecore Node name

Sequence Number

FORMAT = STD

BRISC315BH SDM608 FEB11 04:09:09 **7952** INFO SDM Base Maintenance
 SDM Backup status cleared by user.

BRISC315BH **CM** SDMB610 FEB11 04:09:34 **7953** INFO SDM BILLING
 COMMS
 STREAM= AMA: SDM Communication is out of service.

FORMAT = SCC2

09 SDM 608 **0005** INFO SDM Base Maintenance
 SDM Backup status cleared by user.

09 SDMB610 **0006** INFO SDM BILLING COMMS
 STREAM= AMA: SDM Communication is out of service.

From the above figure it can be clearly seen that the application does not follow the same format for all logs.

- The Node name (ECORE Node name) is not displayed for logs generated on Non-CM node.
- Logs generated in SCC2 format do not display the originator of the log (Example:- CM or SDM).
- The generated Sequence number does not conform to the Dual Sequence Number (Global and Device Sequence Number) format specified in the log standards. Currently the Global and Device Sequence number format is not used. The number is implemented as a single four-digit Sequence Number.
- The logs generated in the configured format (STD or SCC2) by the Log Delivery Application do not conform to the customer document.

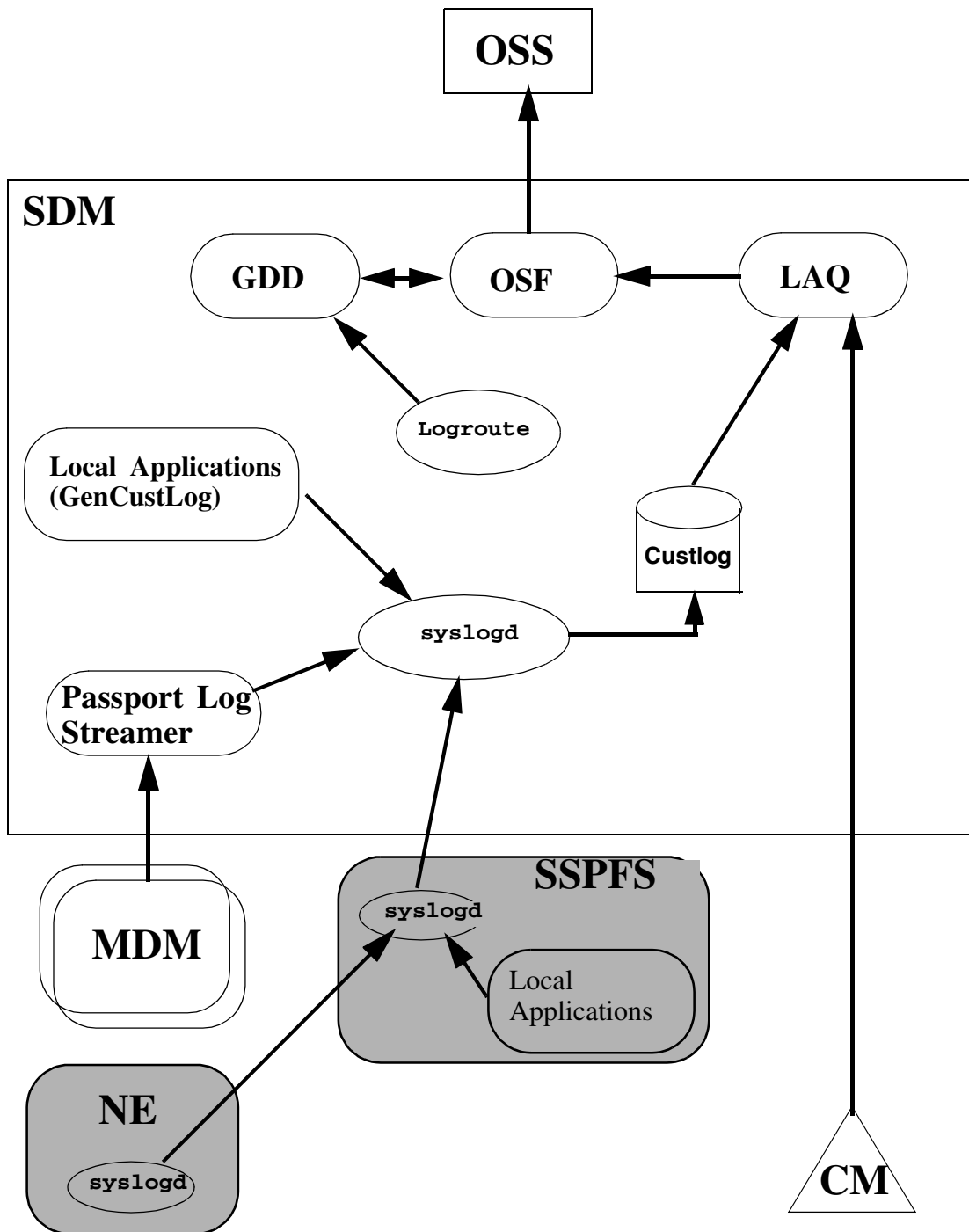
The OSF needs to be upgraded to support the standard log format (either STD or SCC2).

The purpose of the feature is to resolve the current problem scenarios mentioned above.

Functional Components.

The proposed architecture to support customer logs being fed into the syslogd daemon from remote syslogd daemons is as below.

Interaction Between Components



The implementation of this feature can be broken down into the following main components.

Logroute Command Line User Interface (Logroute CLUI).

- Modify the existing screens to enable the user to access and modify the existing information more easily.
- Add new menus and screens to make the Logroute CLUI more user-friendly.

Upgrade all SDM applications to use GENCustLog API Version 2 to generate custlogs.

- Enhance the current custlog to contain information required for lost log detection.
- Upgrade SDM applications to reflect the new custlog format.

Implement initial phase of lost log detection in Log Delivery for Non-CM logs.

- Poll logs from custlog file.
- Detect whether any logs have been lost.
- If lost logs detected, generate log to indicate lost log detection.

Enhance lost log indication mechanism for CM logs.

- Enhance Log Delivery so that an internal log is generated when a lost log scenario is detected for CM logs.

Enhance Log Delivery to support STD, SCC2, STD-OLD and SCC2-OLD formats with ECORE node id enabling and Dual Sequence numbering.

- Enhance Log Delivery to support LOG_OFFICE_ID enabling from SDM.
- Enhance Log Delivery to support ECORE Node Id enabling from SDM.
- Enhance Log Delivery to support Dual Sequence Numbering for logs.
- Enhance STD and SCC2 formats to incorporate the above enhancements (LOG_OFFICE_ID, ECORE Node ID, Dual Sequence Numbering).
- Retain the Pre-SDM20 behavior of Log Delivery with respect to formats.

Handle bursty generation of logs.

- Ensure that the new functionality does not adversely impact the Log Delivery performance and also ensure that the application stays in conformance to the specified limits.

Feature Description

Introduction

As mentioned above, the main task of this feature consists of

- Implementing code changes to make Logroute CLUI more user-friendly.
- Upgrading all SDM applications to use GenCustLog API version 2 to generate custlogs.
- Implementing initial phase of lost log detection in Log Delivery for Non-CM logs.
- Enhancing the lost log indication mechanism for CM logs.
- Enhancing Log Delivery to support STD, SCC2, STD-OLD and SCC2-OLD formats with ECORE node id enabling and dual sequence numbering.
- Handling bursty generation of logs.

Enhancing Logroute CLUI

Logroute tool used for configuration of device and log routing information. This information is used to collect the data in the desired format (STD or SCC2) and send the collected logs to the configured destination. The tool can also be used for configuring the device such that it receives only the desired logs.

Currently the Logroute tool is not very user-friendly (as described previously). This feature seeks to enhance the Logroute tool, so that the user is able to obtain or modify the information more easily.

The enhanced user interface is explained in more detail in the configuration section of this feature.

Upgrading SDM applications to use GenCustLog API version 2 to generate custlogs.

Enhancement to SDM log generation API

On the SDM, the SDM Log Generation (SLG) API will be upgraded to generate the new custlog format GenCustLog version 2. This new custlog format will enhance the content of the logs flowing through syslogd and stored in custlog to include the following data.

- Node Id:- Identifies where the log originated.
- Host Name:- Identifies the machine which generated the log.
- Application Name:- The application which generated the log.
- Sequence Number:- The number of the log which the application has generated.

To initialize and generate the above data, the following options are provided.

- `init_cust_log`:- This function is used to set/reset the sequence number and application name of a particular application.
- `gen_cust_log_v2`:- This function is used by the applications to generate custlogs in the new GENCustLog Version 2 format.
- `gen_foreign_cust_log_v2`:- This function is used by applications that generate a custlog on behalf of a remote system.

Updating all SDM applications

The SDM applications will be updated so that they will call the GenCustLog Version 2 function to generate a custlog.

As part of this update, the application will provide the application name as one of the parameters of the new CustLog version. The application name must be unique.

Implementing initial phase of lost log detection for Non-CM logs

This requirement is achieved by implementing a new lost log detection functionality.

- Create a cache (data structure) to store the latest Hostname, Application name and Sequence number of the custlog generated by each application.

Example of cache storage.

Hostname	Application name	Sequence Number
SDM	GDD	0005
GWC	NULL	0010
SDM	Log Delivery	0090
SDM	OMDD	8768
KEY		

- Log Delivery polls for logs in the custlog file and retrieves the logs.
- While formatting the logs, retrieve the Host name, Application name and Sequence number of the log.
- If the Sequence number of the log has been set to zero abruptly, the LAQ recognizes it as a reset log for that application. accordingly it re-initializes the application details in the cache.

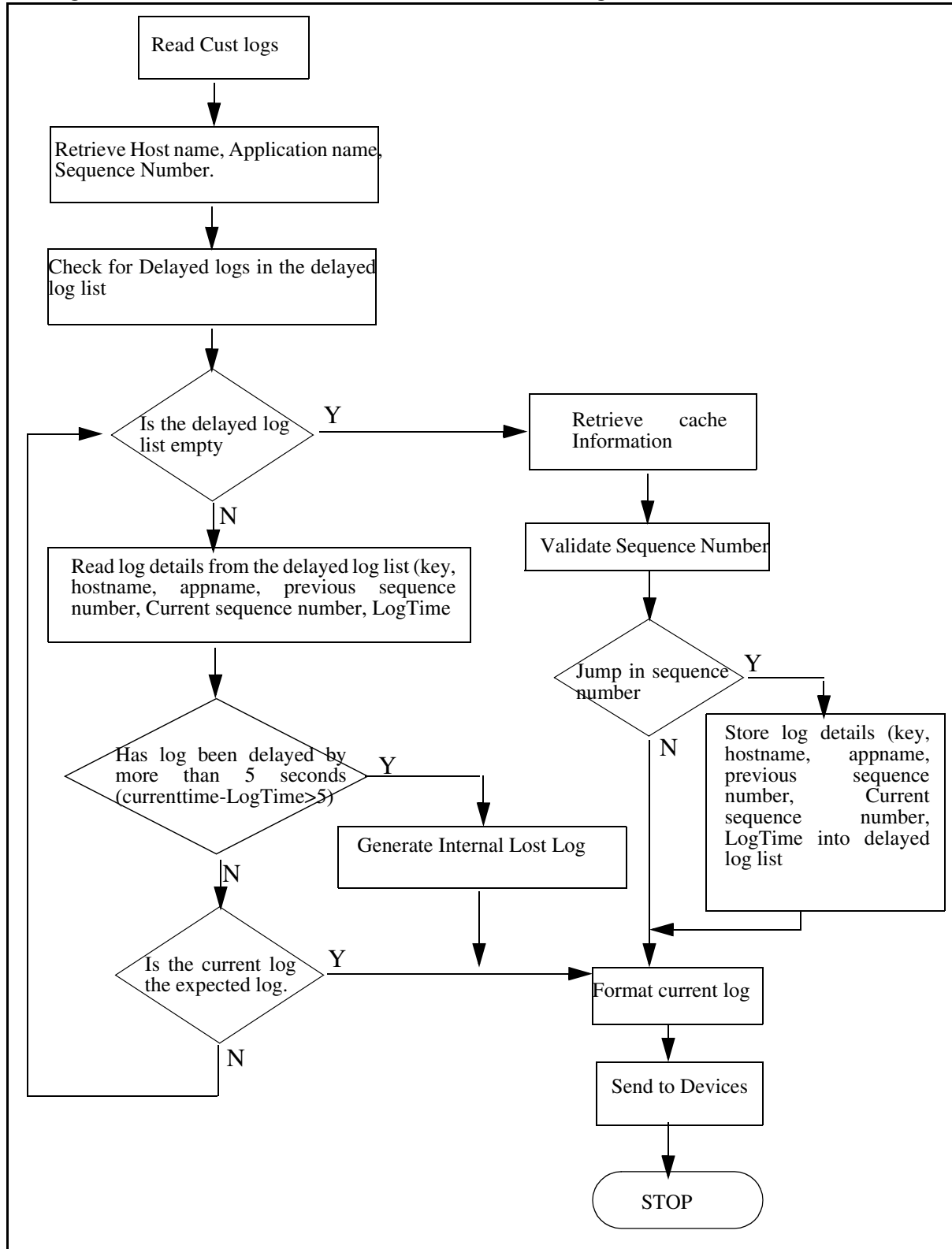
- Validate the sequence number retrieved from the log to the sequence number stored in the cache.
- If the sequence number is found to be breaking the flow (i.e it has skipped by more than one number). Then it is assumed that the following events could have happened.
 - a. The logs missing could have been lost.
 - b. The logs have arrived out of sequence and the missing logs can be expected to arrive immediately.

In order to take the above scenario into consideration, the details of the latest log (Key, hostName, appName, previous sequence number, current sequence number) received are stored as a list in a RWSlistCollectables structure “RWDelayedLogCheckList” along with the time when the log was received. When the next log is received, the following steps are followed.

- i. The list is checked to see if the log is an expected log or not.
- ii. If the log is expected then it is generated.
- iii. If the LAQ does not receive the log in less than 5 seconds, an internal log is generated to indicate that a log has been lost.

If LAQ detects that a lost log scenario exists, it will generate a “<number> Logs lost for application <application name> on host <hostname>” log, else it will increment the sequence number.

If the search is not successful, LAQ assumes that log is the first log from that application and accordingly inserts the log details into the RogueWave structure.

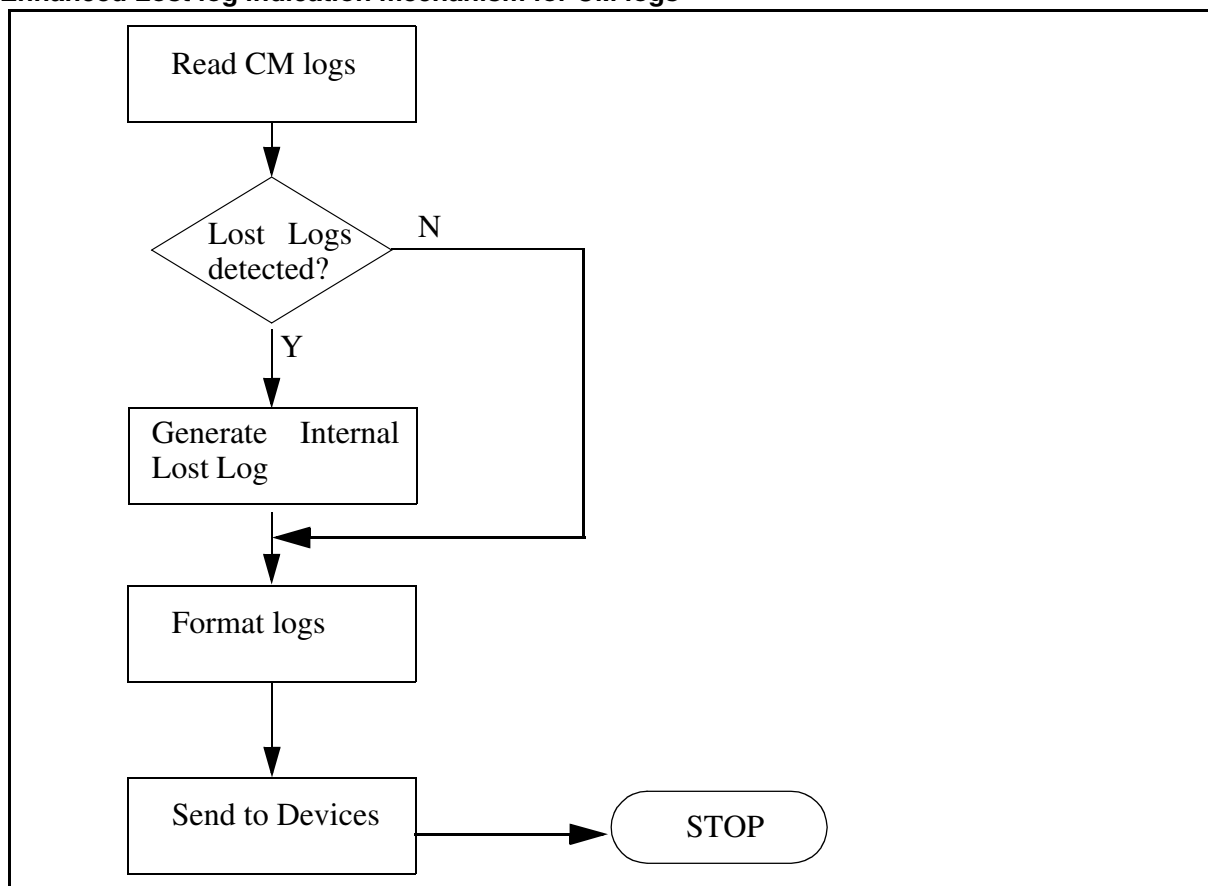
Lost log detection and indication mechanism for Non-CM logs

Enhancing the lost log indication mechanism for CM logs.

The current lost log indication mechanism existing for CM logs is enhanced as shown in the following figure.

- Log Delivery application detects a lost log scenario.
- The application generates an internal log indicating the number of logs lost.
- The internal log is passed to the OSF to be sent to all the devices.

This will ensure that the user will be informed regarding lost logs immediately.

Enhanced Lost log indication mechanism for CM logs

Enhancing Log Delivery to support STD, SCC2, STD-OLD and SCC2-OLD format with ECORE node id enabling and Dual Sequence numbering.

LOG_OFFICE_ID enabling

The LOG_OFFICE_ID parameter currently existing on the core will henceforth be configured from the “Global Parameters” level of the logroute tool. This parameter will be the same for all logs and streams. The LOG_OFFICE_ID will be configured as shown in the following figure.

Logroute tool for configuring LOG_OFFICE_ID option.

Global Parameters	
1 - LOG_OFFICE_ID	: BRISC315BH
2 - Buffer size (number of logs)	: 150
3 - Reconnect timeout value (secs)	: 15
4 - Lost logs threshold (NT only)	: 100
5 - Incoming end of line character	: 10
6 - Outgoing end of line characters	: 10 13
7 - Start of log characters	: 10 13
8 - End of logs characters	: 10 13
9 - Number of days to keep log files	: 5
10 - Maximum size of a log file (Meg)	: 40
11 - Maximum size action	: STOPDEV
12 - Help	
13 - Return to Main Menu	

Select Option ==> **1**

Enter Log_office_Id [CORE-COMPAT]==> **BRISC315BH**

Ecore node id enabling

In order to provide the Ecore Node Name for all the logs, the option shall be provided on the SDM through the Logroute tool.

The option to set the **Ecore** ON/OFF is to be on a per-stream (device) basis and will be provided through the logroute tool. For example, if the user is configuring a TCP-IN device, the device parameters needed for configuring are as shown in the following figure.

Logroute tool for configuring Ecore option.**TCP-IN Device**

- 1 - REMOTE IP : any
- 2 - PORT : 8550
- 3 - FORMAT : STD
- 4 - Ecore : ON**
- 5 - Log Routing
- 6 - Help
- 7 - Return to Main Menu.

Select Option :- 4

Enter Ecore option (ON or OFF) ==> ON

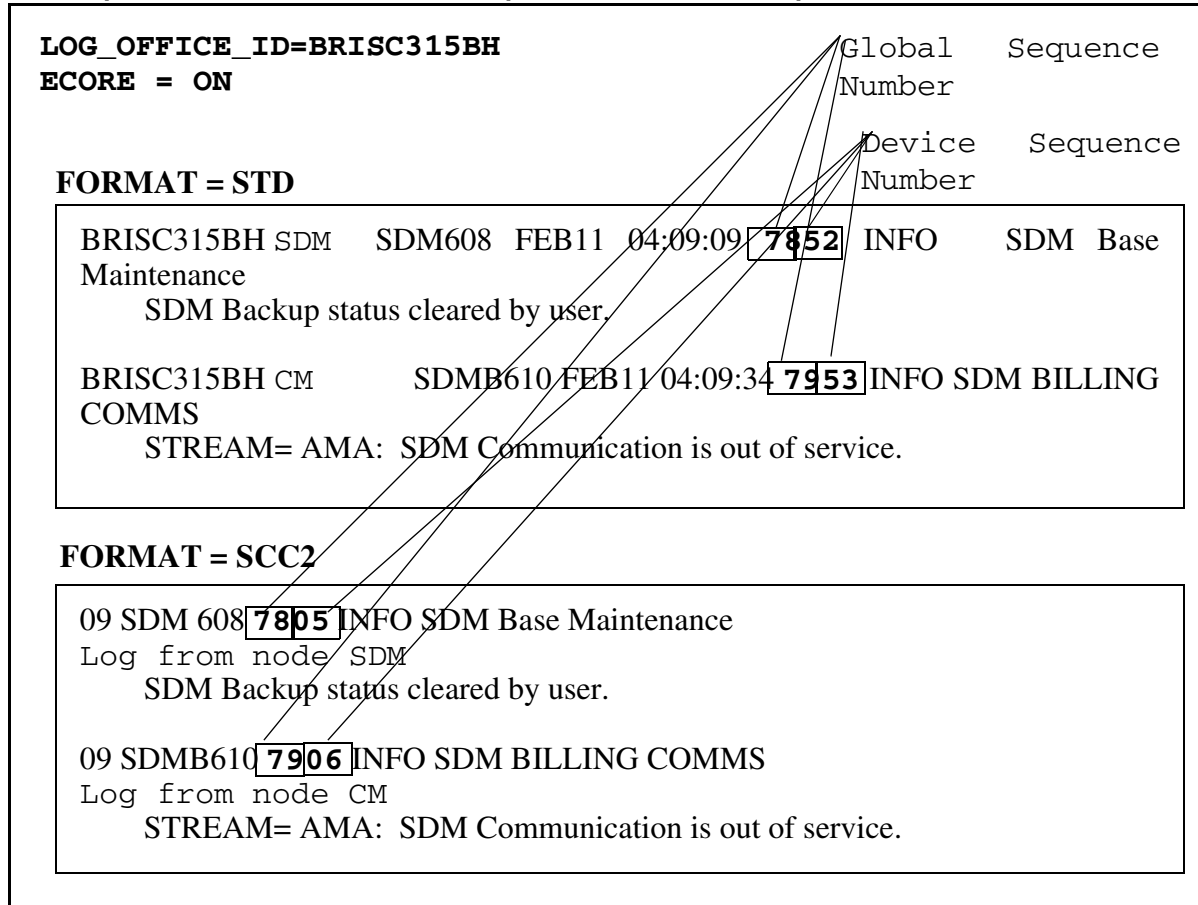
Dual Sequence Numbering

The sequence number field will be implemented as two distinct fields that will be incremented from 0 to 99.

Global Sequence number as a field of 2 digits (from 0 to 99) and
Device Sequence number as a field of 2 digits (from 0 to 99).

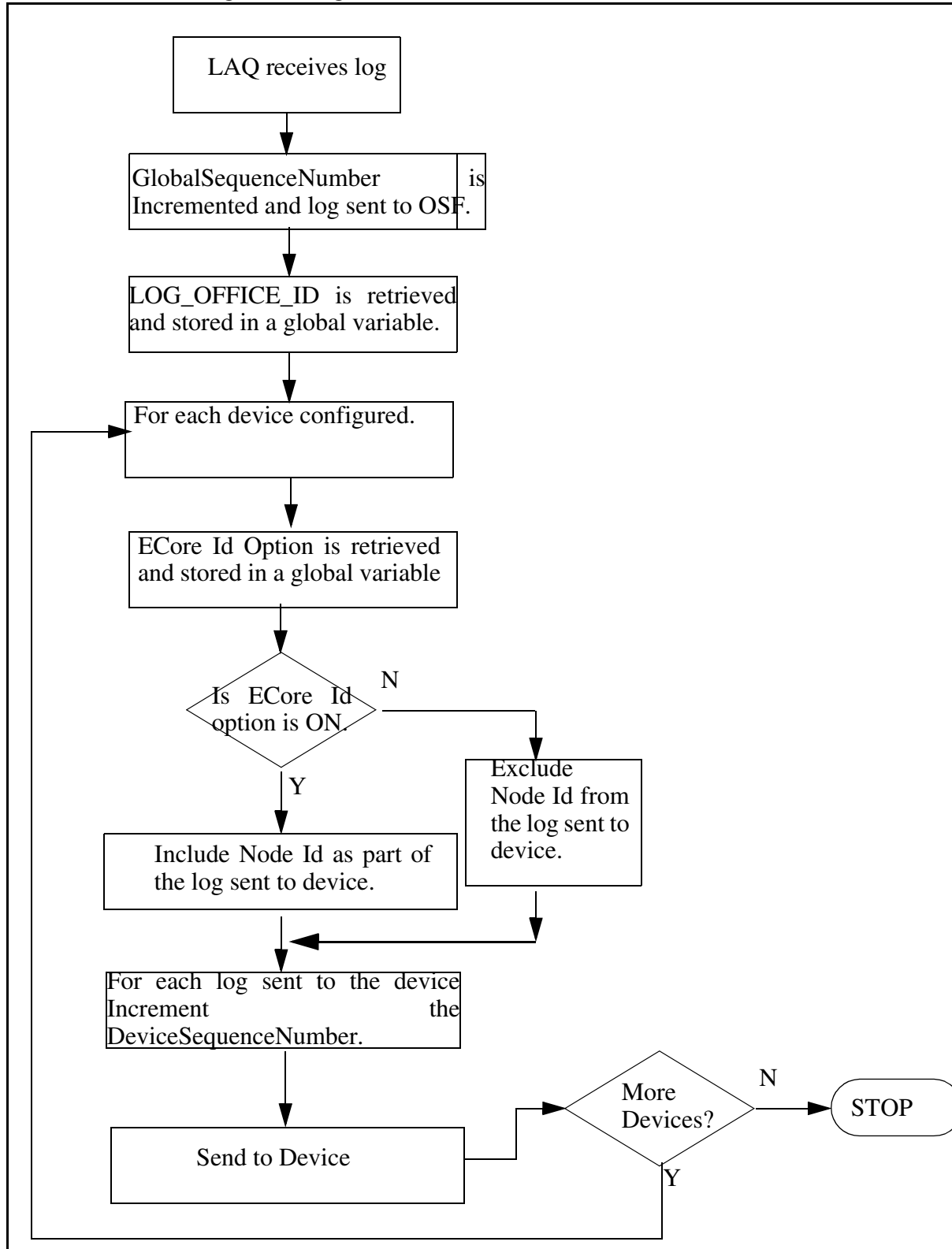
The Global Sequence number of the log will be the same for all the devices and the device sequence number varies based on the device. The LAQ will generate the Global Sequence number and the OSF will generate the Device Sequence number for all logs. These number have a maximum value of 99 after which they are reset to 0.

The following diagram illustrates the usage of the Global Sequence number and the Device Sequence number

OSF output when Global and Device sequence numbers are implemented.**Update current formats to support proposed changes**

The following changes will be made to Log Delivery to support the ECore Node Id and Dual Sequence numbering.

- When the LAQ receives a new log, the Global Sequence number will be retrieved, incremented and stored.
- After formatting the log, LAQ will send the log to the OSF. Upon receiving the log, the OSF will retrieve LOG_OFFICE_ID and ECore node id option.
- If the Ecore option is ON, then the node name which is part of the log information received by OSF will be included in the log sent to the device.
- If the Ecore option is OFF, then the node name is ignored.
- For each log which is to be sent to the particular device, the corresponding device sequence number is retrieved and incremented.
- The data is then updated into the log information and sent to the device.

New mechanism for log formatting

Retain the Pre SDM20 behavior of Log Delivery.

The Pre SDM20 behavior of Log Delivery will be retained in the new formats STD_OLD and SCC2-OLD. Users who wish to receive logs without the above changes can select the format to be either STD-OLD or SCC2-OLD.

Handling bursty generation of logs.

This feature ensures that the new functionality does not adversely impact the Log Delivery performance and also ensures that the application conforms to the specified limits

Hardware Requirements or Dependencies

- Fault tolerant SDM with SDM20/CS2E07 load.
- CM (XACORE / BRISC / 3PC)
- Succession Network Elements like GWC, MDM.
- NSDM

Software Requirements or Dependencies

- Connectivity between various Network Elements and SDM should be up.
- Connectivity between SDM and CM should be up.

Limitations and restrictions**Interactions****Applicable customer facing sections**

Fault Management

Logs ☒Alarms ☐

Configuration

Data Schema ☐User Interface ☒Element Management ☐Security ☐Service Order ☐Office Parameters ☒

Accounting (includes AMA billing)	_____
Performance (includes operational measurements)	_____
Real-time	_____
Engineering Information	___X___

Glossary

Term	Description
API	Application Programming Interface
OSF	Operation System Interface
LAQ	Log Acquisition
CLUI	Command Line User Interface
NE	Network Element
OSS	Operation Support System
DMS	Digital Multiplex System
CPU	Central Processing Unit
MDM	Multi-Service Data Manager
CM	Computing Module
SDM	SuperNode Data Manager
SSPFS	Succession Solaris Platform Foundation Software
STD	Standard
SCC2	Switching Control Centre 2
STD - OLD	PRE-SDM20 STD format Compatible
SCC2 - OLD	PRE-SDM20 SCC2 format Compatible

Product = CS 2000

A00002008 -- CBM Introduction (Succession on DMS)

Description

This document will be broken into two sub sections. The first sub section will describe **Adding a Logical volume for SBA**. The sub section second will describe the procedure for **DVD Billing record backup**.

Adding a Logical volume for SBA

For AIX:

- The instructions have not changed and can be found in Accounting module, chapter, “Adding a logical volume for SBA”
- Alternatively, the “makelv” command described below for CBM can also be used on AIX to create a Logical Volume for SBA billing files
- The recommended “logical_volume_name” remains the same on AIX: “/sba/<stream name>”.
 - i.e. /sba/ama;

For CBM:

- the “makelv” command can also be used on CBM to create a Logical Volume for SBA billing files. Consult the configuration section for the actual instructions on how to do this.

DVD Billing record backup

The purpose of this subsection is to describe a manual procedure for backing up billing data from the CBM to a DVD. Three procedures will be described. The First procedure will be how to blank a DVD-RW disk. The Second procedure will be what the customer will do to back up the closed sent and closed not sent billing directories using a script that is provided to them. The third procedure will document how to create a DVD without the aid of the script. This could be of use in emergency scenarios or when only specific files are to be backed up.

Note: These actions should be performed only during non-peak hours unless a DVD backup is an urgent in special case.

Note: It is worth pointing out that the tape functionality has been removed for the CBM(Solaris) system. Only DVD functionality is supported. And DVD functionality has not been added to SDM (FX) systems. Users of this system should continue to use the current tape backup procedure.

Note: It is necessary to be a root user to execute these procedures

Note: These are best effort procedures. No locking is done on the files being copied

Note: On a CBM850, if a swact occurs during any of the following procedures the action will fail and must be started again on the newly active side.

Blanking a DVD-RW

Blanking the DVD-RW erases the contents of the DVD. It is a necessary step before a DVD-RW can be written to if it has previously been written to. It is unnecessary and not possible to do this to DVD-R type DVDs.

Note: This procedure is not specific to billing. It is an sspfs general procedure.

- You first must insert the DVD-RW which you intend to blank into the DVD drive.
- First, issue the UNIX command “cdrw -l” (as shown below). If it returns a message indicating that there are no devices or media then use the eject button on the front of the DVD drive to open the tray. If the cdrw -l command lists a device then use the UNIX eject command to open the tray as explained in the next point

```
#> /usr/bin/cdrw -l
```

- To open the a drive unit that has media already inserted in it use the UNIX eject command (as shown bellow). If the eject command does not work it may be the case that someone is in the DVD directory or another backup procedure is running.

```
#> /usr/bin/eject cdrom
```

- After successfully inserting your DVD, list the contents of the DVD-RW with the following UNIX command to ensure that it is the DVD you intend to blank.

```
#> /usr/bin/ls /cdrom/cdrom0
```

- If you are satisfied that this is the disc you intend to blank, then enter the following UNIX command. This step can take a significant amount of time to complete. possibly more than one hour.

```
#> /usr/bin/cdrw -b all
```

- To confirm the DVD is now blanked. Ensure the DVD is inserted. Then enter the UNIX command below. It should return some device information and the statement “Media is blank”

```
#> /usr/bin/cdrw -M
```

Using script to back up billing records

This is the procedure the craft person would most likely use to back up the closed sent and closed not sent directories. This method is non selective in the files that it chooses to back up. It backs up the entire contents of the selected

directories. It writes the files to the DVD in the following directory format “/ <Stream name> / <Directory name> / files”.

Note: This procedure does not move the files from closed not sent to closed sent

- The craft person should ensure that he/she has a large enough supply of blank DVDs at least one for each stream they intend to back up. possibly more if the streams are larger than 2GB. The script will alert the craft person as to the number of disks that are required for each stream before proceeding to write the records to the DVD. Note that the DVDs should be blank. Consult the blanking procedure if the DVDs are not blanked.
- You first must insert the DVD-RW which you intend to write into the DVD drive.
- First, issue the UNIX command “cdwr -l” (as shown below). If it returns a message indicating that there are no devices or media then use the eject button on the front of the DVD drive to open the tray. If the cdwr -l command lists a device then use the UNIX eject command to open the tray as explained in the next point

```
#> /usr/bin/cdwr -l
```

- To open the a drive unit that has media already inserted in it use the UNIX eject command (as shown bellow). If the eject command does not work it may be the case that someone is in the DVD directory or another backup procedure is running.

```
#> /usr/bin/eject cdrom
```

- The next step is to enter sbadvdwrite at a UNIX prompt to start the script. you will get the following result

```
#> sbadvdwrite
```

```
Billing Data DVD Backup
```

```
-----
```

```
This is a utility to back up closed sent and closed not sent billing records.
```

```
A blank DVD should be in inserted in the DVDRW drive.
```

```
Press Enter to proceed, or type Abort to abort:
```

- Then press enter to proceed or abort to stop the scripts execution
- Next you will be asked to select the stream you would like to back up as is shown in the following result. If no streams are configured the script will print out and error message stating so and exit.

```
Billing Data DVD Backup Stream Display
```

The following streams are available to be backed up.

AMA
OCC
SMDR

Billing Data DVD Backup Stream Selection

>AMA

Enter the stream that you would like to back up and hit return.

- Now enter the stream that you would like to back up or abort to stop the scripts execution.
- Then press enter to proceed or abort to stop the scripts execution
Press Enter to proceed, or type Abort to abort:
- Next you will be prompted for which directories you would like to back up. Make your selection.

Billing Data DVD Backup Directory Selection

enter the number corresponding to the directory(s) that you want backed up
and hit return:

- 1 - Closed Sent
- 2 - Closed Not Sent
- 3 - Both Closed Sent and Closed Not Sent

>3

Closed sent and Closed Not Sent have been
selected for backup.

Press Enter to proceed, or type Abort to abort:

- Then press enter to proceed or abort to stop the scripts execution
- Then you will be advised of the number of DVDs that will be required to back

'I' blank DVD(s) will be required.

Press Enter to proceed, or type Abort to abort:

- Then press enter to proceed or abort to stop the scripts execution
- Next the DVD(s) are written to. Follow the on screen instructions with regards to when to insert DVDs into the DVD tray if more than 1 DVD is required. The DVD tray will eject automatically when the DVD is finished being written to.

```
creating scratch /tmp/.tar 2046m d97
creating scratch /tmp/.iso 2048m d98
Looking for CD devices...
Checking for media...
Please insert a blank cd and hit <enter> OR type <abort>:
Checking for media...
Media is blank
Start cdwrite of /tmp/.tar/billingdir/, iso_space=/tmp/.iso.
Please wait...
executing /usr/bin/mkisofs -r -J -o /tmp/.iso/iso.img /tmp/.tar/billingdir/
Using P0403021.000;1 for /tmp/.tar/billingdir/closedSent/P040302182716AMA
(P040302182715AMA)
Using P0403021.001;1 for /tmp/.tar/billingdir/closedSent/P040302182715AMA
(P040
302182614AMA)
Using P0403021.002;1 for /tmp/.tar/billingdir/closedSent/P040302182614AMA
(P040302181113AMA)
Using P0403021.003;1 for /tmp/.tar/billingdir/closedSent/P040302181113AMA
(P040302181112AMA)
Using P0403021.004;1 for /tmp/.tar/billingdir/closedSent/P040302181112AMA
(P040302181011AMA)
Using P0403021.005;1 for /tmp/.tar/billingdir/closedSent/P040302181011AMA
(P040
302173310AMA)
Using P0403021.006;1 for /tmp/.tar/billingdir/closedSent/P040302173310AMA
(P040
302173309AMA)
Using P0403021.007;1 for /tmp/.tar/billingdir/closedSent/P040302173309AMA
(P040
302173108AMA)
Using P0403021.008;1 for /tmp/.tar/billingdir/closedSent/P040302173108AMA
(P040
302172307AMA)
Using P0403021.009;1 for /tmp/.tar/billingdir/closedSent/P040302172307AMA
(P040
```


302172306AMA)
Using P0403021.00A;1 for /tmp/.tar/billingdir/closedSent/P040302172306AMA
(P040
U302172205AMA)
Using P0403021.00B;1 for /tmp/.tar/billingdir/closedSent/P040302172205AMA
(P040
302165504AMA)
Using P0403021.00C;1 for /tmp/.tar/billingdir/closedSent/P040302165504AMA
(P040
302165503AMA)
Using P0403021.00D;1 for /tmp/.tar/billingdir/closedSent/P040302165503AMA
(P040
302165402AMA)
Using P0403021.00E;1 for /tmp/.tar/billingdir/closedSent/P040302165402AMA
(P040
302164901AMA)
Using P0403021.00F;1 for /tmp/.tar/billingdir/closedSent/P040302164901AMA
(P040
302164100AMA)
Using P0403021.00G;1 for /tmp/.tar/billingdir/closedSent/P040302164100AMA
(P040
302153832AMA)
Using P0403021.00H;1 for /tmp/.tar/billingdir/closedSent/P040302153832AMA
(P040
302153831AMA)
Using P0403021.00I;1 for /tmp/.tar/billingdir/closedSent/P040302153831AMA
(P040
302153730AMA)
35.63% done, estimate finish Wed Mar 3 16:29:21 2004
71.26% done, estimate finish Wed Mar 3 16:29:21 2004
Total extents actually written = 14049
Total translation table size: 0
Total rockridge attributes bytes: 2364
Total directory bytes: 6144
Path table size(bytes): 42
Max brk space used c000
14049 extents written (27 Mb)

Looking for CD devices...
Initializing device...done.
Preparing to write DVD
Writing track 1...done.
Finalizing (Can take up to 4 minutes)...done.
write /tmp/.tar/billingdir/ succeeds

```
cdwrite exiting with return code 0
removing scratch /tmp/.tar d97
removing scratch /tmp/.iso d98
```

Billing Data DVD Backup Finished

you have now completed the DVD backup operation. Please ensure all requested files have been written to the DVD(s)

- You have now completed the script based backup procedure. Label the DVD(s) with a CD/DVD safe pen and repeat until all of the required streams are backed up. When finished writing all disks use the ls command to confirm that all of the desired files have been copied and are of the correct size.

Manual procedure for writing to DVD

This is a procedure intended mainly for GNPS when they have been contacted by a customer to purge billing files. Probably due to down stream network connectivity problems. Or for a customer who wishes to back up specific files. The sbadvdwrite script is the preferred method for customers who intend to do general back ups

Note: This is not a billing specific procedure it is a general sspfs procedure

Note: This procedure does not move the files from closed not sent to closed sent

Note:

- You first must insert the DVD-RW which you intend to write into the DVD drive.
- First, issue the UNIX command “cdrw -l” (as shown below). If it returns a message indicating that there are no devices or media then use the eject button on the front of the DVD drive to open the tray. If the cdrw -l command lists a device then use the UNIX eject command to open the tray as explained in the next point

```
#> /usr/bin/cdrw -l
```

- To open the a drive unit that has media already inserted in it use the UNIX eject command (as shown bellow). If the eject command does not work it may be the case that someone is in the DVD directory or another backup procedure is running.

```
#> /usr/bin/eject cdrom
```

- Next you want to confirm that all of the data which you want to put on the DVD will fit. You will need to use the cd and ls UNIX commands as

follows. First use the `cd` command to set the current directory to the directory which contains the files you want to back up. In this case the files are in the `/export/tmatt/closedsent` directory, so the following command is issued.

```
#> cd /export/tmatt/closedsent
```

Next use the `ls` command as follows. This command lists all of the files in the current directory. The size of the files in bytes is listed in the fifth column of the output (in bold below). Add the size of each file you intend to back up together and ensure that the total size of all files does not exceed 2000000000 bytes. If it does you will need to use more than one DVD. Divide the files up to make the most efficient use of each DVD.

```
#> /usr/bin/ls -l
total 270524
-rw-r--r--  1 maint  maint 7034800 Feb  3 16:56 data1
-rw-r--r--  1 maint  maint 4915002 Jan 26 18:55 data2
-rw-r--r--  1 maint  maint 10000000 Feb  2 15:21 data3
-rw-r--r--  1 maint  maint 57590000 Jan 23 11:59 data5
```

- Next you need to create a ISO9660 file system from the files you intend to back up. To do this you use the UNIX command `mkisofs`. Use it as follows. Where `<destination file>` is the name of the binary file that contains the ISO9660 file system. This is selected by the crafts person. `<pathspec>` represents the full path of the files that are to be backed up. It is very important to ensure that the directory in which you are creating the ISO9660 binary file has at least 2000000000 bytes of free space or the `mkisofs` command will fail.

```
#> /usr/bin/mkisofs -o <destination file> -a -J -L -R <pathspec>
```

For example if you wanted to create the `<destination file>` `/export/home/maint/tmatt/tempiso` out of the two files `data1` and `data2` from above you would issue the following UNIX command

```
#> /usr/bin/mkisofs -o export/home/maint/tmatt/tempiso -a -J -L -R
/export/tmatt/closedsent/data1 /export/tmatt/closedsent/data2
```

Note: this command will fail if the files in the path spec total more than 2000000000 bytes in size

- Next you will write the binary that you have created to the DVD. For this you will use the UNIX command `cdwr` as follows.

```
#> /usr/bin/cdrw -C -i <iso9660 file>
```

Where `<iso9660 file>` is the binary you just created above. So for example you would use the following command to write the Binary to the DVD.

```
#> /usr/bin/cdrw -C -i export/home/maint/tmatt/tempiso
```

- Now delete the iso9660 file which was created previously with the rm UNIX command as follows. This is an important step which allows you the regain disk space.

```
#> /usr/bin/rm export/home/maint/tmatt/tempiso
```

Software Requirements or Dependencies

N/A

Hardware Requirements or Dependencies

DVDRW must be installed in the system

Limitations and restrictions

none

Interactions

none

Applicable customer facing sections

Fault Management

Logs ___N___

Alarms ___N___

Configuration

Data Schema ___N___

User Interface ___N___

Element Management ___N___

Security ___N___

Service Order ___N___

Office Parameters ___N___

Accounting (includes AMA billing) ___N___

Performance (includes operational measurements) ___N___

Product = CS 2000

A00002009 -- Enhance display on PEPSET (Succession on DMS)

Functional Description

This feature activity is to migrate an existing line option, NAME24, from the MSL layer to the CCM layer.

NAME24 was created in the MSL layer under feature “Name Display Character Extension”. The documentations about the option creation are located in PLS DOC under names of AX1228 (CCM) and AX1240 (MSL).

NAME24 line option enables subscribers to provide a name up to 24 characters for their private network. This NAME will be displayed on a KSET at the other end of the call. The display format will be following:

NAME24 --- Top line

DN --- Bottom line.

A SOC will be associated with this feature in CCM. After the migration, NAME24 will be a SOCed line option in the CCM layer and a non-SOCed line option in the MSL layer.

The SOC will have two functionalities. It controls NAME24 line option processing and the display when NAME24 doesn't apply to the originator. See section 2.6, 2.7 and 2.8 for details.

The SOC_FTR_ ID for this activity is “00002009” with Order Code “MDC00075”

This feature activity involves changes to the MSL layer as well as the CCM layer. But the changes will not affect the behaviors of the existing Name Display Character Extension (NAME24) feature in the MSL layer.

Hardware Requirements or Dependencies

There is no hardware requirement.

Software Requirements or Dependencies

CCM20

Limitations and restrictions

- This display feature will only be applied to KSET phones.
- IVD sets will be supported in MSL as well.
- NAME24 is limited to inter-custgrp or intra-custgrp calls in the same switch.

Servord

Assignment

NAME24 can be assigned to a KSET via Servord ADO command. It also can be added to a line with NEW and COPYSET commands.

Since NAME24 works on top of NAME option NAME24 can only be assigned to a KSET that has NAME option on it or NAME option is going to be added to the line with NAME24 together. And NAME option can't be deleted if NAME24 option still presents on the line.

See Servord section for details and examples.

SO prompt

Here shows a simple assignment of this option in Servord. See the Servord section for more examples.

```
>ado
SONUMBER:  NOW  3 9 16 PM
>
DN_OR_LEN:
>7234532
OPTKEY:
>1
OPTION:
>name24
DISPLAY_NAME:
>name24on7234532
OPTKEY:
>$
COMMAND AS ENTERED:
ADO NOW 3 9 16 PM 7234532 ( 1 NAME24 NAME24ON7234532 ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
```

Interactions

Interaction with REASON

Since NAME24 provides a name up to 24 characters it preserves all spaces of the top line of the display phone for the name and moves DN to the bottom line.

When REASON option presents NAME24 will simply quit processing because the limited display space. The display will be the same as if NAME24 is not on the line.

Interaction with NAME feature

NAME24 works on top of NAME option. It overrides a name provided by NAME option for a specific network_id when it is appreciated.

Name Option - Up to two names

With NAME option two names can be datafilled for two different network ids. The name with network id matching the network_id of the call will be displayed.

The network_id of a call is determined by comparing two network_ids datafilled in table CUSTNTWK for the two parties in the call. If they are the same the network_id datafilled is the network_id of the call. If they are not the same or any one of them is not datafilled the “public” network_id is the network_id of the call.

NAME24 - Only one name

With NAME24 option on top of NAME option, a name up to 24 characters can be datafilled. It was intended to be used as a “private” name for people with long surnames.

In original design, NAME24 overrode any one of the two names datafilled by NAME option as its network_id matching the network_id of the call, which makes the two names for two different networks became one name for two different networks.

This activity will limit NAME24 only to override “private name” if it is datafilled by NAME option. This change will not affect MSL customers.

The following two tables summarizes the interactions with NAME option before and after this activity.

Datafills

	Party A	Party B	Party C	Party D
CUSTGRP	IBNTST	IBNTST	BNR	CLASSDSP
CSUTNTWK	PRIVATE	PRIVATE	PUBLIC	--
NAME option	private: Nice public: Nortel	private: Kevin public: Nortel	public: JCPenny	public: JCPenny
NAME24 option	Nice_PictureFrames	Kevin_Alex_Blazewski	JCPenny_CaryTown	JCPenny_Crabtree

NAME Display Two Names (without NAME24)

Calls	Network ID of the Call	Display on A	Display on B	Display on C	Display on D
A <-> B	private	Kevin	Nice	n/a	n/a
A <-> C	public	JCPENNY	n/a	Nortel	n/a
A <-> D	public	JCPENNY	n/a	n/a	Nortel
C<-> D	public	n/a	n/a	JCPENNY	JCPENNY

Before: NAME24 Overrides Two Names

Calls	Network ID Of the Call	Display on A	Display on B	Display on C	Display on D
A <-> B	private	Kevin Alex Blazejewski	Nice PictureFrames	n/a	n/a
A <-> C	public	JCPenny CaryTown	n/a	Nice PictureFrames	n/a
A <-> D	public	JCPenny Crabtree	n/a	n/a	Nice PictureFrames
C<-> D	public	n/a	n/a	JCPenny Crabtree	JCPenny CaryTown

After: NAME24 only Overrides Private Name

Calls	Network ID of the Call	Display on A	Display on B	Display on C	Display on D
A <-> B	private	Kevin Alex Blazejewski	Nice PicttrueFrames	n/a	n/a
A <-> C	public	JCPenny	n/a	Nortel	n/a
A <-> D	public	JCPenny	n/a	n/a	Nortel
C<-> D	public	n/a	n/a	JCPenny	JCPenny

Interaction with TCAPNM

NAME24 will not override TCAPNM but will display TCAPNM and DN in two separated lines.

NAME24 interacts with TCAPNM in the same way as NAME option. When it detects that TCAPNM applies to the line it will not check if the TCAPNM is retrieved successfully. If no TCAPNM is retrieved no name will be displayed.

Interaction with AUTODISP

NAME24 will display KEY# with DN on the bottom line of the display phone for incoming calls.

ALEXANDER BLAZEJEWSKI
KEY -1 6841000

Interaction with other features

The NAME24 will not work with features that require extra messages being displayed because of the limited display space. Also, NAME24 will not work with features that have their own specific name to be displayed.

When any one of following features is applied to the line NAME24 will quit its processing. The display will be the same as if NAME24 is not on the line.

- a. An E911 call.
- b. Attendant is attached to the call.
- c. Call is forwarded/redirected/transferred/pickUped
- d. The agent is an ACD agent
- e. Agent is a MADN

Move DN to the bottom line - Controlled by NAME24 SOC

Background -- DN being dropped from display

When only the Name and DN are going to be displayed and NAME24 does not apply to the originator, the Name and DN will be displayed on the same top line of the terminator's display phone, and the bottom line will be left empty.

There are some cases that DN will be dropped from display and the bottom line will be left empty on the terminator's display.

Without NAME24 option

- DN will not be displayed on the terminator if originator's Name + DN is over 15 characters long and terminator has a 2x16 display window
- DN will not be displayed on the terminator if originator's Name + DN is over 24 characters long and the terminator has a display window of 2x16 or 2x24.

With NAME24 option but NAME24 doesn't apply

- With NAME24 on the originator, if the terminator has a display window of 2x16, the DN will not be displayed on the terminator if the originator's Name + DN is over 15 characters long.

Why can't we use the bottom line to display DN for those calls?

NAME24 SOC shifts the DN to the bottom line on terminator

Since NAME24 works in the call environment that only NAME and DN are going to be displayed (except AUTODISP), it will display the DN on the bottom line on the terminator's display phone if NAME24 SOC is On, and NAME24 doesn't apply to the originator because of the following reason(s):

- The originator doesn't have NAME24 option on it.
- The originator has NAME24 option on it but the terminator has a display window of 2x16.
- The originator has NAME24 option on it but can not be displayed (possibly, the call is on the public network).
- The TCAPNM applies to the originator

Example:

- Party A (6137234532) has NAME option with a name of "abcdefghijklmno".
- Party B has a 2x16 display KSET,
- Party A calls party B
- Display on B:
 - NAME24 SOC Idle

ABCDEFGHIJKLMNO
<blank>

— NAME24 SOC On

ABCDEFGHIJKLMNO
61372134532

Applicable customer facing sections

Fault Management

Logs _NA_

Alarms _NA_

Configuration

Data Schema _X_

User Interface _NA_

Element Management _NA_

Security _NA_

Service Order _X_

Office Parameters _NA_

Accounting (includes AMA billing) _NA_

Performance (includes operational measurements) _NA_

Realtime _X_

Engineering Information _X_

Glossary

Acronym	Expansion of Acronym
PSET	Proprietary Business Set
KSET	Key Set
IVD	Integrated Voice and Data
MBS	Meridian Business Set
ISDN	Integrated Services Digital Network
CCM	DMS 100 Common Layer
MSL	Meridian Stored Logic
PLS	Product Library System
SOC	Software Optionality Control
CUSTGRP	Customer Group
CUSTNTWK	A table name in DMS

Acronym	Expansion of Acronym
IPL	Initial
PRIVATE	A network ID
PUBLIC	A network ID
IBNTST	A customer group name
BNR	A customer group name
CLASSDSP	A customer group name

Configuration for A00002009

Data schema (DS)

- Table KSETFEAT: The name up to 24 characters provided by this feature will be stored in this table.
- Table LCCOPTS: The list of compatible LCCs of this feature will be specified here.

Service Orders (SO)

Summary of service order impact

NAME24 must be added to a set via SERVORD.

Service order change details

- IDENTIFY any NEW LCC introduced by this feature:
None.
- IDENTIFY any NEW OPTIONS introduced by this feature:
NAME24.
- FOR EACH OPTION, list other options that must be assigned:
NAME option must be assigned for NAME24 option to work.

Line class code compatibility

Compatible LCCs in the CCM layer:

- PSET

- P_Phone
- M5008
- M5009
- M5208
- M5209
- M5112
- M5212
- M5312
- M5216
- M5316

Compatible LCCs in the MSL layer

- P_Phone
- PSET
- M5008
- M5009
- M5208
- M5209
- M5112
- M5212
- M5312
- M5216
- M5316
- M2008
- M2616
- M2216A
- M2216B
- M2008
- M2016s
- M2616ct.

Assignability

The following functionalities apply to this option:

- set functionality: <no>

- subset functionality: <no>
- DN functionality: <yes>
- key functionality: <no>

Option prerequisites

NAME24 has the following prerequisites:

NAME.

New Prompts

New Prompt

Prompt Text	Valid Input	Description	Areas Affected by Prompt
DISPLAY_NAME	Vector of up to 24 chars	This field is used to enter up to 24 characters to be displayed	OPTION

SERVORD examples**NAME option must be on the line**

```
>ado
SONUMBER:  NOW  3 4 9 PM
>
DN_OR_LEN:
>7502537
OPTKEY:
>1
OPTION:
>name24
DISPLAY_NAME:
>yourNameUpto24Characters
OPTKEY:
>$
COMMAND AS ENTERED:
ADO NOW 3 4 9 PM 7502537 ( 1 NAME24 TESTINGTSTINGTESTING1 ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
NAME24 CAN ONLY BE ADDED TO A LINE AFTER
THE NAME OPTION HAS BEEN ADDED .
```

—continued—

```
NAME24 did NOT pass checking.
*** ERROR - INCONSISTENT DATA ***
COMMAND AS ENTERED:
ADO NOW 3 4 9 PM 7502537 ( 1 NAME24 TESTINGTSTINGTESTING1 ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>n
```


Add NAME and NAME24 together

```
>ado
SONUMBER:  NOW  3 4 9 PM
>
DN_OR_LEN:
>7502537
OPTKEY:
>1
OPTION:
>name
NETNAME:
>public
DISPLAYNAME:
>NameForPublic
NETNAME:
>$
OPTKEY:
>1
OPTION:
>name24
DISPLAY_NAME:
>nameUpto24Characters
OPTKEY:
>$
```

—continued—

```
COMMAND AS ENTERED:
ADO NOW 3 4 9 PM 7502537 ( 1 NAME ( PUBLIC TESTING15 ) $ ) ( 1 NAME24
TESTINGTESTINGTESTING1 ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
```

Query the DN

```
>qdn 7502537
-----
DN: 7502537
TYPE: SINGLE PARTY LINE
SNPA: 909 SIG: N/A LNATTIDX: N/A
LINE EQUIPMENT NUMBER: HOST 00 0 18 19
LINE CLASS CODE: M5209 SET
KEY: 1
CUSTGRP: CGA SUBGRP: 0 NCOS: 0 RING: Y
CARDCODE: 6X21AC GND: N PADGRP: PPHON BNV: NL MNO: Y
PM NODE NUMBER : 67
PM TERMINAL NUMBER : 596
OPTIONS:
NAME PUBLIC NAMEFORPUBLIC 3WC CWI CWO
PIC C541 Y NAME24 NAMEUPTO24CHARACTERS CWT Y Y N 1 CFU N $ I 1 CWD PRL
```

Query table KSETFEAT

```
>table ksetfeat
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: KSETFEAT
>
>pos 0 0 18 19 name24
HOST 0 0 18 19 1 NAME24 NAME24 NAMEUPTO24CHARACTERS
```

Can't delete NAME if NAME24 is on the line

```
>deo
SONUMBER: NOW 3 4 9 PM
>
DN_OR_LEN:
>7502537
OPTKEY:
>1
OPTION:
>name
OPTKEY:
>$
COMMAND AS ENTERED:
DEO NOW 3 4 9 PM 7502537 ( 1 NAME ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
CANNOT DELETE NAME FROM A LINE IF NAME24 EXISTS.
NAME did NOT pass checking
*** ERROR - INCONSISTENT DATA ***
COMMAND AS ENTERED:
DEO NOW 3 4 9 PM 7502537 ( 1 NAME ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>n
```

Software optionality control (SOC)

- Option assignment via SERVORD will not be limited by the SOC states (On or Off).
- Option processing will be performed only when the SOC state is On.

SOC

SOC option name:	Enh Name/Num Dis
SOC option title:	00036430
SOC option control type:	state
New SOC option?	Yes
SOC option order code	MDC00075
Option defined in DRU:	CCM
Affected products:	CCM

Product = CS 2000

A00002011 -- Virtual Office Worker (Succession on DMS)

Functional Description

The intent of this activity is to migrate the Virtual Office Worker (VOW) software from the MSL DRU into the CCM DRU.

The function of the VOW software is not changing as a result of this feature with the exception that it will now be available to all DMS-100 customers instead of limited to MSL-100 PBXs. Also, the function of the VOW feature will be controlled by SOC for those customers who are not using MSL-100 loads.

What follows is essentially a cut/paste of the original feature FN with several updates and corrections for items that were found during designer and product verification test phases.

For reference purposes, the original FN can be found in the PLS DOC library under AX1236FN.AA20.

Feature synopsis

This feature will allow telecommuters who do not have dedicated physical phone sets to access their dedicated Directory Number (DN) and associated

features/options by logging into their dedicated DN from any of a pre-designated group of phone sets. Once logged in, all features and options will operate normally, and all calls to the dedicated DN will terminate to the set on which the login occurred. Also, when logged in, all calls originated from the set will be billed to the dedicated DN.

Functional overview

This feature will meet the needs of Virtual Office Workers (VOWs) on a DMS-100 or MSL-100 PBX. A VOW is an individual, such as a telecommuter, who periodically visits an enterprise office location but does not have dedicated office space. VOWs typically retain various services including a dedicated DN, voice mail, departmental billing, and features specific to their set configuration. VOWs often reside in temporary cubicles or shared workspaces when visiting the office, yet they also desire the use of their dedicated DN and associated features. Prior to this functionality, no simple means existed by which VOWs could access their dedicated DN and features from these temporary workspaces that were not specifically tailored for any user.

This feature will enable a VOW to access his/her dedicated DN and features from any of a pre-designated group of Meridian Business Set (MBS), Integrated Voice and Data (IVD), or Integrated Business Network (IBN) phone sets. This includes being able to access any features and associated data which might be assigned to his/her set, as well as being able to both originate and receive calls using his/her dedicated DN. With this feature, a VOW will be able to login to or logout from his/her dedicated DN from any in the group of pre-designated sets. Support and functionality for provisioning, operational measurements, and logs will also be provided.

In general, there will not be a one-to-one relationship between VOWs and the physical sets used to access dedicated DNs and features. As an example, there may be 15 pre-designated sets for a particular customer group, allowing 15 VOWs to access their dedicated DN and features at a time. If all VOWs in this customer group only require access to their dedicated DN and features one day a week during a 5-day work-week, then with the proper coordination, these 15 physical sets could support up to 60 VOWs each week.

Feature description

VOW Setup

To begin with, ensure that feature SOC MDC00076 is turned ON for the office. Note that the SOC is always ON for MSL-100 load types.

In order for VOW to function, the following must be datafilled/provisioned for each customer group that allows VOW functionality:

- In table CUSTSTN, feature VOWDN must be datafilled. The CUSTSTN tuple contains the following:

- NCOS and SUBGRP values for translations purposes on the pre-designated VOW sets when no VOW is logged in;
 - A boolean value specifying whether or not the VOW authorization code is required within the associated customer group during use of the VOWIN feature access code;
 - A boolean value specifying whether the personal (SW) authorization code is required within the associated customer group during use of the VOWIN feature access code;
 - A boolean value specifying whether the associated customer group is to be audited, and if so, a value specifying the hour of the day the audit is to occur;
 - A boolean value specifying whether or not VOW functionality interacts with call forwarding functionality to enable call forwarding for a VOW when s/he logs out and to disable call forwarding for a VOW when s/he logs in;
 - The length of the VOW personal ID code (referred to as passcode throughout the remainder of this document) length values used to uniquely identify a VOW within a customer group; and,
 - The line class code of the sets which will make use of VOW functionality.
- In table IBNXLA, feature translators VOWIN, VOWOUT, VOWPCC, and VOWROUT must be datafilled.
 - In table AUTHCDE, VOW and SW authorization codes must be datafilled if these authorization codes are enabled through the VOWDN tuple in table CUSTSTN. These will be used during use of the VOWIN feature access code.

Within the customer groups that are to offer VOW functionality, a VOW's dedicated DN and features must be provisioned on a phone set pre-designated for use with VOW functionality. On this set, the line option VOW must be assigned. Assignment of the VOW line option includes the specification of the initial passcode for the associated VOW. Once assigned, the VOW will be logged into his/her dedicated DN and features. In other words, when initially assigned, the VOW's dedicated DN and features will still be associated with the physical set on which they were provisioned prior to the assignment of the VOW line option until the VOW logs out, or is logged out by the VOW audit.

The value of the passcode associated with the VOW line option must have a length matching the PCCLLEN value in the associated VOWDN tuple in table CUSTSTN. Once a VOW's passcode has been set, it can be changed by the user through the use of the VOWPCC feature access code in table IBNXLA or by switch personnel by changing the VOWPID field in the appropriate tuple in table VOWINV. When changed, the passcode must still have a length

matching the PCCLN value in the associated VOWDN tuple in table CUSTSTN.

If the value of the PCCLN field in the VOWDN tuple in table CUSTSTN changes, the associated VOWPID fields in table VOWINV will immediately be impacted. If the PCCLN value is changed to a smaller value, then the VOWPID values for VOWs in the corresponding customer group will be truncated to match the new PCCLN value (e.g., changing the PCCLN value from 6 to 4 will change a VOWPID value of '123456' to '1234'). If the PCCLN value is changed to a larger value, then the corresponding VOWPID values will be right-padded with zeros up to the new PCCLN value (e.g., changing the PCCLN value from 6 to 8 will change a VOWPID value of '123456' to '12345600').

Note: If the PCCLN value for a customer group is changed, all VOWs within the corresponding customer group must be notified of the resulting impact to their passcode values. If this notification does not occur, the VOWs within the customer group will not be able to log in.

Also, all pre-designated sets that are to be used by VOWs need to have the VOWDN line option assigned within the customer groups that are to offer VOW functionality.

Switch personnel can log a VOW in or out of his/her dedicated DN and features through the use of CKLN/CLN Servord commands. In these scenarios, the CKLN/CLN commands work as they would normally, but a VOW LEN is provided as either the source or target LEN of the change LEN command.

Practical VOW setup example

VOW is a fairly flexible feature in nature. There are a variety of methods which could be used to setup the feature and get started using it. Unfortunately, this flexibility can lead to confusion. To help alleviate this confusion, a simple, practical example is provided below.

This example demonstrates how telephone company switch personnel might create a group of 2 VOWDN “drop-in” sets which are to be shared by 4 real VOW users.

1. For non MSL loads, turn on the feature SOC MDC00076.
2. Datafill a VOWDN feature tuple in table CUSTSTN.
3. Datafill the VOWIN, VOWOUT, VOWPCC, and VOWROUT feature translators in table IBNXLA.
4. Datafill VOW and SW tuples in table AUTHCDE if required in the CUSTSTN tuple.

Note: For more information on table datafill for CUSTSTN, IBNXLA, and AUTHCDE, see section “VOW Setup” on page 220, or refer to the Appendix B, the Data Schema section in this document.

5. Choose 2 blank lens which will eventually be used as the “drop-in” phones.
6. Using one of the blank lens, use the Servord NEW command to create the real set data for 1 of the VOW users. Add the VOW line option when the set is being created.
7. Using CKLN/CLN, move the newly created VOW user to a VOW len (VOW x y).
8. Repeat steps 6 and 7 until all 4 VOW users real set data has been defined and moved to a free VOW len.
9. Now use the Servord NEW command again to create the set data for the 2 “drop-in” phones using the same 2 blank lens. Add the VOWDN line option when the set is being created.

At this point, the 2 VOWDN “drop-in” phones are ready to take/receive calls or to be used to login any of the 4 VOW users via the VOWIN access code.

It should be noted that at the moment that a VOW user is logged in at one of the VOWDN “drop-in” phones, a new VOWDN tuple will appear in table DNROUTE. This tuple can be considered as a placeholder for the VOWDN information. As soon as the VOW user logs back out, the DNROUTE tuple is removed, and the VOWDN information is restored to the physical line.

VOW Login

On a set with the VOWDN line option assigned, a VOW performs the following steps to log in:

1. Go off-hook.

Note: A VOWDN set which does not have a logged in VOW user will receive stutter dial tone when going off hook.

2. Upon receipt of stutter dial tone, dial the VOWIN feature access code datafilled in table IBNXLA (e.g., ‘*80’) against the appropriate customer group.

3. Upon receipt of dial tone, dial the VOW authorization code datafilled in table AUTHCDE (e.g., '7654321') against the appropriate customer group and NCOS. The length of this authorization code is specified in table AUTHCDE. If a mistake is made when entering the VOW authorization code, pressing the '*' key will restart collection of the VOW authorization code.

Note 1: This step is required only if the use of the VOW authorization code is enabled through the VOWDN tuple in table CUSTSTN for the corresponding customer group.

Note 2: Use of authorization codes can require an ACCT code depending on the datafill for AUTH in table CUSTHEAD. If required, the ACCT code must be appended to the AUTH code.

4. Upon receipt of dial tone, dial the personal (SW) authorization code datafilled in table AUTHCDE (e.g., '1234567') against the appropriate customer group and NCOS. The length of this authorization code is specified in table AUTHCDE. If a mistake is made when entering the personal authorization code, pressing the '*' key will restart collection of the personal authorization code.

Note 3: This step is required only if the use of the personal (SW) authorization code is enabled through the VOWDN tuple in table CUSTSTN for the corresponding customer group.

Note 4: Use of authorization codes can require an ACCT code depending on the datafill for AUTH in table CUSTHEAD. If required, the ACCT code must be appended to the AUTH code.

5. Upon receipt of dial tone, dial the PDN for the VOW set data to whose passcode is being modified (e.g., '2149975005'). If a mistake is made when entering the PDN, pressing the '*' key will restart collection of the PDN.

Note: The PDN must be entered as a 10 digit number.

6. Upon receipt of dial tone, dial the passcode unique to that VOW (e.g., '9975056449'). The length of this passcode is specified in table CUSTSTN in the VOWDN tuple associated with the customer group. If a mistake is made when entering the passcode, pressing the '*' key will restart collection of the passcode.

At this point, logs will be generated and OMs will be pegged to indicate a successful login attempt. If an error occurred, either due to user input or otherwise during any of the above steps, OMs will be pegged to indicate that an error occurred during a login attempt, and the set will return to an idle state.

If successfully logged in, the VOW will be able to make and receive calls using the dedicated DN that would then be associated with the VOW set on which the login took place. Also, any features previously provisioned against the dedicated DN will operate normally, retaining any settings from the previous logout.

Once logged in, the VOWs dedicated DN and associated data will be associated with a physical LEN, as illustrated below in sample QLEN output.

```
>qlen 9975121
```

```
-----
LEN:      HOST 0 0 0 1
```

```
TYPE: SINGLE PARTY LINE
```

```
SNPA: 214
```

```
DIRECTORY NUMBER:      9975121
```

```
LINE CLASS CODE:  M2016S
```

```
CUSTGRP:      BNRRCH  SUBGRP: 0  NCOS: 0  RING: Y
```

```
CARDCODE:  8D02AB  GND: N  PADGRP: NPDGP  BNV: NL  MNO: Y
```

```
PM NODE NUMBER      :      55
```

```
PM TERMINAL NUMBER :      33
```

```
OPTIONS:
```

```
CWI VOW
```

```
CFD F 5122 I 1 2 CWT Y Y N 1 2
```

```
KEY      DN
```

```
---      --
```

```
1      DN      9975121
```

```
KEY      FEATURE
```

```
---      -
```

```
1      CFD F      5000      I 1 2
```

```
4      CWT Y Y N 1 2
```

```
-----
```

Furthermore, some changes will be seen in tables VOWINV and DNROUTE once the VOW user is successfully logged in. In table VOWINV, the VOWDN tuple is removed. The VOW agent DN is now linked to the VOWDN set physical len in the VOW tuple. The same tuple also shows the LOGGEDIN bool as 'Y'. In table DNROUTE, a DN placeholder tuple has been created to store and reserve the VOWDN set DN until the VOW user logs out.

VOW Logout

On a set with the VOW line option assigned, a VOW performs the following to log out:

1. Go off-hook.
2. Upon receipt of dial tone, dial the VOWOUT feature access code datafilled in table IBNXLA (e.g., '*81') against the appropriate customer group.

At this point, logs will be generated and OMs will be pegged to indicate a successful logout attempt. If an error occurred either due to user input or otherwise during any of the above steps, OMs will be pegged to indicate that an error occurred during a logout attempt, and the set will return to an idle state.

If successful, the VOW will be logged out. Calls can terminate on or be originated from the set on which the logout attempt took place. All data, including the dedicated DN and features, associated with the VOW who just logged out will be completely disassociated with the set.

At this point, the VOWDN set will now deliver stutter dial tone upon going off hook in order to denote that no VOW user is logged in at that set.

Once logged out, the VOWs dedicated DN and associated data will not be associated with any physical LEN. Instead, it will be associated with a VOW logical terminal as illustrated below in sample QLEN output. Similarly, when logged out, the pre-designated VOW set returns to the standard line with VOWDN option.

```
>qlen 9975121
```

```
-----
LEN:      VOW 1 1
TYPE: SINGLE PARTY LINE
SNPA: 214
DIRECTORY NUMBER:      9975121
LINE CLASS CODE: M2016S
CUSTGRP:      BNRRCH SUBGRP: 0 NCOS: 0 RING: Y
CARDCODE: NOT APPLICABLE GND: N PADGRP: NPDGP BNV: NL MNO: N
OPTIONS:
CWI VOW
CFD F 5122 I 1 2 CWT Y Y N 1 2

KEY      DN
---
```

```

1          DN          9975121

KEY        FEATURE
---        -
1          CFD F          5000          I  1  2
4          CWT Y Y N  1  2

-----
>qlen HOST 0 0 0 1

-----
LEN:      HOST 0 0 0 1
TYPE: SINGLE PARTY LINE
SNPA: 214
DIRECTORY NUMBER:      9975122
LINE CLASS CODE: M2016S
CUSTGRP:      BNRCH  SUBGRP: 0  NCOS: 0  RING: Y
CARDCODE: 8D02AB  GND: N  PADGRP: NPDGP  BNV: NL MNO: Y
PM NODE NUMBER      :      55
PM TERMINAL NUMBER :      33
OPTIONS:
DTM VOWDN $

KEY        DN
---        -
1          DN          2149975900

KEY        FEATURE
---        -
1  VOWDN

-----

```

Furthermore, some changes will be seen in tables VOWINV and DNROUTE once the VOW user is successfully logged out. In table VOWINV, the VOWDN tuple is restored. The VOW agent DN is now associated with the VOW virtual len in the VOW tuple. The same tuple also shows the LOGGEDIN bool as 'N'. In table DNROUTE, the DN placeholder tuple previously created has now been removed.

VOW Passcode Change

On a set within the same customer group on the same switch as the VOW's set data, a VOW can perform a passcode change as follows:

1. Go off-hook.
2. Upon receipt of dial tone, dial the VOWPCC feature access code datafilled in table IBNXLA (e.g., '*82') against the appropriate customer group.
3. Upon receipt of dial tone, dial the PDN for the VOW set data to whose passcode is being modified (e.g., '2149975005'). If a mistake is made when entering the PDN, pressing the '*' key will restart collection of the PDN.

Note: The PDN must be entered as a 10 digit number.

4. Upon receipt of dial tone, dial the current passcode unique to that VOW (e.g., '9975056449'). The length of this passcode is specified in table CUSTSTN in the VOWDN tuple associated with the customer group. If a mistake is made when entering the current passcode, pressing the '*' key will restart collection of the current passcode.
5. Upon receipt of dial tone, dial the new passcode for that VOW (e.g., '9975056944'). The length of this passcode is specified in table CUSTSTN in the VOWDN tuple associated with the customer group. If a mistake is made when entering the new passcode, pressing the '*' key will restart collection of the new passcode.
6. Upon receipt of dial tone, re-dial for confirmation the new passcode for that VOW (e.g., '9975056944'). The length of this passcode is specified in table CUSTSTN in the VOWDN tuple associated with the customer group. If a mistake is made when re-entering the new passcode, pressing the '*' key will restart collection for the re-entry of the new passcode.

If the first new passcode does not match the second (confirmation) new passcode, then the VOW's passcode will not be changed. Further, if another VOW in the same customer group should have the same passcode as the new passcode, then passcode will not be changed.

Whether successful or not, OMs will be pegged to record the result of the passcode change attempt.

VOW Remote Logout

On a set within the same customer group on the same switch as the VOW's set data, a VOW can perform a remote logout as follows:

1. Go off-hook.
2. Upon receipt of dial tone, dial the VOWROUT feature access code datafilled in table IBNXLA (e.g., '*83') against the appropriate customer group.

3. Upon receipt of dial tone, dial the PDN for the VOW set data which is being remotely logged out(e.g., '2149975005'). If a mistake is made when entering the PDN, pressing the '*' key will restart collection of the PDN.

Note: The PDN must be entered as a 10 digit number.

4. Upon receipt of dial tone, dial the current passcode unique to that VOW (e.g., '9975056449'). The length of this passcode is specified in table CUSTSTN in the VOWDN tuple associated with the customer group. If a mistake is made when entering the current passcode, pressing the '*' key will restart collection of the current passcode.

If the VOW was logged in, this will force a logout from a remote station. At this point, logs will be generated and OMs will be pegged to indicate a successful remote logout attempt. If an error occurred either due to user input or otherwise during any of the above steps, OMs will be pegged to indicate that an error occurred during a logout attempt, and the set will return to an idle state.

The VOW set data will be modified as described in section "VOW Logout" on page 226 if the remote logout attempt is successful.

VOW Audit Process

In the VOWDN tuple in table CUSTSTN, a customer group can specify whether an audit is to be executed every 24 hours against the VOWs in the customer group, and if so, the specific hour at which the audit will execute. If enabled, the audit will execute at the specified hour every day, and will log out those VOWs who are still logged in. Logs will be generated and OMs will be pegged to record any actions taken by the audit.

If the set at which a VOW is logged in is not in an idle state when the audit executes, then that VOW will not be logged out by the audit. Instead, at the next hour, the audit will check the set again, and if the VOW is still logged in and the set is in an idle state, the audit will log the VOW out. If still logged in and the set is not in an idle state, the audit will attempt to log out the VOW at the next hour. This will repeat until the VOW is logged out, either manually or through the audit.

VOWs who are logged out through the audit can log back in just as if they had logged themselves out.

Table VOWINV and CI command VOWCI

As sets/DNs are assigned the VOW and VOWDN line options, table VOWINV will be automatically datafilled with information regarding the sets involved with VOW functionality. Tuples are not permitted to be added or deleted from this table through the TABLE editor. In addition, not all fields can be modified through the TABLE editor. The only field that can be modified is

the VOWPID field, which contains a VOW's passcode. This field can be modified by switch personnel in order to reset a VOW's passcode, if necessary.

The VOWCI CI command provides alternate views of the data present in table VOWINV. For example, it can be used to list details on:

- the physical sets from which VOWs can log in
- the VOWs currently logged in or logged out
- data per customer group

More information on the VOWINV table and the VOWCI CI command can be found in Appendix D of this document.

VOW Limits

Up to 20,500 VOWs can exist within a single switch, if all VOWs require only a single LEN. Within a customer group, there is no limitation on the number of VOWs, except for the maximum number per switch of 20,500. This limit facilitates having more actual VOWs (i.e., VOW set data with the VOW line option assigned) than VOWDN sets (i.e., physical sets with the VOWDN line option assigned).

IVD sets can be configured with a second (mate) LEN. If a VOW's dedicated DN and features are associated with such a set, then that VOW will require two VOW LENs, thus reducing the maximum possible number of VOWs.

Up to 4,095 VOWDNs can exist within a single switch. Within a customer group, there is no limitation on the number of VOWDNs, except for the maximum number per switch of 4,095.

Supplementary information: DDOC sections

Note: When AX1236 was originally written, the DDOC contained separate sections for specific pieces of supplementary information (logs, OM, data schema, etc.). In today's documentation paradigm, this information is typically consolidated into 2 customer facing sections, the CN (Configuration) and FM (Fault Management) sections. In order to avoid the exercise of consolidation, the CN and FM sections of this document will not be used. Instead, each supplementary section will be attached to this FN as an appendix. See Appendix A through Appendix E. Where appropriate, minor changes have been made to these sections.

Logs (LG)

A new log type, VOW, is created for use with VOW functionality. This new log type contains numerous reports. Information concerning these new logs can be found in the Fault Management section of this feature.

The new log reports will be generated for the following events:

- Successful log in
- Successful log in through CLN/CKLN
- Successful log out
- Successful log out through CLN/CKLN
- Successful log out through audit process

Data schema (DS)

A new table, VOWINV, is created for use with VOW functionality. The format of this new table can be found in the Configuration section of this feature.

In addition, other tables must be properly datafilled prior to using VOW functionality. These include tables DNROUTE, CUSTSTN, IBNXL, and AUTHCDE. More detailed information than that provided in this section is available in the Configuration section of this feature.

A new LEN format is introduced by this functionality. A VOW virtual LEN or logical terminal is denoted through type EXT_LEN with the following format:

- VOW <VOW Node Number> <VOW Terminal Number>

A VOW Node Number is a value from 1 to 10, and a VOW Terminal Number is a value 1 to 2050. An example of a VOW LEN is 'VOW 2 955'.

DNROUTE

In table DNROUTE, a unique DN will be allocated for each VOWDN set which already has a VOW user logged in. This tuple is created automatically when a VOW user logs in, and it is automatically removed when a VOW user logs out.

CUSTSTN

In table CUSTSTN, feature VOWDN must be datafilled against each customer group that will allow VOW functionality. The datafill for each customer group contains the following:

- NCOS and SUBGRP values for translations purposes on the pre-designated VOW sets when no VOW is logged in;
- A boolean value specifying whether or not the VOW authorization code is required within the associated customer group during use of the VOWIN feature access code;
- A boolean value specifying whether the personal (SW) authorization code is required within the associated customer group during use of the VOWIN feature access code;
- A boolean value specifying whether the associated customer group is to be audited, and if so, a value specifying the hour of the day the audit is to occur;

- A boolean value specifying whether or not VOW functionality interacts with call forwarding functionality to enable call forwarding for a VOW when s/he logs out and to disable call forwarding for a VOW when s/he logs in;
- The length of the VOW personal ID code (referred to as passcode throughout the remainder of this document) length values used to uniquely identify a VOW within a customer group; and,
- The line class code of the sets which will make use of VOW functionality.

IBNXLA

In table IBNXLA, the feature translators VOWIN, VOWOUT, VOWROUT, and VOWPCC must be datafilled against the appropriate XLANAME and DGLIDX such that VOWs can log in, log out, and change their individual passcodes.

AUTHCDE

In table AUTHCDE, VOW and SW authorization codes must be datafilled if these authorization codes are enabled through the VOWDN tuple in table CUSTSTN. These values will be used when a VOW attempts to log in.

Enhanced AUTHCDE functionality, such as PIN digits and ACCT codes are supported by the VOW authorization code.

Service orders (SO)

Two new line options, VOW and VOWDN, are created for use with VOW functionality. Details on these line options can be found in the Configuration section of this feature.

These line options will be valid on the sets described in the table which follows. *Note: IVD sets apply to MSL loads only.*

VOW/VOWDN Line Option Compatible Sets

Set Type	LCC
MBS	PSET
	M5009
	M5112
	M5209
	M5312
	M5212
	M5008
	M5208
	M5216
	M5316
IVD	M2009
	M2112
	M2018
	M2317
	M2008
	M2616
	M2016S
	M2216A
	M2216B
	M2006
	M2616CT
IBN	IBN

The VOWDN line option applies to a set from which a VOW can log in. It will be compatible with the DTM (Deny Termination) line option in order that calls to the shared VOWDN datafilled in DNROUTE against the corresponding customer group does not terminate when dialed.

Both the VOW and VOWDN line options must be assigned to the PDN of a keyset with a line format in table KSETLINE of DN or to an IBN set with a line format in table IBNLINES of STN. As such, they are both incompatible

with MDN (Multiple Appearance Directory Number), ACD (Automatic Call Distribution), attendant consoles, and GIC (Group Intercom) line formats.

Man Machine interface (MM)

A new CI command, VOWCI, is created to allow easy access to information pertaining to sets involved with VOW functionality. Details on this new command can be found in the MM section (Appendix D) of this document.

Operational measurements (OM)

A new OM group, VOW, is created for use with VOW functionality. Details on this new OM group can be found in the Configuration section of this feature.

The new OM registers will be pegged for the following events:

- Successful log in
- Successful log in through CLN/CKLN
- Successful log out
- Successful log out through CLN/CKLN
- Successful log out through audit process
- Successful passcode change
- Invalid log in attempt
- Invalid log out attempt
- Invalid passcode change attempt

AMA/Billing information (AM)

AMA/Billing information is not impacted by this activity. As such, no AM section is included in this document. While there is an explicit requirement which concerns billing, the existing billing functionality handles the billing of calls from the temporary LEN to the corresponding virtual DN.

Hardware Requirements or Dependencies

Not Applicable.

Software Requirements or Dependencies

None.

Interactions

- The provisioning of the VOW line option to a set results in the creation of a tuple in table VOWINV as well as the allocation of a virtual VOW LEN for use by the set to which the VOW line option is assigned. If the set is an

IVD set whose mate LEN is present, a second virtual VOW LEN will be allocated for the mate LEN.

- The removal of the VOW line option from a set results in the deletion of the corresponding tuple in table VOWINV, and the deallocation of the virtual VOW LEN(s).
- Once logged in, existing features associated with a VOW's dedicated DN will operate as if the VOW's set were originally provisioned against the set from which s/he logged in. This includes originating and receiving calls, billing, message waiting indication, and calling and caller name and number display.
- Similarly, once logged out, options associated with the VOW dedicated DN such as call forwarding will operate as if the VOW were actually logged in, assuming that such features were active at the time the VOW logged out.
- If the VOWDN tuple in table CUSTSTN enables the VOW functionality to interact with call forwarding, then when a VOW logs out, his/her call forwarding will be activated. Similarly, when a VOW logs in, his/her call forwarding will be deactivated. This interaction applies only to the basic call forwarding types CFU, CFF, and CFI. It does not apply to any other call forwarding types such as CFK, CFB or CFD.
- When logged out, the VOW data is moved from a physical LEN to a virtual LEN. When this occurs, the DNs on a VOW's set data which was moved appear to the system to be in a busy (offline) state. As such, calls to logged out VOW DNs will not ring, but will instead receive busy tone. The table below outlines how calls to a logged-out VOW's DN will forward using CFB and CFD. Per normal call forward operation, and active CFU, CFF, CFI, and CFK call forwarding type takes precedence over active CFB and CFD call forwarding types on a logged out VOW's set data.

CFB/CFD Interactions with Logged-out VOWs

	CFB Active	CFB Inactive	CFB Not Provisioned
CFD Active	Calls will forward using CFD	Calls will forward using CFD	Calls will forward using CFD
CFD Inactive	Calls will forward using CFB	Calls will not forward using either CFB or CFD	Calls will not forward using either CFB or CFD
CFD Not Provisioned	Calls will forward using CFB	Calls will not forward using either CFB or CFD	Calls will not forward using either CFB or CFD

- When logged in, VOW users receive normal dial tone upon going off hook. When logged out, the VOWDN sets will deliver stutter dial tone to indicate

that no VOW user is logged in at that set. If using IBN set types, this can cause confusion if stutter dial tone is utilized as a message waiting indicator. The end user will not be able to differentiate between a logged in VOW user with a message waiting and a VOWDN set with no VOW users logged in. For this reason, it is recommended that a lamp be used as the message waiting indicator if the physical equipment is available to accommodate it.

- If a logged in VOW user dials 911, their dedicated VOW DN will be presented to the 911 operator as the call back DN. This number will be used to lookup the address (physical location) of the 911 caller. In some VOW configurations, the VOWDN sets may be physically located in several different areas. In these configurations, the 911 system will not be able to determine which physical location that the VOW user is logged in from. This problem can not be avoided, but can be minimized if the VOWDN sets are physically located as close to each other as possible.

Limitations and restrictions

- In general, this entire feature activity is compatible with most existing features. The exceptions are:
 - a. The VOWDN line option is not compatible with any other line option/feature except for SETMODEL, DGT, DISP, M0200, and NAME.
 - b. The VOW line option is not compatible with MADN, ACD, or HUNT groups. Hence, it is not compatible with the MDN, ACD, and the various HUNT-related line options. It is also not compatible with ACB, AR, BLF, C2USER, CALLOG, DLH, DNH, DOR, DRING, MDN, MLH, NFA, SBLF, SIMRING, SLU, TRANSFER, VOWDN, and XFER.
- Up to 20,500 VOWs can exist within a single switch, if all VOWs require only a single LEN. Within a customer group, there is no limitation on the number of VOWs, except for the maximum number per switch of 20,500.
- Up to 4,095 VOWDNs can exist within a single switch. Within a customer group, there is no limitation on the number of VOWDNs, except for the maximum number per switch of 4,095.
- IVD sets can be configured with a second (mate) LEN. If a VOW's dedicated DN and features are associated with such a set, then that VOW will require two VOW LENs, thus reducing the maximum possible number of VOWs.
- Within a customer group, all VOW's dedicated DNs and features must be associated with the same type of set. The pre-designated physical sets from which these VOWs will log in must also be of that same set type.

- The calls that can be originated from a set with VOWDN assigned are determined/restricted by the translations set up against the corresponding customer group and the NCOS/SUBGRP values in the VOWDN tuple in table CUSTSTN. Translations can limit these VOWDN sets to make only E911 calls, E911 and local calls, E911, local, and long distance calls, etc.
- Once the VOW line option is assigned, the associated set can only be further provisioned in Servord (i.e., using ADO, NEW, etc.) when the associated VOW is logged in. If a VOW is logged out, his/her set data will be associated with a VOW logical terminal instead of with a physical LEN, and any provisioning by switch personnel must be performed as follows:
 1. Use the appropriate CKLN/CLN Servord command to move the VOW's set data from a VOW logical terminal to a physical LEN. This will log the VOW in to the specific physical LEN.⁶
 2. Perform the required provisioning through Servord.
 3. Use the appropriate CKLN/CLN Servord command to move the VOW's set data from the physical LEN back to a VOW logical terminal. This will log the VOW out of the previously-specified LEN.

The previous provisioning statements also apply when removing a VOW line from service. CKLN/CLN must first be used to move the VOW set data to a physical LEN. The set can then be removed via the Servord OUT command.

A VOW login can occur only from a set with VOWDN assigned which is in the same customer group as the VOW's set data for the VOW who is attempting to log in.

Due to the number of tables modified when moving VOW set data from a physical LEN to a virtual LEN and vice versa, access to VOW functionality through the VOWIN, VOWOUT, VOWROUT, and VOWPCC feature access codes will not be allowed during an ONP. This is to ensure data consistency over a software upgrade. Once the ONP is complete, VOW access will again be permitted.

Applicable customer facing sections

Fault Management

Logs __X__

Alarms __N/A__

Configuration

6. The audit time, if activated for the associated customer group, should be considered when performing these actions. If these provisioning actions are executed when the VOW audit runs for the associated customer group, the VOW user will effectively be logged out by the audit process.

Data Schema	__X__
User Interface	__X__
Element Management	__N/A__
Security	__N/A__
Service Order	__X__
Office Parameters	__N/A__
Accounting (includes AMA billing)	__N/A__
Performance (includes operational measurements)	__X__

Glossary

<u>Term</u>	<u>Description</u>
ACD	Automatic Call Distribution (Line option/format)
AUTHCDE	Table AUTHCDE
CCM	DMS-100 Common (DRU)
CFB	Call Forward Busy (Line option)
CFD	Call Forward Don't Answer (Line option)
CFF	Call Forward Fixed (Line option)
CFI	Call Forward Internal (Line option)
CFK	Call Forward Per Key (Line option)
CFU	Call Forward Universal (Line option)
CI	SOS Command Interpreter
CKLN	Change Keyset LEN (Servord Command)
CLN	Change LEN (Servord command)
CUSTSTN	Table CUSTSTN
DGLIDX	Digilator Index (Part of key to table IBNXLA)
DN	Directory Number
DNINV	Table DNINV
DNROUTE	Table DNROUTE
DRU	Development Release Unit

<u>Term</u>	<u>Description</u>
DTM	Deny Termination (Line option)
FNAL	Feature Not Allowed (Treatment type)
GIC	Group Intercom (Line option/KSETLINE line format)
HUNT	HUNT Group
IBN	Integrated Business Network
IBNLINES	Table IBNLINES
IBNXLA	Table IBNXLA
IVD	Integrated Voice and Data
KSETLINE	Table KSETLINE
LEN	Line Equipment Number
MADN	Multiple Appearance Directory Number
MBS	Meridian Business Set
MDN	Multiple Appearance Directory Number (Line option/format)
MSL	Meridian Stored Logic
NCOS	Network Class of Service
NFA	Network Facility Access
OM	Operational Measurement
PBX	Private Branch Exchange
QLEN	Query LEN (CI command)
SOC	Software Optionality Control
STN	Station (IBNLINES Line format)
SUBGRP	Subgroup (of customer group)
SW	System Wide (Authorization code type)
TABLE	Table Editor CI Command
TL	Telecom (DRU)
VOW	Virtual Office Worker (i.e., a Telecommuter)
	Also, any of the following:
	* Line option
	* Authorization code type in table AUTHCDE

<u>Term</u>	<u>Description</u>
VOWCI	VOWCI CI Command
VOWINV	Table VOWINV
VOWDN	Any of the following: * Entry in table CUSTSTN * Entry in table DNINV * Entry in table DNROUTE * KSETLINE/IBNLINES Line format
VOWIN	VOW Login Feature Translator in table IBNXLA
VOWOUT	VOW Logout Feature Translator in table IBNXLA
VOWPCC	VOW Passcode Change Feature Translator in table IBNXLA
VOWROUT	VOW Remote Logout Feature Translator in table IBNXLA
XLANAME	Translations Name (Part of key to table IBNXLA)

Fault Management for A00002011

This section contains the log reference information from the original design document (AX1236LG.AA20).

It has not been modified from the original version.

New/Modified Logs

New/Modified Logs

LOG NAME	LOG NUMBER	NEW/MOD DELETED	SYSTEM (SOS/UNIX)
VOW	501	New	SOS
VOW	502	New	SOS
VOW	601	New	SOS
VOW	602	New	SOS

Log report: VOW501

Example

VOW501 Example

```
VOW501 JAN28 14:08:23 0007 PASS VOW ATTEMPT PASSED
VOW USER = 2149975055
VOW LEN = IPE0 0 1 1 12
ACTION = LOGIN
METHOD = VOWIN
```

Overview

This log report is generated when a VOW access attempt (login, logout, or passcode change) passes.

Format

VOW501 Format

```
VOW501 mmmdd hh:mm:ss nnnn PASS VOW ATTEMPT PASSED
VOW USER = nnnnnnnnnn
VOW LEN = xxxx nn n nn nn
ATTEMPT = xxxxxxxxxxxxxxxx
METHOD = xxxxxxxx
```

Field description

Field name: VOW USER

Field optionality: MANDATORY

Type: digit

Size: 10 digits

Value(s): nnnnnnnnnn, where n=0-9

Descriptions: The directory number of the VOW user who logged in.

NTP table reference: N/A

Field name: VOW LEN

Field optionality: MANDATORY

Type: char/digit

Size: 15 char/digit

Value(s): xxxx nn n nn nn, where x=0-9, A-Z, and n=0-9

Descriptions: The LEN at which the VOW user is logged in.

NTP table reference: N/A

Field name: ATTEMPT

Field optionality: MANDATORY

Type: char

Size: 15 char

Value(s): LOGIN, LOGOUT, PASSCODE CHANGE

Descriptions: LOGIN is specified if the successful action being reported is a login attempt (through VOWIN, CKLN, or CLN). LOGOUT is specified if the successful action being reported is a logout attempt (through VOWOUT,

CKLN, CLN, VOWROUT, or the VOW Audit). PASSCODE CHANGE is specified if the successful action being reported is a passcode change attempt through VOWPCC.

Field name: METHOD

Field optionality: MANDATORY

Type: char

Size: 7 char

Value(s): VOWIN, VOWOUT, VOWROUT, VOWPCC, CKLN, CLN, AUDIT

Descriptions: VOWIN is specified if the successful attempt being reported is a login attempt through the VOWIN access code. VOWOUT is specified if the successful attempt being reported is a logout attempt through the VOWOUT access code. VOWROUT is specified if the successful attempt being reported is a remote logout attempt through the VOWROUT access code. VOWPCC is specified if the successful attempt being reported is a passcode change attempt through the VOWPCC access code. CKLN is specified if the successful attempt being reported is a login or logout attempt through the CKLN Servord command. CLN is specified if the successful attempt being reported is a login or logout attempt through the CLN Servord command. AUDIT is specified if the successful attempt being reported is a logout attempt by the VOW Audit.

Action to be taken

No immediate action.

Post-analysis

This log is generated whenever a VOW access attempt completes successfully. The OM registers available through OM group VOW provide further information to measure the overall use of VOW functionality.

Internal

This log report is specific to VOW functionality, and will only be generated from within VOW-specific code.

OM register

OM Group: VOW.

Registers: INPASS, OUTPASS, CINPASS, COUTPASS, PCCPASS, AUDPASS, ROUTPASS

Log report: VOW502

Example

VOW502 Example

```

VOW502  JAN28 14:08:23 0007 FAIL VOW ATTEMPT FAILED

VOW USER = 2149975055

VOW LEN  = IPE0 0 1 1 12

ACTION   = LOGIN

METHOD   = VOWOUT

```

Overview

This log report is generated when a VOW access attempt (login, logout, or passcode change) fails.

Format

VOW502 Format

```

VOW502  mmmdd hh:mm:ss nnnn FAIL VOW ATTEMPT FAILED

VOW USER = nnnnnnnnnn

VOW LEN  = xxxx nn n nn nn

ATTEMPT  = xxxxxxxxxxxxxxxxx

METHOD   = xxxxxxxx

```

Field description

Field name: VOW USER

Field optionality: MANDATORY

Type: digit

Size: 10 digits

Value(s): nnnnnnnnnn, where n=0-9

Descriptions: The directory number of the VOW user who logged in.

NTP table reference: N/A

Field name: VOW LEN

Field optionality: MANDATORY

Type: char/digit

Size: 15 char/digit

Value(s): xxxx nn n nn nn, where x=0-9, A-Z, and n=0-9

Descriptions: The LEN from which the VOW user logged out.

NTP table reference: N/A

Field name: ATTEMPT

Field optionality: MANDATORY

Type: char

Size: 15 char

Value(s): LOGIN, LOGOUT, PASSCODE CHANGE

Descriptions: LOGIN is specified if the failed action being reported is a login attempt (through VOWIN, CKLN, or CLN). LOGOUT is specified if the failed action being reported is a logout attempt (through VOWOUT, CKLN,

CLN, VOWROUT, or the VOW Audit). PASSCODE CHANGE is specified if the failed action being reported is a passcode change attempt through VOWPCC.

Field name: METHOD

Field optionality: MANDATORY

Type: char

Size: 7 char

Value(s): VOWIN, VOWOUT, VOWROUT, VOWPCC, CKLN, CLN, AUDIT

Descriptions: VOWIN is specified if the failed attempt being reported is a login attempt through the VOWIN access code. VOWOUT is specified if the failed attempt being reported is a logout attempt through the VOWOUT access code. VOWROUT is specified if the failed attempt being reported is a remote logout attempt through the VOWROUT access code. VOWPCC is specified if the failed attempt being reported is a passcode change attempt through the VOWPCC access code. CKLN is specified if the failed attempt being reported is a login or logout attempt through the CKLN Servord command. CLN is specified if the failed attempt being reported is a login or logout attempt through the CLN Servord command. AUDIT is specified if the failed attempt being reported is a logout attempt by the VOW Audit.

Action to be taken

No immediate action.

Post-analysis

This log is generated whenever a VOW access attempt completes unsuccessfully. The OM registers available through OM group VOW provide further information to measure the overall use of VOW functionality.

Internal

This log report is specific to VOW functionality, and will only be generated from within VOW-specific code.

OM register

OM Group: VOW.

Registers: INFAIL, OUTFAIL, CINFAIL, COUTFAIL, PCCFAIL, AUDFAIL, ROUTFAIL

Log report: VOW601

Example

VOW601 Example

```
VOW601  JAN28 14:08:23 0007 INFO VOW AUDIT COMPLETE
      CUSTOMER GROUP      = BNRRCH
      LOGGED IN            = 23
      ATTEMPTED LOGOUTS    = 21
      SUCCESSFUL LOGOUTS   = 20
      FAILED LOGOUTS       = 1
```

Overview

This log report is generated when the VOW audit process completes. It contains counts of the number of VOW users who were logged in when the audit began, the number of VOW users on which logouts were attempted by the audit, and success and failure counts for those attempts.

Format

VOW601 Format

```
VOW601  mmmdd hh:mm:ss nnnn INFO VOW AUDIT COMPLETE
      CUSTOMER GROUP      = xxxxxxxxxxxxxxxxxx
      LOGGED IN            = nnnnn
      ATTEMPTED LOGOUTS    = nnnnn
      SUCCESSFUL LOGOUTS   = nnnnn
      FAILED LOGOUTS       = nnnnn
```

Field description

Field name: CUSTOMER GROUP

Field optionality: MANDATORY

Type: char

Size: 16 char

Value(s): xxxxxxxxxxxxxxxx, where x=0-9, A-Z

Descriptions: The customer group to which the log applies.

NTP table reference: N/A

Field name: LOGGED IN

Field optionality: MANDATORY

Type: digit

Size: 5 digits

Value(s): nnnnn, where n=0-9

Descriptions: The number of VOW users within the customer group which were logged in when the audit began.

NTP table reference: N/A

Field name: ATTEMPTED LOGOUTS

Field optionality: MANDATORY

Type: digit
Size: 5 digits
Value(s): nnnnn, where n=0-9
Descriptions: The number of VOW users against which logouts were attempted through the audit.
NTP table reference: N/A

Field name: SUCCESSFUL LOGOUTS
Field optionality: MANDATORY
Type: digit
Size: 5 digits
Value(s): nnnnn, where n=0-9
Descriptions: The number of audit logout attempts which were successful.
NTP table reference: N/A

Field name: FAILED LOGOUTS
Field optionality: MANDATORY
Type: digit
Size: 5 digits
Value(s): nnnnn, where n=0-9
Descriptions: The number of audit logout attempts which were un-successful.
NTP table reference: N/A

Action to be taken

No immediate action.

Post-analysis

This log is generated whenever the VOW audit process completes. The OM registers available through OM group VOW provide further information to measure the overall use of VOW functionality.

Internal

This log report is specific to VOW functionality, and will only be generated from within VOW-specific code.

OM register

OM Group: VOW.

Registers: AUDPASS, AUDFAIL

Log report: VOW602

Example

VOW602 Example

```
VOW602 JAN28 14:08:23 0007 INFO VOW INFORMATION
INFO: Could not seize line to RTS
```

Overview

This log report is generated when VOW processing finds some error due to which processing cannot continue. It contains a text message describing the error event. This log is always followed by one of the VOW501, VOW502, or VOW601 logs which will provide further information regarding the agents involved with the VOW processing which failed.

Format

VOW602 Format

```
VOW602 mmdd hh:mm:ss nnnn INFO VOW INFORMATION
INFO: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Field description

Field name: INFO

Field optionality: MANDATORY

Type: char

Size: Up to 40 chars

Value(s): 40(x), where x=0-9, A-Z

Descriptions: Provides a textual description of an internal error which has occurred during VOW processing.

NTP table reference: N/A

Action to be taken

No immediate action.

Post-analysis

This log is generated whenever an error occurs during VOW processing.

Watch for VOW501, VOW502, or VOW601 logs to provide further information regarding the agents and actions involved when the error occurred.

Internal

This log report is specific to VOW functionality, and will only be generated from within VOW-specific code.

OM register

OM Group: None

Configuration for A00002011

Data Schema (DS)

This section contains data schema information from the original design document (AX1236LG.AA20).

The original document has been modified in the following manner:

- Removed references to table DNINV. After the feature re-write, this table was no longer impacted.
- Added the VOWDNIDX field information to the DNROUTE tuple description. This is a new field that was added late in the design.
- Added the VOWDNDN field information to the VOWINV tuple (for VOWKEY = VOWDN).

LEN format

Although not specific to any one table, a new LEN format is introduced by this functionality. A VOW virtual LEN or logical terminal is denoted through type EXT_LEN with the following format:

- VOW <VOW Node Number> <VOW Terminal Number>

A VOW Node Number is a value from 1 to 10, and a VOW Terminal Number is a value 1 to 2050. An example of a value VOW LEN is 'VOW 2 955'.

When a VOW logs out, his/her set data will be moved from the associated physical LEN to a virtual VOW LEN. This will impact every table which has a reference to the physical LEN.

When a VOW logs in, his/her set data will be moved from the associated virtual LEN to a physical LEN. This will impact every table which has a reference to the virtual LEN.

New/modified Table List

TABLE NAME	NEW, CHANGED or DELETED	TABLE CONTROL (NEW/OLD/UNCHANGED)
AUTHCDE	CHANGED	UNCHANGED
CUSTSTN	CHANGED	UNCHANGED
DNROUTE	CHANGED	UNCHANGED
IBNXLA	CHANGED	UNCHANGED
VOWINV	NEW	NEW

Table Name: AUTHCDE**General**

A new value is made available in field AUTHTYPE.

Field Information**AUTHCDE Field Modifications**

FIELD NAME	RANGE OF VALUES	STATUS	DEFAULT VALUES
AUTHTYPE	SSAC,SW,SUPAC,ASR,VOW	Changed	N/A

Description of changed or new fields

A new value, VOW, is available in field AUTHTYPE. This value is used to denote the tuple as a VOW authorization code.

Datafill sequence

Datafill sequence is unchanged.

Table sizing

Table sizing is unchanged.

Dump and restore

Dump and restore requirements are unchanged.

Activation

Modified fields do not affect functionality activation.

Example

AUTHPART AUTHCODE INFO

BNRRCH 7654321 IBN 0 N \$ VOW \$

Table Name: CUSTSTN

General

A new value is made available in fields OPTNAME and OPTION. Additional fields are made available in a refinement specific to the new OPTNAME/OPTION value.

Field Information

CUSTSTN Field Modifications

FIELD NAME	RANGE OF VALUES	STATUS	DEFAULT VALUES
OPTNAME	CUSTSTN_OPTN	Changed	N/A
OPTION	CUSTSTN_OPTN	Changed	N/A
NCOS	NETWORK_CLASS_OF_SERVICE: 0 to 511	New	None
SUBGRP	SUBGRP_NUMBER: 0 to 7	New	None
VOWAUTH	YES_NO: Y or N	New	None
SWAUTH	YES_NO: Y or N	New	None
AUDIT	YES_NO: Y or N	New	None
HOUR	INT: 0 to 23 ^a	New	None
CFW	YES_NO: Y or N	New	None
PCCLEN	INT: 4 TO 10	New	None
VOWLCC	LINE_CLASS_CODE	New	None

a. Only prompted if AUDIT = Y

Description of changed or new fields

Fields OPTNAME and OPTION have changed to allow a new CUSTSTN_OPTN value of VOWDN. The remaining new fields are present only in the refinement of CUSTSTN_FEAT for the VOWDN CUSTSTN_OPTN value.

NCOS specifies the network-class-of-service to be associated with all physical sets with the VOWDN line option assigned in the corresponding customer group. Similarly, SUBGRP specifies the sub-group associated with the same physical sets. VOWAUTH and SWAUTH specify whether the VOW and personal (SW) authorization codes are required for a VOW login attempt. AUDIT specifies whether or not the VOW audit is to be executed against the corresponding customer group. If AUDIT is set to Y, then HOUR must also be

specified as the hour (0 denotes midnight/12:00 AM, 12 denotes noon/12:00 PM) at which the VOW audit is to be executed against the corresponding customer group. CFW specifies whether or not call forwarding interactions with VOW logins and logouts are enabled. PCCLLEN specifies the length of the passcode values for VOWs in the corresponding customer group. VOWLCC specifies the line class code of the sets within the customer group which are to make use of VOW functionality (i.e., those sets to which the VOWDN and VOW line options may be assigned).

The PCCLLEN value has a direct relationship on the VOWPID value specified through the use of the VOW line option and on the VOWPID field in table VOWINV. When initially set through the VOW line option, the VOWPID value must have a length matching the PCCLLEN value in the associated VOWDN tuple in table CUSTSTN. Once a VOW's passcode has been set, it can be changed by the user through the use of the VOWPCC feature access code in table IBNXLA or by switch personnel by changing the VOWPID field in the appropriate tuple in table VOWINV. When changed, the passcode must have a length matching the PCCLLEN value in the associated VOWDN tuple in table CUSTSTN.

If the value of the PCCLLEN field in the VOWDN tuple in table CUSTSTN changes, the associated VOWPID fields in table VOWINV will immediately be impacted. If the PCCLLEN value is changed to a smaller value, then the VOWPID values for VOWs in the corresponding customer group will be truncated to match the new PCCLLEN value (e.g., changing the PCCLLEN value from 6 to 4 will change a VOWPID value of '123456' to '1234'). If the PCCLLEN value is changed to a larger value, then the corresponding VOWPID values will be right-padded with zeros up to the new PCCLLEN value (e.g., changing the PCCLLEN value from 6 to 8 will change a VOWPID value of '123456' to '12345600').

Note: If the PCCLLEN value for a customer group is changed, all VOW's within the corresponding customer group must be notified of the resulting impact to their passcode values. If this notification does not occur, the VOW's within the customer group will not be able to log in.

Datafill sequence

Datafill sequence is unchanged.

Table sizing

Table sizing is unchanged.

Dump and restore

Dump and restore requirements are unchanged.

Activation

Modified fields do not affect functionality activation.

Example

CUSTNAME OPTNAME OPTION

BNRRCH VOWDN VOWDN 0 0 Y Y Y 0 Y 7 PSET

BNRRTP VOWDN VOWDN 0 40 Y N N N 4 M2616

Table Name: DNROUTE**General**

A new value is made available in field FEATURE. Additional fields are also made available in a refinement specific to the new FEATURE value.

Field Information**DNROUTE Field Modifications for FEAT Result Selector**

FIELD NAME	RANGE OF VALUES	STATUS	DEFAULT VALUES
FEATURE	FTRDN_CODE	Changed	N/A
VOWDNIDX	{0 to 4095}	New	None
CUSTGRP	CUSTOMER_GROUP	New	None

Description of changed or new fields

FEATURE is modified within the FEAT result selector to allow a new FTRDN_CODE value of VOWDN. If VOWDN is present as the value of FEATURE, then two new fields are required:

- Fields VOWDNIDX of type VOWDN_DN_COUNT_TYPE (range 0 to 4095) is used primarily to provide and display a unique index value for each VOWDN directory number in the system. When adding the FEAT VOWDN tuple, if the index value is already used, the system provides the user with an available index.
- Field CUSTGRP of type CUSTOMER_GROUP represents the customer group associated with the tuple.

Datafill sequence

Datafill sequence is unchanged.

Table sizing

Table sizing is unchanged.

Dump and restore

Dump and restore requirements are unchanged.

Activation

Modified fields do not affect functionality activation.

Example

```
AREACODE OFCCODE STNCODE DNRESULT
-----
919 657 7293 FEAT VOWDN 1045 BNR RTP
```

Table Name: IBNXLA**General**

New values are made available in field FEATURE.

Field Information**IBNXLA Field Modifications**

FIELD NAME	RANGE OF VALUES	STATUS	DEFAULT VALUES
FEATURE	IBN_LOG_FEATURE	Changed	N/A

Description of changed or new fields

The following new values are made available within field FEATURE: VOWIN, VOWOUT, VOWPCC, and VOWROUT. VOWIN indicates the VOW Login feature. VOWOUT indicates the VOW Logout feature. VOWPCC indicates the VOW Passcode Change feature. VOWROUT indicates the VOW Remote Logout feature.

Datafill sequence

Datafill sequence is unchanged.

Table sizing

Table sizing is unchanged.

Dump and restore

Dump and restore requirements are unchanged.

Activation

Modified fields do not affect functionality activation.

Example

```
KEY RESULT
-----
FRCH 30 FEAT N N VOWIN
```

```
FRCH 31 FEAT N N VOWOUT
FRCH 32 FEAT N N VOWPCC
FRCH 33 FEAT N N VOWROUT
```

Table Name: VOWINV**General**

This table is used to store data associated with VOW functionality. It contains the physical or virtual LEN(s) associated with a VOW's dedicated DN and associated data, his or her personal ID code, and his or her primary DN. As VOW log in and log out of their dedicated DNs, this table is automatically updated to keep the information up-to-date. VOWINV also contains information identifying the physical sets which have the VOWDN line option assigned.

Tuples can not be added to or deleted from this table through the Table Editor. In addition, only the VOWPID field can be modified through the Table Editor. Any other modifications to the table through the Table Editor are blocked.

Field Information

VOWINV Fields

FIELD NAME	RANGE OF VALUES	STATUS	DEFAULT VALUES
VOWKEY	VOW_KEY: CUSTGRP: CUSTOMER_GROUP KEYDATA: VOW_KEY_DATA_AREA: VOWTYPE: VOW_TUPLE_TYPE: VOW or VOWDN VOWPDN: VOWPDN_TYPE ^a AREACODE: SERVING_NUMBERING_PLAN_AREA OFCCODE: OFCCODE_DIGIT_REGISTER STNCODE: STNCODE_DIGIT_REGISTER VOWDNLEN: EXT_LEN ^b	New	None
VOWDATA	VOW_DATA_AREA: VOWTYPE: VOW_TUPLE_TYPE: VOW or VOWDN ^c	New	None

a. Only prompted if VOWTYPE = VOW in VOWKEY field.

b. Only prompted if VOWTYPE = VOWDN in VOWKEY field.

c. Value of VOWTYPE field matches value of VOWTYPE in VOWKEY field.

No further fields exist in table for a VOW_TUPLE_TYPE value of VOWDN.
For a VOW_TUPLE_TYPE value of VOW, the fields shown in Table ,
“Remaining VOWINV Fields for VOW_TUPLE_TYPE Value VOW.” exist.

Remaining VOWINV Fields for VOW_TUPLE_TYPE Value VOW

FIELD NAME	RANGE OF VALUES	STATUS	DEFAULT VALUES
VOWPID	VOW_PERSONAL_ID: Vector of 4 to 10 digits	New	None
VOWLEN	EXT_LEN	New	None
VOWMATE	VOW_MATE_VAR_AREA: MATE: YES_NO: Y or N MATELEN: EXT_LEN ^a	New	New
LOGGEDIN	YES_NO: Y or N	New	None
PHYSLEN	EXT_LEN	New	None

Remaining VOWINV Fields for VOW_TUPLE_TYPE Value VOW

FIELD NAME	RANGE OF VALUES	STATUS	DEFAULT VALUES
PHYSMATE	VOW_MATE_VAR_AREA: MATE: YES_NO: Y or N MATELEN: EXT_LEN ^b	New	New
VOWDNDN	VOWPDN_TYPE: AREACODE: SERVING_NUMBERING_PLAN_AREA OFCCODE: OFCCODE_DIGIT_REGISTER STNCODE: STNCODE_DIGIT_REGISTER ^c	New	New

- a. Only prompted if MATE = Y in VOWMATE field.
b. Only prompted if MATE = Y in PHYSMATE field.
c. Only prompted if VOWTYPE = VOWDN in VOWKEY field.

Description of changed or new fields

VOWKEY is the table key and uniquely identifies a tuple through a customer group (CUSTGRP) and VOW_TUPLE_TYPE value (VOWTYPE). If a VOW_TUPLE_TYPE of VOW is specified, then VOWPDN, identifying the primary DN of the VOW, is also part of VOWKEY. If a VOW_TUPLE_TYPE of VOWDN is specified, then VOWDNLN, identifying a physical LEN on which the VOWDN option is assigned, is also part of VOWKEY.

VOWDATA contains the remaining data for the tuples. VOWTYPE within VOWDATA matches the value of VOWTYPE within VOWKEY.

If VOWTYPE within VOWDATA contains the VOW_TUPLE_TYPE VOW, then the following fields are present in the tuple:

- VOWPID provides the associated VOW passcode value.
- VOWLEN provides the pre-assigned virtual VOW LEN for use by the associated VOW user.
- VOWMATE provides the pre-assigned virtual VOW mate LEN for use by the associated VOW user, if appropriate.
- LOGGEDIN specifies whether or not the associated VOW user is logged in or not.
- If LOGGEDIN is set to Y, then PHYSLEN provides the physical LEN through which the VOW user is logged in.
- If LOGGEDIN is set to Y, then PHYSMATE provides the physical mate LEN, if appropriate.

If VOWTYPE within VOWDATA contains the VOW_TUPLE_TYPE VOWDN, then the following field is present in the tuple:

- VOWDNDN provides the directory number associated with the corresponding VOWDN set.

Datafill sequence

This table is datafilled automatically when VOWs log in and log out, as well as when switch personnel manipulate VOW set data through the CKLN and CLN commands. It is also updated as VOWs are logged out through the VOW audit. Switch personnel can modify only the VOWPID value within this table. Tuples can not be added, deleted, or otherwise modified through the table editor.

Virtual VOW LENS are pre-assigned when the VOW line option is added to a set through Servord and a tuple is created in table VOWINV. Virtual VOW LENS are un-assigned only when the VOW line option is removed from a set through Servord and the corresponding tuple is deleted from table VOWINV.

Table sizing

The table below shows the table sizing information. The table takes up 2,406,030 bytes whether full or empty.

VOWINV Table Sizing

Minimum Size	0 tuples
Maximum Size	41,000 tuples ^a
CC restart type required to increase size	N/A

a. A maximum of 20,500 tuples contain a VOWTYPE value of VOW. A maximum of 20,500 tuples contain a VOWTYPE value of VOWDN. The maximum total tuples is 41,000.

Dump and restore

This is a new table. Reformat procedures are not required.

Activation

Functionality activation is not affected by this new table.

Example

VOWKEY VOWDATA

BNRRCH VOWDN LCM1 00 1 09 31 VOWDN 214 997 8880

BNRRCH VOW 2149975134 VOW 839943 VOW 2 66 N N IPE0 0 0 2 3 N

BNRRTP VOWDN IPE0 00 0 00 12 VOWDN 919 657 8181

BNRRTP VOW 9196577665 VOW 5576643 VOW 4 644 Y VOW 4 645 Y DLM0 0 0 4 12 Y DLM0 0 0 4 13

Office parameters

No office parameters are modified, added, or deleted as a result of this feature functionality.

Service Orders (SO)

This section contains service order information from the original design document (AX1236SO.AA20).

The original document has been modified in the following manner:

- Updated the list of incompatible options for VOW and VOWDN.
- Removed the table that documented extra prompts for adding and deleting VOWDN option. These prompts are no longer valid or relevant.

Summary of service order impact

This activity impacts service orders by making two new line options, VOW and VOWDN, available.

A new LEN format is introduced by this functionality. A VOW virtual LEN or logical terminal is denoted through type EXT_LEN with the following format:

- VOW <VOW Node Number> <VOW Terminal Number>

A VOW Node Number is a value from 1 to 10, and a VOW Terminal Number is a value 1 to 2050. An example of a value VOW LEN is 'VOW 2 955'.

Details of service order change

No NEW LCC introduced by this feature.

NEW OPTIONS introduced by this feature: VOW, VOWDN

LIST options NOT compatible with new options introduced:

VOW is not compatible with MDN, ACD, the various HUNT-related options, and the following: ACB, AR, BLF, C2USER, CALLOG, DOR, DRING, NFA, SBLF, SIMRING, SLU, TRANSFER, VOWDN, and XFER.

VOWDN is incompatible with all options except: SETMODEL, DGT, DISP, M0200, and NAME.

No other options which must be assigned.

Meridian digital centrex feature assignment requirements

FEATURE	500 2500	MDC SET	MDC BUSINESS SET SET RELATIONSHIP							
			S E T	S U B S E T	K E Y	D N	D E D K E Y	L A M P	C O D E	D I S P L A Y
VIRTUAL OFFICE WORKER (VOW)	Y	Y		X						
VIRTUAL OFFICE WORKER DN (VOWDN)	Y	Y		X						

On a keyset, these options must be assigned to the primary DN.

New commands

None.

New prompts

One new prompt is implemented by this feature:

VOW Prompts

PROMPT TEXT	VALID INPUT	DESCRIPTION	AREAS AFFECTED BY PROMPTS.
VOWPID	10-digit directory number	When adding VOW to a set, an initial passcode must be specified for the associated VOW user. This value is a digit register between 4 and 10 digits in length as specified by the PCCLLEN field of the VOWDN tuple for the corresponding customer group in table CUSTSTN.	ADO (VOW)

Example of service order

Example of ADO command with VOW line option on keyset:

```
>ado
SONUMBER:      NOW  98  9 24 AM
>
DN_OR_LEN:
>9975057
OPTKEY:
>1
```

```
OPTION:
>VOW
VOWPID:
>12345
OPTKEY:
>$
COMMAND AS ENTERED:
ADO NOW 98 9 24 AM 9975057 ( 1 VOW )$
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>Y
MACHINES OUT OF SYNC OR NO JF, OVERRIDE IN EFFECT.
>
```

Example of ADO command with VOWDN line option on keyset:

```
>ado
SONUMBER:      NOW  98  9 24 AM
>
DN_OR_LEN:
>9975057
OPTKEY:
>1
OPTION:
>VOWDN
OPTKEY:
>$
COMMAND AS ENTERED:
ADO NOW 98 9 24 AM 9975057 ( 1 VOWDN ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>Y
MACHINES OUT OF SYNC OR NO JF, OVERRIDE IN EFFECT.
>
```

Example of ADO command with VOW line option on non-keyset:

```
>ado
SONUMBER:      NOW  98  9 24 AM
>
DN_OR_LEN:
>9975003
OPTION:
```

```
>VOW
VOWPID:
>12345
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 98 9 24 AM 9975003 ( VOW )$
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>Y
MACHINES OUT OF SYNC OR NO JF, OVERRIDE IN EFFECT.
>
```

Example of ADO command with VOWDN line option on non-keyset:

```
>ado
SONUMBER:      NOW  98  9 24 AM
>
DN_OR_LEN:
>9975003
OPTION:
>VOWDN
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 98 9 24 AM 9975003 ( VOWDN ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>Y
MACHINES OUT OF SYNC OR NO JF, OVERRIDE IN EFFECT.
>
```

Example of NEW command with VOW on a keyset:

```
>new
SONUMBER:      NOW  98  9 29 PM
>
DN:
>9975059
LCC_ACC:
>pset
GROUP:
>bnrrch
```

```
SUBGRP:
>0
NCOS:
>0
SNPA:
>214
KEY:
>1
RINGING:
>y
LTG:      0
>
LEN_OR_LTID:
>LCM2  00 0 06 31
OPTKEY:
>1
OPTION:
>VOW
VOWPID:
>12345
OPTKEY:
>$
COMMAND AS ENTERED:
NEW NOW 98 9 29 PM 9975059 PSET BNRRCH 0 0 214 1 Y 0 LCM2 00 0 06 31 ( 1 VOW ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES OUT OF SYNC OR NO JF, OVERRIDE IN EFFECT.
>
```

Example of NEW command with VOWDN on a keyset:

```
>new
SONUMBER:      NOW  98  9 29 PM
>
DN:
>9975059
LCC_ACC:
>pset
GROUP:
>bnrrch
```

```
SUBGRP:
>0
NCOS:
>0
SNPA:
>214
KEY:
>1
RINGING:
>y
LTG:      0
>
LEN_OR_LTID:
>LCM2  00 0 06 31
OPTKEY:
>1
OPTION:
>VOWDN
OPTKEY:
>$
COMMAND AS ENTERED:
NEW NOW 98 9 29 PM 9975059 PSET BNRRCH 0 0 214 1 Y 0 LCM2 00 0 06 31 ( 1 VOWDN ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES OUT OF SYNC OR NO JF, OVERRIDE IN EFFECT.
>
```

Example of NEW command with VOW on a non-keyset:

```
>new
SONUMBER:      NOW  98  9 29 PM
>
DN:
>9975007
LCC_ACC:
>ibn
GROUP:
>bnrrch
SUBGRP:
>0
```



```
NCOS:
>0
SNPA:
>214
LTG:    0
>
LEN_OR_LTID:
>LCM1  00 1 18 00
OPTION:
>VOW
VOWPID:
>12345
OPTION:
>$
COMMAND AS ENTERED:
NEW NOW 98 9 29 PM 9975007 IBN BNRRCH 0 0 214 0 LCM1 00 1 18 00 ( VOW ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES OUT OF SYNC OR NO JF, OVERRIDE IN EFFECT.
>
```

Example of NEW command with VOWDN on a non-keyset:

```
>new
SONUMBER:    NOW  98  9 29 PM
>
DN:
>9975007
LCC_ACC:
>ibn
GROUP:
>bnrrch
SUBGRP:
>0
NCOS:
>0
SNPA:
>214
LTG:    0
>
```

```
LEN_OR_LTID:
>LCM1 00 1 18 00
OPTION:
>VOWDN
OPTION:
>$
COMMAND AS ENTERED:
NEW NOW 98 9 29 PM 9975007 IBN BNRRCH 0 0 214 0 LCM1 00 1 18 00 ( VOWDN ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES OUT OF SYNC OR NO JF, OVERRIDE IN EFFECT.
>
```

Example of DEO command with VOW line option on keyset:

```
>deo
SONUMBER:      NOW 98 9 29 PM
>
DN_OR_LEN:
>LCM2 00 0 06 31
OPTKEY:
>1
OPTION:
>vow
OPTKEY:
>$
COMMAND AS ENTERED:
DEO NOW 98 9 29 PM LCM2 00 0 06 31 ( 1 VOW ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES OUT OF SYNC OR NO JF, OVERRIDE IN EFFECT.
>
```

Example of DEO command with VOWDN line option on keyset:

```
>deo
SONUMBER:      NOW 98 9 29 PM
>
DN_OR_LEN:
>LCM2 00 0 06 31
OPTKEY:
```

```
>1
OPTION:
>vowdn
OPTKEY:
>$
COMMAND AS ENTERED:
DEO NOW 98 9 29 PM LCM2 00 0 06 31 ( 1 VOWDN ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES OUT OF SYNC OR NO JF, OVERRIDE IN EFFECT.
>
```

Example of DEO command with VOW line option on non-keyset:

```
>deo
SONUMBER:      NOW  98  9 29 PM
>
DN_OR_LEN:
>LCM2  00 0 06 31
OPTION:
>vow
OPTKEY:
>$
COMMAND AS ENTERED:
DEO NOW 98 9 29 PM LCM2 00 0 06 31 ( VOW ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES OUT OF SYNC OR NO JF, OVERRIDE IN EFFECT.
>
```

Example of DEO command with VOWDN line option on non-keyset:

```
>deo
SONUMBER:      NOW  98  9 29 PM
>
DN_OR_LEN:
>LCM2  00 0 06 31
OPTION:
>vowdn
OPTKEY:
>$
```

```
COMMAND AS ENTERED:
DEO NOW 98 9 29 PM LCM2 00 0 06 31 ( VOWDN ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>Y
MACHINES OUT OF SYNC OR NO JF, OVERRIDE IN EFFECT.
>
```

Software Optionality Control (SOC)

For non-MSL customers, this feature will be regulated by standard SOC control. VOWs and VOWDNs can be datafilled, but VOW users will not be permitted to log-in or perform passcode changes unless the feature is activated in SOC. If the SOC is turned off, attempts to log-in or perform passcode changes by a VOW user will be routed to FNAL treatment.

SOC

SOC option name:	MDC00076
SOC option title:	Virtual Office Worker
SOC option control type:	state
New SOC option?	Yes
SOC option order code	00036425
Option defined in DRU:	CCM
Affected products:	CCM20

In loads built for the MSL market, the SOC should always be ON.

User interface

This section contains the man-machine interface information from the original design document (AX1236MM.AA20).

It has not been modified from the original version.

Directories

Table of new/modified directories

DIRECTORY NAME	NEW, CHANGED OR DELETED	NEW NAME (if renamed)	TARGET	RES/ NONRES
VOWCIDIR	NEW		BOTH	RES

Accessing directory: VOWCIDIR

To access

>VOWCI

To return to CI

>QUIT

or

>LEAVE

Commands

Table of New/modified commands

COMMAND NAME	NEW, CHANGED OR DELETED	NEW NAME (if renamed)	DIRECTORY NAME
VOWSETS	NEW		VOWCIDIR
VOWALL	NEW		VOWCIDIR
VOWIN	NEW		VOWCIDIR
VOWOUT	NEW		VOWCIDIR
VOWCUST	NEW		VOWCIDIR

Command name: VOWSETS

Command type: NON-MENU

Command target: BOTH

Command availability: RES

Command description

This command will provide a formatted listing of all physical sets which have the VOWDN line option assigned. Included will be the associated set type, the associated customer group, and the customer-group specific information associated with the VOWDN sets, such as the VOWDN/VOW information from table DNROUTE/DNINV and the VOWDN information from table CUSTSTN.

A customer group can be specified to limit the output to a single customer group. If no customer group is specified, output will be provided for all applicable customer groups.

Warning

None

Command syntax

```
>VOWCI
```

```
VOWCI:
```

```
>Q VOWSETS
```

```
COMMAND VOWSETS: LIST VOW SETS
```

```
COMMAND VOWSETS:
```

```
VOWSETS [<CUSTOMER_GROUP>]
```

```
>
```

Parameter definitions

PARAMETER	VALUE	DEFINITION
custgrp	STRING RANGE	CUSTOMER_GROUP

Command name: VOWALL

Command type: NON-MENU

Command target: BOTH

Command availability: RES

Command description

This command will provide a formatted listing of all VOW user's DNs which have the VOW line option assigned. Included will be the set type, the associated customer group, whether the user is logged in or logged out, and the LEN (physical or virtual) with which the user's set data is currently associated.

A customer group can be specified to limit the output to a single customer group. If no customer group is specified, output will be provided for all applicable customer groups.

Warning

None

Command syntax

```
>VOWCI
```

```
VOWCI :
```

```
>Q VOWALL
```

```
COMMAND VOWALL: LIST ALL VOW USERS (LOGGED IN OR  
LOGGED OUT)
```

```
COMMAND VOWALL:
```

```
VOWALL [<CUSTOMER_GROUP>]
```

```
>
```

Parameter definitions

PARAMETER	VALUE	DEFINITION
custgrp	STRING RANGE	CUSTOMER_GROUP

Command name: VOWIN

Command type: NON-MENU

Command target: BOTH

Command availability: RES

Command description

This command will provide a formatted listing of all VOW user's DNs which have the VOW line option assigned and which are also logged into their DNs. Included will be the set type, the associated customer group, and the physical LEN with which the user's set data is currently associated.

A customer group can be specified to limit the output to a single customer group. If no customer group is specified, output will be provided for all applicable customer groups.

Warning

None

Command syntax

```
>VOWCI
```

```
VOWCI :
```

```
>Q VOWIN
```

```
COMMAND VOWIN: LIST ALL LOGGED IN VOW USERS
```

```
COMMAND VOWIN:
```

```
VOWIN [<CUSTOMER_GROUP>]
```

```
>
```

Parameter definitions

PARAMETER	VALUE	DEFINITION
custgrp	STRING RANGE	CUSTOMER_GROUP

Command name: VOWOUT**Command type: NON-MENU****Command target: BOTH****Command availability: RES****Command description**

This command will provide a formatted listing of all VOW user's DNs which have the VOW line option assigned and which are also logged out of their DNs. Included will be the set type, the associated customer group, and the virtual LEN with which the user's set data is currently associated.

A customer group can be specified to limit the output to a single customer group. If no customer group is specified, output will be provided for all applicable customer groups.

Warning

None

Command syntax

```
>VOWCI
```

```
VOWCI :
```

```
>Q VOWOUT
```

```
COMMAND VOWOUT: LIST ALL LOGGED OUT VOW USERS
```



```
COMMAND VOWOUT :  
VOWOUT [<CUSTOMER_GROUP>]  
>
```

Parameter definitions

PARAMETER	VALUE	DEFINITION
custgrp	STRING RANGE	CUSTOMER_GROUP

Command name: VOWCUST**Command type: NON-MENU****Command target: BOTH****Command availability: RES****Command description**

This command provides the same information as VOWSETS and VOWALL.

A customer group can be specified to limit the output to a single customer group. If no customer group is specified, output will be provided for all applicable customer groups.

Warning

None

Command syntax

```
>VOWCI  
VOWCI :  
>Q VOWCUST  
COMMAND VOWCUST: LIST VOW CUSTOMER GROUP INFORMATION  
COMMAND VOWCUST:  
VOWCUST [<CUSTOMER_GROUP>]  
>
```

Parameter definitions

PARAMETER	VALUE	DEFINITION
custgrp	STRING RANGE	CUSTOMER_GROUP

Responses**Response**

NO VOW DATA ASSOCIATED WITH CUSTOMER GROUP.

Explanation:

An attempt was made using one of the subcommands in the VOWCI CI increment to access VOW data for a specific customer group which has no associated VOW data.

System action:

The system response is output at the MAP.

User action:

The user should correct the customer group to one which has associated VOW data.

Notes

None

Examples

None

Alarms

None

Performance Management for A00002011**Operational measurement changes (OM)**

This section contains operational measurement information from the original design document (AX1236OM.AA20).

It has not been modified from the original version.

New/modified OM group list

GROUP NAME (acronym)	GROUP NAME (expanded)	NEW, CHANGED or DELETED	REASON
VOW	VIRTUAL OFFICE WORKER	NEW	Created to track use of VOW functionality.

OM Group: VOW

This OM group tracks the use of VOW functionality.

Group structure

Key field: CUSTOMER_GROUP

Info field: NIL_TYPE_ID

Number of tuples: 1

Datafill

Table VOWINV is related to this OM group.

Register list

The following registers exist within this OM group: INPASS, INFAIL, OUTPASS, OUTFAIL, CINPASS, CINFAIL, COUTPASS, COUTFAIL, AUDPASS, AUDFAIL, PCCPASS, PCCFAIL, ROUTPASS, ROUTFAIL.

Associated OM groups

No OM groups are associated with this group.

Validation formula

$\text{INPASS} + \text{INFAIL} = \text{Total VOWIN Attempts}$

$\text{OUTPASS} + \text{OUTFAIL} = \text{Total VOWOUT Attempts}$

$\text{PCCPASS} + \text{PCCFAIL} = \text{Total VOWPCC Attempts}$

$\text{CINPASS} + \text{CINFAIL} = \text{Total CKLN/CLN Login Attempts}$

$\text{COUTPASS} + \text{COUTFAIL} = \text{Total CKLN/CLN Logout Attempts}$

$\text{AUDPASS} + \text{AUDFAIL} = \text{Total Audit Logout Attempts}$

$\text{ROUTPASS} + \text{ROUTFAIL} = \text{Total VOWROUT Attempts}$

Associated products

This OM group is associated with VOW functionality which is specific to the MSL-100 product.

OMSHOW example

TBD

OM Logic flow or pseudocode

INPASS is pegged for a successful VOWIN attempt.

INFAIL is pegged for a failed VOWIN attempt.

OUTPASS is pegged for a successful VOWOUT attempt.

OUTFAIL is pegged for a failed VOWOUT attempt.

CINPASS is pegged for a successful VOW login attempt using CKLN/CLN.

CINFAIL is pegged for a failed VOW login attempt using CKLN/CLN.

COUTPASS is pegged for a successful VOW logout attempt using CKLN/CLN.

COUTFAIL is pegged for a failed VOW logout attempt using CKLN/CLN.

PCCPASS is pegged for a successful VOWPCC attempt.

PCCFAIL is pegged for a failed VOWPCC attempt.

AUDPASS is pegged for a successful VOW logout through the VOW audit.

AUDFAIL is pegged for a failed VOW logout through the VOW audit.

ROUTPASS is pegged for a successful VOWROUT attempt.

ROUTFAIL is pegged for a failed VOWROUT attempt.

New/modified registers**VOW Registers**

REGISTER NAME (acronym)	REGISTER NAME (expanded)	NEW ACTIVATED CHANGED ZEROED DELETED	BCS NUMBER
INPASS	VOWIN Pass	New	MSL10
INFAIL	VOWIN Fail	New	MSL10
OUTPASS	VOWOUT Pass	New	MSL10
OUTFAIL	VOWOUT Fail	New	MSL10
CINPASS	VOW CKLN/CLN Login Pass	New	MSL10
CINFAIL	VOW CKLN/CLN Login Fail	New	MSL10
COUTPASS	VOW CKLN/CLN Logout Pass	New	MSL10
COUTFAIL	VOW CKLN/CLN Logout Fail	New	MSL10
PCCPASS	VOW Passcode Change Pass	New	MSL10
PCCFAIL	VOW Passcode Change Fail	New	MSL10
AUDPASS	VOW Audit Logout Pass	New	MSL10
AUDFAIL	VOW Audit Logout Fail	New	MSL10
ROUTPASS	VOWROUT Pass	New	MSL10
ROUTFAIL	VOWROUT Fail	New	MSL10

Register name: INPASS**Register type**

Peg

Register description

INPASS is pegged for a successful VOWIN attempt.

Associated register

INFAIL

Validation formula
$$\text{INPASS} + \text{INFAIL} = \text{Total VOWIN Attempts}$$

Associated logs**Log number: VOW501**

This log report is generated when a successful VOWIN attempt occurs.

EXT register

None

Register name: INFAIL**Register type**

Peg

Register description

INFAIL is pegged for a failed VOWIN attempt.

Associated register

INPASS

Validation formula

$\text{INPASS} + \text{INFAIL} = \text{Total VOWIN Attempts}$

Associated logs

Log number: VOW502

This log report is generated when a failed VOWIN attempt occurs.

EXT register

None

Register name: OUTPASS**Register type**

Peg

Register description

OUTPASS is pegged for a successful VOWOUT attempt.

Associated register

OUTFAIL

Validation formula

$\text{OUTPASS} + \text{OUTFAIL} = \text{Total VOWOUT Attempts}$

Associated logs

Log number: VOW501

This log report is generated when a successful VOWOUT attempt occurs.

EXT register

None

Register name: OUTFAIL**Register type**

Peg

Register description

OUTFAIL is pegged for a failed VOWOUT attempt.

Associated register

OUTPASS

Validation formula

$\text{OUTPASS} + \text{OUTFAIL} = \text{Total VOWOUT Attempts}$

Associated logs

Log number: VOW502

This log report is generated when a failed VOWOUT attempt occurs.

EXT register

None

Register name: CINFAIL**Register type**

Peg

Register description

CINPASS is pegged for a successful VOW login attempt using CKLN/CLN.

Associated register

CINFAIL

Validation formula

$\text{CINPASS} + \text{CINFAIL} = \text{Total CKLN/CLN Login Attempts}$

Associated logs

Log number: VOW501

This log report is generated when a successful VOW login through CKLN/CLN occurs.

EXT register

None

Register name: CINFAIL**Register type**

Peg

Register description

CINFAIL is pegged for a failed VOW login attempt using CKLN/CLN.

Associated register

CINPASS

Validation formula

$\text{CINPASS} + \text{CINFAIL} = \text{Total CKLN/CLN Login Attempts}$

Associated logs

Log number: VOW502

This log report is generated when a failed VOW login through CKLN/CLN occurs.

EXT register

None

Register name: COUTPASS**Register type**

Peg

Register description

COUTPASS is pegged for a successful VOW logout attempt using CKLN/CLN.

Associated register

COUTFAIL

Validation formula

$\text{COUTPASS} + \text{COUTFAIL} = \text{Total CKLN/CLN Logout Attempts}$

Associated logs

Log number: VOW501

This log report is generated when a successful VOW logout through CKLN/CLN occurs.

EXT register

None

Register name: COUTFAIL**Register type**

Peg

Register description

COUTFAIL is pegged for a failed VOW logout attempt using CKLN/CLN.

Associated register

COUTPASS

Validation formula
$$\text{COUTPASS} + \text{COUTFAIL} = \text{Total CKLN/CLN Logout Attempts}$$
Associated logs

Log number: VOW502

This log report is generated when a failed VOW logout through CKLN/CLN occurs.

EXT register

None

Register name: PCCPASS**Register type**

Peg

Register description

PCCPASS is pegged for a successful VOWPCC attempt.

Associated register

PCCFAIL

Validation formula
$$\text{PCCPASS} + \text{PCCFAIL} = \text{Total VOWPCC Attempts}$$
Associated logs

Log number: VOW501

This log report is generated when a successful VOWPCC attempt occurs.

EXT register

None

Register name: PCCFAIL**Register type**

Peg

Register description

PCCFAIL is pegged for a failed VOWPCC attempt.

Associated register

PCCPASS

Validation formula
$$\text{PCCPASS} + \text{PCCFAIL} = \text{Total VOWPCC Attempts}$$
Associated logs

Log number: VOW502

This log report is generated when a failed VOWPCC attempt occurs.

EXT register

None

Register name: AUDPASS**Register type**

Peg

Register description

AUDPASS is pegged for a successful VOW logout through the VOW audit.

Associated register

AUDFAIL

Validation formula
$$\text{AUDPASS} + \text{AUDFAIL} = \text{Total Audit Logout Attempts}$$
Associated logs

Log number: VOW501, VOW601

VOW501 is generated when a successful logout through the VOW audit occurs. VOW601 is generated when the VOW audit completes.

EXT register

None

Register name: AUDFAIL**Register type**

Peg

Register description

AUDFAIL is pegged for a failed VOW logout through the VOW audit.

Associated register

AUDPASS

Validation formula

$\text{AUDPASS} + \text{AUDFAIL} = \text{Total Audit Logout Attempts}$

Associated logs

Log number: VOW502, VOW601

VOW502 is generated when a failed logout through the VOW audit occurs.

VOW601 is generated when the VOW audit completes.

EXT register

None

Register name: ROUTPASS**Register type**

Peg

Register description

ROUTPASS is pegged for a successful VOWROUT attempt.

Associated register

ROUTFAIL

Validation formula

$\text{ROUTPASS} + \text{ROUTFAIL} = \text{Total VOWROUT Attempts}$

Associated logs

Log number: VOW501

This log report is generated when a successful VOWROUT attempt occurs.

EXT register

None

Register name: ROUTFAIL**Register type**

Peg

Register description

OUTFAIL is pegged for a failed VOWROUT attempt.

Associated register

ROUTPASS

Validation formula
$$\text{ROUTPASS} + \text{ROUTFAIL} = \text{Total VOWROUT Attempts}$$
Associated logs

Log number: VOW502

This log report is generated when a failed VOWROUT attempt occurs.

EXT register

None

Test case(s)

None

Product = CS 2000**A00002012 -- HIOP-CMIC/RTIF development (Succession on DMS)*****Functional Description***

This document provides an overview of the functionality provided by the Operations, Administration, and Maintenance (OAM) software for the High Performance Input Output Processor card (HIOP) with CMIC, RTIF, TOD, and ETHR functionality (CMIC/RTIF HIOP).

This HIOP card supports the following functionalities:

- Core to Message Switch (MS) InterConnect (CMIC), providing high speed access to the DMS Message Switch via OC3 links,
- Reset Terminal InterFace (RTIF). The RTIF local ports support XA-Core connectivity to Video Display Terminals (VDT) (EIA RS232 standard). The RTIF remote ports provide connection to remote terminals via modem (EIA RS422 standard).

- Time Of Day (TOD) support, and
- Ethernet, providing high speed access to the Succession Network via 100Mb/s full duplex ethernet links.

Note: the OAM changes related to the Ethernet functionality were delivered by the XA-Core Ethernet Maintenance feature and are described in document AT.59019176 in fmdoc.

Note: this feature does not introduce any changes to the Reset Terminal Interface (RTIF) behavior. The RTIF components are backwards compatible to the packetlet.

This software provides the maintenance interface to the craft person for monitoring and manipulating the state of the HIOP common equipment, the CMIC, RTIF, ETHR ports and links, and TOD. For more information on the HIOP circuit pack, please refer to document 'HIOP Maintenance Software' (AT.59029980).

The components of the interface to the XA-Core are consistent with the XA-Core OAM interface. These include the maintenance administration position (MAP), logs, alarms, and operational measurements (OMs). All maintenance, fault handling, redundancy checking, and event reporting functionalities provided by this feature are consistent with established XA-Core maintenance procedures and guidelines.

The software associated with XA-Core CMIC/RTIF HIOP OAM Software provides the following functionality:

- changes the existing CMIC MAP level and MAP commands in order to maintain the new CMIC ports,
- changes the existing RTIF MAP level and MAP commands in order to maintain the new RTIF links (local and remote),
- changes the existing alarms, logs, and operational measurements that report on the maintenance status of the CMIC and RTIF ports and links.

HIOP card description

The CMIC/RTIF HIOP card is similar to the NTLX04CA HIOP card that supports AMDI, ETHR, and RTIF functionality. The main hardware difference between the two is the transmitter used in the OC3 hardware:

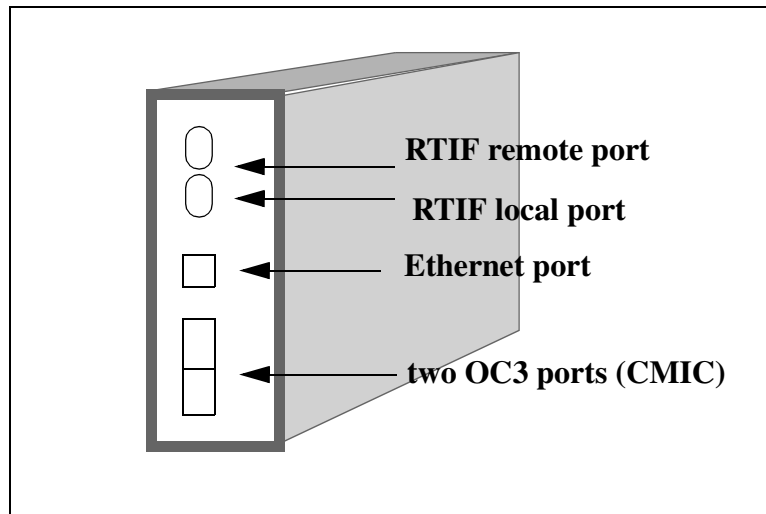
- the NTLX04CA HIOP card has single-mode transmitter (OC3 used for AMDI),
- the CMIC/RTIF HIOP card has multi-mode transmitter (OC3 used for CMIC).

The XA-Core CMIC/RTIF HIOP circuit pack is equipped with:

- two OC3 ports,
- one ethernet port, and
- two RTIF ports: one RS232 RTIF local port and one RTIF remote port.

Unlike circuit pack NTLX03 (IOP), the HIOP card does not support packlets. Please refer to “HIOP card” on page 285.

HIOP card



The HIOP LED strategy follows established XA-Core guidelines: the card is equipped with one red and one green LED which show the status of the card. Three additional amber LEDs represent presence or loss of signal on RTIF, ETHR, and CMIC links respectively.

The XA-Core Visual Indicator (LED) Strategy is described in XA0015FN.

Interactions

- XA-Core HIOP Maintenance Software: AT.59029980,
- XA-Core Ethernet Maintenance feature: AT.59019176,
- XA-Core Visual Indicator (LED) Strategy: XA0015,
- XA-Core provisioning feature: AT.59009527.

Applicable customer facing sections

Fault Management

Logs	__X__
Alarms	__X__
Configuration	
Data Schema	__N/A__
User Interface	__X__
Element Management	__N/A__
Security	__N/A__
Service Order	__N/A__
Office Parameters	__N/A__
Accounting (includes AMA billing)	__N/A__
Performance (includes operational measurements)	__X__

Glossary

Term	Description
AMDI	ATM Multimode Data Interface
CMIC	Core to MS InterConnect
DMS	Digital Multiplex Switch
ETHR	Ethernet
HIOP	High performance Input Output Processor
MAP	Maintenance Administration Position
MS	Message Switch
OAM	Operations, Administration, and Maintenance
OM	Operational Measurement
PIDR	P side IDentification Register
RTIF	Reset Terminal InterFace
SN	SuperNode
SNSE	SuperNode Shelf Extension
TOD	Time Of Day
VDT	Video Display Terminals
XA-Core, XAC	eXtended Architecture Core

Fault Management for A00002012

This feature does not change the fault management strategy of the XA-Core.

Fault management tools and utilities

This feature does not change the fault management tools and utilities of the XA-Core.

Logs

CMIC XAC log changes

Since this feature introduces port/link separation for the CMIC functionality on HIOP, the XAC information and action logs will now show the new CMIC port device, in addition to the CMIC packets and CMIC links. The feature does not change the format of either the information or action logs.

- CMIC packets and CMIC links on packet are going to be shown the same way as before (no port/link separation for CMIC packets),
- CMIC ports and links on HIOP will have the packet field left blank.

The XAC610 log is chosen to show the difference.

Current XAC610 Log for CMIC packet:

```
XA506AX      XAC610 JAN29 06:37:35 8000 RTS   Returned To Service
DESCRIPTION: State has changed from SYSB to INSV by RECOVERY action
CARD:   Type State Site FL Row Bay   Shf/Slt/Pk   EqPEC/Serial
        CMIC INSV  HOST 01 A00 DPCC:00 00 15R L   NTLX05AB/NNTM171VY7C0
```

Current XAC610 Log for CMIC link on packet:

```
XA506AX      XAC610 JAN29 06:37:35 8000 RTS   Returned To Service
DESCRIPTION: State has changed from SYSB to INSV by MS-MTCE action
LINK:   Type State Site FL Row Bay   Shf/Slt/Pk/Lk   EqPEC/Serial
        CMIC INSV  HOST 01 A00 DPCC:00 00 15R L   1   NTLX05AB/NNTM171VY7C0
```

New XAC610 Log for CMIC port on HIOP (packet field blank):

```
XA506ax      XAC610 MAR05 17:54:47 1200 RTS   Returned To Service
DESCRIPTION: State has changed from SYSB to INSV by RECOVERY action
PORT:   Type State Site FL Row Bay   Shf/Slt/Pk/Pt   EqPEC/Serial
        CMIC INSV  HOST 01 A00 DPCC:00 00 15R   1   NTLX17AA/NNTM64422MWV
```

New XAC610 Log for CMIC link on HIOP (packet field blank):

```
XA506ax      XAC610 MAR05 17:54:47 1200 RTS   Returned To Service
DESCRIPTION: State has changed from SYSB to INSV by MS-MTCE action
LINK:   Type State Site FL Row Bay   Shf/Slt/Pk/Lk   EqPEC/Serial
        CMIC INSV  HOST 01 A00 DPCC:00 00 15R   1   NTLX17AA/NNTM64422MWV
```

RTIF XAC log changes

Since this feature introduces port/link separation for the RTIF functionality on HIOP, the XAC information and action logs will now show the new RTIF link

device, in addition to the RTIF packets and RTIF ports. This feature does not change the format of either the information or action logs.

- RTIF packets are going to be shown the same way as before,
- RTIF port representation on packets will be changed to RTIF links: Llink0 and Link1,
- RTIF ports and links on HIOP will have the packet field left blank.

The XAC610 log is chosen to show the difference.

Current XAC610 Log for RTIF packet:

```
XA506BH      XAC605 MAR05 10:11:02 6800 INFO RTIF Alarm Cleared
DESCRIPTION: State has changed from MBSY to INSV by MANUAL action
CARD: Type State Site FL Row Bay   Shf/Slt/Pk   EqPEC/Serial
RTIF INSV  HOST 01 A00 DPCC:00 00 04R U  NTLX08AA/NNTM171P3G37
```

Current XAC610 Log for RTIF port on packet (port will be obsoleted):

```
XA506BH      XAC605 MAR05 10:11:02 6800 INFO RTIF Alarm Cleared
DESCRIPTION: State has changed from MBSY to INSV by MANUAL action
PORT: Type State Site FL Row Bay   Shf/Slt/Pk/Pt   EqPEC/Serial
RTIF INSV  HOST 01 A00 DPCC:00 00 04R U  0 NTLX08AA/NNTM171P3G37
```

New XAC610 Log for RTIF link on packet (no port field on packet):

```
XA506BH      XAC605 MAR05 10:11:02 6800 INFO RTIF Alarm Cleared
DESCRIPTION: State has changed from MBSY to INSV by MANUAL action
LINK: Type State Site FL Row Bay   Shf/Slt/Pk/Lk   EqPEC/Serial
RTIF INSV  HOST 01 A00 DPCC:00 00 04R U  0 NTLX08AA/NNTM171P3G37
```

New XAC610 Log for RTIF port on HIOP (packet field blank):

```
XA506BH      XAC605 MAR05 10:11:02 6800 INFO RTIF Alarm Cleared
DESCRIPTION: State has changed from MBSY to INSV by MANUAL action
PORT: Type State Site FL Row Bay   Shf/Slt/Pk/Pt   EqPEC/Serial
RTIF INSV  HOST 01 A00 DPCC:00 00 04R    0 NTLX17AA/  NNTM171P3G37
```

New XAC610 Log for RTIF link (packet field blank):

```
XA506BH      XAC605 MAR05 10:11:02 6800 INFO RTIF Alarm Cleared
DESCRIPTION: State has changed from MBSY to INSV by MANUAL action
LINK: Type State Site FL Row Bay   Shf/Slt/Pk/Lk   EqPEC/Serial
RTIF INSV  HOST 01 A00 DPCC:00 00 04R    0 NTLX17AA/NNTM171P3G37
```

IO XAC log changes

Since this feature introduces the new CMIC/RTIF HIOP card, minor modifications are needed to the impact statement of the existing XAC logs for this new resource. There is no other change for any information or action logs.

Current XAC312 Log for AMDI/RTIF/ETHR HIOP:

```
S106BI      * XAC312 MAR11 10:24:19 6700 FLT  IOP (Input Output Processor Fault)
IMPACT: AMDI, Ethernet and RTIF services are unavailable on this IO
DESCRIPTION: State has changed from INSV to MBSY by MANUAL action
CARD: Type State Site FL Row Bay   Shf/Slt           EqPEC/Serial
HIOP MBSY  HOST 01 A00 DPCC:00 00 05R           NTLX04BA/  NNTM64422MWV
```

XAC312 Log for new CMIC/RTIF HIOP (different impact statement):

```
S106BI * XAC312 MAR11 10:24:19 6700 FLT IOP (Input Output Processor Fault)
IMPACT: CMIC, Ethernet and RTIF services are unavailable on this IO
DESCRIPTION: State has changed from INSV to MBSY by MANUAL action
CARD: Type State Site FL Row Bay Shf/Slt EqPEC/Serial
      HIOP MBSY HOST 01 A00 DPCC:00 00 05R NTLX17AA/ NNTM64422MWV
```

Alarms

This feature does not add or remove any existing XA-Core system alarms which are displayed under the XAC title in the alarm banner. It only adds to the scenarios by which the MSComm XAC Alarm is raised.

MScomm alarm

The MScomm alarm is raised if there is a communication problem between the XA-Core and the Message Switch (MS).

Current MScomm alarm and CMIC link RTS behavior

Currently, the MScomm alarm is raised only if a hardware component used for the communication between the XA-Core and the Message Switch (MS) goes out of service, on either the XA-Core or MS side. The following severities can be observed:

- CRITICAL: no communication,
- MAJOR: no communication link redundancy,
- MINOR: communication link redundancy is partially lost.

Configuration problems with the CMIC links between the XA-Core and the Message Switch (MS) do *not* directly raise the MScomm alarm. The alarm is raised indirectly by the fact that the system will not bring the misconfigured CMIC link in-service.

Following steps show how the current system behavior handles CMIC link misconfiguration on a packet:

- the CMIC link on the packet gets misconfigured,
- the CMIC link will *not* come in-service,
- the XAC326 'MS link Configuration Mismatch' log is generated,
- the XAC303 'MScomm' log is generated, and
- as a consequence of the CMIC link will being out of service, the MScomm XAC alarm is raised.

Once the correct configuration is established, the following will occur:

- the CMIC link on the packlet will come in-service,
- the XAC626 'MS Link Configuration Restored' log is generated,
- the XAC603 'MScomm Alarm Cleared' log is generated,
- the MScomm XAC alarm is cleared.

Recommended XA-Core to MS configuration

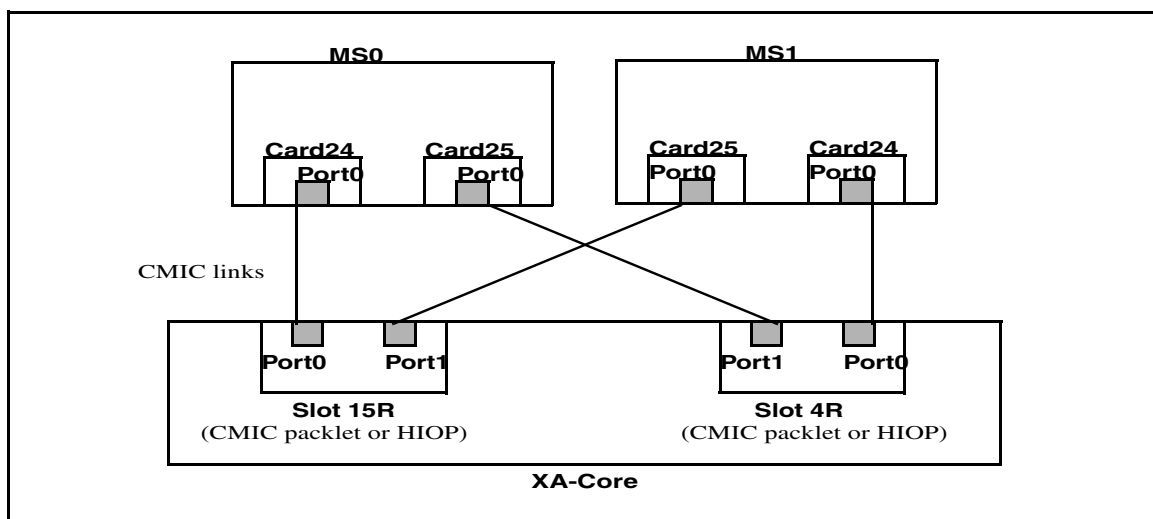
Currently, the only supported configuration between the XA-Core and the Message Switch (MS) requires four CMIC links to be cross-connected between the XA-Core and the Message Switch (MS), with specific mappings between the MS CMIC paddle board ports and the XA-Core CMIC links. This setup provides the maximum CMIC link redundancy, and node and component isolation protection.

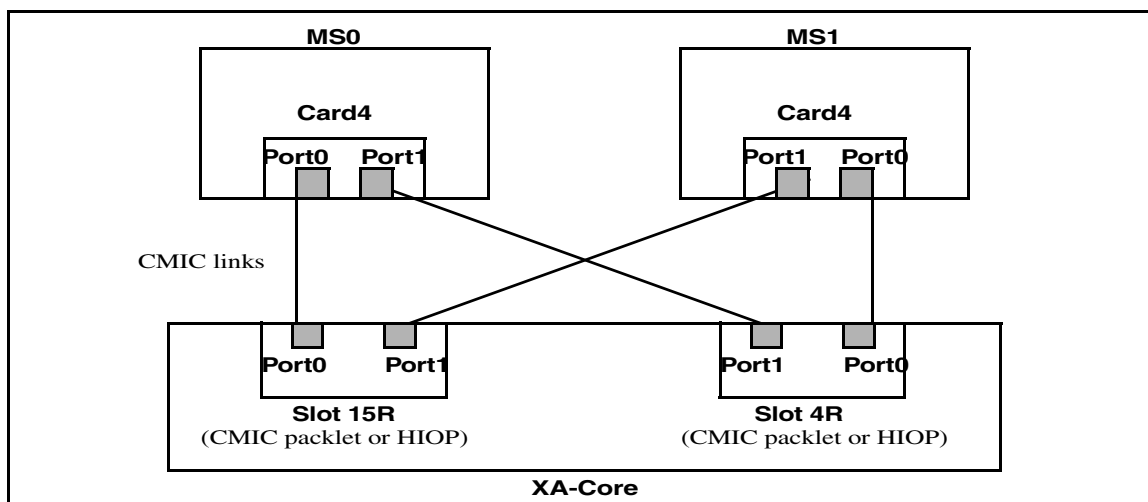
Note: This feature does *not* change the currently recommended XA-Core to MS configuration.

Please refer to “Recommended XA-Core - MS configuration (SuperNode)” on page 290.

Please refer to “Recommended XA-Core - MS configuration (SuperNode SE)” on page 291.

Recommended XA-Core - MS configuration (SuperNode)



Recommended XA-Core - MS configuration (SuperNode SE)**New MSComm alarm and CMIC link RTS behavior**

This feature adds to the scenarios that raise the MSComm XAC Alarm.

Presently, the MSComm alarm is raised only if a hardware component used for the communication between the XA-Core and the Message Switch (MS) goes out of service, on either the XA-Core or MS side.

In addition to these scenarios, from now on, an MSComm MAJOR alarm will also be raised if a CMIC link between the XA-Core and the Message Switch (MS) is in-service but not configured properly.

Support for new XA-Core to MS configuration

This feature does *not* change the currently recommended XA-Core to MS configuration.

Please refer to “Recommended XA-Core - MS configuration (SuperNode)” on page 290.

Please refer to “Recommended XA-Core - MS configuration (SuperNode SE)” on page 291.

However, with the introduction of flexible provisioning of CMIC components, the system will be able to support new XA-Core to MS configurations. CMIC packets or CMIC/RTIF HIOPs can possibly be provisioned in any empty (unequipped) element slots. The same redundancy and isolation protection rules are going to be applied as before.

This new approach will help the system to adapt more gracefully to CMIC link misconfigurations. For example, this will avoid a possible boot loop during commissioning of a new XA-Core office when all CMIC links are

misconfigured with respect to the recommended setup (still satisfying all redundancy and isolation protection rules). Instead of failing the boot, the system will successfully boot and bring the CMIC links in-service. Once the system is up and running, craft personnel can rectify the CMIC link misconfiguration.

The system behavior with respect to bringing a misconfigured CMIC link in-service is different depending on the following scenarios:

- a misconfigured CMIC link is being newly provisioned by the system (e.g. boot, restart, provisioning): the system will bring the misconfigured CMIC link in-service and raise the MScomm MAJOR alarm. Please refer to Section “ Misconfigured CMIC link provisioning” on page 292.
- an already provisioned CMIC link is improperly connected into a different port (e.g. card replacement): the system will *not* bring the misconfigured CMIC link in-service. Please refer to Section “ Provisioned CMIC link is misconfigured” on page 293.

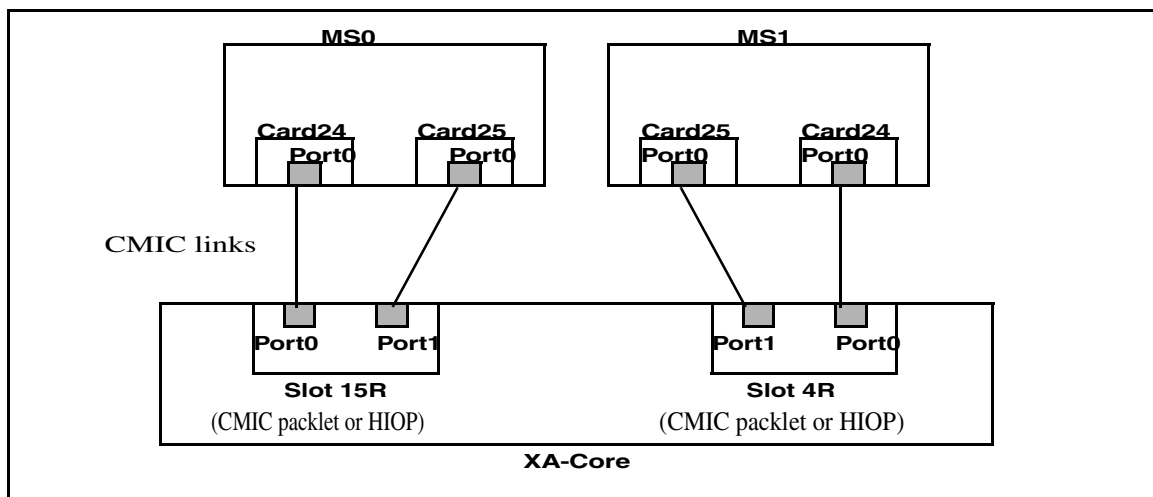
Misconfigured CMIC link provisioning

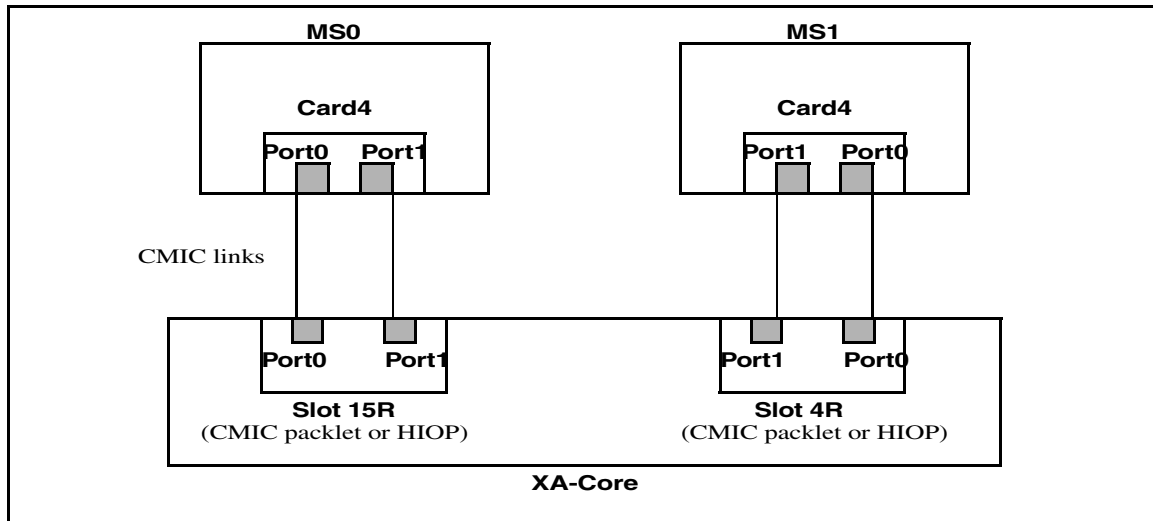
This scenario can happen during boot, restart, and provisioning.

Please refer to “ CMIC links not cross-connected (SuperNode)” on page 292.

Please refer to “ CMIC links not cross-connected (SuperNode SE)” on page 293.

CMIC links not cross-connected (SuperNode)



CMIC links not cross-connected (SuperNode SE)

Following steps show how the new system behavior handles CMIC link misconfiguration during boot, restart, and provisioning:

- the CMIC links get misconfigured (e.g. during commissioning of a new XA-Core office),
- the system will bring the CMIC links in-service,
- the XAC326 MS link Configuration Mismatch log is generated,
- although all CMIC components are in-service, the MScomm XAC MAJOR alarm is raised because of the configuration error.

Once the correct configuration is established, the following will occur:

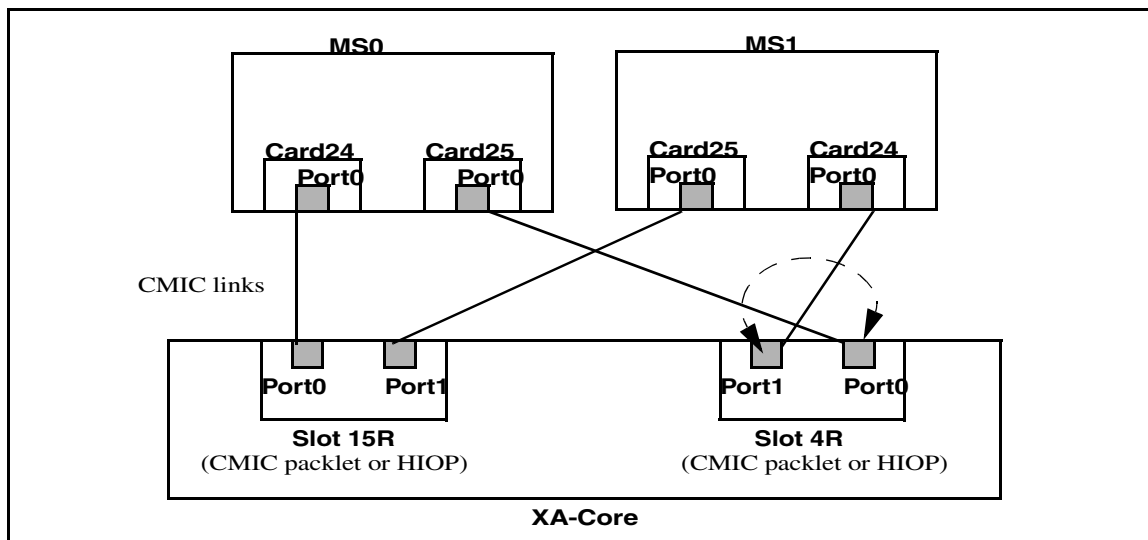
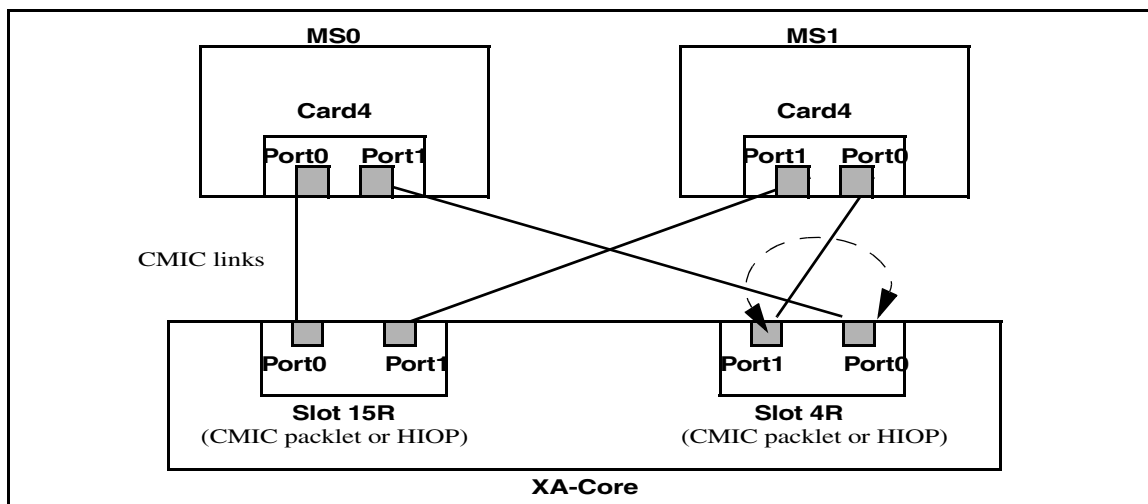
- the XAC626 'MS Link Configuration Restored' log is generated,
- the MScomm XAC alarm is cleared,

Provisioned CMIC link is misconfigured

This scenario can happen during a card replacement procedure. That is, two existing (provisioned) CMIC links on the same FRU are interchanged and incorrectly connected into the other port.

Please refer to “Interchanged CMIC links on same FRU (4R) (SuperNode)” on page 294.

Please refer to “Interchanged CMIC links on same FRU (4R) (SuperNode SE)” on page 294.

Interchanged CMIC links on same FRU (4R) (SuperNode)**Interchanged CMIC links on same FRU (4R) (SuperNode SE)**

Following steps show how the new system behavior handles CMIC link misconfiguration during card replacement:

- during a card replacement procedure, the CMIC links on a given FRU get misconfigured,
- the system will *not* bring the CMIC links in-service,
- the XAC326 MS link Configuration Mismatch log is generated,

- the MScomm XAC MAJOR alarm is raised because of the out of service CMIC links.

Once the correct configuration is established, the following will occur:

- the XAC626 'MS Link Configuration Restored' log is generated,
- the MScomm XAC alarm is cleared,
- the system will attempt to bring the OOS CMIC links in-service.

Configuration for A00002012

Command interface changes

Currently on XA-Core, the CMIC functionality on packet is provided by a CMIC link. The RTIF functionality on packet is provided by an RTIF port. With the introduction of the CMIC/RTIF HIOP card, port/link separation will be implemented for the CMIC and RTIF functionalities on HIOP. That is, both services will be maintained by a port and a link. Hence, the CMIC and RTIF MAP levels have to change to reflect the new port/link separation.

Note: this feature does not implement port/link separation on CMIC and RTIF packets.

Port/link separation has already been done for the ETHR and AMDI functionality on the HIOP card by the Ethernet Maintenance feature (A59019176) and the HIOP ATM Maintenance software feature (A59035251). In order to have consistent MAP representation of ports and links in the XA-Core system, this feature will reuse the OAM design decisions applied for those features.

IO MAP level

Currently on the IO MAP level, the CMIC and RTIF functionality are only represented on packets in lower and upper positions. No 'middle' packets exist. Please refer to "IO MAP with CMIC and RTIF packets on IOPs in slots 4R and 15R" on page 296. With the introduction of the CMIC/RTIF HIOP, these functionalities can be hosted on either packets or HIOP cards. Please refer to "IO MAP with CMIC/RTIF HIOPs in slots 4R and 15R" on page 296.

IO MAP with CMIC and RTIF packets on IOPs in slots 4R and 15R

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.	.	.	.	.	.	.
IO		Front:	111111111	Rear:	111111	SM	PE	IO	PKLT
0 Quit		123456789012345678	456789012345	.	.	.	.	.	.
2		Sta:			0	0	0	0	
3		Dep:							
4		Typ:	*	*	*	*			
5		Slot: Side: Status:			Upper:	Middle:	Lower:		
6 Tst_		2 Front	.		Tape	.	Disk	.	
7 Bsy_		17 Front	.		Tape	.	Disk	.	
8 RTS_		4 Rear	.		RTIF	.	CMIC	.	
9		15 Rear	.		RTIF	.	CMIC	.	
10 LoadFW_									
11									
12 Uneq_									
13									
14 Alarm_									
15									
16									
17 Indicat_									
18 Query_									
XMAP0									
Time 14:12									

IO MAP with CMIC/RTIF HIOPs in slots 4R and 15R

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.	.	.	.	.	.	.
IO		Front:	111111111	Rear:	111111	SM	PE	IO	PKLT
0 Quit		123456789012345678	456789012345	.	.	.	.	.	.
2		Sta:			0	0	0	0	
3		Dep:							
4		Typ:	*	*	*	*			
5		Slot: Side: Status:			Upper:	Middle:	Lower:		
6 Tst_		2 Front	.		Tape	.	Disk	.	
7 Bsy_		17 Front	.		Tape	.	Disk	.	
8 RTS_		4 Rear	.		RTIF	.	ETHR	.	CMIC
9		15 Rear	.		RTIF	.	ETHR	.	CMIC
10 LoadFW_									
11									
12 Uneq_									
13									
14 Alarm_									
15									
16									
17 Indicat_									
18 Query_									
XMAP0									
Time 14:12									

CMIC MAP level

Currently, the CMIC functionality can only be hosted by a CMIC packet on an IOP card. Please refer to “Current CMIC MAP level with CMIC packets in slots 4R and 15R” on page 297.

Current CMIC MAP level with CMIC packets in slots 4R and 15R

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.	.	.	.	.	.	.
CMIC									
0	Quit		Front: 111111111	Rear: 111111	SM	PE	IO	PKLT	
2			123456789012345678	456789012345	.	.	.	.	
3			Sta: . . . - . . . - . .	 -	0	0	0	0	
4			Dep:						
5			Typ:	*	*				
6	Tst_		Slot: 4	Side: Rear	Packlet: Lower	Status: .	Link0: .	Link1: .	TOD: .
7	Bsy_		15	Rear	Lower	.	.	.	.
8	RTS_								
9									
10	loadFW_								
11									
12	Uneq_								
13	Route_								
14	Alarm_								
15	Cntrs_								
16	Trnsl_								
17	Indicat_								
18	Query_								
XMAP0									
Time 14:12 >									

With the introduction of the CMIC/RTIF HIOP, the new CMIC MAP will show the functionality hosted by either a CMIC packet on an IOP card, or by a CMIC/RTIF HIOP. Also, with CMIC port/link separation on CMIC/RTIF HIOP, new CMIC port0 and CMIC port1 components will be shown on the CMIC MAP level. Furthermore, instead of showing one TOD device component per CMIC packet, two TOD devices will be shown for each CMIC/RTIF HIOP card: TOD0 and TOD1.

Summary of CMIC MAP field changes

Component	Current MAP field	New MAP field	New/Deleted/Changed
CMIC Port 0	n/a	'Port0'	new
CMIC Port 1	n/a	'Port1'	new
CMIC Link TOD	'TOD'	'TOD0'	changed
CMIC Link1 TOD	n/a	'TOD1'	new

For CMIC packets represented on the new CMIC MAP level, the following components will be shown as before: Slot, Side, Packlet, Status, link0, and link1. Port0 and port1 components will be left blank. The TOD component will be represented by the new TOD0 component. The TOD1 component will be left blank. Please refer to “New CMIC MAP level with CMIC packets in slots 4R and 15R” on page 298.

New CMIC MAP level with CMIC packets in slots 4R and 15R

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.	.	.	.	.	.	.
CMIC									
0 Quit			Front: 111111111		Rear: 111111	SM	PE	IO	PKLT
2			123456789012345678		456789012345	.	.	.	.
3			Sta:		Dep:	0	0	0	0
4			Typ:	*	*				
5			Slot:		Side:	Packlet	Status:	Port0	Port1
6 Tst_			4	Rear	Lower	.	.	.	.
7 Bsy_			15	Rear	Lower	.	.	.	.
8 RTS_									
9									
10 loadFW_									
11									
12 Uneq_									
13 Route_									
14 Alarm_									
15 Cntrl_									
16 Trnsl_									
17 Indicat_									
18 Query_									
XMAP0									
Time 14:12 >									

For CMIC functionality on CMIC/RTIF HIOP represented on the new CMIC MAP level, since the card does not have packets, the 'Packlet' location field, and the packet 'Status' field will be left blank. Also, in addition to the two CMIC links, there are going to be two new CMIC ports shown (Port0 and Port1), as well as two TOD devices for each CMIC/RTIF HIOP card (TOD0 and TOD1). Please refer to "New CMIC MAP level with CMIC/RTIF HIOPs in slot 4R and 15R" on page 299.

of CMIC packets was not supported since they were part of the 'fixed' XA-Core configuration (slots 4R and 15R). From now on, deprovisioning of CMIC components is needed for the migration of CMIC packets to CMIC/RTIF HIOP cards and back.

Summary of the new 'uneq' CMIC MAP level command

Command	Menu#	Type	Options	Function
uneq	12	Operational	None	- Deprovision a CMIC packet on an IOP card - Deprovision a CMIC link on an HIOP card

Command syntax

The 'uneq' command requires parameters. If you do not enter any parameters or you enter invalid parameters, the MAP terminal displays an error message. The MAP terminal prompts you to enter a correct parameter value.

'uneq' command parameters and variables

Command	Parameters and variables
uneq	- slot number (0 to 17), - side (front, f or rear, r), - packet position (upper, u, or lower, l), - link number (link0 or link1).
Parameters and variables	Description
slot number	Use the 'slot number' parameter value to indicate the number of the physical shelf slot: 0 to 17
side	Use the 'side' parameter value to indicate the component location in the physical shelf: front, f or rear, r
packet position	Use the 'packet position' parameter value to indicate the CMIC packet location on an IOP card: upper, u or lower, l. This is used only for CMIC packet deprovisioning and is not used for CMIC link.
link number	Use the 'link number' parameter value to indicate the CMIC link position on a CMIC/RTIF HIOP card: link0 or link1. This is used only for CMIC link deprovisioning and is not used for CMIC packets.

Note: The 'slot number' parameter value will usually be '4' or '15'. The 'side' parameter value will usually be 'rear' or 'r'. The 'packet position' parameter value will usually be 'lower' or 'l'.

Qualifications and warnings

The 'uneq' command should be used with great care since it deprovisions a component from the XA-Core system. There are some general requirements for the successful completion of the 'uneq' command. They are (in order):

- first, the component must be brought into a 'ManB' state,
- then, the component must be pulled from the shelf,
- finally, the 'uneq' command can be issued for the component.

Since the 'uneq' command on the CMIC MAP level can be issued for the CMIC packlet residing on an IOP card or for a CMIC link residing on an HIOP card, the command usage will be different depending on the component being deprovisioned. Please refer to Section "Example" on page 302.

Note: Deprovisioning of CMIC links on packlets is not supported.

MAP Responses**MAP outputs with associated meanings and actions**

Command
RESPONSE: Command submitted. Uneq 4 Rear Lower completed. Meaning: This response indicates that the 'uneq' command has completed successfully. System or user actions: none
RESPONSE: Command submitted. Improper state for required action, no action take Meaning: this response indicates that the 'uneq' command has been issued without bringing the component into the 'ManB' state first. System or user actions: the craft person has to 'ManB' the component
RESPONSE: Command submitted H/W must be removed from shelf, no action taken Meaning: this response indicates that the 'uneq' command has been issued without removing the component from the shelf, or without waiting long enough for the system to recognize the component's loss of clock. System or user actions: the craft person has to remove the component from the shelf. If the component is already removed, the craft person has to wait long enough (e.g. one minute) for the system to recognize the component's loss of clock.

MAP outputs with associated meanings and actions

Command
RESPONSE: Card/device is unadressable...no action taken. Meaning: this response indicates that there is no provisioned component in the given location. System or user actions: the craft person has to check the FRU location
RESPONSE: Either incorrect optional parameter(s) OR too many parameters Meaning: this response indicates that the 'uneq' command was issued without following the correct syntax. For example, the 'link0' or 'link1' parameter values were entered while deprovisioning a CMIC packet on an IOP card (CMIC link deprovisioning not supported on packets). System or user actions:
RESPONSE: <slot> <side> is an IOP. Packet location must be specified Meaning: this response indicates that the 'uneq' command was issue for a CMIC packet slot, but the packet location parameter value (lower, l or upper, u) was not specified. System or user actions: re-enter the 'uneq' command with correct syntax.
RESPONSE: <slot> <side> is an HIOP. Packet location does not apply. Meaning: this response indicates that the 'uneq' command was issued for a CMIC link on an HIOP card, but a packet location parameter value was entered. System or user actions: re-enter the 'uneq' command with correct syntax.

Example**Usage examples for 'uneq' command on the CMIC MAP level**

Description of task: Command: MAP response:	Deprovision a CMIC packet on an IOP card Example: uneq 4 rear lower Example: Command submitted. Uneq 4 Rear Lower completed
Description of task: Command: MAP response:	Deprovision a CMIC link 0 on an HIOP card Example: uneq 4 rear link0 Example: Command submitted. Uneq 4 Rear Link0 completed.

Command: trns1

With the introduction of the new CMIC/RTIF HIOP card, the CMIC packets will have to be migrated to the new card. Hence, from now on, the 'trns1' command has to support the new HIOP card. This feature does not change the functionality of the command.

Command description

The 'trnsI' MAP command is used on the MAPCI;MTC;XAC;CMIC MAP level to find out the identity of the MS CMIC paddle board ports connected to a given CMIC link on the XA-Core. Until now, the 'trnsI' command was only used on CMIC packlets. From now on, it can be issued for either a CMIC packlet or CMIC component on the HIOP card.

Command syntax

This feature does not change the parameter values expected by the 'trnsI' command, its menu number on the CMIC MAP level. It only makes changes to the usage of the command. That is, for CMIC/RTIF HIOP cards, the packlet location parameter value should not be entered. For CMIC packlets, the 'trnsI' command should be issued as before.

MAP Responses

MAP outputs with associated meanings and actions

Command
RESPONSE: Command submitted. TrnsI 4 Rear completed. Meaning: This response indicates that the 'trnsI' command has completed successfully. System or user actions: none
RESPONSE: Card/device is unadressable...no action taken. Meaning: this response indicates that there is no provisioned component in the given location. System or user actions: the craft person has to check the FRU location
RESPONSE: Either incorrect optional parameter(s) OR too many parameters Meaning: this response indicates that the 'trnsI' command was issued without following the correct syntax. For example, the packlet location parameter value was entered for an HIOP. System or user actions: re-enter the 'trnsI' command with correct syntax.
RESPONSE: <slot> <side> is an IOP. Packlet location must be specified Meaning: this response indicates that the 'trnsI' command was issued for a CMIC packlet slot, but the packlet location parameter value (lower, l or upper, u) was not specified. System or user actions: re-enter the 'trnsI' command with correct syntax.
RESPONSE: <slot> <side> is an HIOP. Packlet location does not apply. Meaning: this response indicates that the 'trnsI' command was issued for a CMIC component on an HIOP card, but a packlet location parameter value was entered. System or user actions: re-enter the 'trnsI' command with correct syntax.

Example

For CMIC packets, the 'trns1' command usage will be the same. For CMIC components on an HIOP card, the 'trns1' command will have to be entered without specifying the packet location (lower or upper). Next table shows some examples.

Usage examples for 'trns1' command on the CMIC MAP level

Description of task: Command: MAP response:	Trns1 a CMIC packet on an IOP card Example: trns1 4 rear lower Example: Command submitted. Trns1 4 Rear Lower completed
Description of task: Command: MAP response:	Trns1 CMIC on an HIOP card Example: trns1 4 rear Example: Command submitted. Trns1 4 Rear completed.

RTIF MAP level

Currently, the RTIF functionality can only be hosted by an RTIF packet on an IOP card. Please refer to "Current RTIF MAP level with RTIF packets on IOPs in slots 4R and 15R" on page 304.

Current RTIF MAP level with RTIF packets on IOPs in slots 4R and 15R

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.	.	.	.	.	.	.
RTIF									
0 Quit		Front: 111111111		Rear: 111111		SM	PE	IO	PKLT
2		123456789012345678		456789012345		.	.	.	.
3		Sta:				0	0	0	0
4		Dep:							
5		Typ:		*		*			
6 Tst_		Slot: Side: Packet:		Status:		Local Port:		Remote Port:	
7 Bsy_		4 Rear Upper		.		.		.	
8 RTS_		15 Rear Upper		.		.		.	
9									
10									
11									
12 Uneq_									
13									
14 Alarm_									
15 Cntrs_									
16									
17 Indicat_									
18 Query_									
XMAP0									
Time 14:12 >									

With the introduction of the new CMIC/RTIF HIOP, the new RTIF MAP will show the functionality hosted by either an RTIF packet on an IOP card or an CMIC/RTIF HIOP card. Also, with RTIF port/link separation on CMIC/RTIF

HIOP, new RTIF link0 and RTIF link1 components will be shown on the RTIF MAP level.

Summary of RTIF MAP field changes

Component	Current MAP Field	New MAP Field	New/Deleted/Changed
RTIF Local Port on Packlet	'Local Port'	'n/a'	Deleted
RTIF Remote Port on Packlet	'Remote Port'	'n/a'	Deleted
RTIF Local Link on Packlet	n/a	'Link0'	New
RTIF Remote Link on Packlet	n/a	'Link1'	New
RTIF Local Port on HIOP	n/a	'Port0'	New
RTIF Remote Port on HIOP	n/a	'Port1'	New
RTIF Local Link on HIOP	n/a	'Link0'	New
RTIF Remote Link on HIOP	n/a	'Link1'	New

For RTIF packets on the new RTIF MAP level, the following components will be shown as before: Slot, Side, Packlet, Status. The RTIF local port will be changed to Link0. The RTIF remote port will be changed to Link1. Port0 and Port1 will be left blank. Hence, the RTIF MAP level will be consistent with other packet MAP levels that have no port/link separation. Please refer to “New RTIF MAP level with RTIF packets on IOPs in slots 4R and 15R” on page 306.

New RTIF MAP level with RTIF packets on IOPs in slots 4R and 15R

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.	.	.	.	.	.	.
RTIF		Front:	111111111	Rear:	111111	SM	PE	IO	PKLT
0 Quit			123456789012345678		456789012345	.	.	.	.
2		Sta:				0	0	0	0
3		Dep:							
4		Typ:		*	*				
5		Slot:	Side:	Packlet:	Status:	Port0:	Port1:	Link0:	Link1:
6 Tst_		4	Rear	Upper	.	.	.	.	.
7 Bsy_		15	Rear	Upper	.	.	.	.	.
8 RTS_									
9									
10									
11									
12 Uneq_									
13									
14 Alarm_									
15 Cntrs_									
16									
17 Indicat_									
18 Query_									
XMAP0									
Time 14:12									>

For RTIF functionality on CMIC/RTIF HIOP represented on the new RTIF MAP, since the card does not have packets, the 'Packlet' location field, and the packet 'Status' field will be left blank. Also, in addition to the local and remote RTIF ports, there are going to be two new RTIF links shown (link0 and link1). Please refer to "New RTIF MAP level with CMIC/RTIF HIOP cards in slots 4R and 15R" on page 306.

New RTIF MAP level with CMIC/RTIF HIOP cards in slots 4R and 15R

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.	.	.	.	.	.	.
RTIF		Front:	111111111	Rear:	111111	SM	PE	IO	PKLT
0 Quit			123456789012345678		456789012345	.	.	.	.
2		Sta:				0	0	0	0
3		Dep:							
4		Typ:		*	*				
5		Slot:	Side:	Packlet:	Status:	Port0:	Port1:	Link0:	Link1:
6 Tst_		4	Rear			.	.	.	.
7 Bsy_		15	Rear			.	.	.	.
8 RTS_									
9									
10									
11									
12 Uneq_									
13									
14 Alarm_									
15 Cntrs_									
16									
17 Indicat_									
18 Query_									
XMAP0									
Time 14:12									>

The new RTIF MAP level will be able to show both, packet and HIOP, configurations during the migration from one configuration to the other (e.g. RTIF packet to CMIC/RTIF HIOP).

Command: uneq

With the introduction of the new CMIC/RTIF HIOP card, the RTIF packets will have to be migrated to the new card. Hence, from now on, the XA-Core system will support the provisioning and deprovisioning of RTIF components. The 'uneq' command will be used for deprovisioning a RTIF packet on an IOP card or an RTIF link on a CMIC/RTIF HIOP card. Currently, RTIF packet deprovisioning is not supported.

New or modified CMIC MAP commands

Command Name	NEW, CHANGED or DELETED	Directory/MAP level name	MENU/NON-MENU/HIDDEN
uneq	changed	MAPCI;MTC;XAC;RTIF	Menu

Command description

The 'uneq' MAP command is used to deprovision a component from the XA-Core system. On the RTIF MAP level, the 'uneq' command will be used to deprovision a RTIF packet residing on an IOP card, or to deprovision a RTIF link residing on a CMIC/RTIF HIOP card. Until now, deprovisioning of RTIF packets was not supported since they were part of the 'fixed' XA-Core configuration (slots 4R and 15R). From now on, deprovisioning of RTIF components is needed for the migration of RTIF packets to CMIC/RTIF HIOP cards and back.

Summary of the new 'uneq' CMIC MAP level command

Command	Menu#	Type	Options	Function
uneq	12	Operational	None	- Deprovision a RTIF packet on an IOP card - Deprovision a RTIF link on an HIOP card

Command syntax

The 'uneq' command requires parameters. If you do not enter any parameters or you enter invalid parameters, the MAP terminal displays an error message. The MAP terminal prompts you to enter a correct parameter value.

<'uneq'> command parameters and variables

Command	Parameters and variables

<'uneq'> command parameters and variables

Command	Parameters and variables
uneq	- slot number (0 to 17), - side (front, f or rear, r), - packet position (upper, u, or lower, l), - link number (link0 or link1).
Parameters and variables	Description
slot number	Use the 'slot number' parameter value to indicate the number of the physical shelf slot: 0 to 17
side	Use the 'side' parameter value to indicate the component location in the physical shelf: front, f or rear, r
packet position	Use the 'packet position' parameter value to indicate the RTIF packet location on an IOP card: upper, u or lower, l. This is used only for RTIF packet deprovisioning and is not used for RTIF link.
link number	Use the 'link number' parameter value to indicate the RTIF link position on a CMIC/RTIF HIOP card: link0 or link1. This is used only for RTIF link deprovisioning and is not used for RTIF packets.

Note: The 'slot number' parameter value will usually be '4' or '15'. The 'side' parameter value will usually be 'upper' or 'u'. The 'packet position' parameter value will usually be 'upper' or 'u'.

Qualifications and warnings

The 'uneq' command should be used with great care since it deprovisions a component from the XA-Core system. There are some general requirements for the successful completion of the 'uneq' command. They are (in order):

- first, the component must be brought into a 'ManB' state,
- then, the component must be pulled from the shelf,
- finally, the 'uneq' command can be issued for the component.

Since the 'uneq' command on the RTIF MAP level can be issued for the RTIF packet residing on an IOP card or for an RTIF link residing on an HIOP card, the command usage will be different depending on the component being deprovisioned. Please refer to Section "Example" on page 310.

Note: Deprovisioning of RTIF links on packets is not supported.

MAP Responses

MAP outputs with associated meanings and actions

Command
RESPONSE: Command submitted. Uneq 4 Rear Upper completed. Meaning: This response indicates that the 'uneq' command has completed successfully. System or user actions: none
RESPONSE: Command submitted. Improper state for required action, no action take Meaning: this response indicates that the 'uneq' command has been issued without bringing the component into the 'ManB' state first. System or user actions: the craft person has to 'ManB' the component
RESPONSE: Command submitted H/W must be removed from shelf, no action taken Meaning: this response indicates that the 'uneq' command has been issued without removing the component from the shelf, or without waiting long enough for the system to recognize the component's loss of clock. System or user actions: the craft person has to remove the component from the shelf. If the component is already removed, the craft person has to wait long enough (e.g. one minute) for the system to recognize the component's loss of clock.
RESPONSE: Card/device is unadressable...no action taken. Meaning: this response indicates that there is no provisioned component in the given location. System or user actions: the craft person has to check the FRU location
RESPONSE: Either incorrect optional parameter(s) OR too many parameters Meaning: this response indicates that the 'uneq' command was issued without following the correct syntax. For example, the 'link0' or 'link1' parameter values were entered while deprovisioning an RTIF packet on an IOP card (RTIF link deprovisioning not supported on packets). System or user actions:
RESPONSE: <slot> <side> is an IOP. Packet location must be specified Meaning: this response indicates that the 'uneq' command was issue for an RTIF packet, but the packet location parameter value (lower, l or upper, u) was not specified. System or user actions: re-enter the 'uneq' command with correct syntax.

MAP outputs with associated meanings and actions

Command
RESPONSE: <slot> <side> is an HIOP. Packet location does not apply. Meaning: this response indicates that the 'uneq' command was issued for an RTIF link on an HIOP card, but a packet location parameter value was entered. System or user actions: re-enter the 'uneq' command with correct syntax.

Example**Usage examples for 'uneq' command on the RTIF MAP level**

Description of task: Command: MAP response:	Deprovision a RTIF packet on an IOP card Example: uneq 4 rear upper Example: Command submitted. Uneq 4 Rear Upper completed
Description of task: Command: MAP response:	Deprovision a RTIF link 0 on an HIOP card Example: uneq 4 rear link0 Example: Command submitted. Uneq 4 Rear Link0 completed.

Configuration Walkthrough**Provisioning and Deprovisioning**

For provisioning and deprovisioning the CMIC, RTIF, IOP, and HIOP components, this feature makes use of the XA-Core provisioning feature. For a more detailed explanation of the provisioning feature please refer to FN-A59009527.

CMIC packet deprovisioning on IOP

Deprovisioning a CMIC packet on an IOP card follows the general guidelines for deprovisioning any component in XA-Core. In addition, deprovisioning of CMIC packets also have some particular characteristics:

- first, the CMIC links have to be manually busied from the MS side (links will go 'CBsy'),
- then the CMIC packet must be brought into a 'ManB' state,
- once the CMIC links are 'CBsy' and the CMIC packet is 'ManB', the craft person should remove the CMIC packet from the IOP card,

- once the CMIC packet is removed from the IOP card, the craft person should issue the 'uneq' command for the CMIC packet. This deprovisions the CMIC packet and the CMIC links.

CMIC link deprovisioning on HIOP

Deprovisioning a CMIC link on an HIOP card follows the general guidelines for deprovisioning any component in XA-Core. In addition, deprovisioning of CMIC links also have some particular characteristics:

- first, the CMIC link has to be manually busied from the MS side (link will go 'CBsy'),
- once the CMIC link is 'CBsy', the craft person should remove the CMIC link from the HIOP card,
- once the CMIC link is 'CBsy' and removed from the HIOP card, the craft person should issue the 'uneq' command for the CMIC link. This deprovisions the CMIC link.

CMIC packet provisioning on IOP

Provisioning of CMIC packets is done as follows:

- have the host IOP card provisioned and in-service, with an empty (unprovisioned) packet location,
- on the MS side, the craft person must manually busy both MS ports for the CMIC packet we want to provision,
- after both MS ports are 'ManB', the craft person should plug in the CMIC packet with no links attached,

Note: when the system provisions the CMIC packet, the CMIC links are automatically added to the system inventory. They will be 'CBsy'.

- once the CMIC packet is provisioned, the craft person should bring the CMIC packet in-service,
- after the CMIC packet is in-service, with the CMIC link 'CBsy', the craft person should plug the CMIC links into the CMIC packet,
- on the MS side, once the CMIC links are provisioned and 'CBsy', the craft person must test both MS ports connected to the CMIC links,
- after the MS port tests pass, the craft person should bring the MS ports in-service. This will also bring the CMIC links in-service.

CMIC link provisioning on HIOP

Provisioning of CMIC links on HIOP is done as follows:

- have the host HIOP card provisioned and in-service, with an empty (unprovisioned) OC3 link location,
- on the MS side, the craft person must manually busy the MS port for the CMIC link we want to provision,
- after the MS port is 'ManB', the craft person should plug the CMIC link into the OC3 port of the HIOP card (the CMIC link will be 'CBsy'),
- on the MS side, once the CMIC link is provisioned and 'CBsy', the craft person must test the MS port connected to the CMIC link,
- after the MS port test passes, the craft person should bring the MS port in-service. This will also bring the CMIC link in-service.

Migration procedures

With the introduction of the new CMIC/RTIF HIOP card, the CMIC and RTIF functionality presently hosted by packlets on IOP cards will have to be migrated to the new HIOP card. Also, a 'back-out' migration procedure has to be available so that the office can go from the CMIC/RTIF HIOP cards back to packlets.

Migration from CMIC and RTIF packlets to CMIC/RTIF HIOP for SuperNode (SN)

This section describes the migration procedure from an XA-Core system with CMIC and RTIF functionality provided by packlets on IOP cards to a system with CMIC and RTIF functionality provided by CMIC/RTIF HIOP cards. The recommended approach will provision the new HIOP cards in the *same* slots (4R and 15R) as the deprovisioned IOP cards with packlets. Because of lost redundancy during the migration, there are two E2 conditions during this procedure.

The following sequence of events shows the steps:

- Start with a CMIC and RTIF packlet configuration on IOP cards in slots 4R and 15R (no CMIC/RTIF HIOP cards in the shelf). Please refer to "Initial CMIC and RTIF packlet configuration - XA-Core rear view" on page 313.

Initial CMIC and RTIF packet configuration - XA-Core rear view

- set the 'xa_component_install_state' office parameter in table OFCENG to 'manbusy',
- verify that table XAFWLOAD is datafilled with valid FW (ROM) and DLL (RAM) loads for the new CMIC/RTIF HIOP card,
- issue the 'trns1' command for the CMIC packet in 4 rear lower: 'trns1 4 rear lower'. The MAP response should look like this:

```
trns1 4 rear lower
Command Submitted.
Trns1 4 Rear Lower completed
```

```
Link 0 is connected to MS1 Shelf 0 Card 24 Port 0
Link 1 is connected to MS0 Shelf 0 Card 25 Port 0
```

- record the MS port numbers returned by the 'trns1' command for the CMIC packet in 4 rear lower,
- on the MS MAP level, manually busy the MS ports returned by the 'trns1' command for CMIC packet in slot 4 rear lower (Port 0 on MS 1, Shelf 0, Card 24 and Port 0 on MS 0, Shelf 0, Card 25). The CMIC links will go 'CBSy'.
- on the CMIC MAP level, manually busy the CMIC packet in slot 4 rear lower,
- on the RTIF MAP level, manually busy the RTIF packet in slot 4 rear upper,
- on the IO MAP level, manually busy the IOP card in slot 4 rear,
- pull the CMIC packet in slot 4 rear lower with links attached,
- pull the RTIF packet in slot 4 rear upper,
- pull the IOP card in slot 4 rear,
- wait one minute for the system to recognize the loss of clock,
- on the CMIC MAP level, issue the 'uneq' command for the CMIC packet: 'uneq 4 rear lower'.
- on the RTIF MAP level, issue the 'uneq' command for the RTIF packet: 'uneq 4 rear upper'.

- on the IO MAP level, issue the ‘uneq’ command for the IOP card: ‘uneq 4 rear’. The following logs should be generated:

```
XAC628 MAR19 14:16:20 5600 INFO XA-Core Provisioning Report
      DESCRIPTION: Resource has been deprovisioned
      CARD: Type State Site FL Row Bay    Shf/Slt/Pk    EqPEC/Serial
            CMIC MBSY  HOST 01 A00 DPCC:00 00 04R L  NTLX05AB/NNTM64422MWV
```

```
XAC628 MAR19 14:17:20 5700 INFO XA-Core Provisioning Report
      DESCRIPTION: Resource has been deprovisioned
      CARD: Type State Site FL Row Bay    Shf/Slt/Pk    EqPEC/Serial
            RTIF MBSY  HOST 01 A00 DPCC:00 00 04R U  NTLX08AA/NNTM64422MWV
```

```
XAC628 MAR19 14:18:20 5800 INFO XA-Core Provisioning Report
      DESCRIPTION: Resource has been deprovisioned
      CARD: Type State Site FL Row Bay    Shf/Slt    EqPEC/Serial
            IO  MBSY  HOST 01 A00 DPCC:00 00 04R NTLX03AB/NNTM64422MWV
```

- at this stage, the CMIC and RTIF functionality is provided only by the packets in slot 15 rear. Please refer to “Reduced CMIC and RTIF redundancy (service on packets) - XA-Core rear view” on page 314.

Reduced CMIC and RTIF redundancy (service on packets) - XA-Core rear view



- plug the CMIC/RTIF HIOP card into slot 4 rear with no links attached. The following log should be generated:

Note: Once the HIOP card is provisioned, all its associated ports will be provisioned as well.

```
XAC628 MAR19 14:20:20 6800 INFO XA-Core Provisioning Report
      DESCRIPTION: New resource has been provisioned
      CARD: Type State Site FL Row Bay    Shf/Slt    EqPEC/Serial
            HIOP MBSY  HOST 01 A00 DPCC:00 00 04R NTLX04BA/NNTM64422MWV
```

- the craft person should verify the success of the system-initiated provisioning test of the HIOP card in slot 4 rear by checking the XAC log 640 in logutil:

```
XAC640 MAR19 14:20:40 6900 INFO Test Report
      Type Link_Num Slot Side Packlet Test_Type Result
      HIOP      4      R      OOS      Passed
      Initiator: Action initiated by the system
```

- once the integrity of the HIOP card in slot 4 rear has been verified, the craft person should manually RTS the card,

Note: Once the HIOP card is in-service, all its associated ports are automatically brought in-service by the system, provided their OOS test passes.

- plug the CMIC links into the OC3 ports of the HIOP card in slot 4 rear. The system will automatically provision the CMIC links, perform an OOS test on them, and bring them into a 'CBsy' state.

Note: use the same configuration as recorded for the 'trns1' command issued for the CMIC packet in slot 4 rear lower. The following log should be generated:

```
XAC628 MAR19 14:22:20 7000 INFO XA-Core Provisioning Report
      DESCRIPTION: New resource has been provisioned
      LINK: Type State Site FL Row Bay      Shf/Slt/Lk      EqPEC/Serial
            CMIC CBSY  HOST 01 A00 DPCC:00 00 04R 0  NTLX04BA/NNTM64422MWV
```

```
XAC628 MAR19 14:22:20 7100 INFO XA-Core Provisioning Report
      DESCRIPTION: New resource has been provisioned
      LINK: Type State Site FL Row Bay      Shf/Slt/Lk      EqPEC/Serial
            CMIC CBSY  HOST 01 A00 DPCC:00 00 04R 1  NTLX04BA/NNTM64422MWV
```

- on the MS MAP level, test the MS ports returned by the 'trns1' command for the CMIC packet in slot 4 rear lower (Port 0 on MS 1, Shelf 0, Card 24 and Port 0 on MS 0, Shelf 0, Card 25).
- on the MS MAP level, if the previous MS port tests passed, bring them in-service (Port 0 on MS 1, Shelf 0, Card 24 and Port 0 on MS 0, Shelf 0, Card 25). On the MS MAP level the MS ports will go from 'M' to '.', while on the XAC CMIC MAP level the CMIC links will go from 'CBsy' to '.'.
- once the CMIC links are in-service, issue the 'trns1' command for the CMIC links on HIOP in 4 rear: 'trns1 4 rear'. The MAP response should look like this:

```
trns1 4 rear
Command Submitted.
Trns1 4 Rear completed
```

```
Link 0 is connected to MS1 Shelf 0 Card 24 Port 0
Link 1 is connected to MS0 Shelf 0 Card 25 Port 0
```

- record the MS port numbers returned by the 'trns1' command for the CMIC links on HIOP card in 4 rear. Verify that they are the same as the MS port numbers recorded before deprovisioning the CMIC packet in 4 rear lower,
- plug the RTIF local link into the HIOP card's local RTIF port in slot 4 rear. The system will automatically provision and attempt to bring the local RTIF link in-service. The following log should be generated:

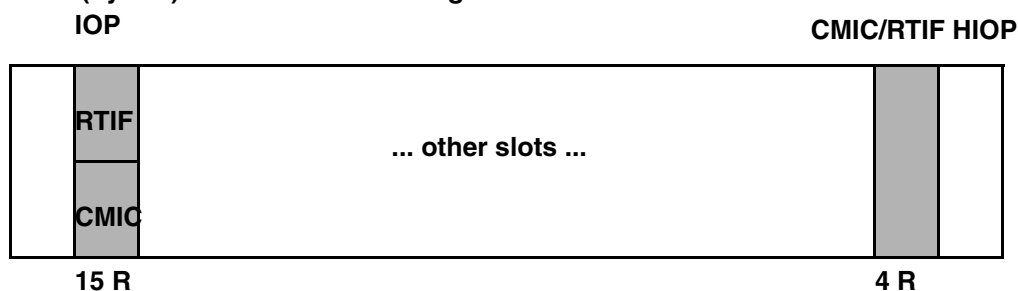
```
XAC628 MAR19 14:23:20 7200 INFO XA-Core Provisioning Report
      DESCRIPTION: New resource has been provisioned
      LINK: Type State Site FL Row Bay      Shf/Slt/Lk      EqPEC/Serial
            RTIF CBSY  HOST 01 A00 DPCC:00 00 04R 0  NTLX04BA/NNTM64422MWV
```

- plug the RTIF remote link into the HIOP card's remote RTIF port in slot 4 rear. The system will automatically provision and attempt to bring the remote RTIF link in-service. The following log should be generated:

```
XAC628 MAR19 14:23:20 7200 INFO XA-Core Provisioning Report
DESCRIPTION: New resource has been provisioned
LINK: Type State Site FL Row Bay Shf/Slt/Lk EqPEC/Serial
      RTIF CBSY HOST 01 A00 DPCC:00 00 04R 1 NTLX04BA/NNMTM64422MWV
```

- at this point, we have a hybrid CMIC and RTIF system: the CMIC and RTIF functionality in slot 15R is still provided by packets on IOP cards, while the CMIC and RTIF functionality in slot 4R is provided by the new CMIC/RTIF HIOP. Please refer to "Intermediate (hybrid) CMIC and RTIF configuration - XA-Core rear view" on page 316.

Intermediate (hybrid) CMIC and RTIF configuration - XA-Core rear view



- issue the 'trns1' command for the CMIC packet in 15 rear lower: 'trns1 15 rear lower'. The MAP response should look like this:

```
trns1 15 rear lower
Command Submitted.
Trns1 15 Rear Lower completed
```

```
Link 0 is connected to MS0 Shelf 0 Card 24 Port 0
Link 1 is connected to MS1 Shelf 0 Card 25 Port 0
```

- record the MS port numbers returned by the 'trns1' command for the CMIC packet in 15 rear lower,
- on the MS MAP level, manually busy the MS ports returned by the 'trns1' command issued for the CMIC packet in slot 15 rear lower (Port 0 on MS 0, Shelf 0, Card 24 and Port 0 on MS 1, Shelf 0, Card 25). The CMIC links will go 'CBsy'.
- on the CMIC MAP level, manually busy the CMIC packet in slot 15 rear lower,
- on the RTIF MAP level, manually busy the RTIF packet in slot 15 rear upper,
- on the IO MAP level, manually busy the IOP card in slot 15 rear,
- pull the CMIC packet in slot 15 rear lower, with links attached,
- pull the RTIF packet in slot 15 rear upper,
- pull the IOP card in slot 15 rear,

- wait one minute for the system to recognize the loss of clock,
- on the CMIC MAP level, issue the ‘uneq’ command for the CMIC packet: ‘uneq 15 rear lower’,
- on the RTIF MAP level, issue the ‘uneq’ command for the RTIF packet: ‘uneq 15 rear upper’,
- on the IO MAP level, issue the ‘uneq’ command for the IOP card: ‘uneq 15 rear’. The following logs should be generated:

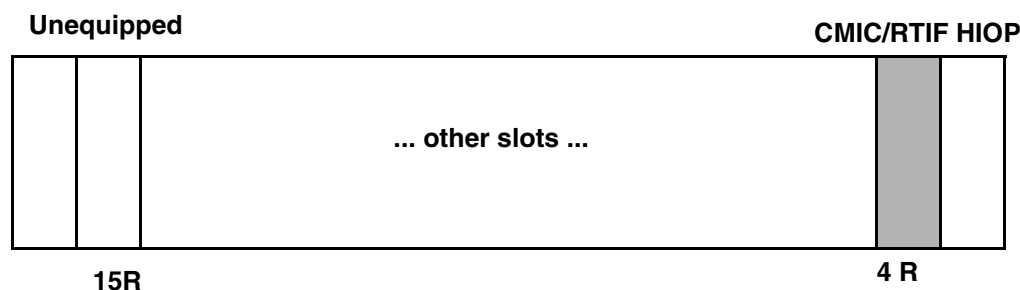
```
XAC628 MAR19 14:25:20 7300 INFO XA-Core Provisioning Report
DESCRIPTION: Resource has been deprovisioned
CARD: Type State Site FL Row Bay Shf/Slt/Pk EqPEC/Serial
CMIC MBSY HOST 01 A00 DPCC:00 00 15R L NTLX05AB/NNMTM64422MWV
```

```
XAC628 MAR19 14:26:20 7400 INFO XA-Core Provisioning Report
DESCRIPTION: Resource has been deprovisioned
CARD: Type State Site FL Row Bay Shf/Slt/Pk EqPEC/Serial
RTIF MBSY HOST 01 A00 DPCC:00 00 15R U NTLX08AA/NNMTM64422MWV
```

```
XAC628 MAR19 14:27:20 7500 INFO XA-Core Provisioning Report
DESCRIPTION: Resource has been deprovisioned
CARD: Type State Site FL Row Bay Shf/Slt EqPEC/Serial
IO MBSY HOST 01 A00 DPCC:00 00 15R NTLX03AB/NNMTM64422MWV
```

- Please refer to “Reduced CMIC and RTIF redundancy (service on HIOP) - XA-Core rear view” on page 317.

Reduced CMIC and RTIF redundancy (service on HIOP) - XA-Core rear view



- plug the CMIC/RTIF HIOP card into slot 15 rear with no links attached. The following log should be generated:

```
XAC628 MAR19 14:28:20 7600 INFO XA-Core Provisioning Report
DESCRIPTION: New resource has been provisioned
CARD: Type State Site FL Row Bay Shf/Slt EqPEC/Serial
HIOP MBSY HOST 01 A00 DPCC:00 00 15R NTLX04BA/NNMTM64422MWV
```

- the craft person should verify the success of the system-initiated provisioning test of the HIOP card in slot 15 rear by checking the XAC log 640 in logutil:

```
XAC640 MAR19 14:29:40 7700 INFO Test Report
Type Link_Num Slot Side Packlet Test_Type Result
HIOP 15 R OOS Passed
Initiator: Action initiated by the system
```

- once the integrity of the HIOP card in slot 15 rear has been verified, the craft person should manually RTS the card,

Note: Once the HIOP card is in-service, all its associated ports are automatically brought in-service by the system, provided their OOS test passes.

- plug the CMIC links into the OC3 ports of the HIOP card in slot 15 rear. The system will automatically provision the CMIC links, perform an OOS test on them, and bring them into a 'CBsy' state.

Note: use the same configuration as recorded for the 'trns1' command issued for the CMIC packet in slot 15 rear lower.

```
XAC628 MAR19 14:30:20 7800 INFO XA-Core Provisioning Report
      DESCRIPTION: New resource has been provisioned
      LINK: Type State Site FL Row Bay      Shf/Slt/Lk      EqPEC/Serial
            CMIC CBSY  HOST 01 A00 DPCC:00 00 15R 0   NTLX04BA/NNMTM64422MWV
```

```
XAC628 MAR19 14:31:20 7900 INFO XA-Core Provisioning Report
      DESCRIPTION: New resource has been provisioned
      LINK: Type State Site FL Row Bay      Shf/Slt/Lk      EqPEC/Serial
            CMIC CBSY  HOST 01 A00 DPCC:00 00 15R 1   NTLX04BA/NNMTM64422MWV
```

- on the MS MAP level, test the MS ports previously returned by the 'trns1' command for CMIC packet in slot 15 rear lower (Port 0 on MS 0, Shelf 0, Card 24 and Port 0 on MS 1, Shelf 0, Card 25).
- on the MS MAP level, if the previous MS port tests passed, bring them in-service (Port 0 on MS 0, Shelf 0, Card 24 and Port 0 on MS 1, Shelf 0, Card 25). On the MS MAP level the MS ports will go from 'M' to '.', while on the XAC CMIC MAP level the CMIC links will go from 'CBsy' to '.'.
- once the CMIC links are in-service, issue the 'trns1' command for the CMIC links on HIOP 14 rear: 'trns1 14 rear'. The MAP response should look like this:

```
trns1 15 rear
Command Submitted.
Trns1 15 Rear completed
```

```
Link 0 is connected to MS0 Shelf 0 Card 24 Port 0
Link 1 is connected to MS1 Shelf 0 Card 25 Port 0
```

- record the MS port numbers returned by the 'trns1' command for the CMIC links on HIOP card in 4 rear. Verify that they are the same as the MS port numbers recorded before deprovisioning the CMIC packet in 15 rear lower,
- plug the RTIF local link into the HIOP card's local RTIF port in slot 15 rear. The system will automatically provision and attempt to bring the local RTIF link in-service.

```
XAC628 MAR19 14:33:20 8100 INFO XA-Core Provisioning Report
      DESCRIPTION: New resource has been provisioned
      LINK: Type State Site FL Row Bay      Shf/Slt/Lk      EqPEC/Serial
            RTIF CBSY  HOST 01 A00 DPCC:00 00 15R 0   NTLX04BA/NNMTM64422MWV
```

- plug the RTIF remote link into the HIOP card's remote RTIF port in slot 15 rear. The system will automatically provision and attempt to bring the remote RTIF link in-service.

XAC628 MAR19 14:34:20 8200 INFO XA-Core Provisioning Report

DESCRIPTION: New resource has been provisioned

LINK: Type State Site FL Row Bay Shf/Slt/Lk EqPEC/Serial
RTIF CBSY HOST 01 A00 DPCC:00 00 15R 1 NTLX04BA/NNTM64422MWV

- set the 'xa_component_install_state' office parameter in table OFCENG back to 'inservice',
- at this point, the CMIC/RTIF HIOP cards in slots 4R and 15R are all in-service, along with their associated CMIC and RTIF links. No CMIC or RTIF packets on IOP cards are provisioned in the shelf. This constitutes the end of the migration procedure from CMIC and RTIF packets to CMIC/RTIF HIOP. Please refer to "Final CMIC/RTIF HIOP configuration - XA-Core rear view" on page 319.

Final CMIC/RTIF HIOP configuration - XA-Core rear view



Migration from CMIC and RTIF packets to CMIC/RTIF HIOP for SuperNode SE (SNSE)

The migration procedure from CMIC and RTIF packets to CMIC/RTIF HIOP cards for SuperNode Shelf Extension (SNSE) is similar to the SuperNode (SN) case. The only exception is the MS port numbers that have to be busied, tested, and enabled during the migration procedure. The 'trns1' command should be used on the CMIC MAP level to get the specific MS port numbers to be busied. Please refer to "SN to SNSE port mapping" on page 319.

SN to SNSE port mapping

SN MS port	SNSE MS port	XA-Core CMIC link
MS 0, Card 24, Port 0	MS 0, Card 4, Port 0	Slot 15 rear, link 0
MS 1, Card 25, Port 0	MS 1, Card 4, Port 1	Slot 15 rear, link 1
MS 1, Card 24, Port 0	MS 1, Card 4, Port 0	Slot 4 rear, link 0
MS 0, Card 25, Port 0	MS 0, Card 4, Port 1	Slot 4 rear, link 1

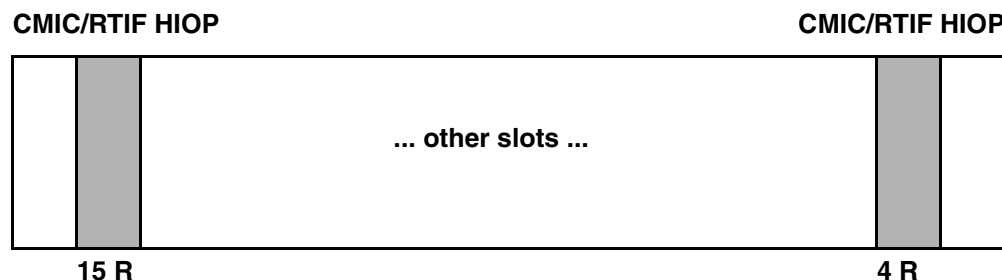
Migration from CMIC/RTIF HIOP back to CMIC and RTIF packets on IOP for SuperNode (SN)

This section describes the migration procedure from an XA-Core system with CMIC and RTIF functionality provided by CMIC/RTIF HIOP cards to a system with CMIC and RTIF functionality provided by packets on IOP cards. The recommended approach will provision the new IOP cards and CMIC and RTIF packets in the *same* slots (4R and 15R) as the deprovisioned HIOP cards. Hence, because of lost redundancy during the migration, there are two E2 conditions during this procedure.

The following sequence of events shows the steps:

- start with a CMIC/RTIF HIOP configuration in slots 4R and 15R (no IOP cards with CMIC or RTIF packets provisioned in the shelf). Please refer to “Initial CMIC/RTIF HIOP locations - XA-Core rear view” on page 320.

Initial CMIC/RTIF HIOP locations - XA-Core rear view



- set the ‘xa_component_install_state’ office parameter in table OFCENG to ‘manbusy’,
- issue the ‘trns1’ command for the CMIC links on the HIOP card in slot 4 rear: ‘trns1 4 rear’. The MAP response should look like this:

```
trns1 4 rear
Command Submitted.
Trns1 4 Rear completed
```

```
Link 0 is connected to MS1 Shelf 0 Card 24 Port 0
Link 1 is connected to MS0 Shelf 0 Card 25 Port 0
```

- record the MS port numbers returned by the ‘trns1’ command for the CMIC links on the HIOP card in slot 4 rear,
- on the MS MAP level, manually busy the MS ports returned by the ‘trns1’ command for CMIC links on the HIOP card in slot 4 rear (Port 0 on MS 1, Shelf 0, Card 24 and Port 0 on MS 0, Shelf 0, Card 25). The CMIC links will go ‘CBsy’.
- pull the CMIC links on the HIOP in slot 4 rear,
- wait one minute for the system to recognize the loss of clock,

- on the CMIC MAP level, issue the ‘uneq’ command for the CMIC links on the HIOP in slot 4 rear: ‘uneq 4 rear link0’ and ‘uneq 4 rear link1’. The following logs should be generated:

```
XAC628 MAR19 14:16:20 5600 INFO XA-Core Provisioning Report
      DESCRIPTION: Resource has been deprovisioned
      LINK: Type State Site FL Row Bay      Shf/Slt/Lk      EqPEC/Serial
            CMIC CBSY  HOST 01 A00 DPCC:00 00 04R 0  NTLX17AA/NNMTM64422MWV
```

```
XAC628 MAR19 14:16:20 5600 INFO XA-Core Provisioning Report
      DESCRIPTION: Resource has been deprovisioned
      LINK: Type State Site FL Row Bay      Shf/Slt/Lk      EqPEC/Serial
            CMIC CBSY  HOST 01 A00 DPCC:00 00 04R 1  NTLX17AA/NNMTM64422MWV
```

- on the RTIF MAP level, manually busy the RTIF links on the HIOP card in slot 4 rear,
- pull the RTIF links from the HIOP card in slot 4 rear,
- wait one minute for the system to recognize the loss of clock,
- on the RTIF MAP level, issue the ‘uneq’ command for the RTIF links on the HIOP card: ‘uneq 4 rear link0’ and ‘uneq 4 rear link1’. The following logs should be generated:

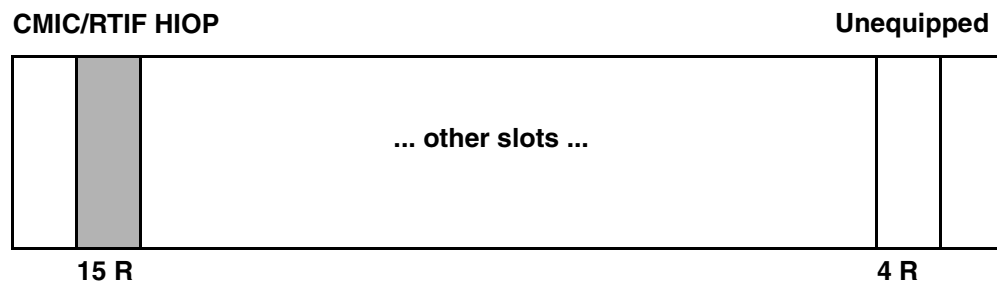
```
XAC628 MAR19 14:16:20 5600 INFO XA-Core Provisioning Report
      DESCRIPTION: Resource has been deprovisioned
      LINK: Type State Site FL Row Bay      Shf/Slt/Lk      EqPEC/Serial
            RTIF MBSY  HOST 01 A00 DPCC:00 00 04R 0  NTLX17AA/NNMTM64422MWV
```

```
XAC628 MAR19 14:16:20 5600 INFO XA-Core Provisioning Report
      DESCRIPTION: Resource has been deprovisioned
      LINK: Type State Site FL Row Bay      Shf/Slt/Lk      EqPEC/Serial
            RTIF MBSY  HOST 01 A00 DPCC:00 00 04R 1  NTLX17AA/NNMTM64422MWV
```

- on the IO MAP level, manually busy the HIOP card in slot 4 rear,
- pull the HIOP card in slot 4 rear,
- wait one minute for the system to recognize the loss of clock,
- on the IO MAP level, issue the ‘uneq’ command for the HIOP card: ‘uneq 4 rear’. The following log should be generated:

```
XAC628 MAR19 14:18:20 5800 INFO XA-Core Provisioning Report
      DESCRIPTION: Resource has been deprovisioned
      CARD: Type State Site FL Row Bay      Shf/Slt      EqPEC/Serial
            HIOP MBSY  HOST 01 A00 DPCC:00 00 04R NTLX17AA/NNMTM64422MWV
```

- at this stage, the CMIC and RTIF functionality is provided only by the packets in slot 15 rear. Please refer to “Reduced CMIC and RTIF redundancy (service on HIOP) - XA-Core rear view” on page 322.

Reduced CMIC and RTIF redundancy (service on HIOP) - XA-Core rear view

- plug an IOP card into slot 4 rear with no packlets attached. The following log should be generated:

```
XAC628 MAR19 14:20:20 6800 INFO XA-Core Provisioning Report
      DESCRIPTION: New resource has been provisioned
      CARD: Type State Site FL Row Bay   Shf/Slt   EqPEC/Serial
            IOP  MBSY  HOST 01 A00 DPCC:00 00 04R NTLX03AB/NNMTM64422MWV
```

- the craft person should verify the success of the system-initiated provisioning test of the IOP card in slot 4 rear by checking the XAC log 640 in logutil:

```
XAC640 MAR19 14:20:40 6900 INFO Test Report
      Type Link_Num Slot Side Packlet Test_Type Result
      IOP         4    R          OOS      Passed
      Initiator: Action initiated by the system
```

- once the integrity of the IOP card in slot 4 rear has been verified, the craft person should manually RTS the card,
- plug the CMIC packlet into the in-service IOP card in slot 4 rear lower with the CMIC links attached. The system will automatically provision the CMIC packlet, perform an OOS test on it, and bring it into a 'ManB' state.

Note: Once the CMIC packlet is provisioned, both CMIC links will be automatically provisioned as well. They will be 'CBSy'.

Note: when plugging the CMIC links into the CMIC packlet, use the same configuration as recorded for the 'trns1' command issued for the CMIC links on the HIOP card in slot 4 rear.

```
XAC628 MAR19 14:22:20 7000 INFO XA-Core Provisioning Report
      DESCRIPTION: New resource has been provisioned
      CARD: Type State Site FL Row Bay   Shf/Slt/Pk   EqPEC/Serial
            CMIC MBSY  HOST 01 A00 DPCC:00 00 04R L   NTLX05AB/NNMTM64422MWV
```

- the craft person should verify the success of the system-initiated provisioning test of the CMIC packlet in slot 4 rear lower by checking the XAC log 640 in logutil:

```
XAC640 MAR19 14:20:40 6900 INFO Test Report
      Type Link_Num Slot Side Packlet Test_Type Result
      CMIC         4    R    L          OOS      Passed
      Initiator: Action initiated by the system
```

- once the integrity of the CMIC packlet in slot 4 rear lower has been verified, the craft person should manually RTS the CMIC packlet,

- on the MS MAP level, test the MS ports returned by the 'trns1' command for the CMIC links on the HIOP in slot 4 rear (Port 0 on MS 1, Shelf 0, Card 24 and Port 0 on MS 0, Shelf 0, Card 25).
- on the MS MAP level, if the previous MS port tests passed, bring them in-service (Port 0 on MS 1, Shelf 0, Card 24 and Port 0 on MS 0, Shelf 0, Card 25). On the MS MAP level the MS ports will go from 'M' to '.', while on the XAC CMIC MAP level the CMIC links will go from 'CBsy' to '.'.
- once the CMIC links are in-service, issue the 'trns1' command for the CMIC links on the CMIC packlet in slot 4 rear lower: 'trns1 4 rear lower'. The MAP response should look like this:

```
trns1 4 rear lower
Command Submitted.
Trns1 4 Rear lower completed
```

```
Link 0 is connected to MS1 Shelf 0 Card 24 Port 0
Link 1 is connected to MS0 Shelf 0 Card 25 Port 0
```

- record the MS port numbers returned by the 'trns1' command for the CMIC links on the CMIC packlet in 4 rear lower. Verify that they are the same as the MS port numbers recorded before deprovisioning the CMIC/RTIF HIOP card in 4 rear,
- plug the RTIF packlet into the IOP card in 4 rear upper, with links attached.
- the system will automatically provision the RTIF packlet, perform an OOS test on it, and bring it into a 'ManB' state.

Note: Once the RTIF packlet is provisioned, the system will automatically provision the local and remote RTIF links.

```
XAC628 MAR19 14:23:20 7200 INFO XA-Core Provisioning Report
DESCRIPTION: New resource has been provisioned
CARD: Type State Site FL Row Bay Shf/Slt/Pk EqPEC/Serial
RTIF CBSY HOST 01 A00 DPCC:00 00 04R U NTLX08AA/NNTM64422MWV
```

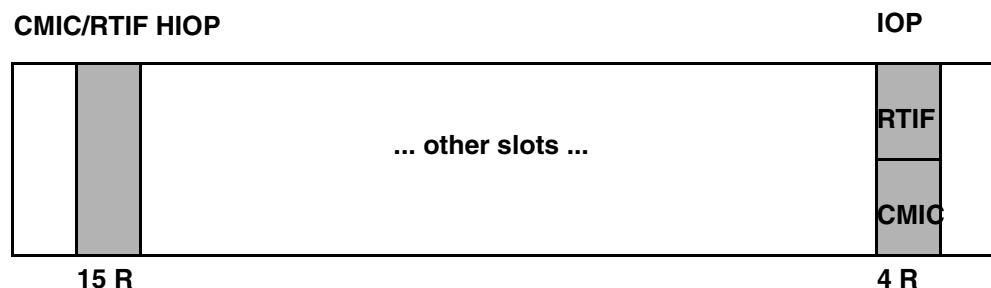
- the craft person should verify the success of the system-initiated provisioning test of the RTIF packlet in slot 4 rear upper by checking the XAC log 640 in logutil:

```
XAC640 MAR19 14:20:40 6900 INFO Test Report
Type Link_Num Slot Side Packlet Test_Type Result
RTIF          4    R    U          OOS      Passed
Initiator: Action initiated by the system
```

- once the integrity of the RTIF packlet in slot 4 rear upper has been verified, the craft person should manually RTS the packlet,
- once the RTIF packlet is in-service, the system will automatically attempt to bring the local and remote RTIF links in-service.
- at this point, we have a hybrid CMIC and RTIF system: the CMIC and RTIF functionality in slot 15R is still provided by an HIOP card, while the CMIC and RTIF functionality in slot 4R is provided by packlets. Please

refer to “Intermediate (hybrid) CMIC and RTIF configuration - XA-Core rear view” on page 324.

Intermediate (hybrid) CMIC and RTIF configuration - XA-Core rear view



- issue the ‘trns1’ command for the CMIC links on the HIOP card in slot 15 rear: ‘trns1 15 rear’. The MAP response should look like this:

```
trns1 15 rear
Command Submitted.
Trns1 15 Rear completed
```

```
Link 0 is connected to MS0 Shelf 0 Card 24 Port 0
Link 1 is connected to MS1 Shelf 0 Card 25 Port 0
```

- record the MS port numbers returned by the ‘trns1’ command for the CMIC links on the HIOP card in slot 15 rear,
- on the MS MAP level, manually busy the MS ports returned by the ‘trns1’ command for CMIC links on the HIOP card in slot 15 rear (Port 0 on MS 0, Shelf 0, Card 24 and Port 0 on MS 1, Shelf 0, Card 25). The CMIC links will go ‘CBsy’.
- pull the CMIC links on the HIOP in slot 15 rear,
- wait one minute for the system to recognize the loss of clock,
- on the CMIC MAP level, issue the ‘uneq’ command for the CMIC links on the HIOP in slot 15 rear: ‘uneq 15 rear link0’ and ‘uneq 15 rear link1’. The following logs should be generated:

```
XAC628 MAR19 14:16:20 5600 INFO XA-Core Provisioning Report
DESCRIPTION: Resource has been deprovisioned
LINK: Type State Site FL Row Bay Shf/Slt/Lk EqPEC/Serial
CMIC CBSY HOST 01 A00 DPCC:00 00 15R 0 NTLX17AA/NNTM64422MWV
```

```
XAC628 MAR19 14:16:20 5600 INFO XA-Core Provisioning Report
DESCRIPTION: Resource has been deprovisioned
LINK: Type State Site FL Row Bay Shf/Slt/Lk EqPEC/Serial
CMIC CBSY HOST 01 A00 DPCC:00 00 15R 1 NTLX17AA/NNTM64422MWV
```

- on the RTIF MAP level, manually busy the RTIF links on the HIOP card in slot 15 rear,
- pull the RTIF links from the HIOP card in slot 15 rear,
- wait one minute for the system to recognize the loss of clock,

- on the RTIF MAP level, issue the 'uneq' command for the RTIF links on the HIOP card: 'uneq 15 rear link0' and 'uneq 15 rear link1'. The following logs should be generated:

```
XAC628 MAR19 14:16:20 5600 INFO XA-Core Provisioning Report
      DESCRIPTION: Resource has been deprovisioned
      LINK: Type State Site FL Row Bay      Shf/Slt/Lk      EqPEC/Serial
            RTIF MBSY  HOST 01 A00 DPCC:00 00 15R 0  NTLX17AA/NNMTM64422MWV
```

```
XAC628 MAR19 14:16:20 5600 INFO XA-Core Provisioning Report
      DESCRIPTION: Resource has been deprovisioned
      LINK: Type State Site FL Row Bay      Shf/Slt/Lk      EqPEC/Serial
            RTIF MBSY  HOST 01 A00 DPCC:00 00 15R 1  NTLX17AA/NNMTM64422MWV
```

- on the IO MAP level, manually busy the HIOP card in slot 15 rear,
- pull the HIOP card in slot 15 rear,
- wait one minute for the system to recognize the loss of clock,
- on the IO MAP level, issue the 'uneq' command for the HIOP card: 'uneq 15 rear'. The following log should be generated:

```
XAC628 MAR19 14:18:20 5800 INFO XA-Core Provisioning Report
      DESCRIPTION: Resource has been deprovisioned
      CARD: Type State Site FL Row Bay      Shf/Slt      EqPEC/Serial
            HIOP MBSY  HOST 01 A00 DPCC:00 00 15R NTLX17AA/NNMTM64422MWV
```

- at this stage, the CMIC and RTIF functionality is provided only by the packets in slot 4 rear. Please refer to "Reduced CMIC and RTIF redundancy (service on packet) - XA-Core rear view" on page 325.

Reduced CMIC and RTIF redundancy (service on packet) - XA-Core rear view



- plug an IOP card into slot 15 rear with no packets attached. The following log should be generated:

```
XAC628 MAR19 14:20:20 6800 INFO XA-Core Provisioning Report
      DESCRIPTION: New resource has been provisioned
      CARD: Type State Site FL Row Bay      Shf/Slt      EqPEC/Serial
            IOP MBSY  HOST 01 A00 DPCC:00 00 15R NTLX03AB/NNMTM64422MWV
```

- the craft person should verify the success of the system-initiated provisioning test of the IOP card in slot 15 rear by checking the XAC log 640 in logutil:

```
XAC640 MAR19 14:20:40 6900 INFO Test Report
      Type Link_Num Slot Side Packet Test_Type Result
      IOP      15      R      OOS      Passed
      Initiator: Action initiated by the system
```

- once the integrity of the IOP card in slot 15 rear has been verified, the craft person should manually RTS the card,
- plug the CMIC packet into the in-service IOP card in slot 15 rear lower with the CMIC links attached. The system will automatically provision the CMIC packet, perform an OOS test on it, and bring it into a 'ManB' state.

Note: Once the CMIC packet is provisioned, both CMIC links will be automatically provisioned as well. They will be 'CBsy'.

Note: when plugging the CMIC links into the CMIC packet, use the same configuration as recorded for the 'trns1' command issued for the CMIC links on the HIOP card in slot 15 rear.

```
XAC628 MAR19 14:22:20 7000 INFO XA-Core Provisioning Report
DESCRIPTION: New resource has been provisioned
CARD: Type State Site FL Row Bay Shf/Slt/Pk EqPEC/Serial
      CMIC MBSY HOST 01 A00 DPCC:00 00 15R L NTLX05AB/NNTM64422MWV
```

- the craft person should verify the success of the system-initiated provisioning test of the CMIC packet in slot 15 rear lower by checking the XAC log 640 in logutil:

```
XAC640 MAR19 14:20:40 6900 INFO Test Report
Type Link_Num Slot Side Packlet Test_Type Result
CMIC          15  R   L      OOS      Passed
Initiator: Action initiated by the system
```

- once the integrity of the CMIC packet in slot 15 rear lower has been verified, the craft person should manually RTS the CMIC packet,
- on the MS MAP level, test the MS ports returned by the 'trns1' command for the CMIC links on the HIOP in slot 15 rear (Port 0 on MS 0, Shelf 0, Card 24 and Port 0 on MS 1, Shelf 0, Card 25).
- on the MS MAP level, if the previous MS port tests passed, bring them in-service (Port 0 on MS 0, Shelf 0, Card 24 and Port 0 on MS 1, Shelf 0, Card 25). On the MS MAP level the MS ports will go from 'M' to '.', while on the XAC CMIC MAP level the CMIC links will go from 'CBsy' to '.'.
- once the CMIC links are in-service, issue the 'trns1' command for the CMIC links on the CMIC packet in slot 15 rear lower: 'trns1 15 rear lower'. The MAP response should look like this:

```
trns1 15 rear lower
Command Submitted.
Trns1 15 Rear lower completed
```

```
Link 0 is connected to MS0 Shelf 0 Card 24 Port 0
Link 1 is connected to MS1 Shelf 0 Card 25 Port 0
```

- record the MS port numbers returned by the 'trns1' command for the CMIC links on the CMIC packet in 15 rear lower. Verify that they are the same as the MS port numbers recorded before deprovisioning the CMIC/RTIF HIOP card in 15 rear,

- plug the RTIF packet into the IOP card in 15 rear upper, with links attached.
- the system will automatically provision the RTIF packet, perform an OOS test on it, and bring it into a 'ManB' state.

Note: Once the RTIF packet is provisioned, the system will automatically provision the local and remote RTIF links.

```
XAC628 MAR19 14:23:20 7200 INFO XA-Core Provisioning Report
DESCRIPTION: New resource has been provisioned
CARD: Type State Site FL Row Bay Shf/Slt/Pk EqPEC/Serial
      RTIF CBSY HOST 01 A00 DPCC:00 00 15R U NTLX08AA/NNTM64422MWV
```

- the craft person should verify the success of the system-initiated provisioning test of the RTIF packet in slot 15 rear upper by checking the XAC log 640 in logutil:

```
XAC640 MAR19 14:20:40 6900 INFO Test Report
Type Link_Num Slot Side Packet Test_Type Result
RTIF      15      R      U      OOS      Passed
Initiator: Action initiated by the system
```

- once the integrity of the RTIF packet in slot 15 rear upper has been verified, the craft person should manually RTS the packet,
- once the RTIF packet is in-service, the system will automatically attempt to bring the local and remote RTIF links in-service.
- set the 'xa_component_install_state' office parameter in table OFCENG back to 'inservice',
- at this point, the CMIC and RTIF packets on IOP cards in slots 4R and 15R are all in-service, along with their associated CMIC and RTIF links. No CMIC/RTIF HIOP cards are provisioned in the shelf. This constitutes the end of the migration procedure from CMIC/RTIF HIOP to CMIC and RTIF packets. Please refer to "Final CMIC and RTIF packet locations - XA-Core rear view" on page 327.

Final CMIC and RTIF packet locations - XA-Core rear view



Migration from CMIC/RTIF HIOP back to CMIC and RTIF packets on IOP for SuperNode Shelf Extension (SNSE)

The migration procedure from CMIC/RTIF HIOP cards to CMIC and RTIF packets on IOP cards for SuperNode Shelf Extension (SNSE) is similar to the SuperNode (SN) case. The only exception is the MS port numbers that have to be busied, tested, and enabled during the migration procedure. The ‘trns1’ command should be used on the CMIC MAP level to get the specific MS port numbers to be busied. Please refer to “SN to SNSE port mapping” on page 319.

Performance management for A00002012

Performance management strategy

This feature does not change the performance management strategy of the XA-Core system.

Performance management tools and utilities

This feature changes the Operational Measurements (OM) structure for the CMIC, RTIF, and AMDI functionality on the XA-Core. This is so that the OMs will reflect port/link separation of the CMIC and RTIF functionality on the new CMIC/RTIF HIOP card. All OMs changed, deleted, or added by this feature belong to the XACORE OM group.

Operational Measurements (OM), Group XACORE

OM description

Current OM structure for CMIC, RTIF, and AMDI

Currently, the CMIC and RTIF functionalities peg the following OMs: XACMIC, XARTIF, XALOCP, and XAREMP. With this OM structure in place for CMIC, RTIF, and AMDI, these OMs do not distinguish between packet or device (port or link) state changes. Please refer to “ ” on page 328.

Current OM structure for CMIC, RTIF and AMDI

Functionality	OM	Pegged by event
CMIC	XACMIC	- CMIC packet Insv -> OOS because of fault - CMIC link Insv -> OOS
RTIF	XARTIF	- RTIF packet InSv -> OOS because of fault
RTIF	XALOCP	- RTIF local port InSv -> OOS because of fault
RTIF	XAREMP	- RTIF remote port InSv -> OOS because of fault

Current OM structure for CMIC, RTIF and AMDI

Functionality	OM	Pegged by event
AMDI	XAMDI	- AMDI packet InSv -> OOS because of fault - AMDI port InSv -> OOS because of fault
AMDI	XAMDILNK	- AMDI link InSv -> OOS because of fault

Release history update

The OM group XACORE is being modified in release CSP20.

With the Ethernet Maintenance feature (A59019176) the Ethernet OMs were extended to support port/link separation. This allowed a more accurate count of the various packet, port, and link faults. Since this feature also implements port/link separation for CMIC and RTIF on HIOP, it will extend the existing CMIC and RTIF OMs to distinguish between packet and device (port or link) state changes. Consequently, we will have a more refined count of the CMIC and RTIF component state changes.

This feature also changes the OMs related to the AMDI functionality. This is so that we'll have a consistent OM structure for components with port and link devices in the XA-Core system.

Refer to the following table.

New OM structure for CMIC, RTIF, and AMDI

Functionality	OM	Pegged by event	New/Deleted/Changed
CMIC	XACMIC	- CMIC packet InSv -> OOS because of fault - CMIC link InSv -> OOS because of fault	Deleted
CMIC	XCMIC	CMIC packet InSv -> OOS because of fault	New
CMIC	XCMICPRT	CMIC port InSv -> OOS because of fault	New
CMIC	XCMICLNK	CMIC link InSv -> OOS because of fault	New
RTIF	XARTIF	RTIF packet InSv -> OOS because of fault	Deleted
RTIF	XALOCP	RTIF local port InSv -> OOS because of fault	Deleted
RTIF	XAREMP	RTIF remote port InSv -> OOS because of fault	Deleted
RTIF	XRTIF	RTIF packet InSv -> OOS because of fault	New
RTIF	XRTIFPRT	- RTIF local port InSv -> OOS because of fault - RTIF remote port InSv -> OOS because of fault	New

New OM structure for CMIC, RTIF, and AMDI

Functionality	OM	Pegged by event	New/Deleted/Changed
RTIF	XRTIFLNK	- RTIF local link InSv -> OOS because of fault - RTIF remote link InSv -> OOS because of fault	New
AMDI	XAMDI	- AMDI packet InSv -> OOS because of fault	Changed
AMDI	XAMDIPRT	- AMDI port InSv -> OOS because of fault	New
AMDI	XAMDILNK	- AMDI link InSv -> OOS because of fault	Unchanged

Registers

The XACORE group new OM register display on the MAP terminal is as follows:

OM XACORE Group Display

XAPE	XARXPE	XASM	XARXSM
XAIOP	XARXIO	XADISK	XATAPE
XRTIF	XRTIFPRT	XRTIFLNK	XCMIC
XCMICPRT	XCMICLNK	XARXABRT	XARXBASE
XARXFULL	XARXALL	XAMDI	XAMDIPRT
XAMDILNK	XETHR	XETHRPRT	XETHRLNK

Register XACMIC**Register description**

Existing XA-Core CMIC (XCMIC) peg register counts the number of critical CMIC packet and link faults detected on the XA-Core.

Register release history update

Register is being removed in CSP20. In order to have consistent naming convention for OMs in the XACORE group, from CSP20, the CMIC packet faults are going to be counted by the new peg register XCMIC. The CMIC link faults are going to be counted by the new peg register XCMICLNK.

Register XCMIC**Register description**

The XA-Core CMIC (XCMIC) peg register counts the number of critical CMIC packet faults detected on the XA-Core.

Register release history update

Register is being introduced in CSP20.

Associated registers

None.

Associated logs

The system generates the MScomm log report (XAC303) when a CMIC packet goes out of service.

The system generates the MScomm Alarm Cleared (XAC603) when the CMIC fault clears on the packet.

Register XCMICPRT**Register description**

The XA-Core CMIC PORT (XCMICPRT) peg register counts the number of critical CMIC port faults detected on the XA-Core.

Register release history update

Register is being introduced in CSP20.

Associated registers

None.

Associated logs

The system generates the MScomm log report (XAC303) when a CMIC port goes out of service.

The system generates the MScomm Alarm Cleared (XAC603) when the CMIC fault clears on the port.

Register XCMICLNK**Register description**

The XA-Core CMIC LINK (XCMICLNK) peg register counts the number of critical CMIC link faults detected on the XA-Core.

Register release history update

Register is being introduced in CSP20.

Associated registers

None.

Associated logs

The system generates the MScomm log report (XAC303) when a CMIC link goes out of service.

The system generates the MScomm Alarm Cleared (XAC603) when the CMIC fault clears on the link.

Register XARTIF

Register description

The existing XA-Core RTIF (XARTIF) peg register counts the number of critical RTIF packet faults detected on the XA-Core.

Register release history update

Register is being removed in CSP20. In order to have consistent naming convention for OMs in the XACORE group, from CSP20, the RTIF packet faults are going to be counted by the new peg register XRTIF.

Register XALOCP

Register description

The existing XA-Core RTIF (XARTIF) peg register counts the number of critical RTIF local port faults detected on the XA-Core.

Register release history update

Register is being removed in CSP20. From CSP20, the RTIF local port faults are going to be counted by the new peg register XRTIFPRT.

Register XAREMP

Register description

The existing XA-Core RTIF (XARTIF) peg register counts the number of critical RTIF remote port faults detected on the XA-Core.

Register release history update

Register is being removed in CSP20. From CSP20, the RTIF remote port faults are going to be counted by the new peg register XRTIFPRT.

Register XRTIF

Register description

The XA-Core RTIF (XRTIF) peg register counts the number of critical RTIF packet faults detected on the XA-Core.

Register release history update

Register is being introduced in CSP20.

Associated registers

None.

Associated logs

The system generates the RTIF log report (XAC305) when an RTIF packet goes out of service.

The system generates the RTIF Alarm Cleared log report (XAC605) when the RTIF fault clears on the packet.

Register XRTIFPRT

Register description

The XA-Core RTIF PORT (XRTIFPRT) peg register counts the number of critical RTIF port faults detected on the XA-Core.

Note: There are no separate peg registers for local and remote RTIF port faults. Both peg XRTIFPRT.

Register release history update

Register is being introduced in CSP20.

Associated registers

None.

Associated logs

The system generates the RTIF log report (XAC305) when an RTIF port goes out of service.

The system generates the RTIF Alarm Cleared log report (XAC605) when the RTIF fault clears on the port.

Register XRTIFLNK

Register description

The XA-Core RTIF LINK (XRTIFLNK) peg register counts the number of critical RTIF link faults detected on the XA-Core.

Note: There are no separate peg registers for local and remote RTIF link faults. Both peg XRTIFLNK.

Register release history update

Register is being introduced in CSP20.

Associated registers

None.

Associated logs

The system generates the RTIF log report (XAC305) when an RTIF link goes out of service.

The system generates the RTIF Alarm Cleared log report (XAC605) when the RTIF fault clears on the link.

Register XAMDI

Register description

Existing XA-Core AMDI (XAMDI) peg register counts the number of critical AMDI packet and port faults detected on the XA-Core.

Register release history update

Register is being changed in CSP20. From CSP20, the AMDI port faults are going to be counted by the new peg register XAMDIPRT. Register XAMDI will peg the critical faults against the AMDI packet. No other modification is introduced.

Register XAMDIPRT

Register description

The XA-Core AMDI PORT (XAMDIPRT) peg register counts the number of critical AMDI port faults detected on the XA-Core.

Register release history update

Register is being introduced in CSP20.

Associated logs

The system generates the AMDI log report (XAC309) when an AMDI port goes out of service.

The system generates the AMDI Link Condition Cleared (XAC609) when the AMDI fault clears on the port.

Product = CS 2000

A00002013--Intelligent Network T1 Timer Expiry Message Suppression (Succession on DMS)

Functional Description

The T1 Timer specifies a length of time, in seconds, the SSP waits for response from an off-board processor after sending it a query message before the call is routed to treatment. When routing the call to treatment, a 'T1 Timer Expiry' message is generated by the SSP.

This feature, when enabled, will suppress 'T1 Timer Expiry' messages from being generated. Suppressing the 'T1 Timer Expiry' messages from being generated will prevent the messages from flooding the network should an SCP go down.

However, suppressing the 'T1 Timer Expiry' messages violates the standard procedure for this situation and is therefore adding optional functionality.

This feature depends on SOC INW00001 to switch the functionality ON/OFF and uses office parameter T1_TIMER_EXPIRY_MSG_SUPPRESS to provide feature optionality control.

The office parameter contains four fields, the first of which allows the user to switch the 'T1 Timer Expiry' message generation ON/OFF. When the feature is on, the remaining three fields allow the user to switch log generation ON/OFF, alarm generation ON/OFF and specify a threshold value. The threshold value is related with the alarm generation and is explained later on.

If the suppress option is switch on, no "T1 Timer Expiry" messages will be generated.

If the log option is switched on, then a GAME101 log will be created when the RSPTMOUT OM count is greater than zero. The RSPTMOUT is an OM peg that is incremented every time the SSP generates a 'T1 Timer Expiry' message.

If the alarm option is switched on, then a GAME102 log will be created when the RSPTMOUT OM count is greater than or equal to the threshold value specified in the office parm T1_TIMER_EXPIRY_MSG_SUPPRESS. This log generates an external minor alarm. It will stay activated while the RSPTMOUT OM count is greater than or equal to the threshold value, as previously described. Or, until an operator clears the minor alarm from the banner. The RSPTMOUT OM count will be checked against the threshold value every time the RSPTMOUT OM transfer period expires. If the RSPTMOUT OM count drops below the threshold value and the minor alarm was generated in the previous RSPTMOUT OM transfer period, then this feature will clear the minor alarm.

For more details on the log or alarm, please refer to the relevant documentation.

Hardware Requirements or Dependencies

None.

Software Requirements or Dependencies

None.

Limitations and restrictions

This feature will impact DMS-100 (including TDM, Succession, MSL), MMP and SSR. All other markets are not affected by this feature.

Interactions

None.

Applicable customer facing sections

Fault Management

Logs ☒

Alarms ☒

Configuration

Data Schema ☐

User Interface ☐

Element Management ☐

Security ☐

Service Order ☐

Office Parameters ☒

Accounting (includes AMA billing) ☐

Performance (includes operational measurements) ☐

Indicate with an X if you are completing the sections of the DDOC listed below. Indicate with “N/A” if these sections do not apply to this functionality.

Realtime ☒

Engineering Information ☒

Glossary

Term	Description
SCP	Service Control Point
SOC	Software Optionality Control
OM	Operational Measurement

Fault Management for A00002013

Fault management strategy

None.

Fault management tools and utilities

None.

Logs

Log GAME101

Explanation

A GAME101 log will be created if the RSPTMOUT OM count is greater than zero. The log will be created during the RSPTMOUT OM transfer period and will record the RSPTMOUT OM count value.

Format

The log report format follows:

```
office * GAME101 mmmdd hh:mm:ss seqno INFO GAME_ERR_REPORT
REASON = reason_field
COUNT = count_field
```

Example

An example of the log report follows:

```
S3_500_17BL CM GAME101 APR04 05:10:16 0504 INFO GAME_ERR_REPORT
REASON      = Suppressed T1 Timer Expiry Message
COUNT      = 25
```

Field descriptions

Field	Value	Description
reason_field	CONSTANT	A string describing the reason the log was created. In this case, it is due to suppressing a 'T1 Timer Expiry' message.
count_field	UNSIGNED INTEGER	A copy of the RSPTMOUT OM count value. It will be a number in the range from 1 to 32,767.

Action

If a high number of GAME101 logs are output it could be an indication that there is a problem with the SCP. The SCP should be checked to verify that it is operating normally.

If a low number of GAME101 logs show occasionally, it could be related to a network congestion.

Any number of GAME101 logs are highlighting a problem that needs to be addressed by your SCP first level support.

Associated Operational Measurements or Performance Measurements

This feature monitors the RSPTMOUT OM count, found in the AIN OM group, checking to see if it increments past zero. The count is incremented every time the T1 timer expires and the SSP, as a consequence, attempts to generate a 'T1 Timer Expiry' message.

Additional information

N/A

Log GAME102

Explanation

A GAME102 log will be created if RSPTMOUT OM count becomes equal to the office parm T1_TIMER_EXPIRY_MSG_SUPPRESS threshold value. The log will be created when this feature suppresses a 'T1 Timer Expiry' message.

When a GAME102 log is created it will raise an external minor alarm. The alarm will need to be cleared before another log entry will be created through the situation described earlier. The alarm will be cleared either by an operator or by this feature. The feature will clear the alarm during the second transfer period to pass after initially creating the log entry. The reason for doing this, will be to expose the alarm for long enough to get noticed by an operator. If the problem persists after clearing the alarm, then a new log will be created, as described earlier and as a consequence, a new external minor alarm will be raised.

Format

The log report format follows:

```
office * GAME102 mmmdd hh:mm:ss seqno INFO GAME_ERR_REPORT
REASON = reason_field
COUNT = count_field
```

Example

An example of the log report follows:

```
S3_500_17BL CM GAME102 APR04 05:10:16 0504 INFO GAME_ERR_REPORT
REASON = Threshold reached for suppressing T1 Timer Expiry Messages
COUNT = 100
```

Field descriptions

Field	Value	Description
reason_field	CONSTANT	A string describing that the number of times a 'T1 Timer Expiry' message was suppressed has reached the office parm T1_TIMER_EXPIRY_MSG_SUPPRESS threshold value.
count_field	UNSIGNED INTEGER	A copy of the RSPTMOUT OM count value. It will be a number in the range from 1 to 32,767.

Action

If you frequently find a high number of GAME102 logs, it could be that you have the office parm T1_TIMER_EXPIRY_MSG_SUPPRESS threshold value set too low. If this is the case, the threshold value should be modified according to the configuration recommendations.

If the office parm T1_TIMER_EXPIRY_MSG_SUPPRESS threshold value is not too low, it could be a problem with the SCP.

If the T1_TIMER_EXPIRY_MSG_SUPPRESS threshold value has been set accordingly, it could be a problem with the application T1 Timer value being set too low.

You should have your SCP first level support look into any of these problems.

Associated Operational Measurements or Performance Measurements

This feature monitors the RSPTMOUT OM count, found in the AIN OM group, checking to see if it increments to value equal to the office parm T1_TIMER_EXPIRY_MSG_SUPPRESS threshold. The count is incremented every time the T1 timer expires and the SSP, as a consequence, attempts to generate a 'T1 Timer Expiry' message.

Additional information

N/A

Alarms

Alarm GAME102

This is a minor external alarm, that is associated with GAME102 log (“Log GAME102” on page 338). This alarm indicates that Service Control Point (SCP) is not responding to each query and the T1 timers associated with each query is expiring.

Related documentation

1. 297-5161-022, Vol 1-3, AIN Service Enablers: Service Implementation Guides.

Configuration for A00002013

Hardware and Software Requirements

There are no hardware or software requirements.

Initial Configuration

During the ONP, if the patch TBF56 is found active on the switch, SOC INW00001 will be switched ON and the office parm T1_TIMER_EXPIRY_MSG_SUPPRESS will be initialized to indicate that all ‘T1 Timer Expiry’ messages should be suppressed.

If the patch TBF56 is found and not active on the switch during ONP, then SOC INW00001 will be switched ON and the office parm T1_TIMER_EXPIRY_MSG_SUPPRESS will be initialized to indicate that no ‘T1 Timer Expiry’ messages should be suppressed.

If the patch TBF56 is not found, then the SOC INW00001 will be switched OFF and the office parm T1_TIMER_EXPIRY_MSG_SUPPRESS will be initialized to indicate that no ‘T1 Timer Expiry’ messages should be suppressed.

Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable.

New/modified office/subnet parameters

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCVAR	T1_TIMER_EXPIRY_MSG_SUPPRESS	NEW	CM

Parameter information**T1_TIMER_EXPIRY_MSG_SUPPRESS**

T1_TIMER_EXPIRY_MSG_SUPPRESS

Functional description

This office parm will be used to provide optionality control for the feature.

Provisioning rules

There will be four fields in office parm

T1_TIMER_EXPIRY_MSG_SUPPRESSION, to switch 'T1 Timer Expiry' message suppression ON/OFF, log ON/OFF, alarm ON/OFF and a threshold value.

If SOC INW00001 is switched OFF, the user will not be permitted to provision the office parm T1_TIMER_EXPIRY_MSG_SUPPRESSION.

The user will be able to switch the log or alarm ON/OFF, if the SOC INW00001 is ON and the office parm

T1_TIMER_EXPIRY_MSG_SUPPRESSION field suppression is switched ON. Additionally, they can only specify a threshold value greater than zero if the alarm creation is ON. If they try to provision incorrectly, then a suitable message will be displayed to indicate the reason for failing the change in SERVORD.

The threshold value is used to determine when to create a GAME102 log entry, which in turn raises an external minor alarm. In order to calculate the value of the threshold, the user should take the highest RSPTMOUT OM count value found within a 24 hour period and multiply this number by 1.25. Calculating the threshold in this way, provides a small amount of padding against the worst situation.

Incidentally, the user will only be permitted to enter a threshold value greater than zero when the alarm option is ON. The threshold value of zero is invalid when the alarm option is ON and if the user attempts to provision it in this way, it will be denied. If denied, a suitable message will be displayed to indicate the problem.

Range information

The table below provides information about all four fields, as described in Provisioning Rules. Fields 1 to 3 are of type BOOLEAN and will only have a value of 'TRUE' or 'FALSE'. It is interpreted that 'TRUE' is equivalent to 'ON' and 'FALSE' is 'OFF'. Field 4 is an UNSIGNED INTEGER with a value range of 0 to 32,767.

Range Information

Field	Minimum	Maximum	Default
1	OFF	ON	OFF
2	OFF	ON	OFF
3	OFF	ON	OFF
4	0	32,767	0

Activation

In order to suppress 'T1 Timer Expiry' messages from being generated, the user will need to switch the SOC INW00001 to ON and the office parm T1_TIMER_EXPIRY_MSG_SUPPRESS field suppression to ON. Once these are ON, the user has the option to activate log or alarm generation when a 'T1 Timer Expiry' message is suppressed.

Dependencies

None.

Consequences

The following fields, as briefly explained above in section 13.3.2.1.3 Provisioning Rules, represent:

SOC INW00001 needs to be switches ON, before any provisioning of office parm T1_TIMER_EXPIRY_MSG_SUPPRESSION is permitted.

Field 1: Suppression (ON/OFF). When 'ON' all 'T1 Timer Expiry' messages will be suppressed and permits provisioning of fields 2 to 4.

Field 2: Log (ON/OFF). When 'ON', creates an entry in GAME101 during the RSPTMOUT OM transfer period, if the RSPTMOUT OM count is greater than zero.

Field 3: Alarm (ON/OFF): When 'ON', creates an entry in GAME102 if the RSPTMOUT OM count equals the office parm T1_TIMER_EXPIRY_MSG_SUPPRESSION threshold value. In turn, when an entry is created, an external minor alarm will be raised.

Field 4: Threshold (0 - 32,767). Used when determining if a entry in the GAME102 log should be created.

For more information on the behavior of these fields, please refer to the relevant customer documentation.

Verification

During the verification of the four fields the following checks will be done:

Field 1: This can only be equal to ON or OFF. In order for this to be equal to ON, SOC INW00001 should be switched ON.

Field 2: This can only equal to ON or OFF. This can only be set to ON, if field 1 is set to ON.

Field 3: This can only equal to ON or OFF. This can only be set to ON, if field 1 is set to ON.

Field 4: This can only be a number in the range 1 to 32,767. It can only change from a value of 0 if field 3 is set to ON. If field 3 is set to OFF, then the only valid value in this field is 0.

Memory requirements

Need memory to store data:

Units per memory block = 1

Words per memory block = 3

If the parameter value = 1

words required = (((parameter value - 1)/units per block) + 1) * words per block = 3

Parameter release history update

New in SN07.

Upgrade Impact

Dump and Restore

Same details as “ Initial Configuration” on page 340.

Element Management Upgrade

N/A

Data schema (DS) (CM, MIBS, RDB)

N/A

Service Orders (SO) (CM & SESM)

N/A

Software optionality control (SOC)**SOC**

SOC option name:	INW00001
SOC option title:	T1 Timer Expiry Msg
SOC option control type:	ON/OFF
New SOC option?	Yes
SOC option order code	INw00001
Option defined in DRU:	SHR
Affected products:	CNA, MMP, MSL, SSR, Succession

Element Management

N/A

Command interface changes

N/A

Security

N/A

Configuration Walkthrough

NA

Product = CS 2000**A00002047 -- SPM Backplane (Succession on DMS)*****Functional Description***

This feature is being implemented in release SN07, under the following activities:

- A00002047 for DMSSHR(20)
- A00002057 for SP(20)--included in A00002047

The feature entails the implementation of a new double density backplane for the Spectrum family of products.

The intent of this feature is to enable space efficiency by collapsing today's two-shelf Spectrum node configuration into a single double density card shelf. This can be accomplished in several ways. One example would be an IW SPM that does not use ECAN, provisioned with two CEMs, two ATM RMs, three DSP RMs, and a Sync RM. This has a straightforward conversion to a single-shelf configuration using the double density backplane. A second example would be a densely configured MG4K node, provisioned with two CEMs, two ATM RMs, two OC3 RMs, four DSP RMs, seven COH RMs, two Sync RMs, two DLC RMs, and an Alarm RM. In this case, when taken together with the new Spectrum resource module, the NTLX45AA Telephony Services Processor (TSP), customers will be able to fit four such Spectrum nodes into a single frame, one node per shelf.

The Double Density SPM program will significantly improve the trunk port density of the Spectrum-based product portfolio. Program benefits are a 50% density increase, achieved by a 50% footprint reduction, and a small yearly operating cost reduction (power and floor-space savings) which lowers the customer cost of ownership. The Double Density SPM program introduces new Spectrum back plane hardware, the NTLX51CA. The new back plane will provide backwards compatibility with the existing Resource Modules. Due to slot limitations, products that use the three-slot LSA complexes will experience slot exhaustion in the Double Density Spectrum-these products currently include MG4K LSA/STS1 and GSM e3 TCU/BSC-and, thus, will not be able to exploit the new backplane.

There are two distinct phases to the Double Density Spectrum Program. The first phase (A00002047, covered in this FN) modifies the existing Spectrum backplane hardware, NTLX51BA, to support four 15-slot Spectrum nodes per frame; currently two 30-slot nodes are supported per frame. The second phase, A00002386, constructs a new high-density DSP/ECAN card (the Telephony Services Processor, or TSP card) creating a new ECAN and DSP applications. This second phase also modifies the Spectrum software to support the concept of dynamic resource re-assignment within a single call and allows DSP and ECAN applications to co-exist on a single card.

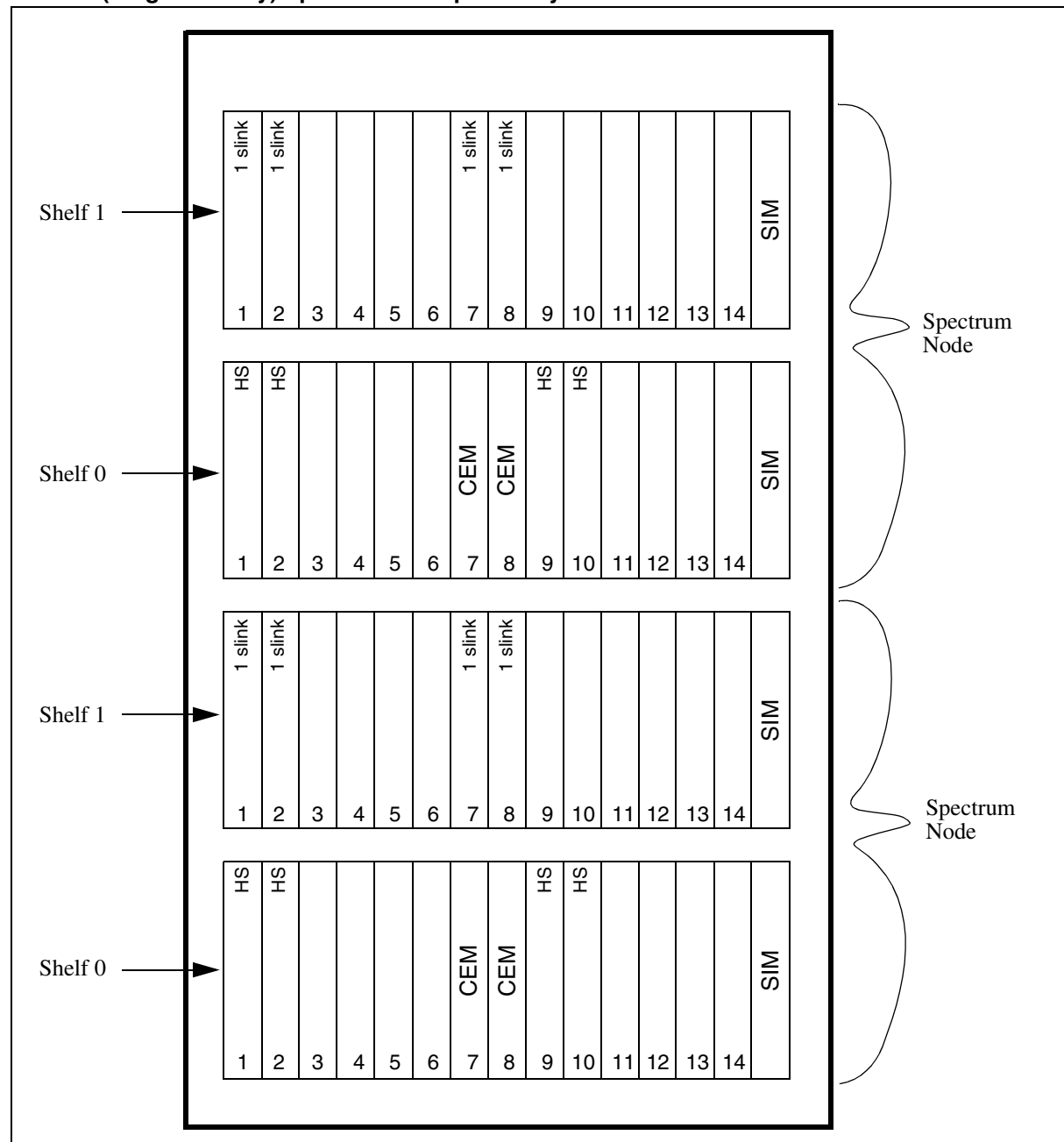
Background Information

Today's Spectrum hardware includes a frame with PEC NTLX91BA that houses a backplane with PEC NTLX51BA which in turn supports **two** Spectrum nodes, each spanning two contiguous card shelves. (Please refer to "Current (Single Density) Spectrum Backplane Layout" on page 346.)

As illustrated, each Spectrum node occupies two shelves within the frame, each shelf housing 15 slots. Slot 15 on each shelf is dedicated for the Shelf

Interface Modules (SIMs). Slots 7 and 8 of shelf 0 for each Spectrum node are dedicated for the Common Equipment Modules (CEMs).

Current (Single Density) Spectrum Backplane Layout



The remaining slots support various Spectrum resource modules (RMs), each having varying serial link (slink) requirements, depending upon the inter-module communication needs. Four high-speed slots are each serviced by 9 slinks and can be used for RM types such as OC3 or ATM. Low-speed slots

are serviced by 3 slinks and can be used for RM types such as DSP or VSP. There are also four slots (1, 2, 7, and 8 on shelf 1) with single slinks which can accommodate DLC, DLC2, and ALM cards.

Feature Description

The new hardware layout for Double Density Spectrum includes a frame with PEC NTLX91CA (identical to the NTLX91BA frame⁷) that houses a backplane with PEC NTLX51CA which in turn supports **four** Spectrum nodes, each spanning only a single card shelf. (Please refer to “New Double Density Spectrum Backplane Layout” on page 348.)

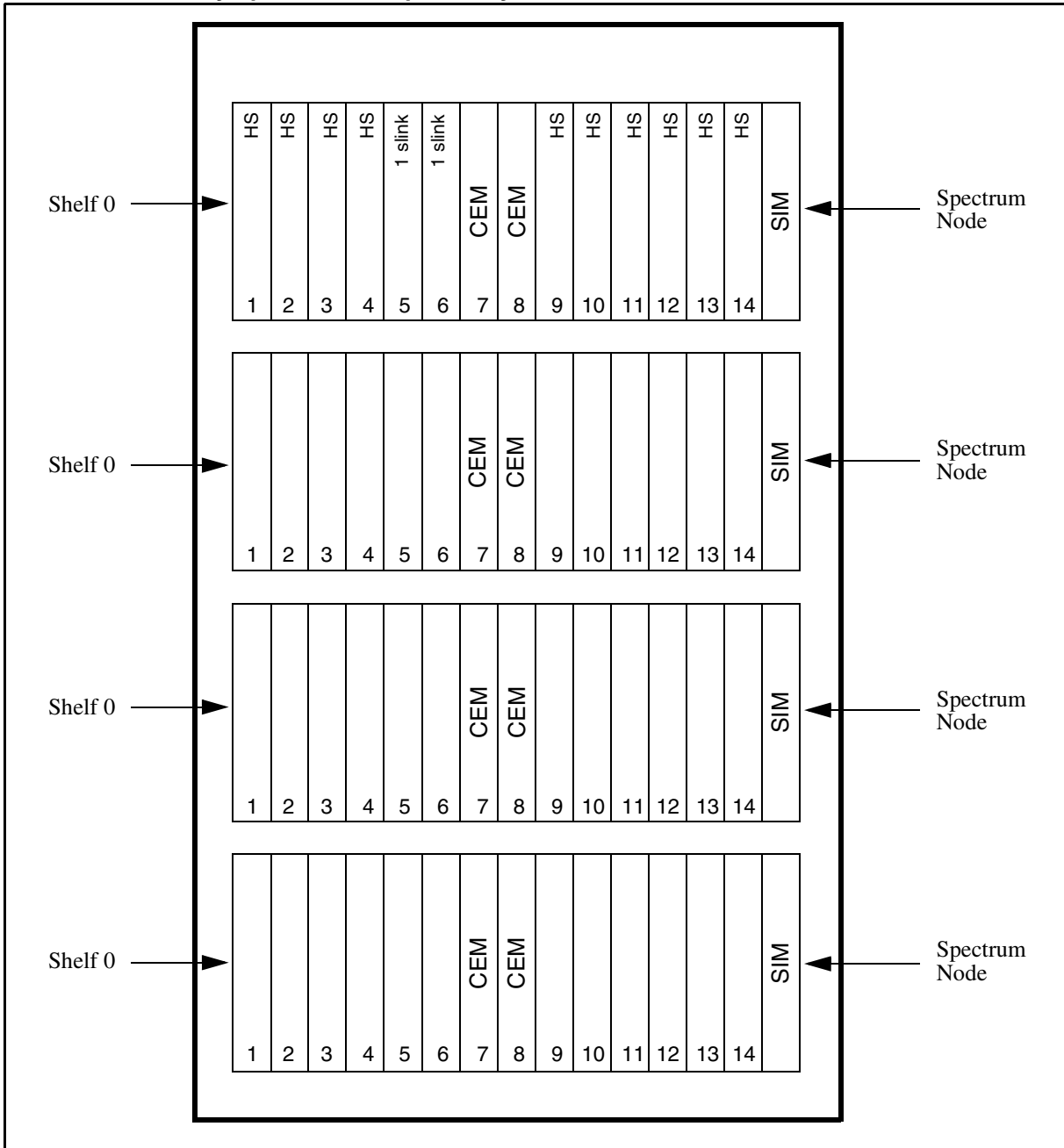
Slot 15 on each shelf is still dedicated for the SIMs. Also, since each shelf is a “shelf 0”, slots 7 and 8 on each shelf are dedicated for CEMs. Of the remaining slots, ten of them are high-speed (9 slink) slots, slots 5 and 6 are single slink slots.

Clock synchronization traces are present in slots 1 and 2 (for use by ATM RMs), slots 9 and 10 (for use by OC3 or ATM RMs), and slots 5 and 6 (for use by Sync RMs, and also suitable for DLC and DLC2 RMs).

The addition of high-speed slots (and consequent reduction in low-speed slots) enable the single-shelf Spectrum layout through compression of DSP and ECAN functionality into a very small number of the new Telephony Services Processor (TSP) RMs.

Note: To provide a future migration path for the Spectrum product (e.g., for OC-12 support), a set of Differential Link (D-Link) signals have been added to the double density backplane assembly. These D-link signals route between slots 5 & 6 and the ten high-speed slots; slots 5 & 6 form the hub of the D-link signals which emanate in a star configuration to the high-speed slots.

7. The new frame PEC code is needed to facilitate ordering, since the frame and backplanes are ordered as a unit.

New Double Density Spectrum Backplane Layout**Limitations and restrictions**

Though high-speed and double density Spectrum backplanes may co-reside in the same office, the two backplanes cannot be mixed within the same Spectrum frame.

Logs (LG)

N/A

Data schema (DS)**New/modified tables**

Table name	NEW, CHANGED or DELETED	Table Control (NEW/OLD/UNCHANGED)
MNSHELF	changed	unchanged
MNCKTPAK	changed	unchanged

There are no new fields for tables MNSHELF or MNCKTPAK. Rather, the verification rules have changed in support of the double density Spectrum backplane. Tables MNSHELF and MNCKTPAK will be modified to enforce the following restrictions with respect to the double density Spectrum backplane:

- a single frame cannot contain both a traditional (high speed) Spectrum shelf assembly (NTLX51BA) and a new double density shelf assembly (NTLX51CA)
- a single NTLX91CA frame can be provisioned with no more than four Spectrum nodes, using only double density Spectrum shelf assemblies (NTLX51CA)
- frames older than NTLX91CA with backplanes older than NTLX51CA cannot be datafilled with more than two Spectrum nodes
- circuit packs cannot be datafilled on shelf 1 of a Spectrum node that resides on a double density backplane (since shelf 1 cannot exist)
- prevent higher speed cards from being datafilled in slots 5 and 6 (the SRM slots) of a double density Spectrum node
- ATM RMs can be datafilled in slots 1 and 2, or 9 and 10 only
- OC3 RMs can be datafilled in slots 9 and 10 only
- Sync RMs can be datafilled in slots 5 and 6 only

Office parameters (OP)

N/A

Service orders (SO)

N/A

Alarms (AL)

N/A

Command interface (CI)

MAP Display Changes

Since a double density Spectrum node will only use up one card shelf, rather than the two shelves used up by a traditional Spectrum node, corresponding changes are necessitated to some of the SPM MAP displays. Specifically, the SPM shelf level and CEM/RM protection level MAP displays will be truncated to display only the one card shelf. The following subsections illustrate the changes.

SPM Shelf Level MAP Changes

The SPM shelf level MAP summarizes the states of all of the SPM's cards. (Figure on page 350 and Figure on page 351.)

> mapci;mtc;pm;post spm 34

Old Single Density Spectrum Node Display

MSH7-t4.map-async.MSH7-test.nortelottawa-dms_0											
XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL		
RExFlt	01CCFB	NODLOG	LOAD	1 SPM	8 RS	.	6CC.	1 Maj	.		
				C	*C*		*C*	M			
SPM				SysB	ManB	OffFL	CBsy	ISTb	InSv		
0 Quit		PM		6	0	81	0	17	2		
2 Post_		SPM		1	0	81	0	4	0		
3 ListSet											
4 ListRes											
5 Trns1											
6											
7 ATMConn											
8											
9 OfClk											
10											
11 Disp_											
12 Next											
13 Select_											
14 QueryPM											
15 ListAlm											
16 Clock											
17 SPERFORM											
18 Upgrade_											
ROB											
Time	11:07	>									

New Double Density Spectrum Node Display

MSH7-t4.map-async.MSH7-test.nortelottawa-dms_0										
XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL	
RExF1t	01CCFB	NODLOG	LOAD	1 SPM	8 RS	.	6CC.	1 Maj	.	
				C	*C*		*C*	M		
SPM				SysB	ManB	OffFL	CBsy	ISTb	InSv	
0 Quit		PM		6	0	81	0	17	2	
2 Post_		SPM		1	0	81	0	4	0	
3 ListSet										
4 ListRes	SPM	34	ISTb	Class: SMG4						
5 Trns1										
6										
7 ATMConn	Sh1f0	SL	A	Stat	Sh1f0	SL	A	Stat		
8	ATM 0	1	I	OffFL	CEM 1	8	I	ISTb		
9 OFClk	ATM 1	2	A	OffFL	OC3 0	9	A	OffFL		
10	-----	3	-	-----	OC3 1	10	I	OffFL		
11 Disp_	-----	4	-	-----	-----	11	-	-----		
12 Next	SRM 0	5	A	OffFL	-----	12	-	-----		
13 Select_	SRM 1	6	I	OffFL	-----	13	-	-----		
14 QueryPM	CEM 0	7	A	ISTb	-----	14	-	-----		
15 ListAlm										
16 Clock										
17 SPERFORM										
18 Upgrade_										
ROB										
Time	11:07	>								

SPM Module Protection Level MAP Changes

The CEM (or RM) protection level MAPs are used for manually switching CEM (or RM) activity between units in the same Protection Group. (Refer to the two figures that follow, here and on page 352.)

> mapci;mtc;pm;post spm 34;select cem 0; prot

Old Single Density Spectrum Node Display

MSH7-t4.map-async.MSH7-test.nortelottawa-dms_0										
XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL	
RExF1t	01CCFB	NODLOG	LOAD	1 SPM	8 RS	.	6CC.	1 Maj	.	
				C	*C*		*C*	M		
Protectn				SysB	ManB	OffFL	CBsy	ISTb	InSv	
0 Quit		PM		6	0	81	0	17	2	
2		SPM		1	0	81	0	4	0	
3										
4										
5	SPM	34	ISTb	Mode: N/A						
6	Prot Grp: CEM			Schema: N/A						
7 Force	Sh0	U	R	A	Stat	Sh0	U	R	A	Stat
8 Manual	1	---	---	---	---	8	1	S	I	ISTb
9	2	---	---	---	---	9	---	---	---	---
10	3	---	---	---	---	10	---	---	---	---
11	4	---	---	---	---	11	---	---	---	---
12	5	---	---	---	---	12	---	---	---	---
13 Select_	6	---	---	---	---	13	---	---	---	---
14	7	0	W	A	ISTb	14	---	---	---	---
15 ListAlm										
16 Prot										
17 EraseFl										
18										
ROB										
Time	11:08	>								

New Double Density Spectrum Node Display

MSH7-t4.map-async.MSH7-test.nortelottawa-dms_0										
XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL	
RExFlt	01CCFB	NODLOG	LOAD	1 SPM	8 RS	.	6CC.	1 Maj	.	
Protectn				*C*	*C*		*C*	M		
0 Quit		PM		SysB	ManB	OffL	CBsy	ISTb	InSv	
2		SPM		6	0	81	0	17	2	
3				1	0	81	0	4	0	
4										
5		SPM 34	ISTb							
6		Prot Grp: CEM			Mode: N/A			Schema: N/A		
7 Force		Sh0 U R A Stat		Sh0 U R A Stat						
8 Manual		1 -- -- --		8 1 S I ISTb						
9		2 -- -- --		9 -- -- --						
10		3 -- -- --		10 -- -- --						
11		4 -- -- --		11 -- -- --						
12		5 -- -- --		12 -- -- --						
13 Select_		6 -- -- --		13 -- -- --						
14		7 0 W A ISTb		14 -- -- --						
15 ListAlm										
16 Prot										
17 EraseFl										
18										
ROB										
Time	11:08	>								

Glossary

Term	Description
TSP	Telephony Services Processor - a new, high-density Spectrum resource module that can be used to replace multiple VSP, DSP, and COH resource modules.

Product = CS 2000**A00002133 -- CBM SDM SW Installation & Commissioning (Succession on DMS)*****Functional Description***

This feature provides the following functionality:

CBM product functionality:

- Software delivery processes for the CBM product
- Installation for the CBM product in both single and dual server high availability configuration

- Preparation work required in SN07 for CBM upgrades in SN08

Product generic functionality:

- A platform for patching for products based on the Solaris operating system
- An easy to use interface for installing and removing software

Software Delivery

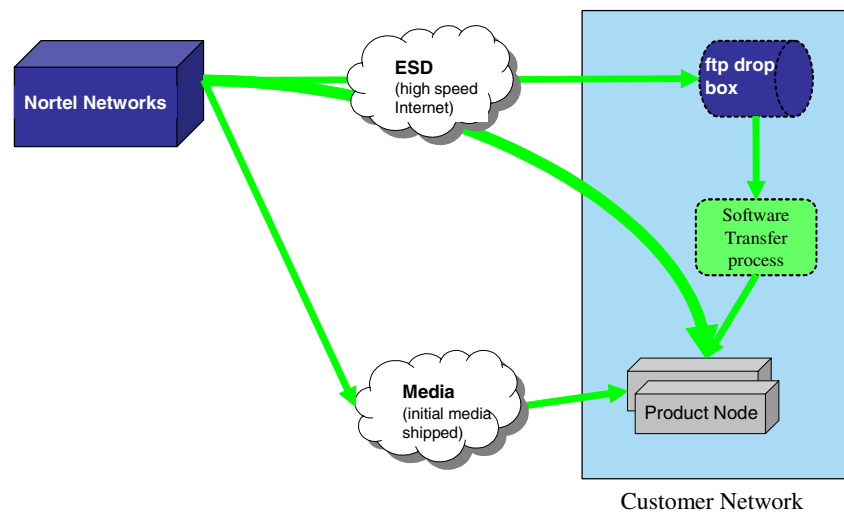
Electronic software delivery (ESD) is the supported method of software delivery for the CBM product. To support ESD, customers will require a high speed internet connection.

ESD provides greater responsiveness than media delivery. ESD provides business value by enabling automatic application of software reducing support costs.

CDROM media will be included with the initial product installation. Patches and maintenance load images will be delivered through ESD

ESD deliveries can be deposited on an intermediary machine, or directly onto the product node if access is provided. The direct access method is preferred as it is simpler.

The following diagram depicts an overview of software delivery.



The CDROM media will contain the final load image for the product and all available packages at the time the CDROM image was mastered. From that point on, the product will be patched using electronic patch delivery.

Installation

Installation procedures will support system preparation prior to shipment to the customer site to add business value. Preparation work includes installation of the SSPFS platform and CBM common software. Value is created by reducing installation technician labour costs as a single technician can perform the common parts of the installation process on many machines at the same time at the factory. This saves installation time and complexity during the install procedure at the customer site.

For two node clusters, the following steps are performed on the active node. Either node can be arbitrarily selected to be the active node for installation.

Installations for a single node cluster are very similar to installations for a two node cluster. Simply skip the last step where the inactive node is cloned.

Installation steps:

1) Install Solaris and the SSPFS platform and the CBM common components

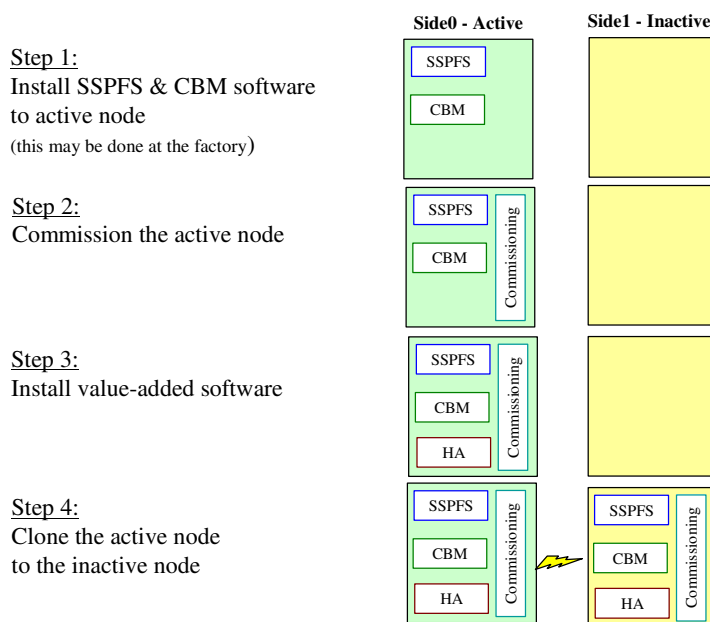
<these steps will be performed at the factory prior to shipment to site>

2) Perform system commissioning

3) Install value added software such as Billing, OM Delivery, or any other purchased software.

If this is a two node cluster, then

4) Clone the inactive node from the active node using the sync mechanism provide with the SSPFS HA framework



CBM Common software installation:

The installation interface is command line driven and common to all CBM based products. The “cbm_setup” installation tool provides a simple interface to initiate, complete, and provide status feedback for the installation.

<Begin screen capture>

```
=====
CBM Setup Program
```

```
=====
Checking available disk space.
```

```
Checking SSPFS setup.
```

```
Checking base directory.
```

```
/opt/nortel/cbm/7 exists.
```

```
Examining installed packages...
```

```
Verifying required packages...
```

```
GNU Compiler and Libraries COMPLETELY INSTALLED
```

RogueWave SourcePro Libraries	COMPLETELY INSTALLED
Platform Base	COMPLETELY INSTALLED
SDM Base Maintenance Interface	COMPLETELY INSTALLED
Platform Utilities	COMPLETELY INSTALLED
Generic Data Delivery	COMPLETELY INSTALLED
Log Delivery Service	COMPLETELY INSTALLED
Table Access Service	COMPLETELY INSTALLED
OM Access Service	COMPLETELY INSTALLED

Verification completed.

<End screen capture>

Upgrade preparation work:

cbm_setup will be used to provide a simple command line interface for upgrades. This adds business value by reducing training costs that would be required to learn multiple interfaces.

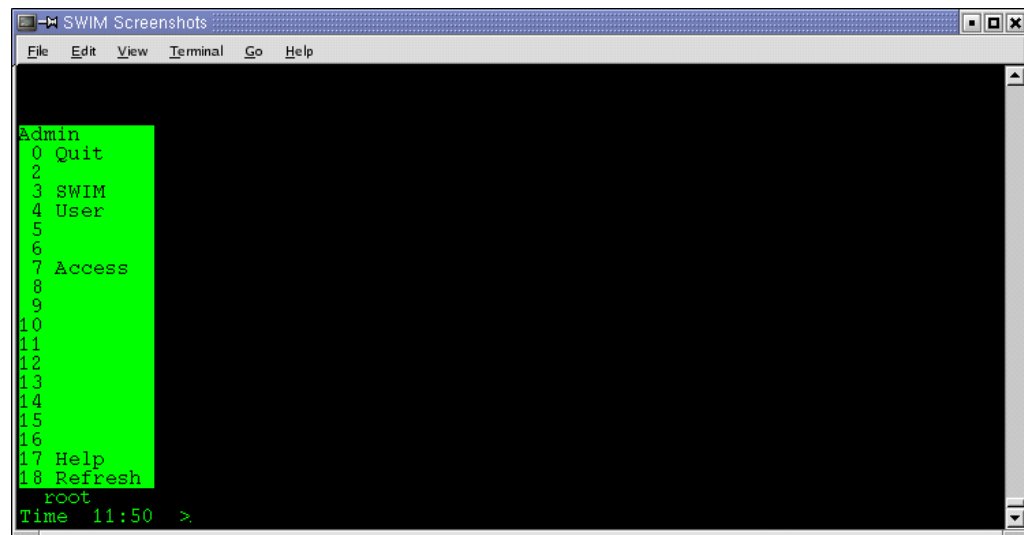
cbm_setup was designed to minimize user interaction prompts which adds business value by preventing user error and reducing labour and training costs.

CBM Upgrades were not completed as part of this activity.

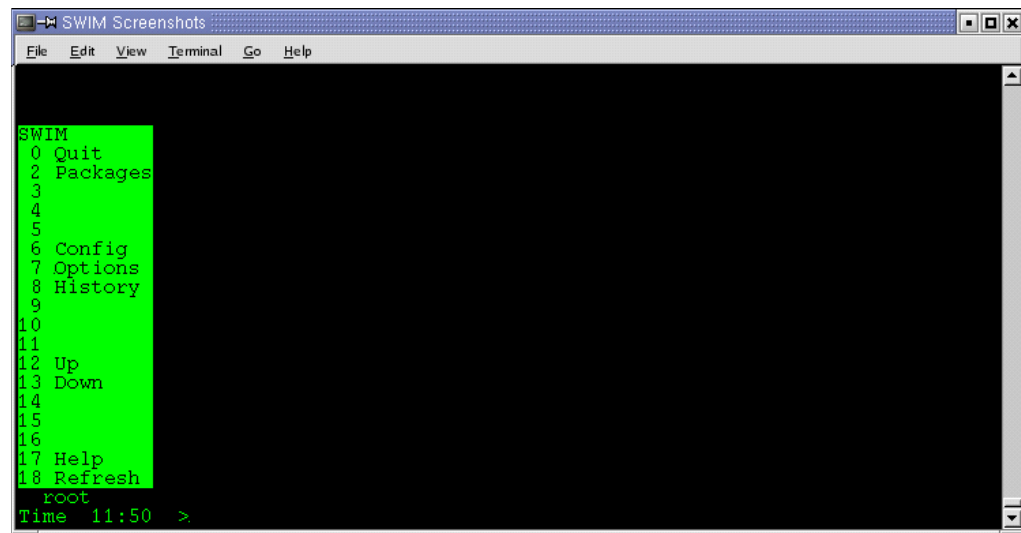
Software management:

Value-added applications are installed via the SWIM level of the cbmmtce interface. Applications can be installed or removed at any time after initial installation. Applications must only be installed from the active node cbmmtce interface. This interface provides business value by providing a common interface across products for package removal and installation.

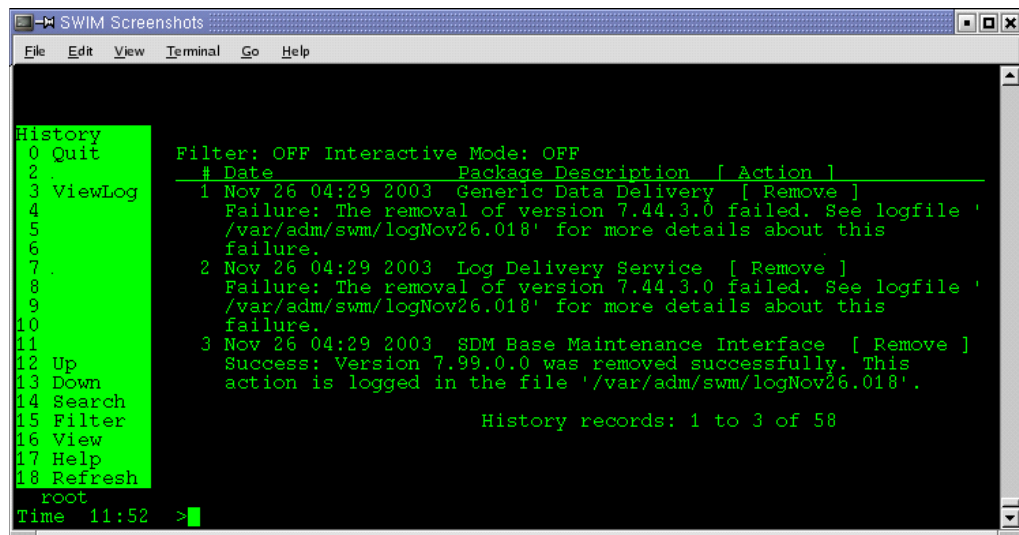
The SWIM level is accessible directly by typing SWIM and then enter in the cbmmtce interface, or through the admin level of the cbmmtce interface as detailed in the following graphic:



The options provided by the SWIM level are shown in the following graphic:



The SWIM -> History level provides a transaction history of packages that were applied using SWIM. These logs are maintained on the system and rotated every week or as disk space requires them to be rotated.



```

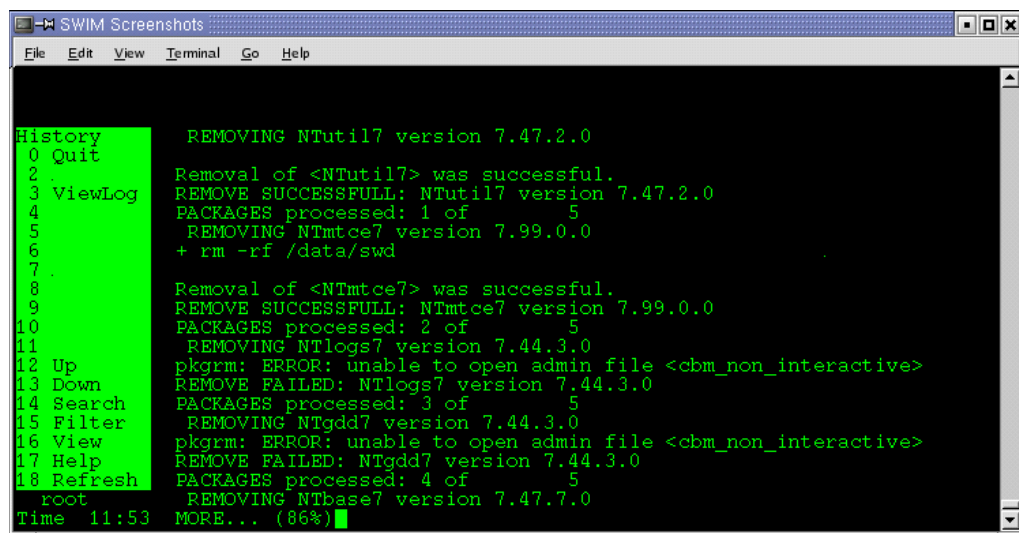
History
0 Quit
2
3 ViewLog
4
5
6
7
8
9
10
11
12 Up
13 Down
14 Search
15 Filter
16 View
17 Help
18 Refresh
root
Time 11:52 >

Filter: OFF Interactive Mode: OFF
# Date Package Description [ Action ]
1 Nov 26 04:29 2003 Generic Data Delivery [ Remove ]
Failure: The removal of version 7.44.3.0 failed. See logfile '
/var/adm/swm/logNov26.018' for more details about this
failure.
2 Nov 26 04:29 2003 Log Delivery Service [ Remove ]
Failure: The removal of version 7.44.3.0 failed. See logfile '
/var/adm/swm/logNov26.018' for more details about this
failure.
3 Nov 26 04:29 2003 SDM Base Maintenance Interface [ Remove ]
Success: Version 7.99.0.0 was removed successfully. This
action is logged in the file '/var/adm/swm/logNov26.018'.

History records: 1 to 3 of 58

```

The SWIM -> History -> ViewLog level can be used to view the details from the application of a package using SWIM.



```

History
0 Quit
2
3 ViewLog
4
5
6
7
8
9
10
11
12 Up
13 Down
14 Search
15 Filter
16 View
17 Help
18 Refresh
root
Time 11:53 >

REMOVING NTutil7 version 7.47.2.0
Removal of <NTutil7> was successful.
REMOVE SUCCESSFULL: NTutil7 version 7.47.2.0
PACKAGES processed: 1 of 5
REMOVING NTmtce7 version 7.99.0.0
+ rm -rf /data/swd
Removal of <NTmtce7> was successful.
REMOVE SUCCESSFULL: NTmtce7 version 7.99.0.0
PACKAGES processed: 2 of 5
REMOVING NTlogs7 version 7.44.3.0
pkgrm: ERROR: unable to open admin file <cbm_non_interactive>
REMOVE FAILED: NTlogs7 version 7.44.3.0
PACKAGES processed: 3 of 5
REMOVING NTgdd7 version 7.44.3.0
pkgrm: ERROR: unable to open admin file <cbm_non_interactive>
REMOVE FAILED: NTgdd7 version 7.44.3.0
PACKAGES processed: 4 of 5
REMOVING NTbase7 version 7.47.7.0
MORE... (86%)

```

The SWIM -> Packages level shows software that is installed. The SWIM -> Packages -> Apply level should be used to apply software. It will provide a listing of available software Packages in a specified or default directory. The default directory is /swd/.

```

SWIM Screenshots
File Edit View Terminal Go Help

Packages
0 Quit
2 Apply
3
4
5
6
7 Select
8 Remove
9
10
11
12 Up
13 Down
14 Search
15 Filter
16 View
17 Help
18 Refresh
root
Time 11:50 >

Filter: sdm Interactive Mode: OFF
# Package Description Version Status
1 RogueWave SourcePro Libraries 4.0.0.0 APPLIED
2 SDM Base Maintenance Interface 7.47.7.0 APPLIED
3 Platform Base 7.47.7.0 APPLIED
4 GNU Compiler and Libraries 3.3.0.0 APPLIED
Packages: 1 to 4 of 4

```

SWIM -> Packages, with an installed package selected

```

SWIM Screenshots
File Edit View Terminal Go Help

Packages
0 Quit
2 Apply
3
4
5
6
7 Select
8 Remove
9
10
11
12 Up
13 Down
14 Search
15 Filter
16 View
17 Help
18 Refresh
root
Time 11:51 >

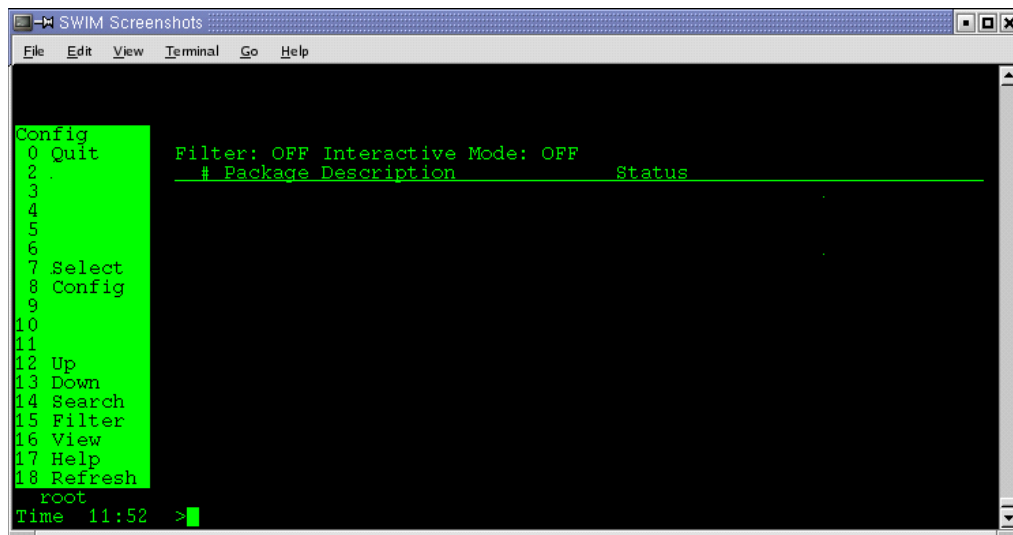
Filter: sdm Interactive Mode: OFF
# Package Description Version # Selected: 1 Status
1 RogueWave SourcePro Libraries 4.0.0.0 APPLIED
2 SDM Base Maintenance Interface 7.47.7.0 APPLIED
3 Platform Base 7.47.7.0 APPLIED
4 GNU Compiler and Libraries 3.3.0.0 APPLIED
Packages: 1 to 4 of 4

```

Application configuration:

Applications that require manual configuration will be configured via a command line interface initiated from the cbmmtee interface's config level. This provides business value as the interface and approach are the same across products preventing re-learning to reduce training costs and user error.

The following graphic depicts the config level:



Applications not requiring manual configuration will automatically be configured during installation or as they are brought into service depending on the scenario. The process of configuring these applications will be transparent to the system user.

Applications requiring manual configuration can be configured in two ways:

1) During installation, SWIM will notice the application requires manual configuration and at the end of the installation it will automatically prompt the user for the configuration steps and information.

Multiple installations requiring configuration will be batch queued such that the manual configuration steps are all executed at the end of the software installation cycle.

2) Should the user decide not to configure the application at installation time. They can configure, or reconfigure the application from the config level of the cbmmtce interface.

Patching:

A suite of tools to control patching are built into the SSPFS product. The tools are available to any products built on top of the SSPFS product, including the CBM product.

The patching suite tools create business value by reducing patching & support costs. They provide simple and product generic user interfaces to apply and remove patches as well as query and audit software.

Corrective content will be made available to the customers as individual patches. These will be provided in Solaris patch format contained within a tar and gzipped archive. The patching tools automatically handle processing and applying the patches.

New for the CBM is a mechanism to guarantee the integrity of patches as they are received. The checksum delivered with the patch is used to verify the integrity of the patch archive. Any patch that is damaged in any way on its way to the CBM will be rejected as damaged. The customer will be informed of any such rejection.

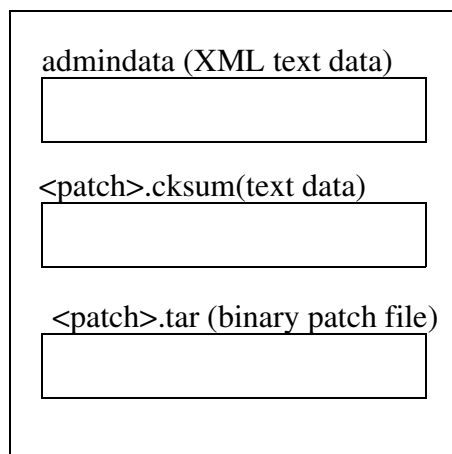
Patches will be compressed and transported as a single file. The compression adds value by reducing disk space requirements and ESD transfer times for patches.

The patch archive will contain checksum data to verify the patches integrity. Should the patch file become corrupt in any way, the system will be able to detect, avoid applying, and alarm the corrupt patch.

An administrative file is provided with all patches to provide status information, release notes for the patch, and handling instructions for the patching tools.

The following diagram denotes the structure of patches provided by Nortel:

<PATCHNAME>.patch (tar & gzipped archive)



Patches are designated as one of three types: active node apply, inactive node apply, and manual apply. The patch type is used to trigger the appropriate handling of the patch while being applied in highly available cluster configuration. For single node configurations, inactive apply patches automatically become manual apply patches.

Both active node apply and inactive node apply patches can be applied automatically by setting a schedule with the patchconfig tool. There are separate schedules for each. Manual patches are never automatically applied, and cannot be scheduled. For non-clustered systems, the inactive apply schedule does not exist as patches are either active apply or manual apply.

Patches have an attribute embedded within them to determine whether they require a system reboot to be applied. If they require a reboot, the patching suite software will initiate the reboot. Depending on the scenario triggered by the patch type, the reboot may be handled either automatically, or manually with user prompts.

Patches applied on the active node will only affect service for specific applications modified or updated by the patch. Patches applied on the inactive side will not be enabled until after a SWACT (which involves a loss of service for all applications). However, applying the patch on the inactive side allows a continuation of service on the active side while the patch is being applied on the inactive.

Patches are only applied to the mate node once the patch has successfully been applied to the first node. Patches that fail to apply successfully will be automatically removed and an alarm will notify the user of the unsuccessful apply attempt.

Patch Handling	Applied Automatically	Can be scheduled	Node applied on	Description
Active Apply	Yes	Yes	Active	This handling is ideal for non disruptive or patches for less sensitive applications.
Inactive Apply	Yes	Yes	Inactive	This handling is ideal for disruptive or sensitive application patches.
Manual Apply	No	No – manually initiated	Inactive node with prompts	This handling is ideal for disruptive patches, patches that require manual interaction, or highly sensitive applications.

Additional Patch Attributes:

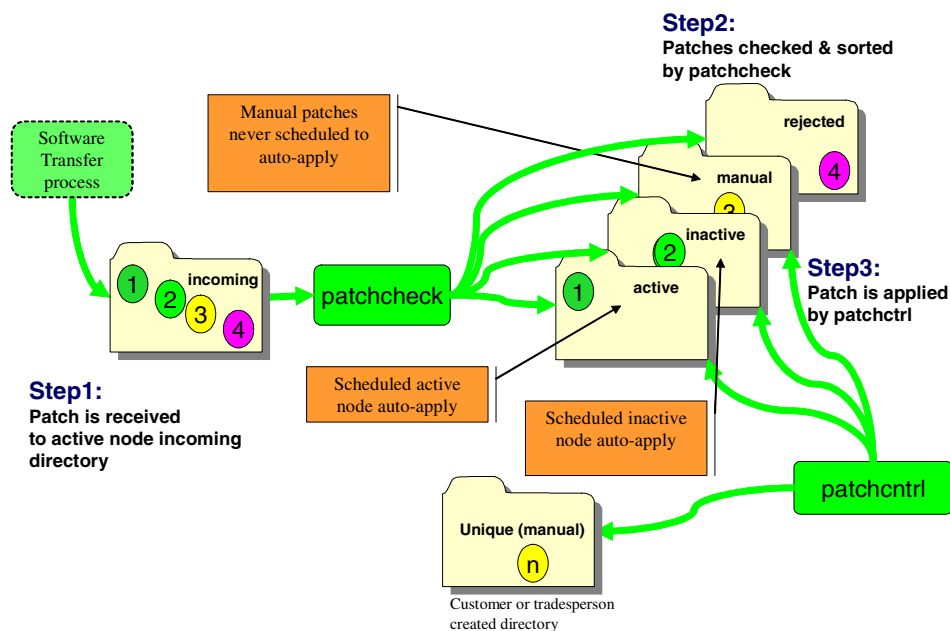
Reboot required: Yes/No

Patch Status: S/V/R/Z

RPS States:
Submitted
Verification
Released
Zapped

These attributes trigger special handling. VO patches = manual apply.

The following diagram details how patches will be received in the incoming directory and processed by patchcheck to be sorted into directories according to required apply handling: Multiple patches will be applied in sequence.



Also new for the CBM is the capability to override embedded patching handling with a more cautious handling procedure. This feature is enabled by setting patch filters. Patch filters allow declaration of patches matching criteria to be always inactive apply, or always manual apply. The filters are set, updated, or removed using the patchfilter command. The filtering mechanism is based on the filter pattern matching the patch name, or the name of the package the patch updates, or the category of the patch.

Patch filters always add more conservative handling to patches. For example, making an active apply application such as Billing a strictly manual apply application. Patches requiring special handling cannot be filtered to remove that special handling. For example, a manual patch cannot be filtered to make it active apply.

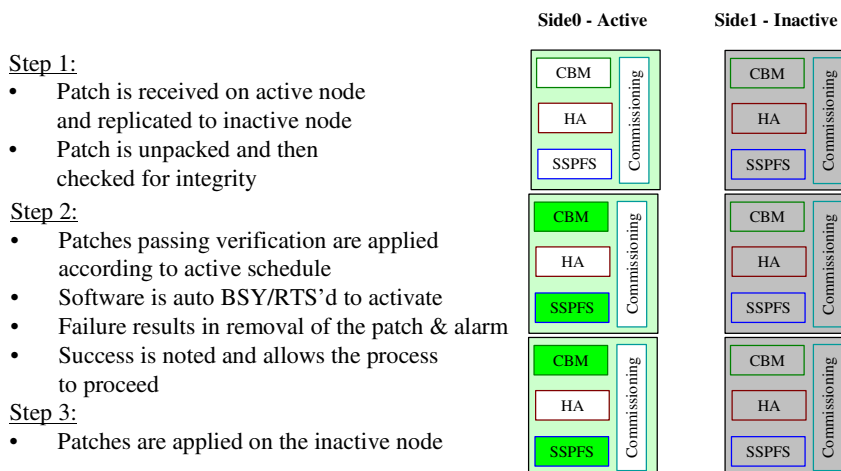
A status field is embedded within the patch to track the deployment state of the patch. This state is referenced to determine the appropriate behavior for patch application. Verification (V) patches will be automatically classed as manual apply patches only. Release (R) status patches will follow their appropriate handling based on the patch type field, or any defined patch filters.

The configurable patch application schedules provide business value by allowing automatic patch application during less busy periods and reducing support costs as that would have been incurred if manual interaction was required.

The patch format used by the patching suite provides automatic patch application and automatic application restart once the patch has been applied (if required). CBM patches will restart applications automatically by default.

The patching tools provide high availability cluster support. This feature enables value by automatically handling sensitive or disruptive patches requiring reboots or restart of important applications. These patches are handled automatically by applying them on the inactive node of the cluster and then SWACT'ing. These inactive apply patches will be applied on the inactive node to minimize service disruption.

The following diagram depicts how active apply patches are handled:



The following diagram depicts how inactive apply patches will be handled:

Patching security & robustness features:Step 1:

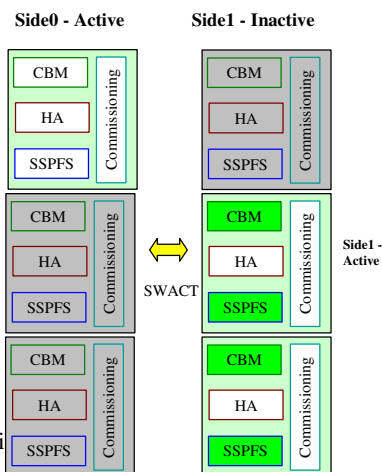
- Patch is received on active node and replicated to inactive node
- Patch is unpacked and then checked for integrity

Step 2:

- Patches passing verification are applied according to inactive schedule
- Failure results in removal of the patch & alarm
- SWACT and RTS is initiated to activate
- Success is noted and allows the process to proceed

Step 3:

- Patches are applied on the inactive (formerly active node)



The patching suite provides several important security features to enable a high level of security for customer networks.

The patching suite includes automatic integrity checking to screen and alarm corrupt patches & prevent their application. The patching suite supports encrypted file transfers & inter node communication.

The manual patch application type is supported to provide complete control over sensitive patches. Patch filters provide the ability to define more sensitive handling for defined applications to minimize service disruption

Important design considerations were factored to ensure a high level of robustness for the patching suite. No application level software required to apply patches. Patches are applied using low level operating system commands to ensure application of patches will not be blocked by a daemon or service being unavailable.

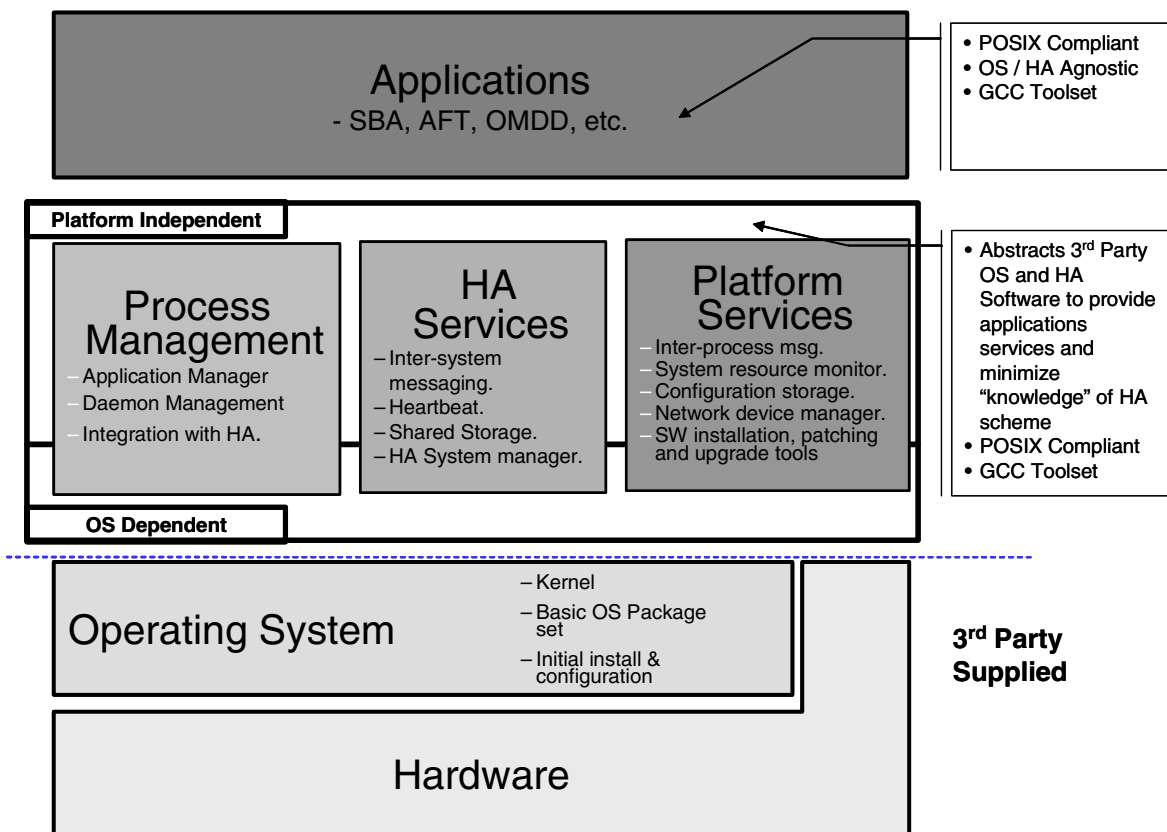
No special daemons required to support patching. For the automatic scheduling functions to work, the cron server must be functioning.

New for this release, the root password not required to control patching. Maintenance users (maint group, or emsadm group) will have access to run patchctrl. This enables them to apply patches without accessing the root password.

Please see the patching limitations section of this document for information regarding a possible security exploit.

Hardware and Software Requirements or Dependencies

The CBM product requires the Sun Microsystems N240 hardware platform that is provided by the SSPFS platform. The CBM product utilizes the Solaris operating system also provided by the SSPFS platform.



Dependencies for Patching include:

- Solaris patchadd and patchrm tools
- High available software
- Alarming facilities

Dependencies for Installation include:

- SSPFS installation script and commissioning interfaces
- Solaris pkgadd and pkgrm tools
- CDROM or ESD Image (ISO) of CDROM

- HA Cloning tool
- Alarming facilities
- Application registration interfaces
- Application set up automation

Upgrade preparation dependencies:

- HA Cloning tool
- Alarming facilities
- Application registration interfaces

Limitations and restrictions

General Limitations:

- There are differences between SDM's legacy patching processes and interfaces and the patching suite interfaces developed in A0002133. These differences are not likely to be accepted by customers creating a requirement to enhance the patching suite tools to understand and support SDM patching. The patching suite tools were designed with this goal in mind.

The following limitations are noted for the following components.

Patching limitations:

- Patches must be provided in Sun patch format
- Patch integrity checking requires a checksum to be include with the patch
- For the patch handling mechanisms (active apply, inactive apply, manual apply) to work, an amindata file containing information defining the intended handling must be included with the patch
- Solaris patches must follow a Solaris patch manager supported naming convention.
- Patches are cumulative until completion of a design activity to create incremental patching tools
- Patches must handle restart of dependent applications until a more sophisticated shared library & dependency handing tool is developed
- Z status patches will never be delivered, but are not automatically removed from products installed in the field.
- **Important:** Patches can not be verified to have originated from Nortel Networks without the development of a patch authenticity checking mechanism. Lack of this mechanism provides a significant security hole.

Installation limitations:

- Packages need to be supplied in Sun package format

Interactions**Installation Interactions:**

Installation of CBM core software is completed through using the `cbm_setup` interface. This tool will automatically install the CBM core (also known as “base”) software. The core software packages will be installed and their installation verified automatically without any prompts.

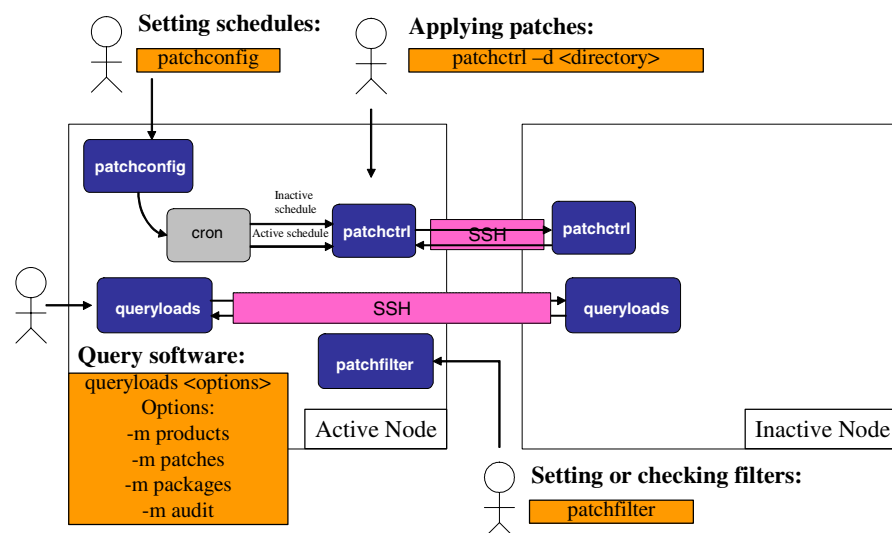
Value-added software such as Billing, OM Delivery, and other applications that are sold separately from the code platform software can be installed at any time after the initial installation using the SWIM interface. For two node cluster configurations, the SWIM interface will automatically install the software packages selected onto both nodes.

Upgrade Interactions:

The planned interface for CBM upgrades will be `cbm_setup`. This work will be completed in a new activity.

Patching Interactions:

There are 4 interfaces for patching. They are depicted in the following graphic:



1) patchconfig

The patchconfig tool is used to set, or reset the patching schedules.

The user will be prompted for two schedules, one for the active apply schedule and one for the inactive apply schedule. These schedules will be used to trigger application of patches for the respective node and patch handling type.

<TODO: Add screen capture for patchconfig>

2) patchctrl

The patchctrl tool provides a single interface for patch application. It automatically handles active patch apply, inactive patch apply, or manual apply scenarios. If patches require a reboot, it will automatically initiate the reboot or prompt when patching manually.

patchctrl will automatically handle triggering a SWACT for patches that require it when the system is a two node cluster. During manual patch application, a SWACT will be preceded by a prompt.

3) queryloads

queryloads provides an easy to use interface to gather software information about the system. queryloads reports information in one of two formats, a human friendly report, or raw XML data.

queryloads reports information on the Nortel products installed on the system, the software packages installed, and the software patches installed. If provided with a product name, queryloads will automatically filter output to report information for that product rather than all software installed on the system.

4) patchfilter

patchfilter provides an interface to set or remove filter instructions. Patch filters allow customers to define more conservative handling for patches. This enables making patches for designated applications either inactive or manual apply even though the patch itself may be an active apply patch. Filters only allow more conservative handling. For example, a manual patch could not be made an active apply patch.

5) Alarms

A minor alarm (Istb) will be raised on the node when a patch has failed to apply. A command line tool will be provided to manually clear this alarm.

A minor alarm (Istb) will be raised and automatically cleared on the node when a patch fails the integrity check

Applicable customer facing sections

Fault Management

Logs

___X___

Alarms	___X___
Configuration	
Data Schema	___X___
User Interface	___X___
Element Management	___X___
Security	___X___
Service Order	___NA___
Office Parameters	___NA___
Accounting (includes AMA billing)	___NA___
Performance (includes operational measurements)	___NA___
Realtime	___NA___
Engineering Information	___NA___

Glossary

Term	Description
CBM	The Nortel Networks Core and Billing Manager product.
SDM	The Nortel Networks SuperNode Data Manager product.
NPM	Network Patch Manager
Patch	An atomic unit for delivering changes to deployed products. Patches may contain files, directories, and links to affect changes on the system.
SSPFS	Nortel's Succession platform based on the Solaris operating system.
SWACT	SWitch of ACTivity from the active cluster node to have the inactive cluster node take over.
cron	The UNIX cron daemon, a facility for scheduling execution of commands.
Value added software	Software that provides additional capability beyond the core product. (and costs extra)

Product = CS 2000

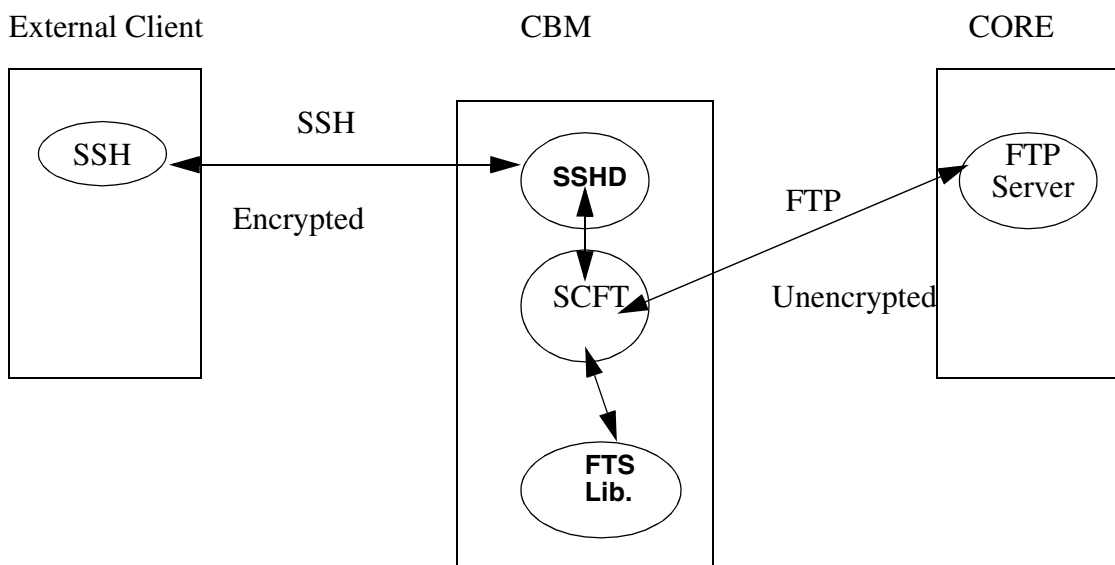
A00002155 -- SSH Core File Transfer (SCFT) for CBM and SDM (Succession on DMS)

Description

This feature is intended to provide a non-DCE option for secure FTP that will allow secure FTP access to the CORE. through the CBM or SDM. The feature can be used to retrieve files from the core and transfer files to the core from an external workstation through the CBM or SDM. The feature provides the security supplied by the SSH (version 2) so that the core will not be compromised by illegal users. The SCTP code that runs on the CBM or SDM provides much of the standard FTP functionality, enabling the remote client to perform all the FTP operation that may be needed to maintain the CORE through the CBM or SDM.

This feature provides the dynamic creation of the CM FTP users. This is accomplished by the SSH core file transfer authorizing the user executing the command based on their group memberships.

SSH Core File Transfer



Hardware Requirements or Dependencies

This feature will run both on the CBM platform as well as the SDM.

Software Requirements or Dependencies

The external client must have standard SSH (version 2) running on his machine. He must also have the SCFT code running on the CBM or SDM. It would also be useful but not necessary to have the Korn shell script created by Nortel for running the SCFT code through SSH loaded on the external client's machine. The SCFT code as well as the Korn Shell script will be delivered to the client as a packaged SDM/CBM load.

Handling SSH authorized_keys file over SWACTs.

If you are using a CBM-850 system that has two CBM clustered together, special care must be taken that the SSH authorized_keys file are kept current on both sides. This is particularly important if you do a swact as you may no longer be able to connect password free if the authorized_keys file is different. The authorized_keys file can be copied over to the cbm on the other side by using the syncFile.ksh command.

```
> /opt/servman/shell/syncFile.ksh /.ssh/authorized_keys
```

Limitations and restrictions

Only a restricted subset of FTP commands are supported with the SSH Core File Transfer. However, it should be noted that one of the commands supported is the "command" feature which allows any FTP command to be entered as a string that will be performed on the FTP server on the core. With this command virtually any FTP command can be entered.

Core image files can not be transferred from an outside client at this time. There is code within the Core that prohibits this.

It should also be noted that all commands must fit onto one line and must be passed to the SCFT code intact. This is necessary because the FTP connection to the core is created and removed after each command. So you can not, for instance, set the output type to Binary in one command then do a put in the next and expect the type to be binary. The binary command will not be remembered for the put and the type will default back to the standard FTP type of ASCII.

Interactions

This feature will use the previously existing FTS code to perform the FTP commands that are requested through the SSH Core File Transfer code. Some changes have been made to allow the output to be returned to the external client. The external client will also be required to have a standard SSH installed on their system.

Applicable customer facing sections

Fault Management

Logs

__X__

Alarms	__N/A__
Configuration	
Data Schema	__N/A__
User Interface	__X__
Element Management	__N/A__
Security	__X__
Service Order	__N/A__
Office Parameters	__N/A__
Accounting (includes AMA billing)	__N/A__
Performance (includes operational measurements)	__N/A__

Glossary

Term	Description
AIX	IBM UNIX operating system on the SDM FX
CBM	Core Billing Manager
CM	Command Module (the CPU of the DMS)
CMFT	Command Module File Transfer Script
AIX	IBM UNIX operating system on the SDM FX
CBM	Core and Billing Manager
Core	DMS switch computing engine
DCE	Distributed Computer Environment
FTP	File transfer protocol
FTS	File transfer System (Nortel proprietary code)
IP	Internet Protocol
SCFT	SSH Core File Transfer
SDM	SuperNode Data Manager
SSH	Secure Shell protocol
SSHD	Secure Shell protocol Daemon

Product = CS 2000

A00002186 -- IOM DDU Capacity Enhancement (Succession on DMS)

Introduction

In 1999, Nortel committed to Netas to deliver sufficient storage for their switches for 25M billing records.

The feature patch was implemented for SN04/CSP17, and this is the source implementation of the enhanced functionality. The FN for the original feature patch can be found in FMDOC library as TURKPFN.

The IOM DDU disk capacity is currently limited to 1G. This feature provides increase in the capacity to 4G by utilizing the additional capacity supported by the new IOM load, IOMEXXXX.

Functional Overview

This feature increases the IOM DDU capacity from 1G to 4G. The maximum number of volumes per DDU increases from 32 to 63. The maximum volume size remains unchanged at 65,536 KBytes. By allocating 63 volumes at maximum volume size, the entire 4G can be used.

There are no HMI changes introduced in this feature. All the maintenance tools, such as DISKDBG, DSKALLOC, and DSKUT will continue to function with no visible changes to their interface.

Soc BASE0015

The ability to use the additional disk capacity is controlled by SOC BASE0015. The status of this SOC must be set to YES before the additional capacity is visible. If the status is set to IDLE after additional volumes have been allocated, further volume allocation maintenance may not be possible, however all volumes and files will continue to be accessible.

Hardware Requirements or Dependencies

- The capacity enhancement is applicable only to the IOM DDU
- The IOM disk drive, NTFX32BA must be Release 7 or later

Software Requirements or Dependencies

- SOC BASE0015 needs to be activated for this functionality.
- The IOM load with version IOMEXXXX must be used in conjunction with this feature

Limitations and restrictions

- Once the IOM has been upgraded to the new load, do not revert back to the old load, as this may cause the DDU to no longer function correctly and potentially require the disk to be reformatted.
- The IOM disk drive, NTFX32BA must be Release 7 or later.
- Setting the SOC BASE0015 to IDLE may prevent further volume allocation maintenance, however the volumes which have already been allocated will continue to be accessible.

Interactions

None

Applicable customer facing sections

Fault Management

Logs	_N/A_
Alarms	_N/A_

Configuration

Data Schema	_N/A_
User Interface	_N/A_
Element Management	_N/A_
Security	_N/A_
Service Order	_N/A_
Office Parameters	_N/A_

Accounting (includes AMA billing) _N/A_

Performance (includes operational measurements) _N/A_

Glossary

DDU	Disk Drive Unit
DIRP	Device Independent Recording Package
HMI	Human Machine Interface
IOM	Input/Output Module
MOP	Method of Procedure

Product = CS 2000

A00002196 -- Do Not Disturb - Residential Market (Succession on DMS)

Functional Description

Do Not Disturb (DND) is an existing DMS feature that makes an MDC station appear busy to incoming calls when the station is idle. DND is scheduled via table DNDSCHED and allows pre-programmed times to be datafilled which specify a begin time to activate DND and an end time to deactivate it. DND is not currently supported on RES lines but will be as a result of this activity.

Selective Call Acceptance (SCA) feature allows a subscriber to selectively accept calls arriving from a limited set of previously identified directory numbers.

There is currently no mechanism to allow a subscriber to create a list of callers that would by-pass DND when it is active. This activity will change the current interaction between SCA and DND so that a subscriber can selectively accept calls while DND is active.

Enhanced Do Not Disturb

Currently there is no combination of features that allows a subscriber to activate a Do Not Disturb feature at a predetermined time each day, for example from 6 p.m. until 7 p.m. each evening (dinner hour), and at the same time maintain a list of DNs that are optionally allowed to bypass DND when it is active.

The Enhanced DND feature will be available to RES & MDC lines and provides the following capabilities:

- Via Table DNDSCHED, calls can be blocked at a predetermined time period each day. Table DNDSCHED allows up to 63 different time periods to be datafilled per customer group.
- A subscriber can dial DND feature access codes to activate or deactivate Do Not Disturb. The DNDACT feature access code will activate Do Not Disturb and the DNDDEACT feature access code will deactivate Do Not Disturb.
- Table DNDSCHED begin and end times will interact with DNDACT and DNDDEACT feature access codes. If a subscriber's line has Do Not Disturb active as a result of a begin time in table DNDSCHED, the subscriber can dial the DNDDEACT feature access code to deactivate DND. Likewise, an end-time deactivation of DND via Table DNDSCHED will turn off Do Not Disturb, whether it was activated via the DND feature access code or a begin time in table DNDSCHED.

- SCA will be enhanced to allow callers on the SCA screening list to bypass DND when it is active. This functionality will be controlled by the new parameter DND_ONLY, which will be visible when provisioning SCA.
- The new field DND_ONLY will default to N during provisioning and is visible during NEW, ADO (Add Option), and CHF (Change Feature) commands.
- Enhanced DND is defined as a line with both the DND and SCA options with SCA field DND_ONLY = Y.
- When Enhanced DND is active (DND and SCA with DND_ONLY=Y are both active), callers not on the SCA screening list will be routed to SCA treatment while callers on the SCA screening list will bypass DND and terminate to the line.
- If DND is active and SCA with DND_ONLY=Y is inactive, then all callers receive DND treatment as defined by Tables DNDSCHED and IBNTREAT.
- If DND is inactive and SCA is active (DND_ONLY=Y) then SCA screening will not be attempted on any termination. With DND_ONLY = Y, SCA screening is only done when DND is active. Under this condition, no SCA OMs will be pegged.
- Enhanced Do Not Disturb will be controlled by SOC RES00102.

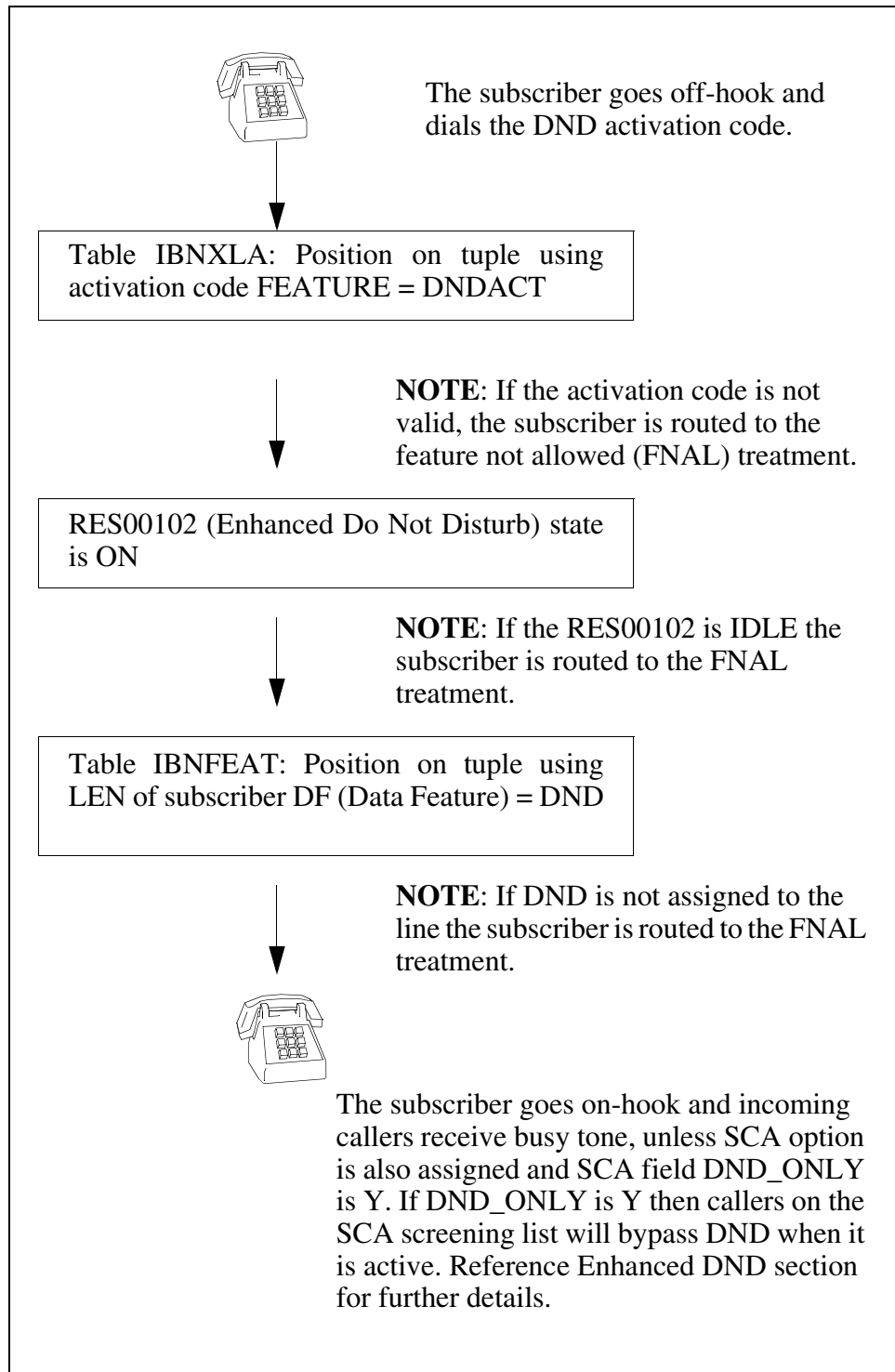
New Activation Code for Table IBNXLA

Current implementation of DND does not allow a MDC or RES line to mark its DN busy by dialing an access code that interworks with scheduled Do Not Disturb times. This will be changed by this activity so that an access code can be datafilled in Table IBNXLA that MDC or RES lines can dial to activate and deactivate DND and that interworks with Table DNDSCHED.

If DND is active on a line as a result of a begin time in table DNDSCHED it is currently not possible to deactivate it by dialling an access code. This activity will enhance DND so a Table DNDSCHED activation of DND can be deactivated by MDC and RES lines by dialling the DND deactivation access code.

The DND Activation and Deactivation access codes will be available when the TRSEL (TRanslation SElector) is set to FEAT in Table IBNXLA. The new Features added are DNDACT (DND Activate) and DNDDEACT (DND Deactivate).

A Table DNDSCHED activation of DND will create an entry in Table DNDMSB with STATUS set to DNDGA. DNDACT and DNDDEACT will interwork with Table DNDSCHED, therefore a subscriber who dials DNDACT to activate DND will also create an entry in Table DNDMSB of DNDGA.

DND Activation

Refer to the configuration section (section optcn) for further details.

Selective Call Acceptance

Background

Currently, the SCA feature allows a subscriber to selectively accept calls arriving from a limited set of previously identified directory numbers.

In its current implementation SCA will not override DND when DND is active. If DND and SCA are active on a subscriber's line, callers on the SCA list will not terminate but will receive busy treatment due to DND. With this activity the interaction between DND & SCA will be modified when the new field DND_ONLY is Y so that callers on the SCA list can bypass DND when DND is active. If DND_ONLY is N then existing behavior remains unchanged.

Enhancement

The SCA enhancement being provided by this activity will change the conditions under which SCA screening can be applied so that SCA screening is only considered if DND is active. This functionality will be provided by a new field DND_ONLY (Y/N) that will be included at SCA servord provisioning. Current SCA subscribers will have the new field DND_ONLY initialized to FALSE over an ONP to preserve existing functionality. Refer to the configuration section (section optcn) for further details.

When DND is active and SCA is active with the DND_ONLY field set to Y on a subscriber's line then only callers on the SCA list will be allowed to terminate to the line. All callers not on the SCA list will be routed to SCA treatment.

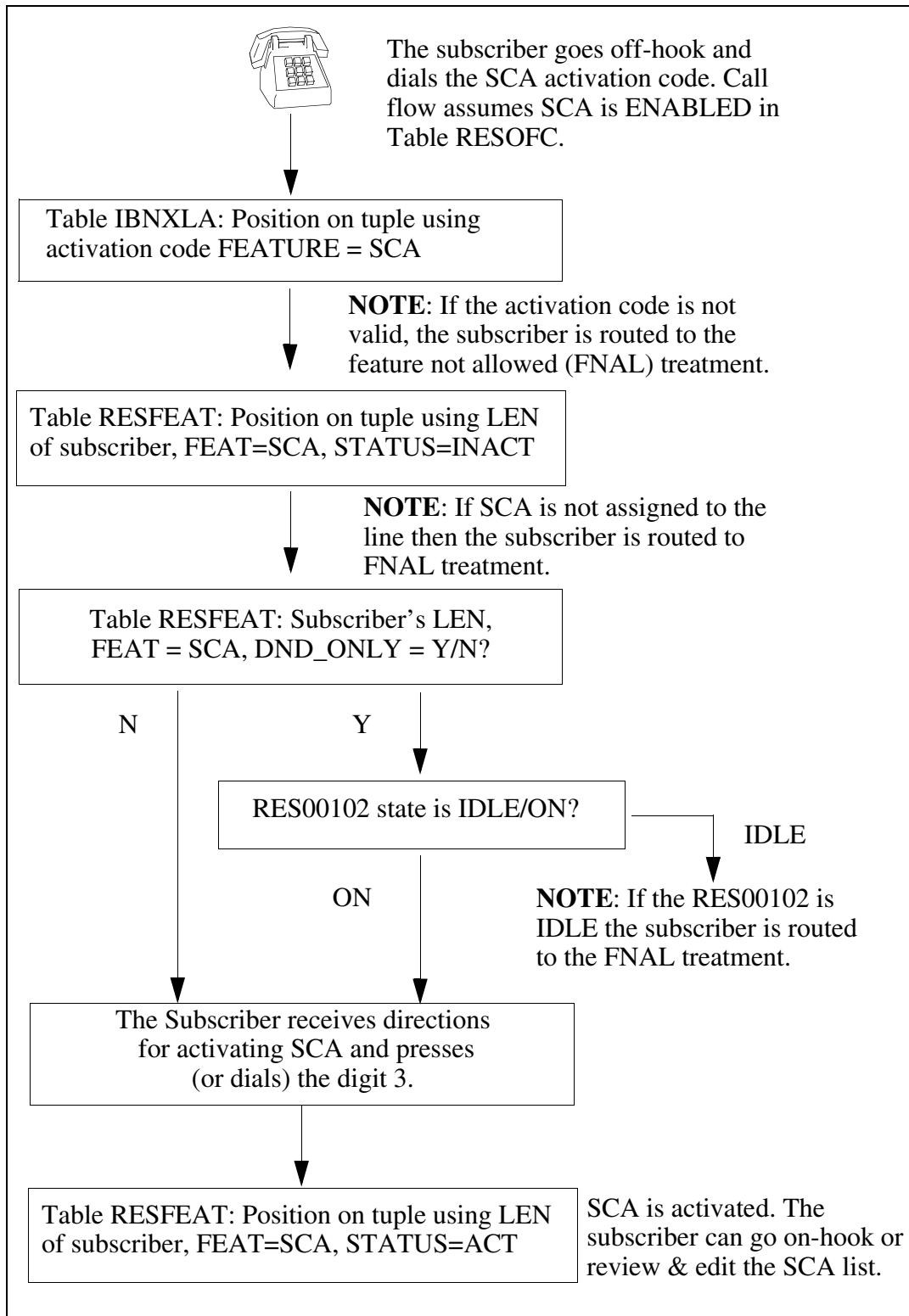
If DND is not active and the SCA field DND_ONLY is set to Y, then SCA screening will not apply to any incoming calls and all callers terminate to the line. The purpose of SCA screening when DND_ONLY is set to Y is to allow a list of callers to bypass the Do Not Disturb feature. If DND is not active then the SCA screening list will not apply to any incoming calls.

If DND_ONLY bool is set to N then the SCA feature (when ACTIVE) will screen callers to the subscriber's line regardless of whether DND is active or not. This preserves existing functionality.

An SCA subscriber with DND_ONLY set to Y can only dial the SCA access code when RES00102 is ON. If RES00102 is IDLE, then the SCA subscriber with DND_ONLY set to Y will receive FNAL (Feature Not Allowed) treatment if the SCA access code is dialed.

The following figure shows the SCA activation call flow:

SCA Activation



Description of Enhanced DND

The following paragraphs and figures show table datafill, servord and a description of call scenarios for Enhanced DND.

Prior to datafilling Table DNDSCHED, Table CUSTSTN should be datafilled to indicate the number of DND groups supported for the customer group. In the example shown, “63” represents the number of Do Not Disturb groups supported by the customer group. Its range is from 1 to 63.

Example datafill for Table CUSTSTN

TABLE: CUSTSTN

<u>CUSTNAME</u>	<u>OPTNAME</u>	<u>OPTION</u>
RESGRP	DND	DND 63

The following figure shows example datafill for Table DNDSCHED.

Example datafill for Table DNDSCHED

TABLE: DNDSCHED

<u>DNDSCKEY</u>	<u>DIVERSN</u>	<u>SCHED</u>
RESGRP 1	1	\$
RESGRP 2	1	(18 0 19 0)\$

Using the above datafill as an example, if a RES subscriber who resides in the RESGRP customer group is assigned the DND option and DNDGRP is set to 2, then DND will be active each evening from 6 p.m. until 7 p.m. for this line. If DND is active and the call will not complete due to SCA overriding DND (SCA with DND_ONLY = Y), then the caller will be diverted to IBN treatment number 1 as defined by the DIVERSN field.

The following figure shows an example datafill for Table IBNTREAT. The DIVERSN field in Table DNDSCHED should be datafilled in Table IBNTREAT so callers who receive DND treatment are routed appropriately.

Example datafill for Table IBNTREAT

TABLE: IBNTREAT

<u>CUSTGRP</u>	<u>IBNTRTMT</u>	<u>ITDATA</u>
RESGRP	1	Y TRMT BUSY

NOTE: A default tuple should be datafilled in Table IBNTREAT with IBNTRTMT set to 0. This should be done for each customer group. An IBNTRTMT of 0 is used as the default treatment for any line with DND that does not have a corresponding entry in Table DNDSCHED to derive a diversion. An example for the RESGRP customer group is shown in the following figure.

Example datafill for Table IBNTREAT

TABLE: IBNTREAT		
<u>CUSTGRP</u>	<u>IBNTRTMT</u>	<u>ITDATA</u>
RESGRP	0	Y TRMT BUSY

Referring to Please refer to “ Example datafill for Table DNDSCHED” on page 381. and Please refer to “ Example datafill for Table IBNTREAT” on page 381., a caller who calls a DND active RESGRP 2 line would be routed to BUSY treatment, provided SCA with DND_ONLY=Y was not active and either allowed the termination or routed the call to SCA treatment.

Example DND ADO with DNDGRP assigned as RESGRP 2

```

ADO $ 6210040
OPTION:
>DND
DNDGRP:
>2

```

If a subscriber in the RESGRP customer group does not want DND to become active at a preset time each day, then they can be assigned to RESGRP 1. This is done by assigning the RESGRP subscriber to DNDGRP 1 at servord time.

Example DND ADO with DNDGRP assigned as RESGRP 1

```

ADO $ 6210042
OPTION:
>DND
DNDGRP:
>1

```

The following ADO example assigns SCA with DND_ONLY set to Y

Example SCA ADO with DND_ONLY = Y

```
ADO $ 6210040
OPTION:
>SCA
BILLING_OPTION: NOAMA
>
STATUS:
>ACT
DNS:
>6136213500
VBCOUNT:
>7
DNS:
>$
DND_ONLY: N
>Y
```

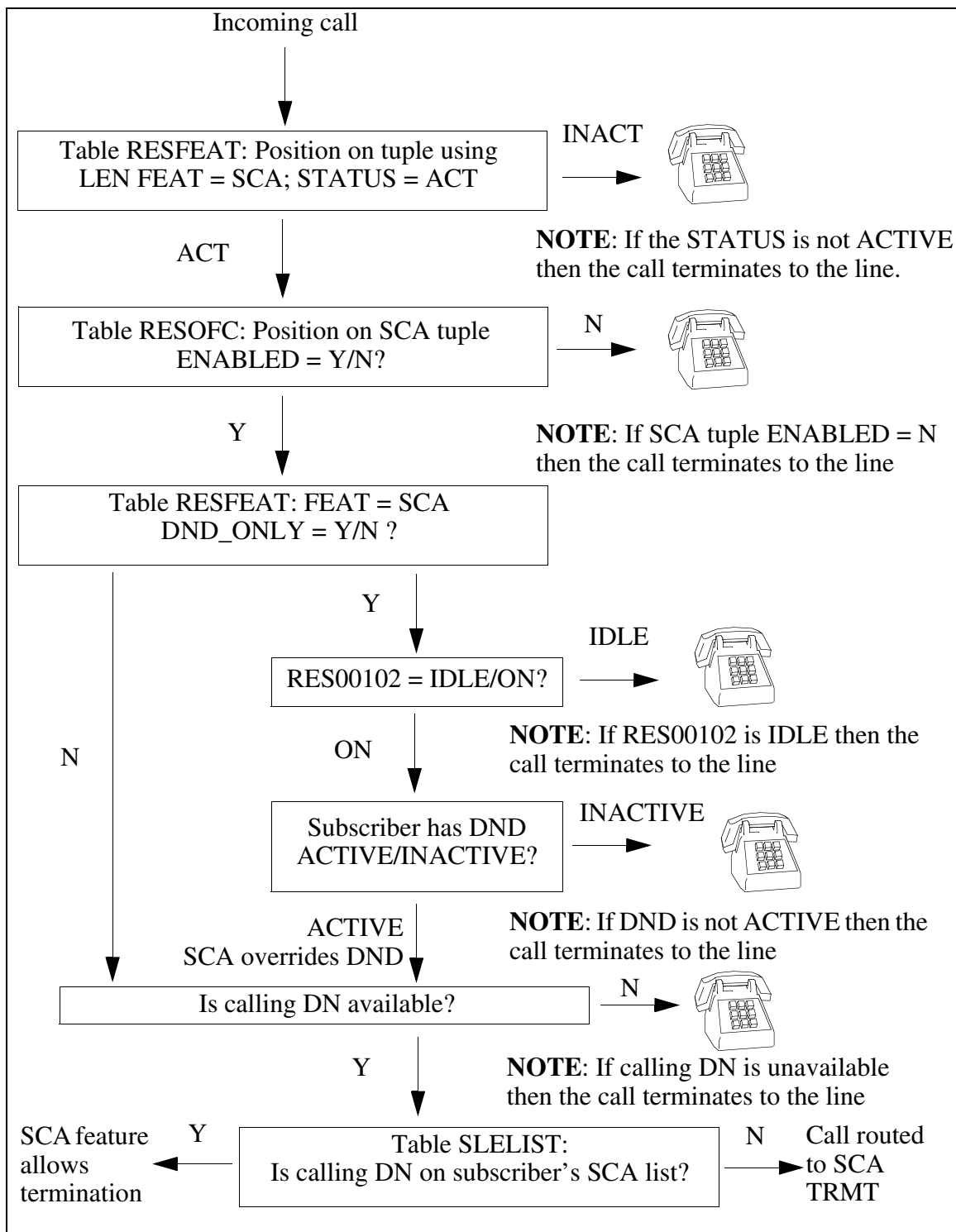
As described in the section 2.2.2, if DND is active on a subscriber's line and it also has subscribed to SCA with DND_ONLY set to "Y" and SCA is active, then callers on the SCA screening list will terminate to a line with DND active, whether DND was activated via Table DNDSCHED or by dialing the DNDACT (DND Activate) access code from Table IBNXLA.

If DND is assigned but not active on a line, and the line has SCA with DND_ONLY bool set to "Y" then SCA screening will not apply to any call termination attempt. Lines with SCA and the DND_Only bool set Y will only apply SCA screening when DND is active.

If the DND subscriber wishes to block all callers when DND is active, then the SCA feature enhancement can be turned off or not subscribed to, or DND_ONLY can be set to "N."

The following diagram shows the Enhanced DND call flow:

Enhanced DND Call Flow



Refer to TablePlease refer to “ DND & SCA (DND_ONLY = Y) Provisioned (RES00102 SOC=ON)” on page 387. for a description of DND & SCA interactions provided by this activity.

Refer to TablePlease refer to “ DND & SCA (DND_ONLY = Y) Provisioned (RES00102 SOC=IDLE)” on page 387. for a description of DND and SCA interactions as they existed prior to this activity. This functionality will be preserved by this activity by setting the SCA DND_ONLY bool to “N” at provisioning time.

No new OMs or billing records are created as a result of this activity. AMA record generation will be not be impacted by Enhanced DND functionality.

Software Optionality Control

Enhanced DND functionality provided by this activity will be under SOC control. The SOC code is RES00102. If SOC is ON then the functionality will be provided:

- MDC & RES subscribers can dial the DNDACT and DNDDEACT access codes.
- MDC & RES SCA subscribers with DND_ONLY set to Y can dial the SCA access code.
- MDC & RES subscribers with DND active and SCA active with DND_ONLY bool set to Y receive Enhanced DND functionality.

If SOC is IDLE then the enhancements just described will not be provided, although datafill will be allowed.

Refer to the Configuration section (optcn) for further details.

If RES00102 is IDLE and the SCA option is added to a line with DND_ONLY set to Y, then DND_ONLY functionality will not be provided. In this scenario a message will be output to the servord user stating that functionality will not be provided until RES00102 is turned ON. An example is provided below:

Assigning DND_ONLY = Y when RES00102 is IDLE

```
>ADO $ 7234500
OPTION:
>SCA
BILLING_OPTION: NOAMA
>
STATUS:
>ACT
DNS:
>$
DND_ONLY: N
>Y
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 3 10 9 PM 7234500 ( SCA NOAMA INACT $ Y ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>Y
DND_ONLY functionality requires RES00102 to be turned ON
```

QSL changes

Query Screening List (QSL) command will not change as a result of this activity, but the display for SCA out will be changed to reflect the status of the new field DND_ONLY. A new line titled “Do Not Disturb Only” will be displayed and will show the status of DND_ONLY field. Refer to the optcn section for details.

Hardware Requirements or Dependencies

None

Software Requirements or Dependencies

RES00035: Selective Call Acceptance

Limitations and restrictions

Enhanced DND is not available on a pay-per-use (PPU) basis.

Existing limitations and restrictions regarding DND will remain unchanged as a result of this activity.

Existing limitations and restrictions regarding SCA will remain unchanged as a result of this activity.

Interactions

With this activity there is a new interaction between DND and SCA. The following tables summarizes these interactions:

Note: Enhanced DND subscriber is defined as a subscriber with DND and SCA with DND_ONLY = Y assigned.

DND & SCA (DND_ONLY = Y) Provisioned (RES00102 SOC=ON)

IF DND_ONLY = Y	THEN
DND Inactive SCA Inactive	All callers terminate to the Enhanced DND subscriber
DND Inactive SCA Active	All callers terminate to the Enhanced DND subscriber
DND Active SCA Active	Callers on SCA List terminate to the Enhanced DND subscriber Callers not on SCA List receive SCA treatment
DND Active SCA Inactive	No callers terminate to the Enhanced DND subscriber

DND & SCA (DND_ONLY = Y) Provisioned (RES00102 SOC=IDLE)

IF DND_ONLY = Y	THEN
DND Inactive SCA Inactive	All callers terminate to the Enhanced DND subscriber
DND Inactive SCA Active	All callers terminate to the Enhanced DND subscriber
DND Active SCA Active	No callers terminate to the Enhanced DND subscriber
DND Active SCA Inactive	No callers terminate to the Enhanced DND subscriber

DND & SCA (DND_ONLY = N) Provisioned (RES00102 SOC=IDLE or SOC=ON)

IF DND_ONLY = N	THEN
DND Inactive SCA Inactive	All callers terminate to DND/SCA subscriber

DND & SCA (DND_ONLY = N) Provisioned (RES00102 SOC=IDLE or SOC=ON)

IF DND_ONLY = N	THEN
DND Inactive SCA Active	Callers on SCA List terminate to DND/SCA subscriber Callers not on SCA List receive SCA treatment
DND Active SCA Active	Callers on SCA List pass SCA screening but are denied termination by DND Callers not on SCA List receive SCA treatment
DND Active SCA Inactive	Callers denied termination by DND

Note: Inactive assumes that the option is assigned but inactive.

Applicable customer facing sections

Fault Management

Logs N/A

Alarms N/A

Configuration

Data Schema X

User Interface N/A

Element Management N/A

Security N/A

Service Order X

Office Parameters N/A

Accounting (includes AMA billing) N/A

Performance (includes operational measurements) N/A

Indicate with an X if you are completing the sections of the DDOC listed below. Indicate with "N/A" if these sections do not apply to this functionality.

Realtime N/A

Engineering Information N/A

Glossary

Term	Description
DND	Do Not Disturb
QSL	Query Screen List
SCA	Selective Call Acceptance

Configuration for A00002196

Hardware and Software Requirements

All hardware and software installation complete and all commissioning activities successful.

Initial Configuration

N/A

Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

Upgrade Impact

Dump and Restore

Lines with the SCA option appear in Table RESFEAT. During the ONP process SCA lines will be restored with the new field DND_ONLY set to its default value of “N.”

Lines with DND active as a result of dialing the DNDACT code in table IBNXLA will appear in Table DNDMSB with a status of DNDGA. This ensures that the DND status is preserved over an ONP.

Element Management Upgrade

N/A

Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

IBNXLA, RESFEAT

New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
IBNXLA	Changed	Unchanged
RESFEAT	Changed	Unchanged

Table Schema information

Name: IBNXLA

IBN Translation

Functional description

Table IBNXLA specifies data for the translation of digits. These digits originate from both an IBN station and a RES station.

Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

Current datafill order unchanged.

Size

Unchanged

Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
IBNXLA	Unchanged	Unchanged	Unchanged

Fields/OIDs

The following table lists fields for Table IBNXLA.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
Key	Unchanged	XLANAME	Vector up to 8 Chars	Translator Name
Key	Unchanged	DGLIDX	Vector up to 18 digits	Digilator Index

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
Result	Unchanged	TRSEL	FEAT	Translator Selector
Result	Unchanged	ACR	Y/N	Account Code Entry
Result	Unchanged	SMDR	Y/N	Station Message Detail Recording
Result	New	FEATURE	DNDACT	DND Activation
Result	New	FEATURE	DNDDEACT	DND Deactivation

Datafill example

The following example shows sample datafill for table IBNXLA.

Table IBNXLA example datafill

TABLE: IBNXLA	
KEY	RESULT

RXCFN 77	FEAT N N DNDACT
RXCFN 78	FEAT N N DNDDEACT

Table release history update

DNDACT (DND Activation) and DNDDEACT (DND Deactivation) added as new FEATURE options (type IBN_LOG_FEATURE).

Supplementary information

A subscriber dials the DNDACT feature access code to activate Do Not Disturb and the DNDDEACT feature access code to deactivate Do Not Disturb.

Translation verification

The following example shows the output from Traver when it is used to verify Table IBNXLA datafill.

DND Activation TraverDND Activation:

```
>TRAVER L 6210040 B77 B
TABLE IBNLINES
HOST 00 0 00 21 0 DP STN RES 6210040 0 613_P621_0
L613_LATA1_0 613 (DND) $
TABLE LINEATTR
0 1FR NONE NT 0 10 NILSFC 0 NIL NIL 00 613_P621_0
L613_LATA1_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
613_P621_0 FR01 613 P621 TSPS Y RESGRP 0 2 $ $
TABLE RATEAREA
L613_LATA1_0 L613 NIL LATA1 $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE IBNFEAT
TUPLE NOT FOUND
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE NCOS
RESGRP 2 0 0 RNCOS2 ( XLAS RXCMN2 NXLA RES)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA,
FEATXLA, VACTRMT, AND DIGCOL
RESGRP NXLA RESXLA RXCFN 0 RES
TABLE DIGCOL
RES specified: RES digit collection
NCOS FEAT XLA name is NIL. Go to next XLA name.
TABLE IBNXLA: XLANAME RXCFN
RXCFN 77 FEAT N N DNDACT
AIN Info Collected TDP: no subscribed trigger.
TABLE TRIGGRP
Trigger AIN LNP is applicable to office.
AIN Info Analyzed TDP: trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

Feature DNDACT not supported by TRAVER

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

DND Deactivation TraverDND Deactivation:

```
>TRAVER L 6210040 B78 B
TABLE IBNLINES
HOST 00 0 00 21 0 DP STN RES 6210040 0 613_P621_0
L613_LATA1_0 613 (DND) $
TABLE LINEATTR
0 1FR NONE NT 0 10 NILSFC 0 NIL NIL 00 613_P621_0
L613_LATA1_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
613_P621_0 FR01 613 P621 TSPS Y RESGRP 0 2 $ $
TABLE RATEAREA
L613_LATA1_0 L613 NIL LATA1 $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE IBNFEAT
TUPLE NOT FOUND
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE NCOS
RESGRP 2 0 0 RNCOS2 ( XLAS RXCMN2 NXLA RES)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA,
FEATXLA, VACTRMT, AND DIGCOL
RESGRP NXLA RESXLA RXCFN 0 RES
TABLE DIGCOL
RES specified: RES digit collection
NCOS FEAT XLA name is NIL. Go to next XLA name.
TABLE IBNXLA: XLANAME RXCFN
RXCFN 78 FEAT N N DNDDEACT
AIN Info Collected TDP: no subscribed trigger.
TABLE TRIGGRP
Trigger AIN LNP is applicable to office.
AIN Info Analyzed TDP: trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

Feature DNDDEACT not supported by TRAVER

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

Name: RESFEAT

RESidential line FEATures

Functional description

Table RESFEAT contains the assignment of custom local area signaling services (CLASS) for residential lines.

Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

Current datafill order unchanged.

Size

Unchanged

Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
RESFEAT	Unchanged	Unchanged	Unchanged

Fields/OIDs

The following table lists fields for Table RESFEAT.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
LINE	Unchanged	N/A	EXT_LEN	Line Equipment Number
KEY	Unchanged	N/A	RESFEAT_KEY_RANGE	0 to 76
FEAT	Unchanged	N/A	SCA	Selective Call Acceptance feature
VAR	Unchanged	DF Subfield	SCA	SCA Data Feature
VAR	Unchanged	AMA Subfield	{AMA, NOAMA}	Automatic Message Accounting
VAR	Unchanged	STATUS Subfield	{INACT, ACT, UNIVI, UNIVA}	Status
DND_ONLY	NEW	DF Refinement (DF=SCA)	{Y, N}	Y if SCA applies only when DND is active N for standard SCA

Datafill example

The following example shows sample datafill for table RESFEAT.

Table RESFEAT example datafill

TABLE: RESFEAT			
LINE	KEY	FEAT	VAR

HOST 00 1 08 05	0	SCA	
		SCA NOAMA	ACT Y

Table release history update

DND_ONLY field added to SCA data feature.

Supplementary information

None

Translation verification

Table RESFEAT is not included in TRAVER output.

Service Orders (SO) (CM & SESM)

This activity does not introduce a new LCC, a new option, or change any existing compatibilities. It does introduce a new field for the SCA option.

Service order change details

A new field DND_ONLY is added to the existing SCA (Selective Call Acceptance) option. Its default value is "N." When DND_ONLY is set to "Y" then this instance of SCA only applies if DND is active. If DND is not active, then SCA screening does not apply to any incoming calls.

LCC and options

Unchanged

Meridian digital centrex feature assignment requirements

Feature	500/2500	MDC SET	ISDN SET
DND	Y	Y	Y
SCA	Y	Y	Y

New commands

None

New Fields

How service order options are presented

Description

A new field will be added to the SCA feature. The new field is DND_ONLY (Y/N). When DND_ONLY is set to “Y” it indicates that this instance of SCA should only apply when DND is active on the line. If DND is not active, then this instance of SCA will not screen any incoming calls. If DND_ONLY is set to “N” then the interaction documented prior to this activity between DND & SCA applies.

ADO Example

The following example shows the SCA option added to a line. The field DND_ONLY is set to Y (Note its default value is N).

Example of the SCA option in prompt mode

```
>ADO $
DN_OR_LEN:
>6210040
OPTION:
>SCA
BILLING_OPTION: NOAMA
>NOAMA
STATUS:
>ACT
DNS:
>6136210042
VBCOUNT:
>7
DNS:
>$
DND_ONLY: N
>Y
OPTION:
>$
```

Example of the ADO option in no-prompt mode

```
ADO $ 6210040 SCA NOAMA ACT 6136210042 7 $ Y $
```

Option prompts

System prompts for <abbreviated option name> option

Prompt	Valid input	Description	Areas affected by prompt
ADO	N/A	Add Option	Servord Command
DN_OR_LEN:	A DN or a LEN	Enter the DN or LEN	DN or LEN prompt
OPTION	SCA	Selective Call Acceptance	Option Prompt
BILLING_OPTION	NOAMA or AMA	AMA Status	SCA suboption prompt (Existing)
STATUS	INACT, ACT, UNIVI, UNIVA	Activity Status	SCA suboption prompt (Existing)
DNS	TEN DIGIT DN	The DN to add to the SCA list	SCA suboption prompt (Existing)
VBCOUNT	0 TO 10	Ten Digit Count	SCA suboption prompt (Existing)
DND_ONLY	Y/N	Enter Y if this instance of SCA applies only when DND is active. Enter N for standard SCA.	SCA suboption prompt (NEW)

CHF Example

The following examples show the SCA feature being changed via the CHF command and the new field DND_ONLY bool defaults to **N**.

Example of the SCA option in prompt mode

```

>CHF $
DN_OR_LEN:
>6210040
OPTION:
>SCA
BILLING_OPTION: NOAMA
>NOAMA
STATUS:
>ACT
DND_ONLY: N
>Y
OPTION:
>$

```

Example of the ADO option in no-prompt mode

```
CHF $ 6210040 SCA NOAMA ACT Y $
```

Option prompts**System prompts for <abbreviated option name> option**

Prompt	Valid input	Description	Areas affected by prompt
CHF	N/A	Change Feature	Servord Command
DN_OR_LEN:	A DN or a LEN	Enter the DN or LEN	DN or LEN prompt
OPTION	SCA	Selective Call Acceptance	Option Prompt
BILLING_OPTION	NOAMA or AMA	AMA Status	SCA suboption prompt (Existing)
STATUS	INACT, ACT, UNIVI, UNIVA	Activity Status	SCA suboption prompt (Existing)

System prompts for <abbreviated option name> option

Prompt	Valid input	Description	Areas affected by prompt
DND_ONLY	Y/N	Enter Y if this instance of SCA applies only when DND is active. Enter N for standard SCA.	SCA suboption prompt (NEW)

Line class code compatibility

Line class code compatibility does not change with this activity.

<abbreviated option name> compatibility to LCC

Line class code	Compatible?
RES	Yes
IBN	Yes
PSET	Yes
M5008	Yes
M5009	Yes
M5112	Yes
M5208	Yes
M5209	Yes
M5212	Yes
M5216	Yes
M5312	Yes
M5316	Yes
M6310	Yes
M6320	Yes
ISDNKSET	Yes

Assignability

Unchanged.

Option prerequisites

Unchanged

Notes

None

Feature identification

Functionality: <functional group>

Feature number: <feature number>

SERVORD+ Exceptions**Software optionality control (SOC)****SOC**

SOC option name:	Enh Do Not Disturb
SOC option title:	No
SOC option control type:	state
New SOC option?	Yes
SOC option order code	RES00102
Option defined in DRU:	CCM
Affected products:	NA100

Element Management**New/modified GUIs**

None

Command interface changes**Directory:** N/A**Command:** QSL**Command type:** NON-MENU**Command target:** All**Command availability:** RES**Command description**

Query Screen List is available from the CI prompt by typing “QSL” and provides the screening lists associated with a line. Command input is not

changing as a result of this activity, but the output will be changed to reflect when SCA DND_ONLY is applicable.

Command syntax

<CommandName> command parameters and variables

Command	Parameters and variables	Description
QSL	DN_OR LEN	7- TO 10-DIGIT DN or LEN
	OPTKEY	1 to 76
	FEATURE	SLE feature name SCA, SCF, or SCRJ, or ALL
	FORMAT	F (Full) or H (Hex)

Qualifications and warnings

None

Responses

<response>

MAP outputs with associated meanings and actions

Command: QSL 6210040 SCA F
<RESPONSE>: ----- DN: 6136210040 LEN: HOST 00 0 00 21 SCA feature is ACTIVE and will not generate AMA records. Do Not Disturb Only: Yes. Contents of SCA list are: 6136210042 ----- Meaning: 6136210042 is on 6136210040 SCA screening list. The output Do Not Disturb Only indicates the value of the SCA field DND_ONLY. In this example the field DND_ONLY is set to Y. When DND_ONLY is Y then SCA screening applies when DND (Do Not Disturb) is active (provided SCA is active & RES00102 is ON). If DND is active, then caller(s) on the SCA screening list (in this example, 6136210042) will bypass DND and terminate. Callers not on the SCA screening list will receive SCA treatment. If DND is not active, then all callers terminate without going through SCA screening as this iteration of SCA (DND_ONLY = Y) only applies screening when DND is active. System or user actions: None.

MAP outputs with associated meanings and actions

Command: QSL 6210040 SCA F
<RESPONSE> ----- DN: 6136210042 LEN: HOST 00 0 00 21 SCA feature is ACTIVE and will not generate AMA records. Do Not Disturb Only: No. Contents of SCA list are: 6136210040 ----- Meaning: 6136210040 is on 6136210042 SCA screening list. The output Do Not Disturb Only indicates the value of the SCA field DND_ONLY. In this example the field DND_ONLY is set to N. When DND_ONLY is N then SCA screening applies to all incoming calls (provided SCA is active). If DND is active, then caller(s) on the SCA screening list (in this example, 6136210042) will receive DND treatment and not terminate. Callers not on the SCA screening list will receive SCA treatment. If DND is not active or not provisioned, then callers on the SCA screening list will terminate and callers not on the SCA screening list will receive SCA treatment. System or user actions: None

Security

None

Configuration Walkthrough

NA

Product = CS 2000**A00002281 -- AMAPRT Expansion (Succession on DMS)*****Functional Description***

Table STDPRTCT, subtable AMAPRT, is a table that allows customers to add AMA specific options that are triggered by translations. The present limit of

8191 tuples in table AMAPRT limits the customer's ability to assign AMA options based on translations. This feature will expand the maximum value of this table to allow for 32000 entries, thus allowing the customer to datafill many more AMA options.

Hardware Requirements or Dependencies

N/A

Software Requirements or Dependencies

N/A

Limitations and restrictions

N/A

Interactions

N/A

Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema __N/A__

User Interface _____

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

Realtime _____

Engineering Information __X__

Product = CS 2000

A00002340 -- Add Extension Registers for CDR OMS (Succession on DMS)

Functional Description

Two new OM groups FCDRTM1E and FCDRTM2E will be provided for the overflows from the groups FCDRTMP1 and FCDRTMP2. One new group FCDRALG2 will be provided for the overflow from the group FCDRALGR.

The OM groups FCDRTMP1 and FCDRTMP2 each contains 32 registers to peg the usage of up to 32 different CDR templates. The OM group FCDRALGR contains eight registers to count the method used to choose the CDR template. The maximum size of a register is 65535 or #FFFF. The maximum size is controlled by the OM sub-system. With the addition of an extension register, every rollover will be pegged. This allows up to a maximum value of 4,294,901,760 before the extension register overflows. This value is calculated by $(65535 * 65535) + 65535$.

The OM subsystem limits the maximum registers per OM group at 32 so new OM extension groups must be defined for the FCDRTMP1 and FCDRTMP2 groups.

The new extension functionality will be implemented under SOC control. This will allow for controlled customer implementation and also provide the ability to disable the new extension if required.

The following displays the current OM group FCDRTMP1 along with the new OM extension group FCDRTM1E. The group FCDRTMP2 will be expanded in the same fashion for templates 32-63 using the new group FCDRTM2E.

The FCDRALGR group will have its extension registers in the new group FCDRALG2 as shown in the following example.

FCDRTMP1

CLASS: HOLDING

START: 2003/04/04 09:35:00 FRI; STOP: 2003/04/04 09:40:00 FRI;

SLOWSAMPLES: 3 ; FASTSAMPLES: 30 ;

TMPLT_0	TMPLT_1	TMPLT_2	TMPLT_3
TMPLT_4	TMPLT_5	TMPLT_6	TMPLT_7
TMPLT_8	TMPLT_9	TMPLT_10	TMPLT_11
TMPLT_12	TMPLT_13	TMPLT_14	TMPLT_15

TMPLT_16	TMPLT_17	TMPLT_18	TMPLT_19
TMPLT_20	TMPLT_21	TMPLT_22	TMPLT_23
TMPLT_24	TMPLT_25	TMPLT_26	TMPLT_27
TMPLT_28	TMPLT_29	TMPLT_30	TMPLT_31

0

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

FCDRTM1E

CLASS: HOLDING

START:2003/04/04 09:35:00 FRI; STOP: 2003/04/04 09:40:00 FRI;

SLOWSAMPLES: 3 ; FASTSAMPLES: 30 ;

TMPLT_0	TMPLT_1	TMPLT_2	TMPLT_3
TMPLT_4	TMPLT_5	TMPLT_6	TMPLT_7
TMPLT_8	TMPLT_9	TMPLT_10	TMPLT_11
TMPLT_12	TMPLT_13	TMPLT_14	TMPLT_15
TMPLT_16	TMPLT_17	TMPLT_18	TMPLT_19
TMPLT_20	TMPLT_21	TMPLT_22	TMPLT_23
TMPLT_24	TMPLT_25	TMPLT_26	TMPLT_27
TMPLT_28	TMPLT_29	TMPLT_30	TMPLT_31

0

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

FCDRTMP2

CLASS: ACTIVE

START:2003/04/24 13:00:00 THU; STOP: 2003/04/24 13:08:17 THU;

SLOWSAMPLES: 5 ; FASTSAMPLES: 50 ;

TMPLT_32	TMPLT_33	TMPLT_34	TMPLT_35
TMPLT_36	TMPLT_37	TMPLT_38	TMPLT_39
TMPLT_40	TMPLT_41	TMPLT_42	TMPLT_43
TMPLT_44	TMPLT_45	TMPLT_46	TMPLT_47
TMPLT_48	TMPLT_49	TMPLT_50	TMPLT_51
TMPLT_52	TMPLT_53	TMPLT_54	TMPLT_55
TMPLT_56	TMPLT_57	TMPLT_58	TMPLT_59
TMPLT_60	TMPLT_61	TMPLT_62	TMPLT_63

0

0	0	0	0

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

FCDRTM2E

CLASS: ACTIVE

START:2003/04/24 13:00:00 THU; STOP: 2003/04/24 13:08:17 THU;

SLOWSAMPLES: 5 ; FASTSAMPLES: 50 ;

TMPLT_32	TMPLT_33	TMPLT_34	TMPLT_35
TMPLT_36	TMPLT_37	TMPLT_38	TMPLT_39
TMPLT_40	TMPLT_41	TMPLT_42	TMPLT_43
TMPLT_44	TMPLT_45	TMPLT_46	TMPLT_47
TMPLT_48	TMPLT_49	TMPLT_50	TMPLT_51
TMPLT_52	TMPLT_53	TMPLT_54	TMPLT_55
TMPLT_56	TMPLT_57	TMPLT_58	TMPLT_59
TMPLT_60	TMPLT_61	TMPLT_62	TMPLT_63

0

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

FCDRALGR

CLASS: ACTIVE

START:2003/09/18 03:45:05 THU; STOP: 2003/09/18 03:54:45 THU;

SLOWSAMPLES: 1 ; FASTSAMPLES: 3 ;

INTERNAL	CALLTYPE	SUBRNUM	TRK
TCAP	FIXED	BESTFIT	RTEATTR

0

0	0	0	0
0	0	0	0

FCDRALG2

CLASS: ACTIVE

START:2003/09/18 03:45:05 THU; STOP: 2003/09/18 03:54:45 THU;

SLOWSAMPLES: 1 ; FASTSAMPLES: 3 ;

INTERNAL	CALLTYPE	SUBRNUM	TRK
TCAP	FIXED	BESTFIT	RTEATTR

0

0	0	0	0
0	0	0	0

Hardware Requirements or Dependencies

None.

Software Requirements or Dependencies

The capabilities will be under SOC control.

This activity only impacts offices using the UCS software layer.

Limitations and restrictions

None

Interactions

The existing OM groups will not be changed. The new groups will contain only new registers. The new OM groups are:

- FCDRTM1E
- FCDRTM2E
- FCDRALG2

Applicable customer facing sections

Fault Management

Logs

Alarms

Configuration

Data Schema

User Interface

Element Management

Security

Service Order

Office Parameters

Accounting (includes AMA billing)

Performance (includes operational measurements)

Fault Management for A00002340

Performance management strategy

This feature provides the new OM groups FCDRTM1E, FCDRTM2E and FCDRALG2.

Performance management tools and utilities

None

Performance Measurements (PM), Operational Measurements (OM), and stats

PM, OM, and stats format

N/A

OM Group FCDRTM1E (applies only to DMS)

OM description

OM Group FCDRTM1E

The group FCDRTM1E is only pegged when the UBFR0008 SOC is ON.

This group is used for register overflows from the OM group FCDRTMP1.

Release history update

The OM group is being provided new in the UCS20 release.

Registers

OM group registers display on the MAP terminal as follows:

FCDRTM1E

CLASS: HOLDING

START:2003/04/04 09:35:00 FRI; STOP: 2003/04/04 09:40:00 FRI;

SLOWSAMPLES: 3 ; FASTSAMPLES: 30 ;

TMPLT_0	TMPLT_1	TMPLT_2	TMPLT_3
TMPLT_4	TMPLT_5	TMPLT_6	TMPLT_7
TMPLT_8	TMPLT_9	TMPLT_10	TMPLT_11
TMPLT_12	TMPLT_13	TMPLT_14	TMPLT_15
TMPLT_16	TMPLT_17	TMPLT_18	TMPLT_19
TMPLT_20	TMPLT_21	TMPLT_22	TMPLT_23
TMPLT_24	TMPLT_25	TMPLT_26	TMPLT_27
TMPLT_28	TMPLT_29	TMPLT_30	TMPLT_31

0

0

0

0

0

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

Group structure

This OM group provides 32 pre-defined tuples.

Associated OM groups

This OM group is used as register overflows for the OM group FCDRTMP1.

Associated functional groups

None

OM group registers logic flow chart

Refer to the comments in the Associated Register section.

Register (applies only to DMS)

TMPLT_0 through TMPLT_31

Register description

Each register is associated with the CDR template being used for a CDR billing record. The CDR template index corresponds to the register number. The index number of a CDR template may be viewed from the MAP under the CI CTMPLT. The “TEMPLATE ALL” command will list out the indexes.

The data range for these registers is a decimal value of 0-65535.

This OM group supports indexes 0-31.

Example: CDR template UCS13 is index 9. The related OM register will be TMPLT_9.

```
>ctmplt
>template all
The list of indices and defined templates is as follows:
0 : CDR2AMA
1 : CDR2AMA2
2 : CDR2AMA3
3 : RESERVED03
4 : RESERVED04
5 : AMAREC
6 : UCS09
7 : UCS11
8 : UCS12
9 : UCS13
```

Register release history update

All the registers in this group are new in the UCS20 release.

Associated registers

Each register in this OM group is related to a register in group FCDRTMP1. When the register in group FCDRTMP1 reaches 65535, the associated extension register in group FCDRTM1E will be incremented. If the SOC is IDLE, the FCDRTM1E register will not be pegged. In either case, the register in group FCDRTMP1 will wrap to 0 when it overflows.

Example:

Group FCDRTMP1; Register TMPLT_9

Group FCDRTM1E; Register TMPLT_9

A FCDRTM1E register is pegged once for every FCDRTMP1 register overflow. A value of 1 in the FCDRTM1E overflow register indicates 65535 pegs. A value of 1 in the FCDRTMP1 register indicates one peg.

Once the FCDRTM1E overflow register is pegged, the register in FCDRTMP1 will reset to 0 and resume pegging.

Associated logs

None

OM Group FCDRTM2E (applies only to DMS)**OM description**

OM Group FCDRTM2E

The group FCDRTM2E is only pegged when the UBFR0008 SOC is ON.

This group is used for register overflows from the OM group FCDRTMP2.

Release history update

The OM group is being provided new in the UCS20 release.

Registers

OM group registers display on the MAP terminal as follows:

FCDRTM2E

CLASS: ACTIVE

START: 2003/04/24 13:00:00 THU; STOP: 2003/04/24 13:08:17 THU;

SLOWSAMPLES: 5 ; FASTSAMPLES: 50 ;

TMPLT_32 TMPLT_33 TMPLT_34 TMPLT_35

TMPLT_36	TMPLT_37	TMPLT_38	TMPLT_39
TMPLT_40	TMPLT_41	TMPLT_42	TMPLT_43
TMPLT_44	TMPLT_45	TMPLT_46	TMPLT_47
TMPLT_48	TMPLT_49	TMPLT_50	TMPLT_51
TMPLT_52	TMPLT_53	TMPLT_54	TMPLT_55
TMPLT_56	TMPLT_57	TMPLT_58	TMPLT_59
TMPLT_60	TMPLT_61	TMPLT_62	TMPLT_63
0			
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

Group structure

This OM group provides 32 pre-defined tuples.

Associated OM groups

This OM group is used as register overflows for the OM group FCDRTMP2.

Associated functional groups

None

OM group registers logic flow chart

Refer to the comments in the Associated Register section.

Register (applies only to DMS)

TMPLT-32 through TMPLT_63

Register description

Each register is associated with the CDR template being used for a CDR billing record. The CDR template index corresponds to the register number. The index number of a CDR template may be viewed from the MAP under the CI CTMPLT. The “TEMPLATE ALL” command will list out the indexes.

The data range for these registers is a decimal value of 0-65535.

This OM group supports indexes 32-63.

Example: CDR template UCS13 is index 9. The related OM register will be TMPLT_9.

```
>ctmpl
>template all
The list of indices and defined templates is as follows:
0 : CDR2AMA
1 : CDR2AMA2
```

2 : CDR2AMA3
3 : RESERVED03
4 : RESERVED04
5 : AMAREC
6 : UCS09
7 : UCS11
8 : UCS12
9 : UCS13

Register release history update

All the registers in this group are new in the UCS20 release.

Associated registers

Each register in this OM group is related to a register in group FCDRTMP2. When the register in group FCDRTMP2 reaches 65535, the associated extension register in group FCDRTM2E will be incremented. If the SOC is IDLE, the FCDRTM2E register will not be pegged. In either case, the register in group FCDRTMP2 will wrap to 0 when it overflows.

Example:

Group FCDRTMP2; Register TMPLT_21
Group FCDRTM2E; Register TMPLT_21

A FCDRTM2E register is pegged once for every FCDRTMP2 register overflow. A value of 1 in the FCDRTM2E overflow register indicates 65535 pegs. A value of 1 in the FCDRTMP2 register indicates one peg.

Once the FCDRTM2E overflow register is pegged, the register in FCDRTMP2 will reset to 0 and resume pegging.

Associated logs

None

OM Group FCDRALG2 (applies only to DMS)

OM description

OM Group FCDRALG2

The group FCDRALG2 is only pegged when the UBFR0008 SOC is ON.

This group is used for register overflows from the OM group FCDRALGR.

Release history update

The OM group is being provided new in the UCS20 release.

Registers

OM group registers display on the MAP terminal as follows:

FCDRALG2

CLASS: ACTIVE

START:2003/09/18 03:45:05 THU; STOP: 2003/09/18 03:54:45 THU;

SLOWSAMPLES: 1 ; FASTSAMPLES: 3 ;

	INTERNAL TCAP	CALLTYPE FIXED	SUBRNUM BESTFIT	TRK RTEATTR
0	0	0	0	0
	0	0	0	0

Group structure

This OM group provides 8 pre-defined tuples.

Associated OM groups

This OM group is used as register overflows for the OM group FCDRALGR.

Associated functional groups

None

OM group registers logic flow chart

Refer to the comments in the Associated Register section.

Register (applies only to DMS)

INTERNAL
CALLTYPE
SUBRNUM
TRK
TCAP
FIXED
BESTFIT
RTEATTR

Register description

These registers have the same description as those in the group FCDRALGR. The only difference is that these are extension registers. This means that one count here is equal to 65535 counts of the same register in FCDRALGR. They keep track of the number of times the register in group FCDRALGR have overflowed.

Register release history update

All the registers in this group are new in the UCS20 release.

Associated registers

Each register in this OM group is related to a register in group FCDRALGR. When the register in group FCDRALGR reaches 65535, the associated extension register in group FCDRALG2 will be incremented. If the SOC is IDLE, the FCDRALG2 register will not be pegged. In either case, the register in group FCDRALGR will wrap to 0 when it overflows.

Example:

Group FCDRALGR; Register FIXED

Group FCDRALG2; Register FIXED

A FCDRALG2 register is pegged once for every FCDRALGR register overflow. A value of 1 in the FCDRALG2 overflow register indicates 65535 pegs. A value of 1 in the FCDRALGR register indicates one peg.

Once the FCDRALG2 overflow register is pegged, the register in FCDRALGR will reset to 0 and resume pegging.

Associated logs

None

Software Optionality Control

This feature creates new SOC UBFR0008 as follows.

SOC details

SOC option name:	UCS CDR OM Expansion
SOC option title:	UCS CDR OM Expansion
SOC option control type:	state
New SOC option?	Yes
SOC option order code	UBFR0008
Option defined in DRU:	UCS
Affected products:	SN07

Product = CS 2000

A00002431 -- LX82BA capacity delivery (Succession on DMS)

Functional Description

This activity provides a mechanism for NORTEL to provide incremental call processing capacity for the NTLX82BA CEM card to its DMSCP SPM customers. The various levels of capacities for DMSCP class of SPMs are

1. Standard capacity - Call processing capacity equal to that of the NTLX82AA CEM card.
2. Enhanced capacity - Call processing capacity approximately equal to that of 2 times that of the NTLX82AA.
3. Premium capacity - Call processing capacity approximately equal to that of 3 times that of the NTLX82AA.

For Non-DMSCP class of SPMs, only two levels of capacities, Standard and Premium are provided based on the CEM PEC (NTLX82BA) that are datafilled in table MNCKTPAK. If both the CEMs are datafilled with NTLX82BA PEC, then the capacity is Premium else the capacity is Standard.

Currently, NTLX82BA CEMs running CST and CEM loads (DMSCP SPM) have their CALLP capacity reduced to that of the NTLX82AA whereas NTLX82BA CEMs running IWS (IW SPM) or MG4 (MG4K SPM) load have their CALLP capacity equivalent to that of NTLX82BA.

DMSCP class of SPMs:

This activity provides the ability to control the call processing capacity at the node level for DMSCP class of SPMs provisioned with NTLX82BA cards, using core SOC options. The customer can provision the desired capacity in table MNNODE if appropriate SOC keys are available.

The various functionalities provided as part of this activity are:

- Two usage SOCs, one for Enhanced and the other for Premium capacity.
- Table control changes in table MNNODE and table MNCKTPAK.
- New CI tool to display the capacity provisioned on the SPMs present in the office

Two Usage SOCs to provide Enhanced and Premium Capacity

Two new USAGE SOCs are created under the existing SPMS group for DMSCP class of SPMs. The SOC option SPMS0020 corresponds to the SPMs with Enhanced capacity and the SOC option SPMS0028 corresponds to the SPMs with Premium capacity. When the SOC keys are not available, the limit and the usage are zero and no DMSCP class of SPMs are capable of running at Enhanced or Premium capacity. Refer to the following figure for the format of the two SOCs. Both the SOC options have hard usage limit. RTU is 'Y' for usage limit >0 and RTU is 'N' for usage limit = 0. For each value of the hard limit a separate SOC key is available for the customer. The threshold value for these SOC options are set to 100%.

The hard limit value of SPMS0020 denotes the maximum number of DMSCP class of SPMs in the office that can be provisioned with Enhanced capacity and the hard limit value of SPMS0028 denotes the maximum number of DMSCP class of SPMs in the office that can be provisioned with Premium capacity.

The value of the USAGE of SPMS0020 and SPMS0028 denotes the number of DMSCP class of SPMs currently running with the Enhanced and Premium capacity respectively from Core's perspective.

Please refer to section "Software optionality control (SOC)" for more details on the Usage SOC.

SPMS group options as listed in SOC framework

```
>select option SPMS0020 verbose

GROUP:SPMS
OPTION  NAME                RTU STATE  USAGE  LIMIT  UNITS  LAST_CHG
-----  ----
SPMS0020 Enhanced Call cap      Y   -      0      0      1SM  03/06/13
replaces options:      NONE
threshold:      100%    high water mark:      0

FEATURE  STATE  USAGE  UNITS
-----  ----  ----  ----
00002431 -    0      1SM
NAME:    SPMS Enhanced Call cap

>select option SPMS0028 verbose

GROUP:SPMS
OPTION  NAME                RTU STATE  USAGE  LIMIT  UNITS  LAST_CHG
-----  ----
SPMS0028 Premium Call cap    Y   -      0      0      1SM  03/06/13
replaces options:      NONE
threshold:      100%    high water mark:      0

FEATURE  STATE  USAGE  UNITS
-----  ----  ----  ----
00002432 -    0      1SM
NAME:    SPMS Premium Call cap
```

Note: SOC option SPMS0028 uses the feature id 00002432.

Table control support to provision the desired capacity in table MNNODE

For DMSCP class of SPMs, table control changes are made to provision the desired capacity per node in table MNNODE. A new field 'capindx' is added in table MNNODE, only for DMSCP class of SPMs to provision this capacity. This new field can take the values 'Standard', 'Enhanced' or 'Premium', 'Standard' being the default value.

During an ONP from an earlier release where the capindx field is not present to a release where the capindx field is introduced in table MNNODE, this field is set to 'Standard'. For using 'Enhanced' or 'Premium' values during tuple

addition, the respective SOC options must have its RTU set to Y and Usage count must be less than its Limit. Also for using 'Enhanced' capacity, number of DMSCP SPMs provisioned with Enhanced capacity must be less than the limit of SPMS0020 SOC option and for using 'Premium' capacity, number of DMSCP SPMs provisioned with Premium capacity must be less than the limit of SPMS0028 SOC option.

SOC 504 is an existing log that gets generated when the RTU is set for any SOC option.

While changing the capindx field to 'Enhanced' or 'Premium' values, the PEC codes of the CEM units provisioned in table MNCKTPAK for this node are also verified for NTLX82BA, in addition to the SOC check. If all the check passes, the appropriate SOC usage value is incremented. For capindx field changes from 'Enhanced' or 'Premium' values to 'Standard', appropriate SOC usage counts are decremented only if both the CEM tuples are present in table MNCKTPAK. Tuple change without any change to the 'capindx' field is not validated. For tuple deletion, there are no restrictions enforced on this field.

In table MNCKTPAK, the CEM tuples of DMSCP variant of SPM are allowed to be provisioned only with the PECs - NTLX82AA, NTLX82AB and NTLX82BA. The provisioning of the PEC is dependent on the capindx field present in table MNNODE. In case the capindx in table MNNODE is 'Standard', the PEC shall be allowed to be datafilled as NTLX82AA, NTLX82AB or NTLX82BA. In case of 'Enhanced' or 'Premium' capindx, the PEC must be datafilled as NTLX82BA.

The provisioned capacity in table MNNODE, is downloaded to the local using DDM framework. Local throttles the callp capacity based on the capacity index downloaded.

Please refer to section "Data schema (DS) (CM)" for more details on the error, warning and success messages introduced by this activity during table control operations in table MNNODE and table MNCKTPAK.

CI tool to display capacity information

A new CI tool, SPMCPCAP, is introduced to display the capacity information of SPM. This tool enables to list the SPM and their capacities based on the variant type or list the SPMs based on the capacities. There is also a provision to find out capacity for a given SPM number. Remarks field in this tool displays if CEM(s) are not datafilled in table MNCKTPAK.

Please refer to section "Command interface changes" for more details on the CI tool.

Non-DMSCP class of SPMs

Table MNNODE is not modified for Non-DMSCP class of SPMs. Also in table MNCKTPAK no validations for CEM PEC are introduced by this activity.

The CI tool, SPMPCAP, is used to display the capacity information of Non-DMSCP class of SPMs also. Only two capacities, 'Standard' and 'Premium' are displayed in this case. For Non-DMSCP variants, MG4K and IW, the capacity information is derived based on the table MNCKTPAK datafill. If both the CEM are datafilled with NTLX82BA PEC cards, then capacity is set to 'Premium'. For other combinations of PEC cards, the capacity is set to 'Standard'. Remarks field in this tool displays if CEM(s) are not datafilled in table MNCKTPAK.

Please refer to section "Command interface changes" for more details on the CI tool.

Hardware Requirements or Dependencies

None.

Software Requirements or Dependencies

None.

Limitations and restrictions

- SOC limit can be decremented to a value less than the usage count.
- The CI tool displays the callp capacities for SPMs from core's perspective only. The capacity will be enforced if there is a PEC mismatch at the local.

Interactions

None.

Applicable customer facing sections

Fault Management

Logs __N/A__

Alarms __N/A__

Configuration

Data Schema __X__

User Interface __X__

Element Management __N/A__

Security __N/A__

Service Order	__N/A__
Office Parameters	__N/A__
Accounting (includes AMA billing)	__N/A__
Performance (includes operational measurements)	__N/A__

Glossary

Term	Description
CEM	Common Equipment Module
CI	Command Interpreter
PEC	Product Engineering Code
RTU	Right to Use
SOC	Software Optionality Control
SPM	Spectrum Peripheral Module

Configuration for A00002431

Hardware and Software Requirements

None.

Initial Configuration

None.

Office/Subnet parameters (OP/SP) (CM & SESM)

None.

Upgrade Impact

Dump and Restore

During an ONP from an earlier release where the capindx field is not present to a release where the capindx field is introduced in table MNNODE, this field is set to 'Standard'.

Element Management Upgrade

Not Applicable.

Data schema (DS) (CM)

New/modified tables

Table name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
MNNODE	CHANGED	NEW
MNCKTPAK	CHANGED	NEW

Table information

Name: MNNODE

Functional description

A new field 'capindx' is added in table MNNODE for DMSCP class of SPMs only. This new field can take the values 'Standard', 'Enhanced' or 'Premium' where 'Standard' is the default value.

During tuple addition in table MNNODE, for using 'Enhanced' or 'Premium' values, the respective SOC options must have its RTU set to Y and the Usage count must be less than its Limit. Also for using 'Enhanced' capacity, number of DMSCP SPMs provisioned with Enhanced capacity must be less than the limit of SPMS0020 SOC option and for using 'Premium' capacity, number of DMSCP SPMs provisioned with Premium capacity must be less than the limit of SPMS0028 SOC option.

While changing the capindx field to 'Enhanced' or 'Premium' values, the PEC codes of the CEM units provisioned in table MNCKTPAK for this node are also verified for NTLX82BA, in addition to the SOC check. If all the check passes, the appropriate SOC usage value is incremented. For capindx field changes from 'Enhanced' or 'Premium' values to 'Standard', appropriate SOC usage counts are decremented if both the CEM tuples are present in table MNCKTPAK.

Tuple change with No change to the 'capindx' field is not validated. For tuple deletion, there are no restrictions enforced on this field. Refer to "New Error Messages", "New Warning Messages" and "New Success Messages" for the various Error, Warning and Success messages that are introduced in table MNNODE as part of this activity.

Note: All the table control operations in “New Error Messages” shall be failed with appropriate error messages and all the table control operation in “New Warning Messages” and “New Success Messages” shall be passed with appropriate messages.

New Error Messages

No.	Table Control operations	Pre - conditions
	Error Messages	
1	a. Tuple addition in MNNODE with 'Enhanced' capacity. b. Tuple change in MNNODE from 'Standard' to 'Enhanced' capacity. c. Tuple change in MNNODE from 'Premium' to 'Enhanced' capacity.	SPMS0020 SOC option's RTU set to 'N'
	RTU value not set for SPM Enhanced capacity SOC option SPMS0020.	
2	a. Tuple addition in MNNODE with 'Premium' capacity. b. Tuple change in MNNODE from 'Standard' to 'Premium' capacity. c. Tuple change in MNNODE from 'Enhanced' to 'Premium' capacity.	SPMS0028 SOC option's RTU set to 'N'
	RTU value not set for SPM Premium capacity SOC option SPMS0028.	
3	a. Tuple addition in MNNODE with 'Enhanced' capacity. b. Tuple change in MNNODE from 'Standard' to 'Enhanced' capacity. c. Tuple change in MNNODE from 'Premium' to 'Enhanced' capacity.	SPMS0020 SOC option's Limit is equal to the No. of SPMs provisioned with 'Enhanced' capacity.
	Capindx cannot be provisioned as Enhanced capacity for more SPMs than the limit of SOC option SPMS0020. Check existing tuples using SPMPCAP tool.	

New Error Messages

No.	Table Control operations	Pre - conditions
	Error Messages	
4	a. Tuple addition in MNNODE with 'Premium' capacity. b. Tuple change in MNNODE from 'Standard' to 'Premium' capacity. c. Tuple change in MNNODE from 'Enhanced' to 'Premium' capacity.	SPMS0028 SOC option's Limit is equal to the No. of SPMs provisioned with 'Premium' capacity.
	Capindx cannot be provisioned as Premium capacity for more SPMs than the limit of SOC option SPMS0028. Check existing tuples using SPMPCAP tool.	
5	a. Tuple change in MNNODE from 'Standard' to 'Enhanced' capacity.	a. No. of SPMs provisioned with Enhanced capacity is less than the Limit and b. One or Both the CEM PEC is/are not NTLX82BA.
	Both CEM PEC codes must be NTLX82BA for Enhanced capacity. Verify MNCKTPAK datafill.	
6	a. Tuple change in MNNODE from 'Standard' to 'Premium' capacity.	a. No. of SPMs provisioned with Premium capacity is less than the Limit and b. One or Both the CEM PEC is/are not NTLX82BA.
	Both CEM PEC codes must be NTLX82BA for Premium capacity. Verify MNCKTPAK datafill.	

New Warning Messages

No.	Table Control operations	Pre - conditions
	Warning Messages	
1	a. Tuple addition in MNNODE with 'Enhanced' capacity. b. Tuple change in MNNODE from 'Standard' to 'Enhanced' capacity. c. Tuple change in MNNODE from 'Premium' to 'Enhanced' capacity	a. SPMS0020 SOC option's RTU set to Y, No. of SPMs provisioned with Enhanced capacity is less than the Limit and b. One or both the CEM tuples in table MNCKTPAK is/are not provisioned.
	WARNING: Capindx provisioned as Enhanced capacity. Both CEMs must be provisioned as NTLX82BA.	
2	a. Tuple addition in MNNODE with 'Premium' capacity. b. Tuple change in MNNODE from 'Standard' to 'Premium' capacity. c. Tuple change in MNNODE from 'Enhanced' to 'Premium' capacity.	a. SPMS0028 SOC option's RTU set to Y, No. of SPMs provisioned with Enhanced capacity is less than the Limit and b. One or both the CEM tuples in table MNCKTPAK is/are not provisioned.
	WARNING: Capindx provisioned as Premium capacity. Both CEMs must be provisioned as NTLX82BA.	

New Success Messages

No.	Table Control operations	Pre - conditions
	Success Messages	
1	a. Tuple change in MNNODE from 'Enhanced' to 'Standard' capacity.	Both the CEM tuples are present in table MNCKTPAK.
	Datafill conditions met for de-activation of SPM Enhanced capacity SOC option SPMS0020.	
2	a. Tuple change in MNNODE from 'Premium' to 'Standard' capacity.	Both the CEM tuples are present in table MNCKTPAK.
	Datafill conditions met for de-activation of SPM Premium capacity SOC option SPMS0028.	

New Success Messages

No.	Table Control operations	Pre - conditions
	Success Messages	
3	a. Tuple change in MNNODE from 'Standard' to 'Enhanced'. b. Tuple change in MNNODE from 'Premium' to 'Enhanced'.	a. No. of SPMs provisioned with Enhanced capacity is less than the Limit and b. Both the CEM tuples are present in table MNCKTPAK and both the CEM PEC are NTLX82BA.
	Datafill conditions met for activation of SPM Enhanced capacity SOC option SPMS0020.	
4	a. Tuple change in MNNODE from 'Standard' to 'Premium'. b. Tuple change in MNNODE from 'Enhanced' to 'Premium'.	a. No. of SPMs provisioned with Premium capacity is less than the Limit and b. Both the CEM tuples are present in table MNCKTPAK and both the CEM PEC are NTLX82BA.
	Datafill conditions met for activation of SPM Premium capacity SOC option SPMS0028.	

Usage sequence and implications (CM Only)

Current datafill order unchanged.

Size

Not impacted.

Fields/OIDs

The following table lists fields for table MNNODE which are changed as part of this activity.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CAPINDX	New	Not Applicable		This field is introduced for DMSCP class of SPMs only in table MNNODE.

Datafill example

Datafill examples for each capacity datafilled in table MNNODE are shown below.

Datafill example

```
SPM 1 SPM_1 DMSCP 1 SYNC LOOP 15 (COT 60) (DTMF 60) (ECAN 60) (TONESYN 60)
(MF 60) $ (SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT) (SYSBNA CR RPT)
(MANBNA MJ RPT) (COTLOW MN RPT) (DTMFLOW MN RPT) (ECANLOW MN RPT)
(TONESLOW MN RPT) (MFLOW MN RPT) (CMRLOW MN RPT) (PATCHFAIL MJ RPT)
(SMCHLD MJ RPT) (SMCHLD24 CR RPT) $ (ABTRK SPME) $ STANDARD

SPM 2 SPM_2 DMSCP 1 SYNC LOOP 15 (COT 60) (DTMF 60) (ECAN 60) (TONESYN 60)
(MF 60) $ (SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT) (SYSBNA CR RPT)
(MANBNA MJ RPT) (COTLOW MN RPT) (DTMFLOW MN RPT) (ECANLOW MN RPT)
(TONESLOW MN RPT) (MFLOW MN RPT) (CMRLOW MN RPT) (PATCHFAIL MJ RPT)
(SMCHLD MJ RPT) (SMCHLD24 CR RPT) $ (ABTRK SPME) $ ENHANCED

SPM 3 SPM_3 DMSCP 1 SYNC LOOP 15 (COT 60) (DTMF 60) (ECAN 60) (TONESYN 60)
(MF 60) $ (SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT) (SYSBNA CR RPT)
(MANBNA MJ RPT) (COTLOW MN RPT) (DTMFLOW MN RPT) (ECANLOW MN RPT)
(TONESLOW MN RPT) (MFLOW MN RPT) (CMRLOW MN RPT) (PATCHFAIL MJ RPT)
```

Table release history update

Not Applicable

Supplementary information

Not Applicable

Translation verification other tools

Not Applicable

Name: MNCKTPAK**Functional description**

The CEM tuples of DMSCP variant of SPM are allowed to be provisioned only with the PECs - NTLX82AA, NTLX82AB and NTLX82BA in table MNCKTPAK. With the introduction of the new field 'CAPINDX' in table MNNODE, the provisioning of the PEC is dependent on the capindx value. The capindx can be provisioned with 'Standard', 'Enhanced' or 'Premium'.

If the capindx in table MNNODE is 'Standard', the PEC shall be allowed to be datafilled as NTLX82AA, NTLX82AB or NTLX82BA. In the case of an 'Enhanced' or 'Premium' capindx, the PEC must be datafilled as NTLX82BA.

For Non-DMSCP class of SPMs, no validations for CEM PEC are introduced by this activity. The PEC that is datafilled for both the CEMs in table MNCKTPAK automatically determines the capacity for that SPM. If both the CEMs are datafilled with NTLX82BA PEC cards, then capacity is 'Premium' and for any other combinations of PEC cards, the capacity is 'Standard'. Refer to "New Error Messages" and "New Success Messages" for the various Error and Success messages that are introduced in table MNCKTPAK as part of this activity.

New Error Messages

No.	Table Control operations	Pre - conditions
	Error Messages	
1	a. Addition of a CEM tuple in table MNCKTPAK with NTLX82AA. b. Update of a CEM PEC from NTLX82BA to NTLX82AA.	a. The capindx field in table MNNODE is Enhanced or Premium and b. The other CEM tuple may or may not be present.
	Cannot allocate NTLX82AA card for an SPM that has been datafilled with Enhanced or Premium capacity. Check MNNODE datafill.	
2	a. Addition of a CEM tuple in table MNCKTPAK with NTLX82AB. b. Updation of a CEM PEC from NTLX82BA to NTLX82AB.	a. The capindx field in table MNNODE is Enhanced or Premium and b. The other CEM tuple may or may not be present.
	Cannot allocate NTLX82AB card for an SPM that has been datafilled with Enhanced or Premium capacity. Check MNNODE datafill.	

New Success Messages

No.	Table Control operations	Pre - conditions
	Success Messages	
1	a. Addition of a CEM tuple in table MNCKTPAK with NTLX82BA.	a. The capindx field in table MNNODE is Enhanced and b. The other CEM tuple is already present.
	Datafill conditions met for activation of SPM Enhanced capacity SOC option SPMS0020.	
2	a. Addition of a CEM tuple in table MNCKTPAK with NTLX82BA.	a. The capindx field in table MNNODE is Premium and b. The other CEM tuple is already present.
	Datafill conditions met for activation of SPM Premium capacity SOC option SPMS0028.	
3	a. Deletion of a CEM tuple in table MNCKTPAK with NTLX82BA.	a. The capindx field in table MNNODE is Enhanced and b. The other CEM tuple is already present.
	Datafill conditions met for de-activation of SPM Enhanced capacity SOC option SPMS0020.	
4	a. Deletion of a CEM tuple in table MNCKTPAK with NTLX82BA.	a. The capindx field in table MNNODE is Premium and b. The other CEM tuple is already present.
	Datafill conditions met for de-activation of SPM Premium capacity SOC option SPMS0028.	

Usage sequence and implications (CM Only)

Current datafill order unchanged.

Size

Not impacted.

Fields/OIDs

The following table lists fields for table MNCKTPAK which are changed as part of this activity.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action

Datafill example

Not Applicable.

Table release history update

Not Applicable

Supplementary information

Not Applicable

Translation verification other tools

Not Applicable

Service Orders (SO) (CM & SESM)

Not Applicable

Software optionality control (SOC)

Two new USAGE SOC's are created under a new group called CAP. These SOC's are used only by DMSCP class of SPMs. The SOC option SPMS0020 corresponds to the SPMs with Enhanced capacity and the SOC option SPMS0028 corresponds to the SPMs with Premium capacity.

The hard limit value of SPMS0020 denotes the maximum number of DMSCP class of SPMs in the office that can be provisioned with Enhanced capacity and the hard limit value of SPMS0028 denotes the maximum number of DMSCP class of SPMs in the office that can be provisioned with Premium capacity. The threshold value of these SOC options are set to 100%.

The value of the USAGE of SPMS0020 and SPMS0028 denotes the number of DMSCP class of SPMs currently running with the Enhanced and Premium capacity respectively from Core's perspective. Refer to "Appendix A: SOC commands" for the syntax of some of the SOC commands.

Enhanced SOC option

SOC option name:	SPMS Enhanced Call cap
SOC option title:	Yes
SOC option control type:	usage
New SOC option?	Yes
SOC option order code	SPMS0020
Option defined in DRU:	SHR
Affected products:	SPM

Premium SOC option

SOC option name:	SPMS Premium Call cap
SOC option title:	Yes
SOC option control type:	usage
New SOC option?	Yes
SOC option order code	SPMS0028
Option defined in DRU:	SHR
Affected products:	SPM

Element Management

Not Applicable.

Command interface changes

Directory: None

Directory description

Accessing directory: CI

Access to directory or MAP level and return to CI

Command: SPMCPCAP

Command type: NON-MENU

Command target: All

Command availability: RES

Command description

Command SPMCPCAP is used to display CallP capacity information for SPMs.

Command syntax

The command syntax is as shown in the following figure.

Syntax of SPMCPCAP command

```
>help spmcpcap
SPM Callp Capacity information tool.
SPMCPCAP - Displays Callp Capacity information for SPMs.
Remarks field displays if CEM(s) are not
datafilled for the SPM.

Parms: <OPTION> {Class <Class type> {DMSCP,
                                     IW,
                                     MG4K,
                                     ALL},
                Capacity <Capacity type> {Standard,
                                     Enhanced,
                                     Premium,
                                     ALL},
                SPM <SPM Number> {0 TO 85}}
```

Syntax : spmcpcap**Parameter Description:**

CLASS DMSCP	: List CallP capacities of all the DMSCP SPMs provisioned in the office.
CLASS MG4K	: List CallP capacities of all the MG4K SPMs provisioned in the office.
CLASS IW	: List CallP capacities of all the IW SPMs provisioned in the office.
CLASS ALL	: List CallP capacities of all the classes of SPMs provisioned in the office.
CAPACITY Standard:	List all the SPMs in an office that have 'Standard' CallP capacity.
CAPACITY Enhanced:	List all the SPMs in an office that have 'Enhanced' CallP capacity.
CAPACITY Premium	: List all the SPMs in an office that have 'Premium' CallP capacity.
CAPACITY ALL	: List all the SPMs in an office and their corresponding CallP capacity.
SPM <SPM NO>	: List CallP capacity for a given SPM node number.

Qualifications and warnings

If either or both the CEM tuple are not present in table MNCKTPAK for an SPM, then the remarks field against that SPM displays that the CEM datafill is incomplete. If the both the CEM tuples are datafilled, remarks field displays 'None' against that SPM.

CallP capacity information is taken from table MNNODE datafill for DMSCP class of SPMs. Supported capacities for this class are 'Standard', 'Enhanced' and 'Premium'.

For other classes (MG4K and IW) this capacity is derived from CEM PEC datafill in table MNCKTPAK. Supported capacities for these classes are 'Standard' and 'Premium'. If the CEM(s) are not datafilled in table MNCKTPAK, then the tool displays 'Standard' capacity for MG4Ks and IWs.

Responses

Listing SPMs with Enhanced CallP capacity

Listing of SPMs with Enhanced capacity will not display information of MG4K and IW SPMs as this capacity is invalid for these classes. This option is valid for DMSCP class of SPMs only.

Example

The following table lists various usage examples for SPMPCAP command.

Usage examples for SPMPCAP command

Description of task:	Display CallP Capacity information for a SPM node
Command:	CI: >spmcp cap class DMSCP
MAP response:	<pre> ----- SPM No Capacity Remarks ----- 3 Premium CEM(s) not datafilled. 4 Enhanced CEM(s) not datafilled. 10 Enhanced None. 13 Premium None. 14 Standard None. ----- </pre>

Usage examples for SPMPCAP command

Command:	CI: >spmcpicap class MG4K
MAP response:	<pre> ----- SPM No Capacity Remarks ----- 0 Standard None. 1 Standard None. 6 Standard None. 7 Standard None. 8 Premium None. 9 Standard None. 12 Standard None. 27 Standard None. 29 Standard None. 30 Standard None. ----- </pre>
Command:	CI: >spmcpicap class IW
MAP response:	<pre> ----- SPM No Capacity Remarks ----- 11 Premium None. ----- </pre>

Usage examples for SPMPCAP command

Command:	CI: >spmcpcap class ALL																																																									
MAP response:	DMSCP : <table><tr><td>SPM No</td><td>Capacity</td><td>Remarks</td></tr><tr><td>3</td><td>Premium</td><td>CEM(s) not datafilled.</td></tr><tr><td>4</td><td>Enhanced</td><td>CEM(s) not datafilled.</td></tr><tr><td>10</td><td>Enhanced</td><td>None.</td></tr><tr><td>13</td><td>Premium</td><td>None.</td></tr><tr><td>14</td><td>Standard</td><td>None.</td></tr></table> IW : <table><tr><td>SPM No</td><td>Capacity</td><td>Remarks</td></tr><tr><td>11</td><td>Premium</td><td>None.</td></tr></table> MG4K : <table><tr><td>SPM No</td><td>Capacity</td><td>Remarks</td></tr><tr><td>0</td><td>Standard</td><td>None.</td></tr><tr><td>1</td><td>Standard</td><td>None.</td></tr><tr><td>6</td><td>Standard</td><td>None.</td></tr><tr><td>7</td><td>Standard</td><td>None.</td></tr><tr><td>8</td><td>Premium</td><td>None.</td></tr><tr><td>9</td><td>Standard</td><td>None.</td></tr><tr><td>12</td><td>Standard</td><td>None.</td></tr><tr><td>27</td><td>Standard</td><td>None.</td></tr><tr><td>29</td><td>Standard</td><td>None.</td></tr><tr><td>30</td><td>Standard</td><td>None.</td></tr></table>	SPM No	Capacity	Remarks	3	Premium	CEM(s) not datafilled.	4	Enhanced	CEM(s) not datafilled.	10	Enhanced	None.	13	Premium	None.	14	Standard	None.	SPM No	Capacity	Remarks	11	Premium	None.	SPM No	Capacity	Remarks	0	Standard	None.	1	Standard	None.	6	Standard	None.	7	Standard	None.	8	Premium	None.	9	Standard	None.	12	Standard	None.	27	Standard	None.	29	Standard	None.	30	Standard	None.
SPM No	Capacity	Remarks																																																								
3	Premium	CEM(s) not datafilled.																																																								
4	Enhanced	CEM(s) not datafilled.																																																								
10	Enhanced	None.																																																								
13	Premium	None.																																																								
14	Standard	None.																																																								
SPM No	Capacity	Remarks																																																								
11	Premium	None.																																																								
SPM No	Capacity	Remarks																																																								
0	Standard	None.																																																								
1	Standard	None.																																																								
6	Standard	None.																																																								
7	Standard	None.																																																								
8	Premium	None.																																																								
9	Standard	None.																																																								
12	Standard	None.																																																								
27	Standard	None.																																																								
29	Standard	None.																																																								
30	Standard	None.																																																								
Command:	CI: >spmcpcap capacity Enhanced																																																									
MAP response:	<table><tr><td>SPM No</td><td>Capacity</td><td>Remarks</td></tr><tr><td>4</td><td>Enhanced</td><td>CEM(s) not datafilled.</td></tr><tr><td>10</td><td>Enhanced</td><td>None.</td></tr></table>	SPM No	Capacity	Remarks	4	Enhanced	CEM(s) not datafilled.	10	Enhanced	None.																																																
SPM No	Capacity	Remarks																																																								
4	Enhanced	CEM(s) not datafilled.																																																								
10	Enhanced	None.																																																								
Command:	CI: >spmcpcap SPM 7																																																									
MAP response:	<table><tr><td>SPM No</td><td>Capacity</td><td>Remarks</td></tr><tr><td>7</td><td>Standard</td><td>None.</td></tr></table>	SPM No	Capacity	Remarks	7	Standard	None.																																																			
SPM No	Capacity	Remarks																																																								
7	Standard	None.																																																								

Security

Not Applicable.

Configuration Walkthrough

Not Applicable.

Appendix A: SOC commands

Appendix A lists the syntax for various SOC commands.

- To display information about SOC group and options.

SOC:

>SELECT GROUP CAP

>SELECT OPTION SPMS0020

>SELECT OPTION SPMS0028

- To assign a limit to the new SOC options, SPMS0020 and SPMS0028.

SOC:

>ASSIGN LIMIT <value of limit> <key code> TO SPMS0020

>ASSIGN LIMIT <value of limit> <key code> TO SPMS0028

- To assign the threshold value (percentage and absolute).

SOC:

>ASSIGN THRESHOLD <percentage value> PERCENT TO SPMS0020

>ASSIGN THRESHOLD <absolute value> ABSOLUTE TO SPMS0020

Product = CS 2000

A00002432 -- SPM Enhanced Overload OMs and Logs (Succession on DMS)

Functional Description

In the SP20 release, two new software optionality control (SOC) keys will be available that provides enhanced and premium call processing capability on the NTLX82BA CEM card. These keys are being added in feature A00002431. This capacity increase will allow the NTLX82BA card's performance to be approximately 2x that of an NTLX82AA card for 'enhanced' capability and approximately 3x for 'premium'. This additional capacity capability requires improvements to the SPM engineering information available to our customers.

This feature is also being used as a reference for the CAP00002 SOC key. That functionality is documented under feature ID A00002431.

This feature implements new operational measurements (OMs, or 'pegs') that will allow a craftsperson to monitor the performance of SPMs when the SPM is experiencing peak traffic levels that are in excess of the SPM engineering limit. It also augments an existing OM group, SPMACT, to include the capacity level.

There are two components that control the number of calls that can be handled by a given SPM. The first is the System Overload Control subsystem, which is controlled by the core and is dependent on core resources. The second is the SPM flow control system, which is controlled by the SPM and is influenced by SPM resource levels. The OMs and logs that are presented in this section will include data from both components.

Hardware requirements

None, the OMs and logs described in this section apply to all CEM platforms.

Limitations and restrictions

Core and local loads must both support the new functionality.

Interactions

The OMs and logs are driven by call processing on the SPM.

A new OM group will be added (SPMOVLD), and one new OM will be added to an existing group (SPMACT). For logs, a new log type (SPM399) will be introduced that indicates transitions in and out of the SPM overload conditions.

Logs (LG)

A new log will be introduced (SPM399) for flagging overload conditions in SPMs. This log is generated whenever an SPM enters/leaves an overload condition. The reason and the action for the craft are displayed in the log so that some action can be taken to rectify the condition. In addition, some diagnostic information for the designer is also printed in the log.

New/modified logs

Log name	Log number	NEW/MOD/DELETED	System (SOS/UNIX)
SPM	399	New	SOS
SPM	313	Mod	SOS

The format/field-details and examples of the new log SPM 399 are given in detail in the 'Fault Management' section of this document.

Data schema (DS)**New/modified tables**

Table MNNODE will be modified in a related feature: A00002431. Please refer to that design document for more details.

Office parameters (OP)

Not applicable.

Service orders (SO)

Not applicable.

Alarms (AL)

Not applicable.

Command interface (CI)

Not applicable.

Operational measurements (OM)**New/modified OM groups**

Group name (acronym)	Group name (expanded)	NEW, CHANGED or DELETED	Reason
SPMACT	Spectrum Activity	Changed	One register added
SPMOVLD	Spectrum Overload	New	

One new register will be added to the SPMACT OM group - CAPLEVEL, which indicates what the SPM's capacity index is. The capacity index is a numeric value, with possible values of 0, 1, or 2, corresponding to regular, enhanced and premium capacity, respectively.

The new SPMOVL D group will have 18 OM registers that give metrics on the SPM flow control system and the system overload control component. All OM registers that apply to the system overload control component start with an 'S', all others apply to the flow control system:

Flow Control Peg	SOC Peg	Description
OVL DNUM	SOVL DNUM	Number of times the system entered overload. For SOC (system overload control), this means the CM is in beyond_capacity state.
OVL DPNUM	not applicable	Number of times the SPM entered 'overload pending'.
OVL DUSG	SOVL DUSG	For Flow control, OVL DUSG represents the number of seconds the system was in overload. For SOC, SOVL DUSG represents the number of messages that were processed by SOC while the CM was in a beyond_capacity state.
OVL DPUSG	not applicable	Number of seconds the SPM was in 'overload pending'.
CLSDLYD	SCLSDLYD	The number of calls delayed by the two systems. When flow control and SOC are active, this will be equal to the number of new originations.
CLSDND	SCLSDND	In flow control, CLSDND represents calls that were denied due to there being too many calls in the flow control system, while CLSPTQ represents calls denied because of too many messages on a PTQ. In SOC, these two registers are combined into a single 'Calls Denied' register that counts calls that were tossed regardless of the reason. This register in SOC includes origination messages that were counted in SMSGPTQ and SHDROVFL (see below).
CLSABDN	SCLSABDN	Calls in either system that were abandoned by the client. Normally the abandon message comes from call processing on the Core.
CLSMSC	not applicable	Calls lost to miscellaneous resource failures.
not applicable	SNUMORIG	Total number of originations passing through SOC (delayed or not).
not applicable	SMSGLOST	Number of messages lost because of SOC system limits (includes SMSGPTQ and SHDROVFL)
not applicable	SMSGPTQ	Number of messages of any type that were lost due to PTQ overflow.
not applicable	SHDROVFL	Number of messages of any type that were lost due to SOC header array overflow.

All of the above OMs will be presented in OMSHOW on a per-node basis. The 'Performance' section of this book gives details about the new and the changed OM groups.

AMA/Billing information (AM)

Not applicable.

Glossary

Term	Description
PTQ	Per Terminal Queue - in SOC (System Overload Control) and Spectrum flow control, this is a queue that stores messages that are to be delivered to a given terminal ID.
SOC	An overloaded acronym that can mean either System Overload Control or Software Optionality Control, depending on the context.

References

A00002431 - Core/SPM Software Optionality Control implementation, available elsewhere in this document.

Fault Management for A00002432

Fault management strategy

This activity introduces a new core log (SPM 399) for flagging the overload conditions in the SPMs. This log is generated whenever an SPM enters/leaves an overload condition. The reason and the action for the craft are displayed in the log so that some action can be taken to rectify the condition. In addition, some diagnostic information for the designer is also printed in the log.

Fault management tools and utilities

LOGUTIL in the core is the standard tool for looking at the logs. The commands for looking for the new log SPM 399 are given below.

CI: logutil; open spm 399;back all

Logs

Explanation

Log Title: SPM 399

Name: SPM Overload Report

Description: This log is generated whenever an SPM enters/leaves a pre-defined overload condition. The overload conditions are given in section 12.3.4, Table 1.

Event type: This log will have a severity of 'Minor' when the SPM enters the overload condition and a severity of 'No alarm' when the SPM leaves the overload condition. A 'Minor' severity will show one asterisk in the first line of the log and a 'No alarm' severity will show none.

Format

```
<LABCLLI> <*> SPM399 <MMdd hh:mm:ss SSSS> TBL SPM Overload Report
SPM <xx> CEM <y> : <Activity> <state> Time: <hh:mm:ss.SSS>
Reason: <Reason string>
Prev: <previous state> Curr: <current state> Diagnostic: <#HHHH>
Action: <Action string>
Location: SPM <SPM no> Type: <Type> Fabric: <Fabric>
```

The last line shown in the log format will be present only when the SPM_ENHANCED_OUTPUT office parameter in OFCVAR is activated.

Example

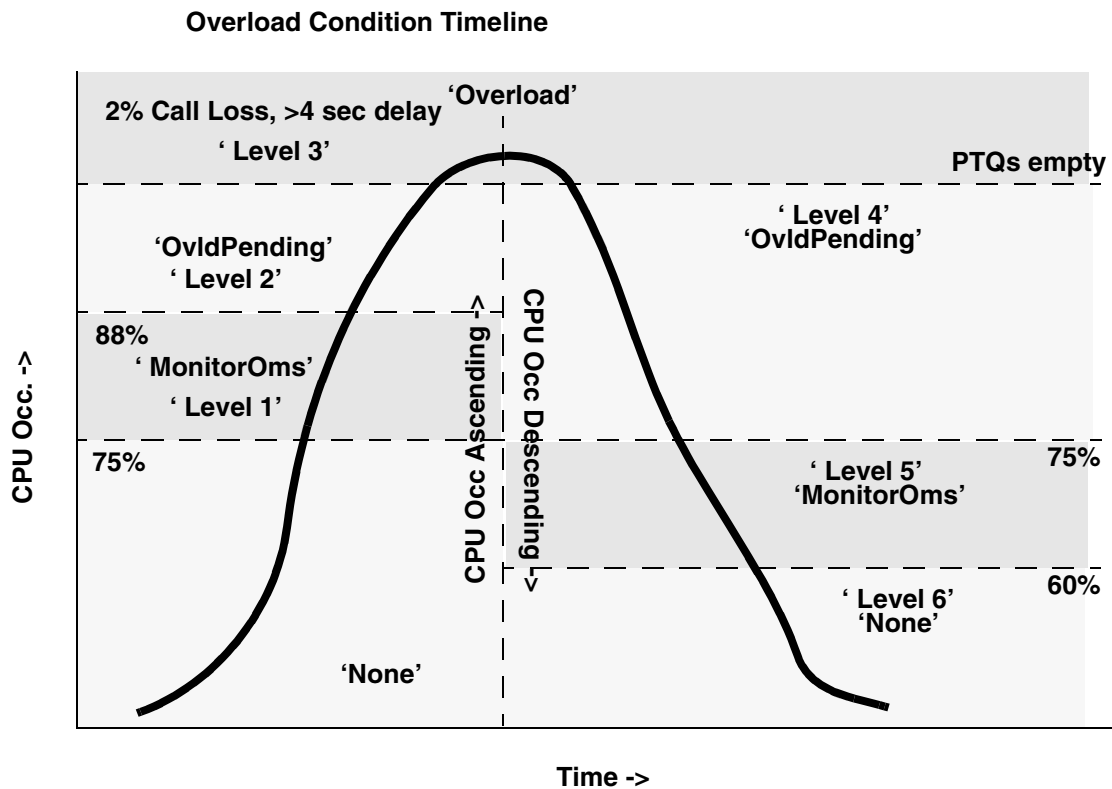
The following two examples show how the log will look like for the onset of an overload condition and for the clearing of an overload condition.

Example of the log when entering an overload condition

```
RSN06BPINDY1 * SPM399 APR25 11:01:06 9256 TBL SPM Overload Report
SPM 2 CEM 1 : A INSV Time: 11:01:06.685
Reason: CEM in Overload Pending state
Prev: None Curr: OvldPending Diagnostic: #0C2B
Action: Check SPMACT and SPMOVLD OMs.
Location: SPM 2 Type: SMG4 Fabric: ATM
```

Example of the log when clearing an overload condition

```
RSN06BPINDY1 SPM399 APR25 11:01:06 9256 TBL SPM Overload Report
SPM 2 CEM 1 : A INSV Time: 11:01:06.685
Reason: Overload cleared.
Prev: OvldPending Curr: None Diagnostic: #0000
Action: None.
```



The overload control mechanism has four different levels; two when going into overload and two when leaving overload.

Level 1: When Application + System Occupancy goes over 75%

- Check Overload OMs MIP (maintenance in progress) indicator is seen in the MAP (Maintenance and Administration Position), when the active CEM is posted.
- No effect on processing of calls (no call flow control).
- SPM399 'SPM Overload Report' log with a blank (no alarm) alarm level and reason 'Overload OMs initiated' is generated
- No alarm against the SPM node or CEM card.

Level 2: When Application + System Occupancy goes over 88%

- Overload Pending MIP indicator is seen in the MAP, when the active CEM is posted.
- No alarm against the SPM node or CEM card.
- SPM399 'SPM Overload Report' log with an alarm level of 'Minor' and reason 'CEM in Overload Pending state' is generated

- Call flow control is initiated: Messages from new calls are queued. One queued message from new calls is handled for every 10 messages from calls in progress.

Level 3: When >2% of calls are lost, or any calls are delayed > 4 seconds

- Overload MIP indicator is seen in the MAP, when the active CEM is posted.
- Unit state changes to ISTB (In-Service Trouble)
- SPM500 reporting the SPM state change.
- SPM399 'SPM Overload Report' log with an alarm level of 'Major' and reason 'CEM experiencing Overload' is generated
- Call flow control continues. One queued message from new calls is handled for every 10 messages from calls in progress.

Level 4: When the backlog of CallP messages in flowcontrol are processed. (CallP FlowControl PTQ empty.)

- Overload pending MIP indicator is seen in the MAP, when the CEM is posted.
- Unit state changes back to INSV (In-Service)
- SPM500 log reporting the SPM state change.
- SPM399 'SPM Overload Report' log with an alarm level of 'Minor' and reason 'CEM in Overload Pending state' is generated
- Call flow control continues. One queued message from new calls is handled for every 10 messages from calls in progress.

Level 5: When Application + System Occupancy goes below 75%

- Check Overload OMs MIP indicator is seen in the MAP, when the CEM is posted.
- SPM399 'SPM Overload Report' log with reason 'Overload Pending cleared' is generated
- Call flow control increases handling of originations: One queued message from new calls is handled for every three messages from calls in progress. Messages from new calls are no longer queued.

Level 6: When Application + System Occupancy goes below 60% (The application occupancy is set to this level to avoid the risk of toggling back and forth between level 1 and level 6)

- Overload OMs Started MIP indicator is cleared.
- SPM399 'SPM Overload Report' log with a blank (no alarm) alarm level and reason 'Overload cleared' is generated

- Call flow control increases handling of originations: One queued message from new calls is handled for every two messages from calls in progress.

Note: Application and System Occupancy is calculated during the last minute interval.

Field descriptions

The following table gives the field descriptions for the variable fields (fields within '< >' in the "Format" section of this document) of the new log.

Field descriptions

Field	Value	Description
LABCLLI	The CLLI of the office where the log is getting generated	
Priority of Alarm	Two asterisks (**), one asterisk (*) or empty space	Two asterisks (**) appear for a log of 'Major' severity, one asterisk (*) appears for a log of severity 'Minor' and empty space appears for a log of severity 'No Alarm'.
MMMd d hh:mm:ss	MMM - JAN to DEC dd - 01 to 31 hh - 00 to 23 mm - 00 to 59 ss - 00 to 59	Date and Time when the log was generated in the core.
SSSS	0000 to 9999	Log serial number.
xx	00 to 85	SPM number for which the log is generated.
y	0,1	CEM number of the SPM for which the log is generated.
Activity	A,I	Activity of the CEM. 'A' for Active and 'I' for Inactive.
State	INSV,ISTB,MANB,SYSB	State of the CEM.
hh:mm:ss.SSS	hh - 00 to 23 mm - 00 to 59 ss - 00 to 59 SSS - 000 to 999	Time when the error/error-clearing event happened in the SPM. This time will be earlier than the time that appears on the first line because the event happens in the SPM first and then the core generates the log.

Field descriptions

Field	Value	Description
Reason	1) "Overload OMs initiated" 2) "CEM in Overload Pending state" 3) "CEM experiencing Overload" 4) "Overload Pending cleared" 5) "Overload cleared"	These are the four possible strings that can appear in the 'Reason' field of the log. The first three reasons are for error scenarios and the fourth one is for the error-clearing scenario.
Prev	1)"None" 2) Man-at-arms 3)"OvldPending" 4)"Overload"	This field gives the overload condition of the SPM before the error/error-clearing event happened.
Curr	1)"None" 2) MonitorOMs 3)"OvldPending" 4)"Overload"	This field gives the current overload condition of the SPM.
Diagnostics	"#0000" to "#FFFF"	This field is for the designers who are doing the trouble-shooting. The craft need not look in to this field.
Action	1)"Check SPMACT and SPMOVL D OMs." 2) "Contact your next level of support." 3)"None."	This field gives the craft information on the action that needs to be taken. The string 1) is for logs generated for "Check OMs" and "Overload Pending". String 2) is generated in addition to String 1) when an "Overload" event occurs. The last string is for logs generated for an error-clearing scenario.
SPM no	00 to 85	SPM number
Type	DMSCP,SMG4,IW	Variant of the SPM
Fabric	ATM,IP,ENET	The switching fabric

The 4 reason strings correspond to the following 4 conditions respectively.

- 1) When the CPU occupancy exceeds 75%
- 2) When flow control is activated. The CPU threshold for this is 88%. If the SPM was previously in Overload, it reverts to Overload Pending when Flow Control's PTQs are empty.
- 3) Once 2% of calls are lost, or a call is delayed for > 4 seconds, while in flow control
- 4) When CPU occupancy drops below 75%
- 5) When CPU occupancy drops below 60%

Action

The 'Action' field of the log contains the action that is needed to be taken by the craft. For the situations when the SPM is leaving an overload condition, the 'Action' field will have 'None' and no action need be taken.

Associated Operational Measurements

In the OM group SPMOVL, the OVLDNUM register is pegged when the SPM enters the 'Overload' condition and register OVLDUSG maintains the number of seconds the SPM was in the 'Overload' condition in the present OM collection interval. Similarly, the register OVLDPNUM is pegged when the SPM enters the 'Overload Pending' condition and register OVLDPUSG maintains the number of seconds the SPM was in the 'Overload Pending' condition in the present OM collection interval.

Performance for A00002432

Performance management strategy

Customers, field support and design must have a means of monitoring and troubleshooting the overload conditions that lead to call processing problems in the Spectrum Peripheral Module (SPM). This activity introduces some means to do the same. SPM variants supported by this activity are DMSCP, SMG4 (also called MG4K), IW Bridge and IW DPT. The following performance monitoring components are introduced.

1. A new OM group SPMOVL is added to provide aggregate overload statistics of each SPM
2. A new register CAPINDEX is added to the existing OM group SPMACT to display the capacity level at which the SPM is running. (Refer to ACT.A00002431 in the FMDOC for the feature which enabled SPMs to run at three different capacity levels)

Performance management tools and utilities

PM information in general can be accessed with the following tool.

- DMS OM system (i.e. OMSHOW command)

This command can be used as follows on the CI prompt.

CI: OMSHOW SPMOVL ACTIVE

This will display the registers of SPMOVL OM group for which the statistics is being gathered.

Since the OM registers are incremented on the SPM, the 'active' registers will not have the most up-to-date information. At the end of each OM collection interval, the latest register values from the SPM are uploaded to the core.

CI: OMSHOW SPMOVL D HOLDING

This will display the registers of SPMOVL D OM group with the contents of the previous collection period.

It is recommended to use the OMSHOW command with the 'HOLDING' option.

Operational Measurements

The following table gives the list of new and modified OM groups as a result of this activity.

List of New/Modified OM groups

Group Name (acronym)	Group Name (expanded)	New/Modified	Registers
SPMOVL D	Spectrum Overload statistics	New	OVLDNUM OVLDPNUM OVLDUSG OVLDPUSG CLSDLYD CLSDND CLSPTQ CLSABDN CLSMSC SOVLDNUM SOVLDUSG SCLSDLYD SCLSDND SCLSABDN SNUMORIG SMSGLOST SMSGPTQ SHDROVFL

Group Name (acronym)	Group Name (expanded)	New/Modified	Registers
SPMACT	Spectrum Occupancy statistics	Modified (New register given in bold)	CEMSYSHI CEMAPPHI CEMBAKHI AVGCEMSY AVGCEMAP AVGCEMBK ORIGHI TERMHI AVGORIG AVGTERM TOTLORIG TOTLTERM NUMREPTS CAPINDEX

SPMOVLD

OM description

SPMOVLD - Spectrum Overload Statistics

The new SPMOVLD group will have 18 OM's that give metrics on the SPM flow control system and the system overload control component. All OM's that apply to the system overload control component start with an 'S', all others apply to the flow control system.

The actual peg counts and usage counts (accurate to one second) are accumulated on the peripheral and then uploaded to the OM group using the Spectrum OM Transfer System (SOTS).

Release history update

OM group SPMOVLD is introduced in SN07 as part of this feature.

Group structure

OM group SPMOVLD provides one tuple for each SPM (as datafilled in table MNNODE).

Key field: <spm_no>

- <spm_no> is an integer in the range {0 to 85}.

The following figure shows OM group SPMOVLD as displayed on the MAP terminal.

OM Group Display for SPMOVL

```

>omshow spmovld holding

SPMOVL

CLASS: HOLDING
START:2003/04/27 08:23:57 SUN; STOP: 2003/04/27 08:30:00 SUN;
SLOWSAMPLES:          3 ; FASTSAMPLES:          24 ;

      INFO (SOTS_NODE_INFO_TYPE)
      OVLDNUM   OVLDPNUM   OVLDUSG   OVLDPUSG
      CLSDLYD   CLSDND    CLSPTQ    CLSABDN
      CLSMSC    SOVLNUM    SOVLUSG    SCLSDLYD
      SCLSDND   SCLSABDN   SNUMORIG   MSGGLOST
      MSGGPTQ   SHDROVFL

0
      SPM  0
           0
           0
           0
           0
           0
           0
           0
           0
           0

```

Associated OM groups**SPMACT**

The register CAPINDEX in the OM group SPMACT gives the capacity level at which the SPM is running. The overload conditions existing in an SPM depend on this capacity level.

If there is a PEC mismatch between what is datafilled in MNCKTPK and the actual card in the CEM slot, the CAPINDEX register for an SPM may not match what is datafilled in MNNODE. That is, if an SPM is datafilled as having 'premium' capacity and one of the CEMs is an LX82AA card, then the CAPINDEX register will indicate that the SPM is running at 'standard' capacity, effectively overriding the datafill.

A new CI tool is available called SPMCPCAP - this tool will indicate what the datafilled capacity level is for a given SPM. For more information on this tool, please refer to feature A00002431's design documentation.

Associated functional groups

None.

Associated functionality codes

Not Applicable.

OM group registers logic flow chart

Not Applicable.

Registers

Details of the registers in SPMOVL D are given in the following table. Peg registers keep a count of a particular event and usage registers keep a count of the time (in seconds) for which a particular condition persisted.

Registers in the new OM group SPMOVL D

Register Name (acronym)	Register Name (expanded)	Type of the register	Associated Registers	Associated Logs
Description				
OVL DNUM	Overload Number	Peg		SPM 399
Gives the number of times the node entered overload due to the flow control component.				
OVLDPNUM	Overload Pending Number	Peg		SPM 399
Gives the number of times the node entered 'overload pending' due to the flow control component				
OVL DUSG	Overload Usage	Usage		
Gives the number of seconds the node was in overload due to the flow control component.				
OVLDPUSG	Overload Pending Usage	Usage		
Gives the number of seconds the node was in 'overload pending' due to the flow control component				
CLSDLYD	Calls Delayed	Peg		
Gives the number of calls delayed by the node due to the flow control component				
CLSDND	Calls Denied	Peg		
Gives the number of calls that were denied due to there being too many calls in the flow control component.				
CLSPTQ	Calls Per Terminal Queue	Peg		
Gives the number of calls denied because of too many messages on a Per Terminal Queue in the flow control component.				
CLSABDN	Calls Abandoned	Peg		
Gives the number of calls that were abandoned by the node in the flow control component.				
CLSMSC	Calls Miscellaneous	Peg		

Registers in the new OM group SPMOVL

Register Name (acronym)	Register Name (expanded)	Type of the register	Associated Registers	Associated Logs
Description				
Gives the number of calls lost to miscellaneous resource failures in the flow control component.				
SOVLNUM	SOC Overload Number	Peg		
Gives the number of times the system entered overload (the CM is in beyond_capacity state)				
SOVLUSG	SOC Overload Usage	Peg		
Gives the number of messages that were processed by the system overload component while the CM was in a beyond_capacity state.				
SCLSDLYD	SOC Calls Delayed	Peg		
Gives the number of calls delayed by the system overload component.				
SCLSDND	SOC Calls Denied	Peg		
Gives the number of calls that were tossed regardless of the reason. This register includes origination messages that were counted in SMSGPTQ and SHDROVFL.				
SCLSABDN	SOC Calls Abandoned	Peg		
Gives the number of calls that were abandoned by the system due to the system overload component.				
SNUMORIG	SOC Number of Originations	Peg		
Gives the number of originations passing through the system overload component (delayed or not).				
SMSGLOST	SOC Messages Lost	Peg		
Gives the number of messages lost because of system overload control limits (includes SMSGPTQ and SHDROVFL)				
SMSGPTQ	SOC Message PTQ	Peg		
Gives the number of messages of any type that were lost due to PTQ overflow.				
SHDROVFL	SOC Header Overflow	Peg		
Gives the number of messages of any type that were lost due to system overload control header array overflow.				

SPMACT**OM description**

SPMACT - Spectrum Occupancy Statistics

Release history update

OM group SPMACT is modified to include a new register CAPINDEX, in SN07 as part of this feature.

Group structure

OM group SPMACT provides one tuple for each SPM (as datafilled in table MNNODE).

Key field: <spm_no>

- <spm_no> is an integer in the range {0 to 85}.

The following figure shows OM group SPMACT as displayed on the MAP terminal. The new register CAPINDEX is made bold in the figure (but not on the actual display)

OM Group Display for SPMACT

```
>omshow spmact holding
SPMACT
CLASS: HOLDING
START:2003/04/28 13:00:00 MON; STOP: 2003/04/28 13:30:00 MON;
SLOWSAMPLES:          18 ; FASTSAMPLES:          180 ;

      INFO (SOTS_NODE_INFO_TYPE)
      CEMSYSHI  CEMAPPHI  CEMBAKHI  AVGCEMSY
      AVGCEMAP  AVGCSEMBK  ORIGHI    TERMHI
      AVGORIG   AVGTERM   TOTLORIG  TOTLTERM
      NUMREPTS  CAPINDEX

0
      SPM  1
           1          1          97          1
           1          97          0          0
           0          0          0          0
           2          1
```

Associated OM groups

None.

Associated functional groups

None.

Associated functionality codes

Not Applicable.

OM group registers logic flow chart

Not Applicable.

Registers

Details of the new register added in SPMACT OM group are given in the following table. The type of the register is given as 'Index', which means that it is not a regular Peg/Usage kind of a register. This register gives the capacity index of the particular SPM.

New register in SPMACT OM group

Register Name (acronym)	Register Name (expanded)	Type of the register	Associated Registers	Associated Logs
Description				
CAPINDEX	Capacity Index	Index		
Gives the capacity level at which the SPM is running. This can take values 0,1 or 2. For non-DMSCP variants of SPMs, this can take only 0 and 2 as values. Indices 0,1 and 2 refer to Standard, Enhanced and Premium capacities respectively. Non-DMSCP variants of SPMs include SMG4, IW-DPT and IW-BRDG-ONLY.				

Glossary

PTQ - Per Terminal Queue
 SOC - System Overload Control
 SPM - Spectrum Peripheral Module

Product = CS 2000**A00002433 -- XA-Core Baseline Control (Succession on DMS)*****Functional Description***

Field baseline implies the minimum HW/FW release/version that Nortel Networks requires for reliable XA-Core operation. The HW field baseline is updated due to a class 'A' HW change. The FW field baseline is updated due to a severe FW bug.

1. HW baseline compatibility is based on PEC presence in table PECINV and meeting Release constraints.

- FW baseline compatibility is based on PEC presence in table FWINV and FW/DLL meeting Version constraints.

See *“Activity Behavior” on page 454* for detailed info.

Activation

The activity is activated by default, in all XA-Core loads.

Baseline Defaults

XA-Core **hardware** baselines are stored in table **PECINV**.

XA-Core **firmware** baselines are stored in **New table FWINV**.

These tables are provisioned in the loadbuild stage of software delivery.

Tables PECINV and FWINV are user modifiable, but caution must be exercised in making any changes, since the changes can impact the system, as further described below. Both tables are NOT restored over an ONP. CSP20 defaults are shown in the following table. HW/FW exceptions can be provisioned to indicate a HW release or FW version which **must** not be allowed. Any release/version greater than or equal to the baseline release/version is OK to use, as long as it is NOT listed as an exception. There are currently no exception values.

CSP20 Baseline HW Releases, FW Versions

Grp	Type	PEC	PECINV HW Release	FWINV FW Version ^a [s]:	
			Baseline	FW Baseline	DLL Baseline
Cards	PE	NTLX02AA	n/a	Not supported	
		NTLX02CA	01	XAPE01AG	Not user modifiable
		NTLX02DA		XAPE02AB	
	IOP	NTLX03AA	28	XAIO01AK	N/A
		NTLX03AB	03		
		NTLX03BA	28		
		NTLX03BB	03		
	HIOP	NTLX04AA	01	XHIO02AA	XHIO02AH
		NTLX04BA			
		NTLX04CA		XHIO02AH	
		NTLX17AA		XHIO03AA	
Pklt	CMIC	NTLX05AA	n/a	Not supported	
		NTLX05AB	01	PK12CE12	N/A
	AMDI	NTLX05BA			
	ETHR	NTLX09AA		EP14D003	
No FW	SM	NTLX14CA		N/A	

CSP20 Baseline HW Releases, FW Versions

	DISK	NTLX06AA			
		NTLX06AB			
		NTLX06AC			
	TAPE	NTLX07AA			
		NTLX07BA			
	RTIF	NTLX08AA			
		NTLX08AB			

a. There are currently no hardware or firmware exceptions.

Activity Behavior

HW and FW baseline behavior is summarized below for Hardware (PECINV) and Firmware (FWINV) respectively.

Details follow in subsequent sections.

Baseline Behavior - PECINV vs. Hardware

Input Conditions		Behaviour		
PEC	Hardware Rel vs. PECINV Rel	RTS	Baseln Alarm	SREx
Not in PECINV	n/a	Fail	Raise	No SREx for X if X non-baseline. X=PE&SM IO
IN PECINV	= exception Rel OR < baseline Rel	Fail	Raise	No SREx for X if X non-baseline. X=PE&SM IO
	>= baseline Rel	Pass	Lower	OK

Baseline Behavior - FWINV vs. Firmware

Input Conditions		Behaviour		
PEC	Firmware Ver vs. FWINV Ver	RTS	Baseln Alarm	SREx
NOT in FWINV: pe, iop, hiop cards cmic, amdi, ethr pkts	n/a	Fail	Raise	No SREx for X if X non-baseline. X=PE&SM IO
IN FWINV pe, iop, hiop ^a card, cmic, amdi, ethr pkts	= exception Ver	Fail	Raise	No SREx for X if X non-baseline. X=PE&SM IO
	< baseline Ver	Pass ^b	Raise	OK
	>= baseline Ver	Pass	Lower	OK
NOT in FWINV: sm, disk, tape, rtif	don't care. FRU have no FW	Pass	Lower	OK

a. HIOP: Both FW & DLL must pass baseline checks.

b. FW/DLL updated AFTER unsplit, so we must RTS, since later SREx/ManB/Reload would leave a previously working FRU OOS.

Baseln Alarm

New Baseln Major alarm is used to indicate that at least one non-baseline (Hardware or Firmware) FRU is present in the system.

Baseln alarm raising or lowering is triggered by:

1. Manual “MAPCI;MTC;XAC;QUERY CARD” of a below baseline FRU
2. Manual “MAPCI;MTC;XAC;QUERY SHELF”
3. System initiated query - occur periodically and after certain events
4. Manual “MAPCI;MTC;XAC;<level>;UNEQ” after FRU BSY, then pull

The alarm is lowered when all FRU have baseline compatible HW and FW⁸.

To get a list of the non-baseline FRU responsible for the alarm, type, from MAPCI;MTC;XAC level:

1. ALARM Baseln - lists the problem FRU, but no baseline specific info
2. QUERY SHELF - ALL FRU info in the XA-Core shelf.
Look for “*” in Hardware and Firmware “OK” columns.

Related Logs

1. **New XAC337 (FLT)** - generated when the Baseln alarm is first raised, and whenever the list of non-baseline items changes, and is non-empty.
The log lists the non-baseline FRU with related baseline information.
2. **New XAC637 (INFO)**- generated when the Baseln alarm is lowered, indicating all FRU are now baseline compatible. The log is NOT generated due to a restart clearing the alarm, as discussed in *“Limitations and restrictions” on page 457*.
3. **XAC415** - generated when SREx Baseline precheck determines that a PE or SM card is non-baseline, so no SREx is permitted.
New reason added: “XACore Hardware or Firmware is not at baseline”.

SREx Impact

SREx is **bypassed** and an XAC415 log generated if a PE or SM card is not at baseline. Subsequent AutoDump is disallowed, since no image test was run.

OOS IO tests are bypassed if ONLY IO related FRU are non-baseline.

Table Control

Table PECINV - **new warning** is displayed if the user attempts a change or delete operation on a tuple with a subsystem of XACHW.

Warn that FRU WILL NOT RTS if the tuple is deleted or if the baseline or exception list change is not compatible with existing/newly inserted hardware.

8. Or any restart occurs. See *“Limitations and restrictions” on page 457*

New table FWINV - contains firmware (and DLL) baseline(s) indexed by PEC. Also provides the ability to indicate a FW release which should not be allowed if declared an “exception” version(s).

Table XAFWLOAD - **new warning** is displayed if the user attempts to provision a non-baseline firmware loadname.

Warn that Baseln alarm will be raised after the FRU is RTS'd, if a non-baseline loadname is used.

OAM

From MAPCI;MTC;XAC level (or sublevels), QUERY SHELF output **adds** Hardware and Firmware baseline[s] and FRU status indicator (“OK”).

Any “*” in the OK column requires investigation.

The OK column entry is of the form “x” where x is:

1. **P*** = PEC not in table **PECINV**
2. **F*** = PEC not in table **FWINV**, and FRU has FW (and DLL - HIOP only)
3. **N*** = Not baseline compatible. I.e. Below baseline.
4. **X*** = Release/Version is an eXception Rel/Ver in table **PECINV/FWINV**
5. **I*** = Could not read MIM IDPROM, to get PEC/Rel.
This occurs during some maintenance activities.
Baseln alarm/log will NOT be generated solely from this info.
6. **Y** = Yes, this FRU is baseline compatible.

“HW-SW vintage” column is **removed** from QUERY SHELF output, to allow for new baseline information. Vintage is still visible from the QUERY CARD command.

CI “POLL SHORT <dev1> <dev2>” is **enhanced** to show the output from a “QUERY SHELF” command. On a Supernode, it currently displays the output from MAPCI;MTC;CM;QUERYCM NOEMPTY.

XAC;QUERY SHELF is the XA-Core logical equivalent.

ONP Prechecks

The following **ONP precheck steps are enhanced** to detect non-baseline FRU on the active image. The steps fail if the equivalent of a QUERY SHELF displays “P*, F*, X* or N*”, as previously described in *“OAM” on page 456*.

1. “ONPREADY”, step “DISPLAY_PEC_INFO”
2. “SWUPGRADE READY; START”, step “VERIFY_SN_PECs_INFO”
3. “BCSUPDATE; PRECHECK”, step “DISPLAY_PEC_INFO”

ONP Pre-SWACT

While split, a **new pre-SWACT check** requests/receives the new-side PECINV (hardware baseline) data, to see if existing HW meets new-side baseline requirements. Alert the user if it does not.

FW checks are NOT done, since FW is currently updated in the first available Mtc window AFTER the unsplit succeeds. The Baseln Major alarm WILL be raised shortly after the unsplit, if the FWINV baselines have changed from one CSP release to another - this is a reminder to do the suggested FW/DLL upgrades.

Hardware Requirements or Dependencies

This activity applies only to XA-Core.

The XA-Core must be at hardware baseline for new ONP prechecks to pass. Hardware baselines are detailed in “XA-Core Maintenance Manual” (NTP 297-8991-510).

A patch will be developed for each of CSP17-CSP19, in order to determine the switch’s current hardware baseline status. The intent is to avoid any ONP baseline issues when upgrading to CSP20-CSP22.

Software Requirements or Dependencies

No new software dependencies.

Since XA-Core firmware is upgraded after the ONP, below baseline firmware must be permitted to RTS; however, it will cause the Baseln alarm to be raised. Firmware baselines are detailed in the “DMS-100 Family NA100 Peripheral Module Software Release Document” (NTP 297-9081-599).

Limitations and restrictions

New Baseln alarm is cleared over all restarts. The alarm is re-raised when the non-baseline item is queried manually or by the system (within 10 minutes).

Since XA-Core firmware is upgraded after the ONP, below baseline firmware must be permitted to RTS; however, it will cause the Baseln alarm to be raised.

No incompatibilities with other features.

Interactions

Table XAFWLOAD - a new warning is displayed if the user attempts to provision a non-baseline firmware loadname.

Warn that Baseln alarm will be raised after the FRU is RTS’d.

Table PECINV - a new warning is displayed if the user attempts a change or delete operation on a tuple with a subsystem of XACHW.

Warn that FRU **WILL NOT** RTS if the tuple is deleted.

Warn that FRU **MAY NOT** RTS if the baseline or exception list change is not compatible with existing/newly inserted hardware.

Applicable customer facing sections

Fault Management

Logs _X_

Alarms _X_

Configuration

Data Schema _X_

User Interface _X_

Element Management _n/a_

Security _n/a_

Service Order _n/a_

Office Parameters _n/a_

Accounting (includes AMA billing) _n/a_

Performance (includes operational measurements) _n/a_

Realtime _n/a_ Mtc Code

Engineering Information _X_

Glossary

Term	Description
Baseline	The minimum HW/FW release/version that Nortel Networks requires for reliable XA-Core operation.
DLL	DownLoadable Loader
Exception	A HW release/FW version greater than or equal to the baseline release/version is OK to use, as long as it is NOT listed explicitly as an exception. I.e. an exception indicates HW/FW which must not be used.
FRU	Field Replaceable Unit - card or IOP packet
FW	FirmWare
HW	HardWare
IOP	Input Output Processor Card

Term	Description
ManB	Manual Busy
MIM	Module Information Memory
ONP	One Night Process
OOS	Out Of Service
PE	Processor Element Card
RTS	Return To Service
SM	Shared Memory Card
SREx	System Routine Exercise

Fault Management for A00002433

Fault management strategy

Baseln Alarm

System alarm “Baseln” is raised whenever any XA-Core Field Replaceable Unit (FRU) installed in the shelf is not at Hardware (HW) or Firmware (FW) baseline. Only the Major level is used.

“ALARM Baseln” command will list the non-baseline components from MAPCI;MTC;XAC level, or its sub-levels.

1. Baseln alarm is raised due to HW issue when:
 - a. Product Equipment Code (PEC) is missing from table PECINV
 - b. Actual PEC HW release is less than PECINV baseline release
 - c. Actual PEC HW release equals one of the PECINV exception releases
2. Baseln alarm is raised due to FW issue when:
 - a. PEC is missing from table FWINV, and associated FRU has FW
 - b. Actual PEC FW version is less than FWINV baseline version
 - c. Actual PEC FW version equals one of the FWINV exception releases

Logs

1. New XAC337 FLT log is produced when:
 - a. Baseln alarm is first raised
 - b. Baseln alarm still raised, and non-baseline component list changes. The log lists all of the non-baseline components known.

2. New XAC637 INFO log is produced when Baseln alarm is cleared, due to an empty list of non-baseline components.
3. Existing XAC415 log adds “not at baseline” reason for not running the SREx test.

Fault management tools and utilities

MAPCI;MTC;XAC; ALARM BASELN

Returns a list of field replaceable unit (FRU) which are not at HW or FW baseline.

MAPCI;MTC;XAC; QUERY SHELF

Returns a list of FRU installed in the XA-Core shelf. Those FRU which are not at HW or FW baseline are indicated with a “*” in the OK column[s] - see CN section for more info.

LOGUTIL; OPEN XAC 337/637/415

XAC337 - list of components not at baseline

XAC637 - all components now at baseline

XAC415 - system state at time SREx test was bypassed, due to HW or FW not being at baseline.

Update HW

BSY, remove, and replace with correct PEC/release.

Update FW

FW is updated from MAPCI;MTC;XAC; <level> as per MTC manual steps, summarized briefly here:

- a. update table XAFWLOAD PEC/NEW tuple to baseline FW (and HIOP DLL) version found in table FWINV
- b. BSY <pos>; LOADFW <pos> FILE NEW; RTS <pos>
(Note that RTS downloads HIOP DLL during OOS TST)
- c. update table XAFWLOAD by changing current to old, new to current

Logs

Three logs are detailed below: XAC415, XAC337, XAC637.

Explanation

Log Title: XAC415

Name: INFO Routine Exercise (REx) Report

Description: Generated when SREx is bypassed, due to:

One or more non-baseline PE/SM card being found in the XA-Core shelf.
 SREx is not impacted by FW being BELOW baseline on the PE, since FW is updated AFTER the ONP; however, SREx is not run if the PE/SM's entry is absent from FWINV, or it uses an exception version.

Event type: Log severity = MAJOR

Format

XAC415 Format and Example

<switch> XAC415 <mmdd hh:mm:ss ssd> INFO Routine Exercise (REx) Report		
INITIATOR	CLASS	RESULT
System	<class>	Not Run
Reason:<reason>		

** XAC415 JAN08 19:47:22 5201 INFO Routine Exercise (REx) Report		
INITIATOR	CLASS	RESULT
System	Full	Not Run
Reason: XA-Core HW (PECINV) or FW (FWINV) is not at baseline		

Field descriptions

Field	Value	Description
<class>	Existing list: "BASE", "ALL", "FULL", "IO", "PE", "SM"	SREx class requested.
<reason>	"XA-Core HW (PECINV) or FW (FWINV) is not at baseline" <other existing reasons>	Self-explanatory

Action

Investigate non-baseline components using:

1. LOGUTIL; OPEN XAC337 or
2. MAPCI;MTC;XAC;ALARM BASELN.

Update HW or FW/DLL as required.

Associated Operational Measurements or Performance Measurements

None.

Explanation

Log Title: XAC337

Name: FLT Baseln Alarm Raised

Description: Log is produced when:

- a. Baseln alarm is first raised
- b. Baseln alarm still raised, and non-baseline component list changes.
The log lists the non-baseline components known at generation time.

Event type: Log severity = MAJOR

Format

XAC337 Format and Example

Type	FRU	PEC+Release	BL	OK	Typ	Version	Baseline	OK

<fru> <pos> <pec+rel><rel><ok><fw_dll><fwname><fwname><ok>								

** XAC337 JAN15 22:55:35 7176 FLT Baseln Alarm Raised Card/packlets below have non-baseline HW and/or FW. Investigate items with "N*" or U* in OK column. - HW vs. PECINV - -- Firmware vs. FWINV -- Type FRU PEC+Release BL OK Typ Version Baseline OK ----- eg. HIOP 14 R NTLX14CA 01 02 N* FW XHIO02AH XHIO02AH Y DLL XHIO02AI XHIO02AH N* CMIC 4 R L NTLX05AB 01 01 Y FW PK12CE12 ?? N* PE 4 F NTLX02DA 01 ?? N* FW XAPE02AB XAPE02AB Y PE 5 F NTLX02AA 01 ?? U* FW XAPE02AB XAPE02AB Y								

```

** XAC337 <mmmmdd hh:mm:ss ssd> FLT Baseln Alarm Raised
Card/packlets below have non-baseline HW and/or FW.
Investigate items with "N*" or U* in OK column.
- HW vs. PECINV - -- Firmware vs. FWINV --

```

Field descriptions

Field	Value	Description
fru	Valid fru names: cards: pe, iop, hiop, sm pkIts: cmic, amdi, ethr, disk, tape, rtif	FRU (field replaceable unit) names. Bolded FRU have no FW.
pos	Slot number: 1-30 front/rear: F or R upper/lower: U or L	Position of FRU in XA-Core shelf.
pec	8 character alphanumeric. NTLXnnaa: n=0-9, a=A-Z	Product Equipment Code (PEC)
rel	2 character alphanumeric. "00" through "ZZ"	HW rel
OK	2 chars: "Y " = Yes - at baseline "N*" = Non-baseline	Indicates if HW and/or FW is baseline compatible.
fw_dll	FW or DLL	Indicates if following fw_name field is for FirmWare or DLL.
fw_name	8 character alphanumeric.	Firmware load name.

Action

See *"Action" on page 461*

Associated Operational Measurements or Performance Measurements

None.

Explanation

Log Title: XAC637

Name: INFO Baseln Alarm Cleared

Description: Log is produced when alarm was raised, but now lowered, since no longer any non-baseline components.

Event type: Log severity = NONE

Format

XAC637 Format and Example

```
<switch>      XAC637 <mmmd hh:mm:ss ssd> INFO Baseln Alarm Cleared
               <string>
```



```
XAC637 JAN15 23:13:26 4432 INFO Baseln Alarm Cleared
All XAC HW at PECINV baseline. All XAC FW/DLL at FWINV baseline.
```

Field descriptions

Field	Value	Description
string	All XAC HW at PECINV baseline. All XAC FW/DLL at FWINV baseline.	XA-Core now at baseline.

Action

See [“Action” on page 461](#).

Associated Operational Measurements or Performance Measurements

None.

Alarms

System alarm Baseln is added.

See [“Fault management strategy” on page 459](#) for alarm behavior, and associated logs. The components listed should be investigated, and likely replaced. ALARM Baseln output simply lists the problem FRU and locations. More useful information appears in XAC337 log/QUERY SHELF outputs.

The alarm is cleared when no XA-Core components are non-baseline.

The output format for MAPCI; MTC; XAC; ALARM BASELN lists those components which are non-baseline.

ALARM BASELN Format

Alarm	Severity	Status
SysBTh	<sev>	<Enabled/Disabled>
Cause	Resource	State Slot/Pk/Dev
<cause>	<res>	<st> <slot> <dev>
....		
<cause>	<res>	<st> <slot> <dev>
Where:		
<sev> = Cleared, Minor, Major, Critical		
<cause> = HW or FW is non-baseline.		
<res> = NIL, PE, SM, IOP, HIOP, Tape, Disk, RTIF, CMIC, AMDI, ETHR, RTIFp, RTIFp, AMDIp, CMICp, AMDIl, CMICl, ETHRp, ETHRl, TOD};		
<st> = ' ', INSV, ISTB, SYSB, CBSY, MBSY, SPLT, UNEQ		
<slot> = <slot number> + '<' ' F R>' + '<' ' L U>		
<dev> = '<' ' 0 1		

ALARM SysBTh Example - alarm OFF

Alarm	Severity	Status
Baseln	Cleared	<Enabled/Disabled>

ALARM SysBTh Example - alarm ON

Alarm	Severity	Status
Baseln	Major	Enabled
Cause	Resource	State Slot/Pk/Dev
HW or FW is non-baseline.	RTIF	INSV 15R U
HW or FW is non-baseline.	IOP	INSV 15R

Related documentation

XA-Core Maintenance Manual - 297-8991-510.

XA-Core Reference Manual - 297-8991-810.

Configuration for A00002433

Hardware and Software Requirements

This feature is intended to verify that an XA-Core meets baseline HW and FW requirements, that may vary from one SW release to another.

Initial Configuration

No configuration steps are required to enable this feature in CSP20. For CSP17/18/19, a patch must be developed which does a “precheck” to alert the user that they are not at HW baseline for CSP20, and that these components will not come into service if they were to continue with the unsplit. Documentation will also indicate the required HW PEC and HW releases required.

Office parameters

No new or modified office parameters.

Upgrade Impact

Dump and Restore

No dump and restore impact, as existing table PECINV, and new table FWINV are NOT restored over an ONP.

CSP20 XA-Core Baselines

HW baselines and optional exception releases are listed in table PECINV. FW baselines and optional exception versions are listed in table FWINV. XA-Core baselines are shown below - these should be added to customer ONP documentation. Used in ONP prechecks weeks prior to ONP, while unsplit: (a) ONPREADY, b) SWUPGRADE READY; START, c) BCSUPDATE; PRECHECK) as well as during ONP pre-swact checks, while split (BCSUPDATE; SWACTCI; PRESWACT):

XA-Core HW Baselines, CSP20 - Table PECINV

```

>TABLE PECINV; FORMAT PACK
>RANGE SSYSBASE
      2 SSYSBASE          SN_SSYS_BASELINE
TYPE IS SN_SSYS_BASELINE VECTOR OF UP TO 11 MULTIPLES WITH
      SUBSYS              SN_SUBSYSTEM_HW
      BASELINE            TABLE OF 2 CHAR'S
      EXCPTN              VECTOR OF UP TO 4 TABLES OF 2 CHAR'S

>LIST ALL (SSYSBASE GE XACHW)
TOP
PEC          SSYSBASE
-----
NTLX02CA (XACHW 01 $) $
NTLX02DA (XACHW 01 $) $
NTLX03AA (XACHW 28 $) $
NTLX03AB (XACHW 03 $) $
NTLX03BA (XACHW 28 $) $
NTLX03BB (XACHW 03 $) $
NTLX04AA (XACHW 01 $) $
NTLX04BA (XACHW 01 $) $
NTLX04CA (XACHW 01 $) $
NTLX05AB (XACHW 01 $) $
NTLX05BA (XACHW 01 $) $
NTLX06AA (XACHW 01 $) $
NTLX06AB (XACHW 01 $) $
NTLX06AC (XACHW 01 $) $
NTLX07AA (XACHW 01 $) $
NTLX07BA (XACHW 01 $) $
NTLX08AA (XACHW 01 $) $
NTLX08AB (XACHW 01 $) $
NTLX09AA (XACHW 01 $) $
NTLX12AA (XACHW 04 $) $
NTLX14CA (XACHW 01 $) $
NTLX17AA (XACHW 01 $) $
NTLX22AA (XACHW 07 $) $
NTLX22BA (XACHW 02 $) $
NTLX27AA (XACHW 01 $) $
BOTTOM

>COUNT (SSYSBASE GE XACHW)
BOTTOM
SIZE = 26

```

XA-Core FW Baselines, CSP20 - Table FWINV

```

>TABLE FWINV; FORMAT PACK
>RANGE FWBASE
  2 FWBASE          TFWINV_TUPLE
TYPE IS TFWINV_TUPLE VECTOR OF UP TO 2 MULTIPLES WITH
      FWTYPE        {FW,DLL}
      VERSION        TABLE OF 8 CHAR'S
      EXCEPTIONS     VECTOR OF UP TO 4 TABLES OF 8 CHAR'S

>LIST ALL
TOP
PEC          FWBASE
-----
NTLX02CA (FW XAPE01AG $) $
NTLX02DA (FW XAPE02AB $) $
NTLX03AA (FW XAIO01AK $) $
NTLX03AB (FW XAIO01AK $) $
NTLX03BA (FW XAIO01AK $) $
NTLX03BB (FW XAIO01AK $) $
NTLX04AA (FW XHIO02AA $) (DLL XHIO02AJ $) $
NTLX04BA (FW XHIO02AA $) (DLL XHIO02AJ $) $
NTLX04CA (FW XHIO02AH $) (DLL XHIO02AJ $) $
NTLX17AA (FW XHIO03AA $) (DLL XHIO03AA $) $
NTLX05AB (FW PK12CE12 $) $
NTLX05BA (FW PK12CE12 $) $
NTLX09AA (FW EP14D003 $) $
BOTTOM

>COUNT
BOTTOM
SIZE = 13

```

Pre-ONP checks (while usnplit)

Existing steps have been enhanced for XA-Core, and to check for non-baseline XA-Core HW/FW/DLL.

1. ONPREADY % Step "DISPLAY_PEC_INFO"
Step saves MAP output to file, then scans it for baseline failures.
2. BCSUPDATE; PRECHECK% Step "DISPLAY_PEC_INFO"
Step display MAP output to screen ONLY.
Step always "fails", so that user will manually scan for non-baseline indicators.
Override the step to continue, once all resources are at baseline.
3. SWUPGRADE READY; START % Step "VERIFY_SN_PECs_INFO"
Step saves MAP output to file, then scans it for baseline failures.

PRESWACT checks (while split)

A new preswact check is added, and run while the XA-Core is split. Active side queries are sent to inactive side for comparison against NEW PECINV baselines. Incompatible cards/packlets are sent back to active side for display. If list is nil, step passes, else preswact step fails.

PRESWACT - Baseline Check Behavior

ACTIVE SIDE	INACTIVE SIDE
-----	-----
1- Card/pklt query list -> Buf	
	Buf
2- preswact_transfer(PSEND, INITIAL) --->	
Invokes	3- Compare card/pklt vs NEW PECINV baseline
	Non-baseline items->Buf
	Buf
4- preswact_transfer(PRECEIVE)	<---
Pass: Display OK OR	
Fail: list problem card/pklt	

Sample output, when HW is NOT compatible with NEW side baselines:

Sample PRESWACT output - step XACORE_BASELN_CHECK

```
>BCSUPDATE; SWACTCI; PRESWACT
XACORE_BASELN_CHECK          executing
16 of 23 cards+packlets compatible with NEW SIDE baselines.

*****
** XACore resources incompatible with NEW baselines. **
** ABORT PRESWACT AND UPDATE RESOURCES TO MEET      **
** NEW BASELINES, ONCE SYSTEM IS UNSPLIT.           **
*****

Non-baseline XA-Core Resources vs NEW side:
-----
--HW vs. PECINV--
Type NT Loc  PEC+Release BL OK  Failure reason on NEW side
-----
Disk  2 F L   NTLX06AC 00 01 N* Below PECINV Baseline
IOP   17 F    NTLX03BB 02 03 N* Below PECINV Baseline
IOP    4 R    NTLX03AA 03 28 N* Below PECINV Baseline
CMIC   4 R L   NTLX05AB 00 01 N* Below PECINV Baseline
HIOP  14 R    NTLX04BA 00 01 N* Below PECINV Baseline
IOP   15 R    NTLX03AB 00 03 N* Below PECINV Baseline
RTIF  15 R U   NTLX08AB 00 01 N* Below PECINV Baseline

XACORE_BASELN_CHECK          not complete

Investigate and correct if needed.
```

Data schema (DS)

New/modified tables

Table name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
PECINV	CHANGED	UNCHANGED (NEW)
FWINV	NEW	NEW

Table Data Schema information

Name: PECINV

PECINV is changed in the following ways:

1. Maximum number of tuples is increased from 200 to 256.
2. Default datafill (added at loadbuild time using PLS DMSPL module EXTPECHWSUB) is updated:
 - a. Added new PECs and their correct baseline releases.
 - b. Corrected baseline release on some existing PECs.

Functional description

PECINV is intended to maintain the HW baseline PEC, release and exception releases for various subsystems.

Its data is accessed by:

1. CHECKMS CI - MSHW and STDHW subsystems only.
2. CHECKREL CI - all supported subsystems.
3. SREX - through run_hardware_monitor() check.
Only MSHW subsystem. has a target procedure bound currently.

Usage sequence and implications

No table dependencies. Current datafill order unchanged.

Size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
PECINV	0	256	Store for 256 tuples is pre-allocated in DSPROT. Each tuple approx 20 bytes

Datafill example

The following example shows sample datafill for table FWINV:

PECINV examples

```
PEC SSYSBASE
```

```
-----
```

```
1. NTLX02CA (XACHW 01 $) $
```

Table release history update

1. Extended maximum tuple range from 200 to 256.
2. Added missing PEC/releases to default datafill: (now 211 entries at IPL)
 - NTLX02DA XACHW 01 % ATLAS PE
 - NTLX03AB XACHW 03 % single width IOP card
 - NTLX03BB XACHW 03 % double width IOP card
 - NTLX04AA XACHW 01 % HIOP card - ETHR
 - NTLX04BA XACHW 01 % HIOP card - ETHR/AMDI
 - NTLX04CA XACHW 01 % HIOP card - ETHR/CMIC
 - NTLX05AB XACHW 01 % CMIC packlet
 - NTLX05BA XACHW 01 % AMDI packlet
 - NTLX06AC XACHW 01 % Disk packlet - 34.2 GB
 - NTLX07BA XACHW 01 % Tape packlet - 20 GB DDS4
 - NTLX08AB XACHW 01 % RTIF Packlet
 - NTLX09AA XACHW 01 % ETHR Packlet
 - NTLX17AA XACHW 01 % HIOP Card - CMIC/RTIF .
3. Corrected baseline releases on existing PECs:
 - NT9X13DE LIMHW 01 --> 03
 - NT9X63AA MSHW 01 --> 10
 - NT9X71AB LIMHW 00 --> 01
 - NT9X72BA LISHW 00 --> 01
 - NTLX02AA XACHW 04 --> 01
 - NTLX03AA XACHW 04 --> 28
 - NTLX03BA XACHW 04 --> 28
 - NTLX05AA XACHW 02 --> 01
 - NTLX06AA XACHW 02 --> 01
 - NTLX07AA XACHW 02 --> 01
 - NTLX12AA XACHW 02 --> 04
 - NTLX14CA XACHW 02 --> 01
 - NTLX22AA XACHW 02 --> 07
 - NTLX27AA XACHW 02 --> 01
4. Removed XA-Core PECs - no longer supported
 - NTLX02AA XACHW % HIPPO based PE
 - NTLX05AA XACHW % CMIC packlet

Supplementary information

NONE

Translation verification other tools

PECINV does not use translation verification tools.

Name: FWINV

FWINV is a NEW table.

Functional description

FWINV is intended to maintain the FW baseline for a PEC, and allows from 0 up to 4 exception versions.

Its data is accessed by:

1. MAPCI;MTC;XAC;QUERY SHELF/CARD
2. Periodic internal queries
3. SREx
4. Card/Packet RTS
5. ONP prechecks, prior to ONP
6. ONP preswact, while split, during ONP

Usage sequence and implications

No table dependencies. Current datafill order unchanged.

Size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
FWINV	0	64	Store for 64 tuples is pre-allocated in DSPROT. Each tuple is 90 bytes.

Fields/OIDs

The following table lists fields for table FWINV. Only 2 fields are shown by the RANGE command: PEC (key) and FWBASE. FWBASE is further broken down into FWTYPE/FWBASE/EXCEPTIONS

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
PEC	NEW	Subfield	8 chars	Must begin with NTLX

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
FWBASE	NEW	Subfield	Sum of 3 below	
FWTYPE	NEW	Subfield	FW or DLL	FW for ROM baseline. DLL for DLL baseline.
VERSION	NEW	Subfield	8 chars	ASCII A-Z, 0-9, beginning with: PE: XAPE IOP: XAIO HIOP: XHIO CMIC: PKdd, d=0-9 AMDl: PKdd, d=0-9 ETHR: EPdd, d=0-9 NO FW for: SM, DISK, TAPE, RTIF
EXCEPTIO NS	NEW	Subfield	8 chars	Same restrictions as above. This FW/DLL version is bad, and will be alarmed if used.

Datafill example

The following example shows sample datafill for table FWINV.

FWINV examples

```

PEC FWBASE
-----
1. NTLX02CA (FW XAPE01AG $) $
2. NTLX04CA (FW XHIO02AH $) (DLL XHIO02AI $)

%% Eg. ONLY, to show exception format.
3. NTLX05AB (FW PK12CE12 (PK12CE13) $) $

```

Table release history update

Initial release.

Supplementary information

NONE

Translation verification other tools

FWINV does not use translation verification tools.

Service Orders (SO)

No impact to Service Orders.

Software optionality control (SOC)

Feature is not SOC controlled.

Command interface changes

QUERY CARD and QUERY SHELF commands are enhanced to show if FRU is HW and FW/DLL baseline compatible.

Directory: MAPCI; MTC; XAC

Directory description

Existing levels are still used - only the display is changed for QUERY SHELF. QUERY SHELF is available from XAC and its sublevels: XACMTC, SM, PE, IO, CMIC, RTIF, DISK, TAPE, AMDI, ETHR

Accessing directory: XACDIR

Access to directory or MAP level and return to CI

enter XAC level from CI:

MAPCI;MTC;XAC

exit to CI:

QUIT ALL

Command: QUERY SHELF

Command type: Listed MENU

Command target: XA-Core

Command availability: RES

Command description

QUERY SHELF lists:

1. Last REX data: time, type, result
2. Information per FRU installed in the shelf.

Command syntax

QUERY SHELF command parameters and variables

Command	Parameters and variables
QUERY SHELF	No additional parameters available.

Qualifications and warnings

NA

Example

See the following figure.

Query SHELF Example

```
>MAPCI NODISP;MTC;XAC
>QUERY SHELF

LAST REX DATA
-----
RExtst run at: 1976/01/02 01:56:52
RExtst type  : full
RExtst result: pass

SHELF DATA
-----
Notes:
  FW: ROM version. HIOP adds DLL version on following line.
  OK: Yes, No, IDPROM read fail, Unsupported.  "*"=Investigate!
      --HW vs. PECINV--          ----FW vs. FWINV----
Pos   Type  PEC+ HW Rel BL OK Serial Number  FW Vers. Baseline OK
-----
  2 F   IOP   NTLX03BA 30 28 Y   NNTM6441882N XAIO01AK XAIO01AK Y
  2 F L Disk NTLX06AC 01 01 Y   NNTM171W2SKC n/a      n/a      Y
  2 F U Tape NTLX07AA 02 01 Y   NNTM171XLG8W n/a      n/a      Y
  4 F   PE    NTLX02CA 02 01 Y   NNTM64419MYX XAPE01AG XAPE01AG Y
  5 F   PE    NTLX02CA 01 01 Y   NNTM64416MJB XAPE01AG XAPE01AG Y
 11 R   SM    NTLX14CA 02 01 Y   NNTM64415KXH n/a      n/a      Y
  7 F   SM    NTLX14CA 09 01 Y   NNTM64429LK2 n/a      n/a      Y
 10 R   SM    NTLX14CA 02 01 Y   NNTM1721FG2L n/a      n/a      Y
  8 F   SM    NTLX14CA 09 01 Y   NNTM64429LM1 n/a      n/a      Y
 12 F   PE    NTLX02CA 05 01 Y   NNTM171WT19M XAPE01AG XAPE01AG Y
 13 F   PE    NTLX02CA 12 01 Y   NNTM64415C78 XAPE01AG XAPE01AG Y
 16 F   PE    NTLX02CA 05 01 Y   NNTM171WMXQ9 XAPE01AG XAPE01AG Y
 17 F   IOP   NTLX03BB 02 03 N*  NNTM6441VHPX XAIO01AK XAIO01AK Y
 17 F L Disk NTLX06AA 02 01 Y   NNTM1721FDZW n/a      n/a      Y
 17 F U Tape NTLX07AA 02 01 Y   NNTM171Z17HM n/a      n/a      Y
  4 R   IOP   NTLX03AA 03 28 N*  NNTM17218T79 XAIO01AK XAIO01AK Y
  4 R L CMIC NTLX05AB 01 01 Y   NNTM171VY7C9 PK12CE12 PK12CE12 Y
  4 R U RTIF NTLX08AA 02 01 Y   NNTM171BP2Y0 n/a      n/a      Y
 10 F   SM    NTLX14CA 02 01 Y   NNTM64419R6Q n/a      n/a      Y
 14 R   HIOP  NTLX04BA 01 01 Y   NNTMEM0135GG XHIO02AA XHIO02AA Y
                                XHIO02AH XHIO02AJ N*
 15 R   IOP   NTLX03AB 01 03 N*  NNTM6441DSGW XAIO01AK XAIO01AK Y
 15 R L CMIC NTLX05AB 03 01 Y   NNTM171Z1GWG PK12CE12 PK12CE12 Y
 15 R U RTIF NTLX08AB 01 01 Y   NNTM171ZQ2DS n/a      n/a      Y
```

Command: QUERY CARD**Command type: Listed MENU****Command target: XA-Core****Command availability: RES****Command description**

QUERY CARD output varies per FRU type. Common to all is:

1. Information per FRU installed in the shelf.

Command syntax

QUERY SHELF command parameters and variables

Command	Parameters and variables
QUERY CARD <position>	position = <slot> <front rear> [<upper lower>]

Qualifications and warnings

NA

Example

See the following figure.

Query CARD Examples

```
>MAPCI NODISP;MTC;XAC
```

```
>QUERY CARD 2 F
```

```
Notes:
```

```
OK: Yes, No, IDPROM read fail, Unsupported. "*"=Investigate!
```

```
--HW vs. PECINV--
```

```
----FW vs. FWINV----
```

Pos	Type	PEC+	HW	Rel	BL	OK	Serial Number	FW Vers.	Baseline	OK
2	F	IOP	NTLX03BA	30	28	Y	NNTM6441882N	XAIO01AK	XAIO01AK	Y

```
HW/SW Vintage : 01
```

```
>QUERY CARD 17 F L
```

```
Notes:
```

```
OK: Yes, No, IDPROM read fail, Unsupported. "*"=Investigate!
```

```
--HW vs. PECINV--
```

```
----FW vs. FWINV----
```

Pos	Type	PEC+	HW	Rel	BL	OK	Serial Number	FW Vers.	Baseline	OK
17	F L	Disk	NTLX06AA	02	01	Y	NNTM1721FDZW	n/a	n/a	Y

```
HW/SW Vintage : 01
Vendor : SEAGATE
Product ID : ST39216W
Revision : 0004
Nom Capacity(MB): 8602
Block Size (B): 512
```

```
>QUERY CARD 4 R L
```

```
Notes:
```

```
OK: Yes, No, IDPROM read fail, Unsupported. "*"=Investigate!
```

```
--HW vs. PECINV--
```

```
----FW vs. FWINV----
```

Pos	Type	PEC+	HW	Rel	BL	OK	Serial Number	FW Vers.	Baseline	OK
4	R L	CMIC	NTLX05AB	00	01	N*	NNTM171VY7C9	PK12CE12	PK12CE12	Y

```
HW/SW Vintage : 01
```

```
>QUERY CARD 4 R U
```

```
Notes:
```

```
OK: Yes, No, IDPROM read fail, Unsupported. "*"=Investigate!
```

```
--HW vs. PECINV--
```

```
----FW vs. FWINV----
```

Pos	Type	PEC+	HW	Rel	BL	OK	Serial Number	FW Vers.	Baseline	OK
4	R U	RTIF	NTLX08AA	02	01	Y	NNTM171BP2Y0			Y

```
HW/SW Vintage : 01
```

```
>QUERY CARD 14 R
```

```
Notes:
```

```
OK: Yes, No, IDPROM read fail, Unsupported. "*"=Investigate!
```

```
--HW vs. PECINV--
```

```
----FW vs. FWINV----
```

Pos	Type	PEC+	HW	Rel	BL	OK	Serial Number	FW Vers.	Baseline	OK
14	R	HIOP	NTLX04BA	00	01	N*	NNTMEM0135GG	XHIO02AA	XHIO02AA	Y

```
HW/SW Vintage : 01
Ethernet MAC Address : 00603887A969
Port IP Address : n/a % Actual IP addresses, if provsioned
Assigned IP Address 1: n/a
Assigned IP Address 2: n/a
```

Security

No impact to switch security.

Configuration Walkthrough

NA

Product = CS 2000**A00002499 -- Store Audit for XA-CORE (Succession on DMS)*****Functional Description***

This feature is to implement refinements to the XA-Core Store Audit in preparation for enabling the audit in the field.

There are no external customer requirements addressed by this feature. The driver requirements for this feature work are all from the design community which felt that the existing audit code was incomplete, and in fact the audit was left disabled by default in previous releases.

This feature does intend to add new logs to report any detected faults in Store Allocator data. When the audit was initially created, STOR600 logs were used to flag problems found by the audit's original code. In later releases new functionality was added to the audit code base, but instead of using logs, detected faults were reported using footprints and swerrs. It is the intention of this audit to consolidate the fault reporting mechanisms and make them consistent.

Hardware Requirements or Dependencies

No dependencies identified at this time.

Software Requirements or Dependencies

No dependencies identified at this time.

Limitations and restrictions

None identified at this time.

Interactions

None identified at this time.

Applicable customer facing sections

Fault Management

Logs	__X__
Alarms	__N/A__
Configuration	
Data Schema	__N/A__
User Interface	__N/A__
Element Management	__N/A__
Security	__N/A__
Service Order	__N/A__
Office Parameters	__N/A__
Accounting (includes AMA billing)	__N/A__
Performance (includes operational measurements)	__N/A__

Fault Management for A00002499

Fault management strategy

Three new logs are introduced by this feature to flag the detection of faults by the XA-Core Store Audit. There are existing STOR logs already defined for use by the audit which the new logs will augment.

Fault management tools and utilities

N/A.

Logs - STOR605

Explanation

Log Title: STOR605

Name: Store Bstree Corruption

Description: This log is output when the Store Audit has detected a corruption in the Bstree structures containing the information about the data address space STOR is responsible for.

Event type: Critical.

Format

STOR605 Format

```
HHHHHHH STOR605 mmmdd hh:mm:ss ssdd INFO Store Bstree Corruption
Bstree nodes corrupt= XXXX
Check SOSB Footprint data - STORE FP EVENT generated.
```

Field descriptions

Field	Value	Description
Bstree nodes corrupt	1 - 9999	Number of problems detected by a single pass of the audit.

Action

The log text indicates to the support personnel that footprints should be collected. This log is only notification that a problem was detected; the detailed fault information is dumped in the SOSB footprints (with the title text "STORE FP EVENT"). Once the details of the corruption(s) is analyzed further recovery action may be required. The corruption may be an invalid pointer or a bad state in the data, and may affect any store type. If DSTEMP is affected the corruption may be cleared by a core restart. If DSPROT is affected the core image may no longer be viable and a reboot or system SWACT may be needed to recover.

Associated Operational Measurements or Performance Measurements

None.

Additional information

None.

Logs - STOR606

Explanation

Log Title: STOR606

Name: Dump Data Corruption

Description: This log indicates that the Store Audit has found a corruption in the allocation information for data store which is dumped (such as DSPROT) and it is very likely that a attempt to perform a dump while in this state would fail.

Event type: Critical.

Format

STOR606 Format

HHHHHHH STOR606 mmmdd hh:mm:ss ssdd INFO Store Dump Data Corruption
ADDR= XXXXXXXX STORTYPE= YYYYYYYY BLOCKSIZE= ZZZZZZZ

Field descriptions

Field	Value	Description
ADDR	00000000 - FFFFFFFF (hexidecimal)	Address of the block of store flagged as corrupt.
STORTYPE	STORTYPE2 (module STOR)	Storetype of the corrupted block.
BLOCKSIZE	00000000 - FFFFFFFF (hexidecimal)	Size in bytes of the corrupted block.

Action

Should these logs be generated the state of the system's allocation information for protected store is such that a valid image dump cannot be performed. Nortel Networks support personnel should be contacted immediately to further investigate the problem. If a valid image file exists then the system may need to be rebooted or otherwise restored to the valid image using a SWACT.

Associated Operational Measurements or Performance Measurements

None.

Additional information

None.

Logs - STOR607

Explanation

Log Title: STOR607

Name: Store Attribute Corruption

Description: This log is generated when the Store Audit detects a mismatch between the Store Allocator's internal setting of an address' blocking attribute and the actual setting of the attribute in memory hardware. The attribute is either blocking or write-blocking. An incorrect value could mislead the Store Allocator's initialization routines and cause traps.

Event type: Major.

Format

STOR607 Format

```
HHHHHHH STOR607 mmmdd hh:mm:ss ssdd INFO Store Attribute Corruption  
ADDR= XXXXXXXX ST2ATTR= YYYY HW_ATTR= ZZZZ
```

Field descriptions

Field	Value	Description
ADDR	00000000 - FFFFFFFF (hexidecimal)	Address of the block of store flagged as having mismatching attributes.
ST2ATTR	0 - blocking memory 1 - write-blocking memory 2 - attribute read error	Blocking attribute of the memory recorded internally by the Store Allocator.
HW_ATTR	0 - blocking memory 1 - write-blocking memory 2 - attribute read error	Blocking attribute of the memory as reported by hardware.

Action

In the event of blocking attribute mismatches being detected support personnel will have to investigate further. Footprints and logs should be collected, as well as FQT (Fault Query Tool) data to determine if any memory hardware failures have occurred.

If blocking attribute mismatches exist in the system, it is possible that there will be no other immediate symptoms as long as there is no Store Allocator activity related to the affected memory. However if a restart occurs the Store Allocator may be unable to correctly access this memory, and in the worst case a restart progression may lead to a system reboot. Thus, manual restarts should be avoided until technical support can determine exactly what memory is affected.

Associated Operational Measurements or Performance Measurements

None.

Additional information

None.

Product = CS 2000

A00002505--Universal Signaling Point Interface Client - GUI (PT-IP, UA-IP, IAC)

Feature Synopsis

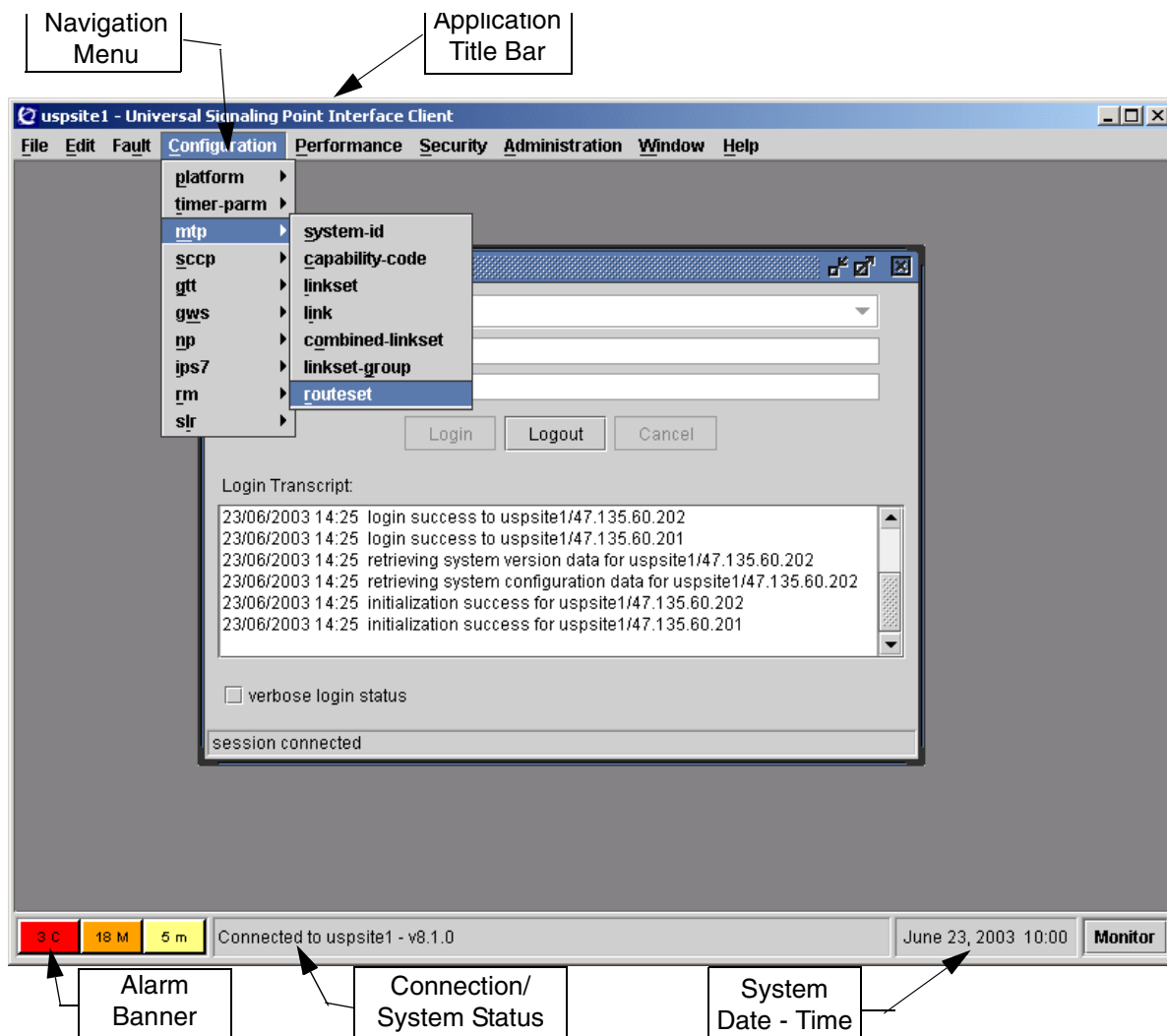
Provide a graphical user interface (GUI) capable of running on multiple operating system platforms in a windows based environment. The GUI will have provisions for administering, monitoring and reporting on the Universal Signaling Point (USP). The GUI delivered by this feature is a replacement for the GUI provided with previous software releases (pre USP8.1.0) and will include and expand upon the functionality and usability provided by the previous GUI version.

Feature Description

The GUI provides a complete multi-platform solution for managing the operation of the USP by providing an intuitive user interface client to perform administration, system monitoring and reporting. The GUI client implements a consistent interface model to present all USP data to ensure ease-of-use and quick navigation of the data retrieved from the USP.

All communication with the USP is accomplished by establishing a standard TELNET connection to the USP Command Line Interface (CLI) and will maintain that connection, reestablishing the connection if necessary. There are no custom protocols or ports to configure which simplifies interoperability and allows for all existing security restrictions and firewalls to be enforced. Local security is also enhanced by initiating idle session lockout and re-authentication if a session is left unattended for an extended period of time. Interoperability is enhanced through context-sensitive launching, using command line arguments, which allows external applications to control the launch sequence of the GUI to have it automatically navigate to the desired table and records using the supplied retrieval criteria.

The GUI is designed as a single encapsulating window manager to help organize and manage the layout of the large number of tables offered by the USP. Access to each table is achieved by a hierarchical menu structure. This structure provides fast and simple navigation to the desired table by simply clicking on the desired table from the pull down menus. See the following figure for an example of the main window of the GUI application.

GUI Main Window

For monitoring purposes, the bottom panel of the main window has connection and status information related to the currently connected site. The alarm banner presents a summary of the current alarmed components of the USP. The status panels provide further overall site information about the current connected site; including, connection information, running software versions and the current system date-time.

The GUI is built on a proven transaction based multi-threaded framework to ensure it will remain responsive even under heavy operation. This permits multiple tasks to be performed simultaneously and assures that progress and status information can always be relayed to the user for the current operation. The cross-platform support of the GUI is accomplished by exploiting the multi-platform support of the Java 2 technology.

Management of all system operations and provisioning data is achieved through a common table interface. This common interface simplifies usability and reduces learning times by providing consistent presentation formats and navigation controls. The common table interface consists of an Administration and Search panel for each table accessible from the USP.

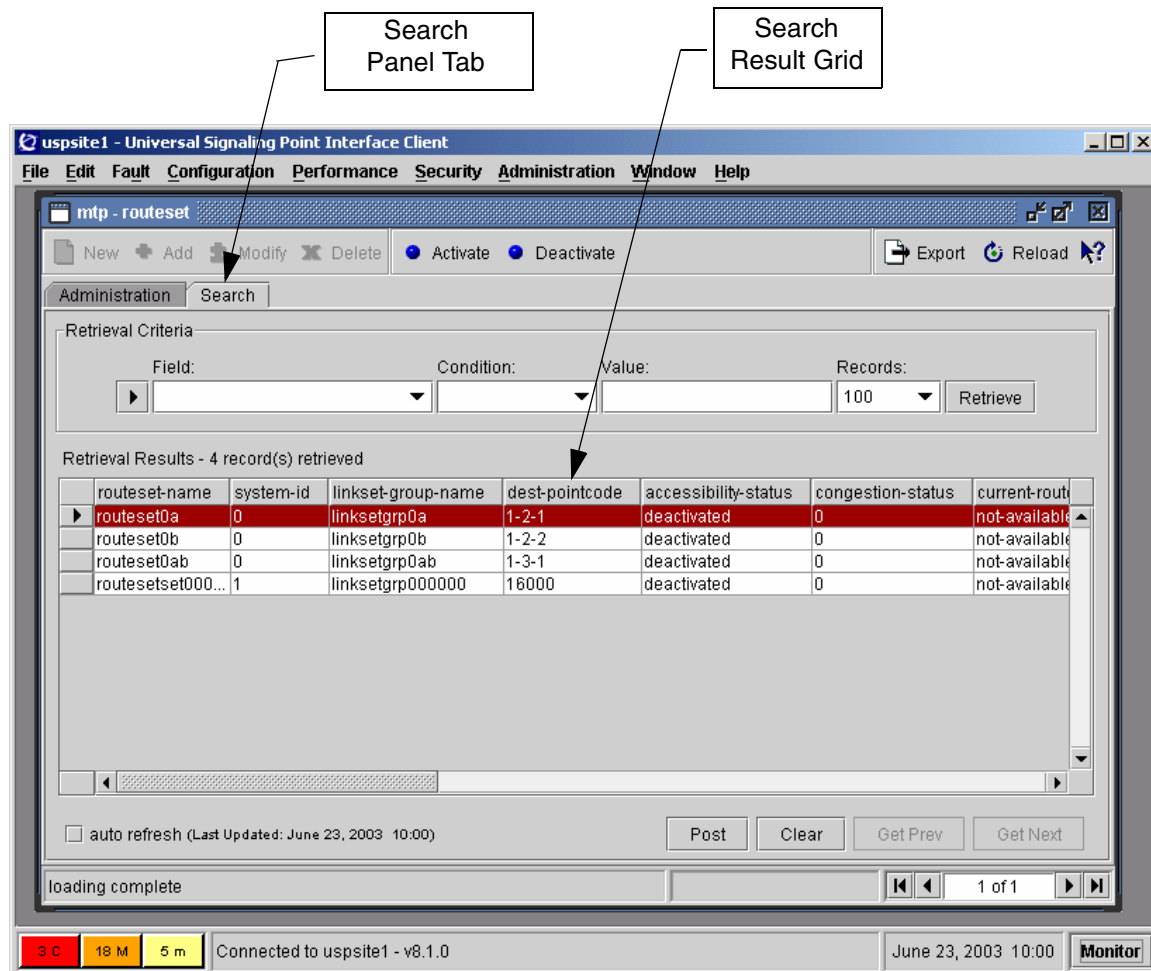
The Administration panel provides the provisioning and maintenance operations for that table. All record manipulation can be performed by the Administration screen for a particular table, including the addition, modification and deletion of records. To enhance usability, all table fields are linked to context-sensitive help to provide a complete field description; including field type, data type, minimum and maximum values, input restrictions, allowed value lists and optional descriptive text for field explanation or special notes. See the following figure for an example of a table Administration panel.

Table Administration Panel

The screenshot displays the 'uspsite1 - Universal Signaling Point Interface Client' window. The 'Administration' tab is selected, showing the 'mtp - routeset' table. The interface includes a menu bar (File, Edit, Fault, Configuration, Performance, Security, Administration, Window, Help) and a toolbar with buttons for New, Add, Modify, Delete, Activate, Deactivate, Export, Reload, and Help. The main area is divided into two sections: 'Provisioning Data' and 'Operational Data'. The 'Provisioning Data' section contains fields for routeset-name, system-id, linkset-group-name, and dest-pointcode. The 'Operational Data' section contains fields for accessibility, alarm-status, current-route, congestion, and network-congestion. Below these are sections for 'Normal Route', 'Alternate Route 1', and 'Alternate Route 2', each with route name, route 1, and route 2 fields. A status bar at the bottom shows 'loading complete', '1 of 1', and a 'Monitor' button.

The Search panel provides record retrieval and navigation, with the added capability of supplying search criteria for most table fields. All tables support both basic and advanced data retrieval and search capabilities to allow for quick navigation to the data of concern. See the following figure for an example of a table Search panel.

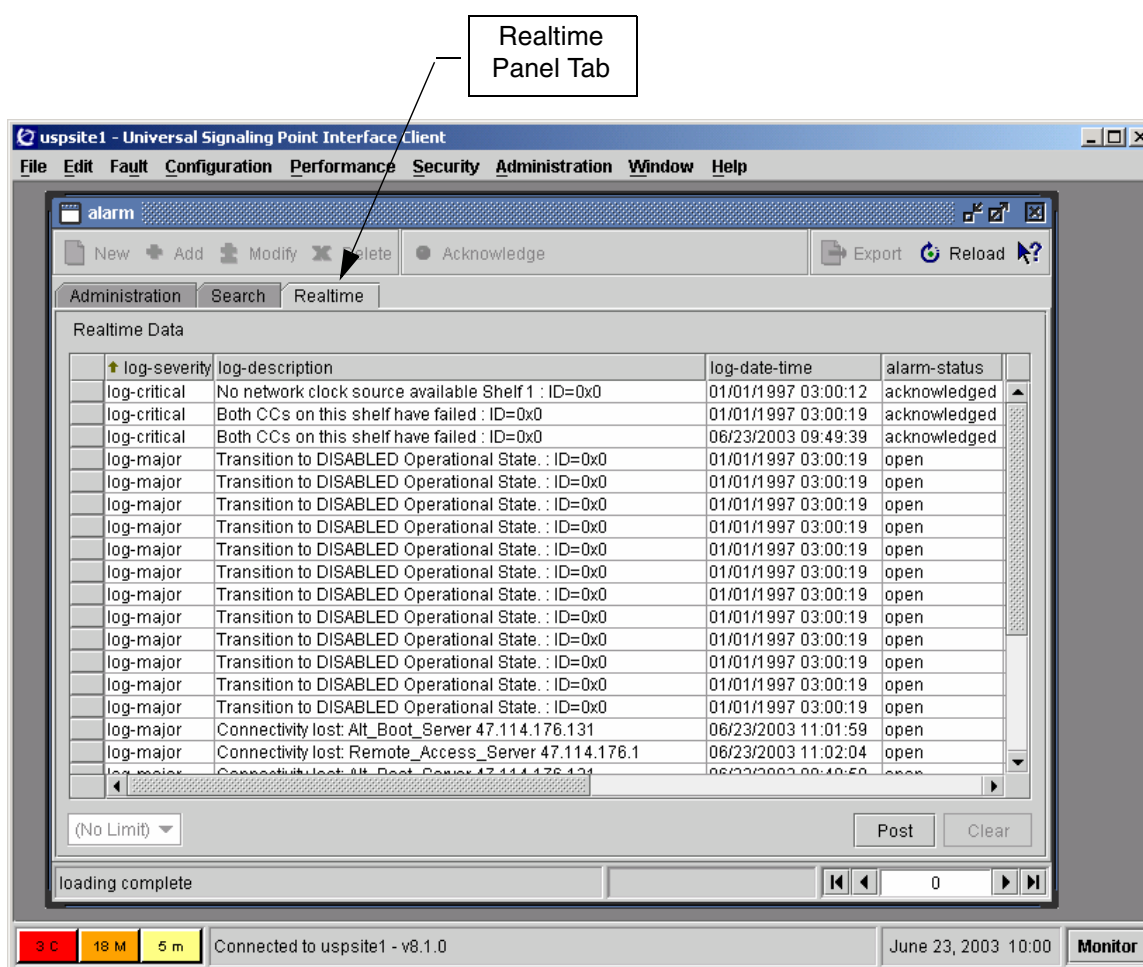
Table Search Panel



All data retrieved from the USP can be formatted and exported to an external file for the purpose of capturing the data in static form. Data can be exported in HTML, CSV and plain text formats. The Search panel facilitates the data capture and customized reporting through the search result grid containing the retrieved table records. Customization is accomplished by adjusting the appearance, presence and location of table fields of a table grid to help organize and report on the critical data.

Fault monitoring of a specific site can be performed in real-time by viewing the summary information from the status bar of the main window, or by accessing the specific fault information from the alarm and log tables. In addition to Administration and Search panels, the fault management tables have a Realtime panel which allows for real-time monitoring and viewing of USP events (i.e. logs and alarms). Similar to search screens, the data presented by the Realtime panel can be customized and navigated using the same common interface. See the following figure for an example of a table Realtime panel.

Table Realtime Panel



Hardware Information

The GUI has been verified on the following platforms running JRE1.4.1_02:

- Windows (NT4.0+SP5/2000 prof+SP2/XP)
- Solaris OS + patches (<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/J2SE>)

The following system requirements must be met to run the GUI application:

- minimum of 64 megabytes of RAM, recommended 128 megabytes
- minimum of 100 megabytes of disk space to install JRE and to store site configuration, preferences and local logs required by GUI application
- graphical window environment running at least 16-bit color depth

GUI/CLI Information

The summary of the changes have been outlined in the “Feature Description” section. For a complete and detailed description of the changes and the usage of the GUI, please refer to the document titled *Universal Signaling Point GUI - User Guide*.

CLI changes

All communication (data exchange) with the USP will be performed through a TELNET connection to the USP using the CLI. The GUI will make use of the CLI-API machine interface of the USP and will therefore require no additional functionality.

GUI changes

Refer to the “Feature Description” section for details of GUI changes. The new GUI is a replacement for the GUI distributed with the previous software releases (pre USP8.1.0).

OMs

Not Applicable.

Logs, and Alarms

Not Applicable.

Interactions

The GUI facilitates administration, monitoring and reporting of all existing functions of the USP. The functionality provided by the USP will continue to operate as normal and will not be affected by the interface changes introduced by the GUI.

Restrictions and Limitations

None.

Definitions and Terms

CLI - Command Line Interface

CPU- Central Processing Unit

GUI - Graphical User Interface

J2SE- Java 2 Standard Edition

JRE - Java Runtime Engine

MDI- Multiple Document Interface

USP - Universal Signaling Point

Product = CS 2000

A00002510 -- LANCOMM IP over IRM (Succession on DMS)

Functional Description

This document provides the design intent for the feature to provide LANCOMM IP over the IRM on XA-CORE. The purpose of this feature is to provide LANCOMM TCP and UDP availability when communicating over the XACORE Ethernet messaging system. This feature does not address LANCOMM issues of performance or robustness.

At present the IRM IP is used to transmit and receive packets to and from the XACORE IO hardware. The IRM implementation of IP is very minimal with some of the features such as ARP routing being performed by the firmware. The IRM IP implementation does not support TCP or features like IP fragmentation and extra options. The LANCOMM version of IP supports IP more completely. This feature will use the IRM IP to receive packets from the IO cards, however the IRM will then will use callback routines that will be registered with the IRM for packets intended for LANCOMM to pass the packets to LANCOMM UDP or TCP. The LANCOMM IP will be used to process the packets. A TCP or UDP packet coming from the LANCOMM intended for the IRM will be injected in to the IRM IP after it has passed through the LANCOMM IP to be transmitted to Ethernet.

The specific purpose of this feature is to support the Next generation Supernode Data Manager (nSDM) that is being developed on a Solaris platform to replace the existing SDM FX which uses a DS512 to connect to the CORE. The nSDM will not have a DS512. It will connect to the CORE via Ethernet. This feature will also support FTP or TELNET over IRM from

another source other than the SDM like for instance an workstation.⁹ This will not be a EIU replacement but will exist in the same load as EIU. This Feature will support the following SDM applications with LANCOMM IP over IRM.

- RPC (UDP)
- NTP -Network Time Protocol (UDP)
- FTP (TCP)
- Telnet (TCP)
- SBA -Billing (RFC TCP)

Hardware Requirements or Dependencies

A nSDM and a SDM FX which are connected to the Core by HIOP are required to fully test the feature. We also need a nSDM system that is connected to a core that has both EIU and HIOPs.

Software Requirements or Dependencies

There should be no software dependencies as this feature will work with both the existing SDM FX and NSDM.

Limitations and restrictions

Only one SDM will be connected to the CORE at a time.

Any application that wants to use LANCOMM IP over IRM is required to bind to the NIL IP address. All present SDM applications are compliant.

Any application that are using the EIU will continue to function.

Under this CSP20 release only, the SDM will be the only application node making use of the LANCOMM IP over IRM feature. The number of SDM nodes are limited to four.

Interactions

All applications using LANCOMM IP over IRM on the nSDM will function as they did before on the SDM fx without any impact to the user.

Applicable customer facing sections

Fault Management

Logs

X

Alarms

N/A

Configuration

9. Telnet and FTP over IRM will be enabled for all devices connected to a CORE that is in lab mode. In field mode the only recognised device allowed to access the CORE through the Ethernet will be SDM.

Data Schema	<u>X</u>
User Interface	<u>N/A</u>
Element Management	<u>N/A</u>
Security	<u>N/A</u>
Service Order	<u>N/A</u>
Office Parameters	<u>N/A</u>
Accounting (includes AMA billing)	<u>N/A</u>
Performance (includes operational measurements)	<u>X</u>
Realtime	<u>N/A</u>
Engineering Information	<u>X</u>

Glossary

Term	Description
Arp	Address Resolution Protocol
Core	DMS switch computing engine
FTP	File Transfer Protocol
HIOP	High Performance I/O processor packet
IP	Internet Protocol
IRM	IP routing and Maintenance
LANCOMM	Core network layer for Telnet and FTP
nSDM	next Generation Supernode Data Manager
SDM	Supernode Data Manager
SDM FX	SDM Fault tolerant platform based on IBM AIX UNIX and redundant Motorola hardware.
TCP	Transmission Control Protocol
UDP	internet User Datagram Protocol

Fault Management for A00002510

Fault management strategy

Unchanged

Fault management tools and utilities

Unchanged

Logs**Explanation**

Log Title: ITN307

Name:

Description:

XASKY07BD ITN313 SEP30 11:09:34 8200 INFO IP TRANSMIT
FAILED

NODE:CM

Route to Destination Known but Unavailable

SRC IP: 47.129.216.60

DST IP: 47.80.0.209

Configuration for A00002510**Hardware and Software Requirements**

NA

Initial Configuration

NA

Office/Subnet parameters (OP/SP) (CM & SESM)

NA

Upgrade Impact

NA

Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
IPNETWRK	changed	old

Table/MIB/Remote Database Schema information

Table schema for IPNETWRK has been modified as follow.

Field name PARM in table IPNETWRK has been refined, a new value IRM_INTERFACE is added. The introduction of this new value has an impact to the dump and restore table transfer order. Table CMIPADDR needs to be transferred before IPNETWRK.

Name:

IP Network Table

Functional description

A new field has been introduced in CSP20 to specify the IP address that has been assigned for the XA-Core IOP (IRM). This IP Address must have been datafilled in table CMIPADDR.

Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

Transfer order must be changed such that CMIPADDR is transferred before IPNETWRK.

CMIPADDR

IPNETWRK

Size

NA

Datafill example

NA

Table release history update

NA

Supplementary information

NA

Translation verification other tools

NA

Service Orders (SO) (CM & SESM)

NA

Software optionality control (SOC)

NA

Element Management

NA

Security

NA

Configuration Walkthrough

NA

Product = CS 2000**A00002538 -- Performance Measurement Tools (Succession on DMS)*****Functional Description***

This feature will remove the COMPLEX (call complexity) measurement from the XA-Core platform as this measurement is not valid for XA-Core.

The COMPLEX measurement is currently displayed in:

- the CAPCI CI command
- the CAPACITY level of MAPCI
- the DETAIL level of MAPCI
- the SCHEDMAP level of MAPCI
- CAPLOGS - specifically the CAP100 and CAP101 logs
- XASTAT OM - XASCMPLX measurement

Hardware Requirements or Dependencies

None

Software Requirements or Dependencies

None

Limitations and restrictions

None

Interactions

None

Applicable customer facing sections

Fault Management

Logs

☒

Alarms

☐

Configuration

Data Schema

☐

User Interface

☐

Element Management

☐

Security

☐

Service Order

☐

Office Parameters

☐

Accounting (includes AMA billing)

☐

Performance (includes operational measurements)

☒***Fault Management for A00002538*****Fault management strategy**

N/A

Fault management tools and utilities

N/A

Logs**CAP 100****Explanation**

Log Title: CAP100

Name: Capacity Summary Log

Description: Since the complexity (COMPLEX) measurement is not valid on an XA-CORE (multiple processing) switch, it will be removed from the capacity summary log data collection and display.

Event type: INFO

Format

In previous releases, the CAP100 is displayed as:

```
XASKY07AZ      CAP100 SEP09 20:59:33 8800 INFO CAPACITY_SUMMARY
CATMP/HR        0 UTIL  --  ENGCATMP      --  MAXCATMP      --  COMPLEX  --
```

The field “COMPLEX” will be removed from CAP log 100 in this release (CSP20) as displayed below:

```
XASKY07AZ      CAP100 SEP09 20:59:33 8800 INFO CAPACITY_SUMMARY
CATMP/HR        0 UTIL  --  ENGCATMP      --  MAXCATMP      --
```

Field descriptions

The remaining fields are not changed.

Action

No change

Associated Operational Measurements or Performance Measurements

No change

Additional information

No change

CAP log 101

Explanation

Log Title: CAP101

Name: Capacity log

Description: Since the complexity (COMPLEX) measurement is not valid in XA-CORE (multiple processing) switch, it will be removed from CAP log 101 data collection and display.

Event type: INFO

Format

In previous releases, the CAP101 is displayed as:

```

XASKY07AZ      CAP101 SEP09 20:59:33 8700 INFO CAPACITY_DATA
11: CATMP/HR      0 UTIL  --  ENGCATMP      --  MAXCATMP      --
COMPLEX  --  ENGLEVELE BELOW CCOVRD OFF CMICOVRD OFF PESC  NO
12: CATMP/HR      0 UTIL  --  ENGCATMP      --  MAXCATMP      --
COMPLEX  --  ENGLEVELE BELOW CCOVRD OFF CMICOVRD OFF PESC  NO
13: CATMP/HR      0 UTIL  --  ENGCATMP      --  MAXCATMP      --
COMPLEX  --  ENGLEVELE BELOW CCOVRD OFF CMICOVRD OFF PESC  NO
14: CATMP/HR      0 UTIL  --  ENGCATMP      --  MAXCATMP      --
COMPLEX  --  ENGLEVELE BELOW CCOVRD OFF CMICOVRD OFF PESC  NO
15: CATMP/HR      0 UTIL  --  ENGCATMP      --  MAXCATMP      --
COMPLEX  --  ENGLEVELE BELOW CCOVRD OFF CMICOVRD OFF PESC  NO

```

The field “COMPLEX” will be removed form CAP101 in this release (CSP20) as displayed below:

```

XASKY07AZ      CAP101 SEP09 20:59:33 8700 INFO CAPACITY_DATA
11: CATMP/HR      0 UTIL  --  ENGCATMP      --  MAXCATMP      --
ENGLEVEL BELOW CCOVRD OFF CMICOVRD OFF PESC  NO
12: CATMP/HR      0 UTIL  --  ENGCATMP      --  MAXCATMP      --
ENGLEVEL BELOW CCOVRD OFF CMICOVRD OFF PESC  NO
13: CATMP/HR      0 UTIL  --  ENGCATMP      --  MAXCATMP      --
ENGLEVEL BELOW CCOVRD OFF CMICOVRD OFF PESC  NO
14: CATMP/HR      0 UTIL  --  ENGCATMP      --  MAXCATMP      --
ENGLEVEL BELOW CCOVRD OFF CMICOVRD OFF PESC  NO
15: CATMP/HR      0 UTIL  --  ENGCATMP      --  MAXCATMP      --
ENGLEVEL BELOW CCOVRD OFF CMICOVRD OFF PESC  NO

```

Field descriptions

The remaining fields are not changed.

Action

No change

Associated Operational Measurements or Performance Measurements

No change

Additional information

No change

Performance Management for A00002538

Performance management strategy

N/A

Performance management tools and utilities

N/A

Performance Measurements (PM), Operational Measurements (OM), and stats

XASTAT OM group

OM Group template (applies only to DMS)

XASTAT OM group

OM description

OM group XASTAT

Capacity operational measurements

Release history update

The OM group XASTAT is being modified in CSP20. It will be changed as follows:

Register XASCMPLX will be removed from OM group XASTAT since this measurement is not valid in XA-Core.

Registers

It is the same as in previous releases except the register XASCMPLX is removed.

In previous releases, XASTAT OM group registers display on the MAP terminal as follows:

XASTAT

```
CLASS: ACTIVE
START:2003/09/11 12:30:00 THU; STOP: 2003/09/11 12:48:29 THU;
SLOWSAMPLES:      12 ; FASTSAMPLES:      111 ;
```

XASUTIL	XASPUTIL	XASCMPLX	XASSCHED
XASFORE	XASMAINT	XASDNC	XASOM
XASGTERM	XASBKG	XASAUXCP	XASNETM
XASSNIP	XASPESC	XASNXFR	XASOVER
XASOTHLD			

0				
	0	0	0	0
	0	0	0	0
	0	0	0	0
	0	0	0	0
	0			

After removing XASCMPLX in CSP20, it will be displayed as:

XASTAT

```
CLASS: ACTIVE
START:2003/09/11 12:30:00 THU; STOP: 2003/09/11 12:48:29 THU;
SLOWSAMPLES:      12 ; FASTSAMPLES:      111 ;
```

XASUTIL	XASPUTIL	XASSCHED	XASFORE
XASMAINT	XASDNC	XASOM	XASGTERM
XASBKG	XASAUXCP	XASNETM	XASSNIP
XASPESC	XASNXFR	XASOVER	XASOTHLD

0

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

Group structure

No change

Associated OM groups

No change

Associated functional groups

No change

Associated functionality codes

No change

OM group registers logic flow chart

No change

Register (applies only to DMS)

No change

Product = CS 2000**A00002549 -- CSP20 CALLP Robustness (Succession on DMS)*****Functional Description***

- *Design Component 2: OM threshold alarms for call processing resources - table ALARMTAB.*
- *Design Component 3: Extension Block Format Code expansion.*
- *Design Component 4: Increase Cpwakeup Accuracy.*

Design Component 2: OM threshold alarms for call processing resources - table ALARMTAB

This feature component adds datafill to the system table ALARMTAB. The table is datafilled prior to the release of the nodata load to the field. This adds an alarm to the existing EXT alarm banner component and the existing log OM2200 to be triggered upon depletion of the base call processing resource ECCB (Extended Call Condense Blocks). This alarm is based on the existing Operational Measurement register defined in CP2 - ECCBOVFL (ECCB Overflow). The table ALARMTAB currently exists for several base call processing resources. This addition is an enhancement to this set of alarms.

All actions and explanations are already documented for the existing base call processing resources and are identical for the ECCB resource depletion. Documentation for the logs and the alarm already exist and can be found in the following NTPs:

- 297-8991-500 04.02 *Maintenance and Operations Manual*
- 297-2621-851P1 09.02 *UCS DMS-250 Data Schema Reference Manual Vol 1 of 5*
- 297-2621-8141 10.03 *DMS-250 Operational Measurements Reference Manual Vol 1 of 2*
- 297-8101-8141 06.01 *Operational Measurements Reference Manual Vol. of 3*
- 297-2621-8403 09.01 *UCS DMS-250 Logs Reference Manual Vol 3 of 6*
- 297-2621-8405 09.01 *UCS DMS-250 Logs Reference Manual Vol 5 of 6*
- 297-8101-3503 06.01 *Base DMS STP Translations Guide Vol. 3 of 6*
- 297-2621-106 07.02 *UCS DMS-250 ISDN Reference Manual*
- 297-2621-395 08.02 *DMS-250 Billing Records Application Guide*
- 297-2621-851P5 09.02 *UCS DMS-250 Data Schema Reference Manual Vol 5 of 5*
- 297-5051-914 07.02 *DDMS and GUIDE Install and Admin Reference Manual*
- 297-8101-8142 06.01 *Operational Measurements Reference Manual Vol. 2 of 3*

Extension Block Format Code expansion

Currently, there are only a total of 256 extension format codes in the system. We are quickly approaching this limit thereby limiting the number of available extension format codes for new users. Design Component 3 of this feature - EXT Format Code Expansion - addresses this issue. In particular, the total number of extension format codes in the system will be increased from 256 to 511.

Increasing the total number of extension format codes from 256 to 511 causes the size of the extension format codes to increase from 8-bits to 9-bits. The extension format code is a field within the extension block header (the first structure/field in every extension block). This may affect downstream processors if they extract the format code from the extension blocks hex dump. The total size of the extension block header is not being increased; however, two of its fields were re-arranged so that the new size of the format code could be accommodated. Specific details of this change are presented in the FM (Fault Management) section of this feature.

For each extension format code, there is a corresponding (unique) AUD and XAUD log. The XAUD logs are output whenever an extension block is reclaimed by the XA-Core audit process and the AUD logs are used to dump extension block contents for all other processes (i.e., non-audit reclaims such as call deaths).

Currently the AUD logs assume the values 400 through 431, and 500 through 723. The XAUD logs assume values 600 through 610 (for standard call processing resources) and 700 through 955 (for extension blocks).

This feature will require that the ranges for the before mentioned AUD logs be extended beyond 723 to accommodate the new extension format codes. The XAUD logs will also be extended and the numbering convention (numeric range) will be changed to match that for the AUD logs for simplicity. That is, each extension format code will now have the same AUD and XAUD number (i.e., the associated logs for extfc 109 will be AUD577 and XAUD577).

Please note that as each new extension format code is defined/added in the system, it is the responsibility of the user to define and document it. Therefore, the only changes visible to the customer will be for the existing XAUD log numbers (those currently defined at the time of this feature). Furthermore, the contents of these logs (apart from the location and number of bits of the extfc in the extension block head) are in no way being changed.

Increase Cpwakeup Accuracy

This component of the feature will affect the real-time of the switch. This real-time increase will be minimal.

Hardware Requirements or Dependencies

Not applicable.

Software Requirements or Dependencies

Not applicable.

Limitations and restrictions

Not applicable.

Interactions

Not applicable.

Applicable customer facing sections

Fault Management

Logs

___X___

Alarms

___N/A___

Configuration	
Data Schema	___N/A___
User Interface	___N/A___
Element Management	___N/A___
Security	___N/A___
Service Order	___N/A___
Office Parameters	___N/A___
Accounting (includes AMA billing)	___N/A___
Performance (includes operational measurements)	___N/A___
Realtime	___X___
Engineering Information	___N/A___

Fault Management for A00002549

Fault management strategy

N/A

Fault management tools and utilities

N/A

Logs

Explanation

Log Title: AUDmmm & XAUDnnn (where mmm & nnn are numeric values)

Name: Call Processing Resource Dump

Description: XAUD logs are generated whenever a call processing resource is recovered by the audit process running on the XA-Core platform. AUD logs are generated/used by all other non-audit processes.

The numeric values for the XAUD logs used to cover the range from 600 to 610 for standard resources (i.e., XAUD600, XAUD601, XAUD602, and XAUD609) and 700 to 955 for extension block resources. The numeric values for the XAUD logs are being extended and changed to match those for the AUD logs for simplicity. The new numeric values for the XAUD logs will now be 395, 397, 432, 434 and ranges from 400 to 431 and 500 to 982. A table is

being included below (in the 'Additional Information' section) to illustrate the new numbering system for the XAUD logs.

Please note, the total number of AUD and XAUD logs will vary from load to load. This feature is not adding more AUD or XAUD logs to the load, it is only setting the framework so that applications will be able to add more in the future.

The size, format and contents for the AUD and XAUD logs of standard resources is not being changed. However, the location and number of bits used to represent the extension block's format code in the header (within the hex dump of the log) has changed for all extension block logs. **The only noticeable difference to the customer will be the number following the XAUD string in the log title.**

Event type: INFO

Format

No change to the format of the AUD or XAUD log (originally defined by feature ACT.A19011742). A sample format is being included for reference.

General format of all XAUD logs:

```
XAUD<nnn> <date> <time> <sequence> INFO <resource> Recovery
REMARK: <remark>
PTR: <item> INDEX: <prim> <sec> CURRENT AUDIT GENERATION: <gen>
STATE: <state> PROBLEM: <problem>
<hex dump>
```

Sample of an encapsulator recovery log (standard resource):

```
XAUD397 APR29 10:34:37 2900 INFO Encapsulator Recovery
REMARK: Associated CCB queue is empty
PTR: 4B1EF920 INDEX: 0001 000F CURRENT AUDIT GENERATION: 00BD
STATE: UNAVAILABLE_ENC PROBLEM: ERROR_LINKS
444B B9D4 0000 0001 0001 FDCF 7BCD FDFD FDFD FDFD
FDFD FDFD FDFD FDFD FDFD FDFD FD72 0001 0000 FDFD
FDFD FDFD FDFD FDFD FDFD FDFD FDFD FDFD FDFD FDFD
FDFD FDFD FFFF 0000 FD02 FFFF 0000 FFFF 0000 0000
FDFC FFFF 0000 FDFD FDFD FDFD FDFD FDFD
```

The total size of the extension block header has not been increased and hence the total size of the hex dump has not been increased. However, the location and number of bits used to represent the extension block format code in the header portion of the hex dump has changed for all extension block logs.

Sample hex dump portion of an extension block recovery log:

```
<XAUD or AUD log title>
<hex_dump>:
FFFF 0000 7340 CF5 FDFD FDFD FDFD FDFD FDFD FDFD
FDFD FDFD FDFD FDFD FDFD FDFD
```


The extension format code will now be 9-bits starting at offset 6 (i.e., 14th hex digit) in the hex dump. As illustrated in the above, the format code will be 9-bits of CF5.

i.e., CF5 hex = 1100 1111 0101 bin ==> FORMAT CODE = 245

Only the right-most 9-bits of the 14th, 15th and 16th hex digits in the hex dump will be used to represent the format code. In this case the format code is 245. The remaining three bits of the 14th hex digit are unused at present.

Field descriptions

No change. The field descriptions are being provided here for reference.

Field	Value	Description
nnn	numeric	Value from ranges outlined in description above
date	date	System supplied, when the recovery happened
time	time	System supplied, when the recovery happened
sequence	numeric	System supplied, sequence within log system
resource	text	Name of the resource recovered
remark	text	Further clarification as to why it was recovered
item	hex numeric	Memory address of item
prim	hex numeric	Primary index into item's resource pool
sec	hex numeric	Secondary index into item's resource pool
gen	hex numeric	Audit generation when recovered
state	text	State of item at the time of recovery
problem	text	Description of problem that resulted in the log
hex dump	hex numeric	Multi line dump of the contents of the resource

Action

No immediate action required.

Associated Operational Measurements or Performance Measurements

N/A

Additional information

New mapping of XAUD log numbers being introduced by this feature.:

New mapping for Standard resources:

AUDnnn	Old XAUDxxx	New XAUDnnn
AUD397	XAUD600	XAUD397
AUD395	XAUD601	XAUD395
AUD432	XAUD602	XAUD432
AUD434	XUAD609	XAUD434

New mapping for extension block resources

AUDnnn	Old XAUDxxx	New XAUDnnn
AUD400	XAUD700	XAUD400
AUD401	XAUD701	XAUD401
...	...	...
AUD430	XAUD730	XAUD430
AUD431	XAUD731	XAUD431
AUD500	XAUD732	XAUD500
AUD501	XAUD733	XAUD501
...	...	...
AUD708	XAUD940	XAUD708
AUD709	XAUD941	XAUD709
AUD979	XAUD942	XAUD979
AUD980	XAUD943	XAUD980
AUD981	XAUD944	XAUD981
AUD982	XAUD945	XAUD982
AUD714	XAUD946	XAUD714
AUD715	XAUD947	XAUD715
...	...	...
AUD723	XAUD955	XAUD723
AUD724	N/A	XAUD724
AUD725	N/A	XAUD725

New mapping for extension block resources

AUDnnn	Old XAUDxxx	New XAUDnnn
...	...	...
AUD977	N/A	XAUD977
AUD978	N/A	XAUD978

Product = CS 2000**A00002555 -- SERVORD manipulation of the GND option (Succession on DMS, UA-IP)*****Functional Description***

This SN07 activity allows Servord commands ADO, DEO and CLN to manipulate the GND option. The GND option for lines resides in table LNINV. Table LNINV contains the hardware information about the line including the Line Equipment Number (LEN) card code and GND. If GND is set to Y, the line will be a ground start line if the line card is supportive. The list of line cards supported are:

- 3A06BA
- 7A25AA
- RDTCON
- RDTLSG
- SCD271

The GND option appears as a line option when a query is performed on the DN or LEN but it is currently not an option that can be manipulated via Servord. This activity will allow Servord to manipulate the GND option on the above line cards, including

- ADO and DEO of the GND option
- CLN will propagate the GND information of the OLD_LEN to the NEW_LEN

Lines that currently auto populate table LNINV on NEW, EST and ADD such as Succession and lines off of RDT peripherals will continue to function as before.

The redundant feature which is turned on by table OFCVAR parm SO_ALLOW_REDUNDANT_FEATURE is now supported for the GND option for the ADO, DEO and CLN Servord commands.

CLN will set the value of GND to that of the OLD_LEN if the NEW_LEN is one of the supported line cards. A warning message will be output that GND being set to the OLD_LEN value. The below example shows the warning message if GND will be set to TRUE on the NEW_LEN

```
WARNING: GND will be changed to TRUE in Table LNINV
        on the NEW LEN, same setting as the OLD LEN
```

Also for CLN, if the NEW_LEN is not a supported line card and the value of GND is different than the OLD_LEN GND value, the below warning message will be output

```
WARNING: GND is FALSE in Table LNINV on the NEW LEN
        the setting was TRUE on the OLD LEN
```

If the value of GND is the same on the OLD_LEN and the NEW_LEN, no warning message is output.

There are additional line cards that support GND but also require some manual intervention such as a strap or a switch to be toggled in order for the GND to take effect. Attempts to manipulate GND on these type line cards will result in an error message as in releases prior to this feature.

It may be necessary to BSY and RTS the line at the MAP in order for the change in GND value to effect.

Hardware Requirements or Dependencies

There is no new hardware introduced by this feature. It is limited to the servord commands and line cards aforementioned

Software Requirements or Dependencies

This is an SN07 deliverable.

Limitations and restrictions

Servord GND manipulation is limited to the ADO, DEO and CLN commands and to the supported line card types

- 3A06BA
- 7A25AA

- RDTCON
- RDTLSG
- SCD271

Currently, GND can be added via NEW, NEWACD, EST, ADD, EXBEST and EXBADD for lines that can be auto populated into table LNINV. This is not changed by this feature.

Interactions

If the Servord Redundant feature which is activated by table OFCVAR parameter SO_ALLOW_REDUNDANT_FEATURE is turned off, attempts to manipulate GND on commands or line cards not supported will be rejected. If this office parameter is turned on, then a warning message will be output that GND will be ignored for non-supported commands and line cards.

Applicable customer facing sections

Fault Management

Logs _n/a_____

Alarms _n/a_____

Configuration

Data Schema _n/a_____

User Interface _n/a_____

Element Management _n/a_____

Security _n/a_____

Service Order _X_____

Office Parameters _n/a_____

Accounting (includes AMA billing) _n/a_____

Performance (includes operational measurements) _n/a_____

Glossary

Term	Description
GND	GROUND as in GROUND START
MAP	Maintenance Administration Position
BSY	BUSY -Refers to maintenance action at MAP
RTS	Return To Service -Refers to maintenance action at MAP

Configuration for A00002555

This feature allows the ADO, DEO and CLN Servord commands to manipulate the GND Bool in table LNINV for certain adaptive line cards.

Hardware and Software Requirements

SN07

Service Orders (SO) (CM & SESM)

This feature allows the ADO, DEO and CLN Servord commands to manipulate the GND Bool in table LNINV for the below list of the supported line cards.

- 3A06BA
- 7A25AA
- SCD271
- RDTCON
- RDTLSG

The above line cards are referred to in this document as the supported line cards.

There are other line cards that support GND but they are not supported by this feature. Other Servord commands are not affected. Commands that establish new service such as NEW and EST will function as before.

If table OFCVAR parm SO_ALLOW_REDUNDANT_FEATURE is set to Y, then the redundant feature is turned on. Redundant feature is now supported for GND for the ADO, DEO and CLN commands. This means for example, if the ADO of GND is attempted to a line that already has the GND option, the command will not be rejected and no journal file update will occur.

Service order change details

LCC and options

There are no new options introduced by this feature. The behavior of the ADO, DEO and CLN Servord commands is changed for the GND option for the supported line cards only. The GND option is not applicable to key sets or ISDNSETs. The option pertains mostly to COIN and PBX lines.

New commands

There are no new commands introduced by this feature.

How service order options are presented

Description

The GND option is used to specify that the line will be a GROUND START line. It is determined by the value of GND in table LNINV for the tuple associated with the line. Only certain line cards can be ground start lines and only the supported line cards apply to this feature. Prior to this feature, the ADO, DEO and CLN Servord commands could not change the GND Bool for any line. This value was set when the tuple was datafilled in table LNINV. This feature doesn't add the GND option or additional prompts as the option already exists. It allows the Servord commands ADO, DEO and CLN to change the value for GND for the supported line cards. Prior to this feature, an error message was given when GND was attempted to be ADO-ed or DEO-ed. The error message is still given for lines that do not have a supported line card. Use QLEN or QDN to determine the line card and GND value. Positioning on the LEN in table LNINV can also be used.

Perhaps the biggest enhancement of this feature is with the CLN command. If the NEW_LEN has a supported line card, the value of GND will be set to that of the OLD_LEN. If the value will change, a warning message is output. If the NEW_LEN does not have a supported line card, the value of GND on the NEW_LEN will be the same as it was prior to execution of the CLN command. If the value of GND is different between the OLD_LEN and the NEW_LEN, a warning message will be output.

QLEN or QDN can be used to determine the line card and the value of GND. GND will also appear in the option list if it set to Y in table LNINV. The below example shows a line with a RDTLSG line card with GND set to Y.

```
>qlen rdt0 1 0 1 2
-----
---
LEN:      RDT0  01 0 01 02
TYPE: SINGLE PARTY LINE
SNPA: 908
DIRECTORY NUMBER:      9451104
LINE CLASS CODE:       1FR
SIGNALLING TYPE:  DIGITONE
LINE TREATMENT GROUP:   0
LINE ATTRIBUTE INDEX:   400
CARDCODE: RDTLSG   GND: Y PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER      :    221
PM TERMINAL NUMBER  :     2
OPTIONS:
DGT GND NAME PUBLIC C1FR1RGB
OFFICE OPTIONS:
AIN TIID
-----
---
```

Example

Example of ADO of the GND option in Prompt mode

```
>ado
SONUMBER:      NOW   3   12   1 PM
>
DN_OR_LEN:
>RDT0 1 0 1 2
OPTION:
>GND
OPTION:
>$
COMMAND AS ENTERED:
ADO NOW 3 12 1 PM RDT0 1 0 1 2 ( GND ) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y
```

Example of DEO of GND in No Prompt mode

```
>deo
SONUMBER:      NOW   3   12   1 PM
>
DN_OR_LEN:
>RDT0 1 0 1 2
OPTION:
>GND
OPTION:
>$
COMMAND AS ENTERED:
DEO NOW 3 12 1 PM RDT0 1 0 1 2 ( GND ) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y
```

The following example shows a CLN from a OLD_LEN that has GND set to a NEW_LEN that has a supported line card.

Note: The warning is output only if the GND values are different between the OLD_LEN and NEW_LEN prior to the execution of the command.

Example of CLN command to a NEW_LEN with Supported Line Card

```

>CLN
SNUMBER:    NOW   3   12   1 PM
>
OLD_LEN:
>RSC0 0 0 3 0
NEW_LEN:
>RSC0 0 0 0 7
COMMAND AS ENTERED:
CLN NOW 3 12 1 PM RSC0 00 0 03 00 RSC0 00 0 00 07
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
y
WARNING: GND will be changed to TRUE in table LNNIV
         on the NEW_LEN, same setting as the OLD_LEN

```

The following example shows a CLN from a OLD_LEN that has GND set to a NEW_LEN that doesn't have a supported line card.

Note: The warning is output only if the GND values are different between the OLD_LEN and NEW_LEN prior to the execution of the command.

Example of CLN, NEWLEN is not a Supported Line Card

```

>CLN
SNUMBER:    NOW   3   12   1 PM
>
OLD_LEN:
>RSC0 0 0 3 0
NEW_LEN:
>0 0 0 3
COMMAND AS ENTERED:
CLN NOW 3 12 1 PM RSC0 00 0 03 00 HOST 00 0 00 03
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
y
WARNING: GND is FALSE in table LNNIV on the NEW_LEN
         The setting was TRUE on the OLD_LEN

```

Example of ADO and DEO of the GND option in no-prompt mode for SERVORD+

```

ADO $ RDT0 1 0 1 2 GND $ Y Y
DEO $ RDT0 1 0 1 2 GND $ Y Y

```

Option prompts

There are no changes to prompts. The GND option already exists.

Line class code compatibility

There are no changes to LCC compatibility for GND

Assignability

The following functionalities apply to this option:

- set functionality: NO
- subset functionality: NO
- DN functionality: NO
- key functionality: NO

The GND option is not a typical line option in that it gives added functions to the line or set. It determines how the line card detects when the subscriber goes off hook. It is a hardware function of the line card, transparent to the subscriber.

Option prerequisites

GND has the following prerequisites:

None

Notes

The following notes apply to GND:

This feature applies only to the supported line cards. It may be necessary to post the line at the MAP and BSY and RTS the line in order for the change to take effect

Feature identification

Feature number: A00002555

SERVORD+ Exceptions

none known.

Software optionality control (SOC)

NA

Element Management

NA

Command interface changes

NA

Security

NA

Configuration Walkthrough

NA



SN07 Feature Deltas

Product = CS 2000

A00002585 -- TMM Development for PTS Trunk (PT-IP)

Functional Description

Purpose:

This FN describes the new feature added to TMM by ACTID00002585 which includes the following new components:

1. Post by Carrier. This component allows TMM to post and perform maintenance actions on trunks based on a specific carrier.
2. Show trunk type. This component enhance the operation “PostByGatewayName” to add trunk type in result.
3. Add online help. This component provides online help for TMM.

Introduction

This document details the OAM&P functionality being delivered by the feature “TMM Support PTS Trunk, Post By Carrier” in SN07. This document will describe the changes being made to the web-based GUI and interface via OSSGate. This activity will deliver the changes required to extend TMM functionality to support the following:

- PTS Trunk maintenance--PTS trunk maintenance will be supported by TMM. All maintenance commands related to ISUP trunk and PRI trunk will be supported for PTS trunk.
- Post By Carriers name--In addition to selecting a trunk gateway, the user can select a specific carrier name, post trunks and perform all maintenance operations supported by “Maintenance by Gateway Name” today for ISUP, PRI and PTS trunks from GUI and OSSGate.
- General TMM Robustness Enhancements:
 - Show trunk types (ISUP, PRI, PTS) in post result sets.

- Return codes will be kept compliance with OSSGate NTP documents.
- TMM Help page.

For “PTS Trunk maintenance”, no changes are made on either web-based GUI or the interface via OSSGate.

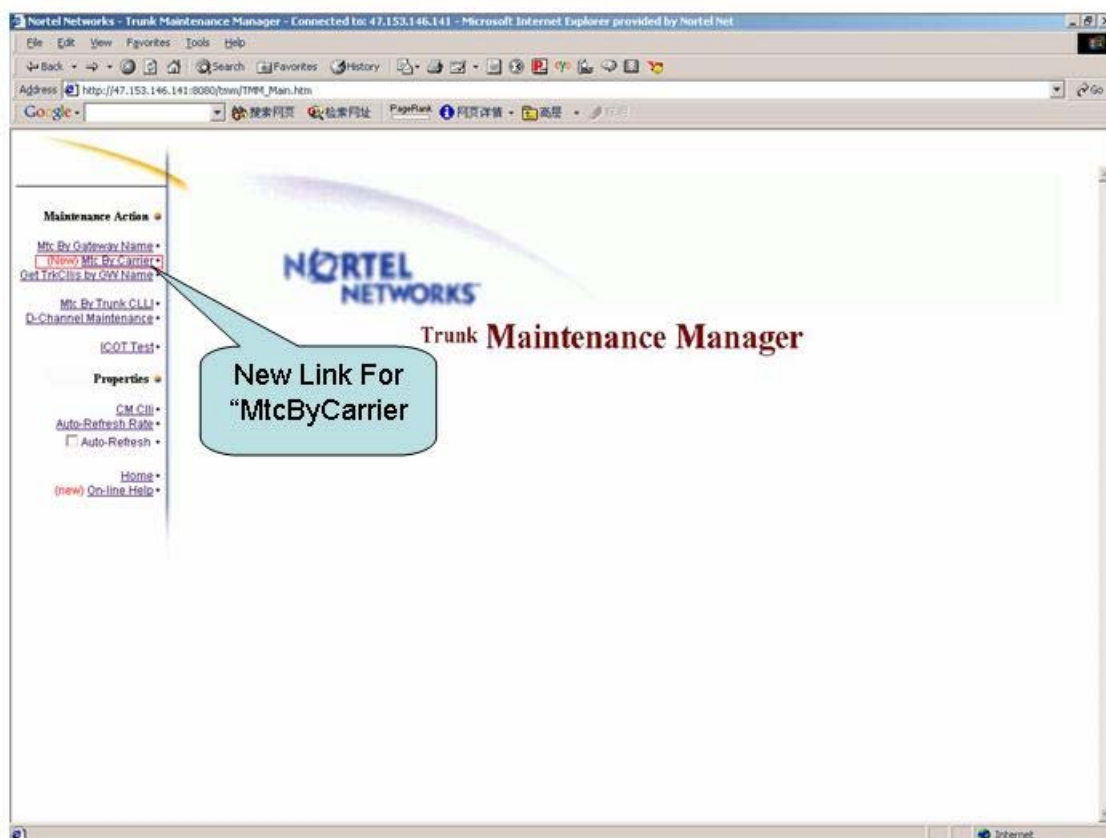
Web GUI Modifications

This section describes all the changes being made on web-based GUI by activity A00002585 in SN07. This section is not meant to be a complete description of the web-based GUI. The TMM NTP document will be updated to provide details of the changes.

Post By Carrier

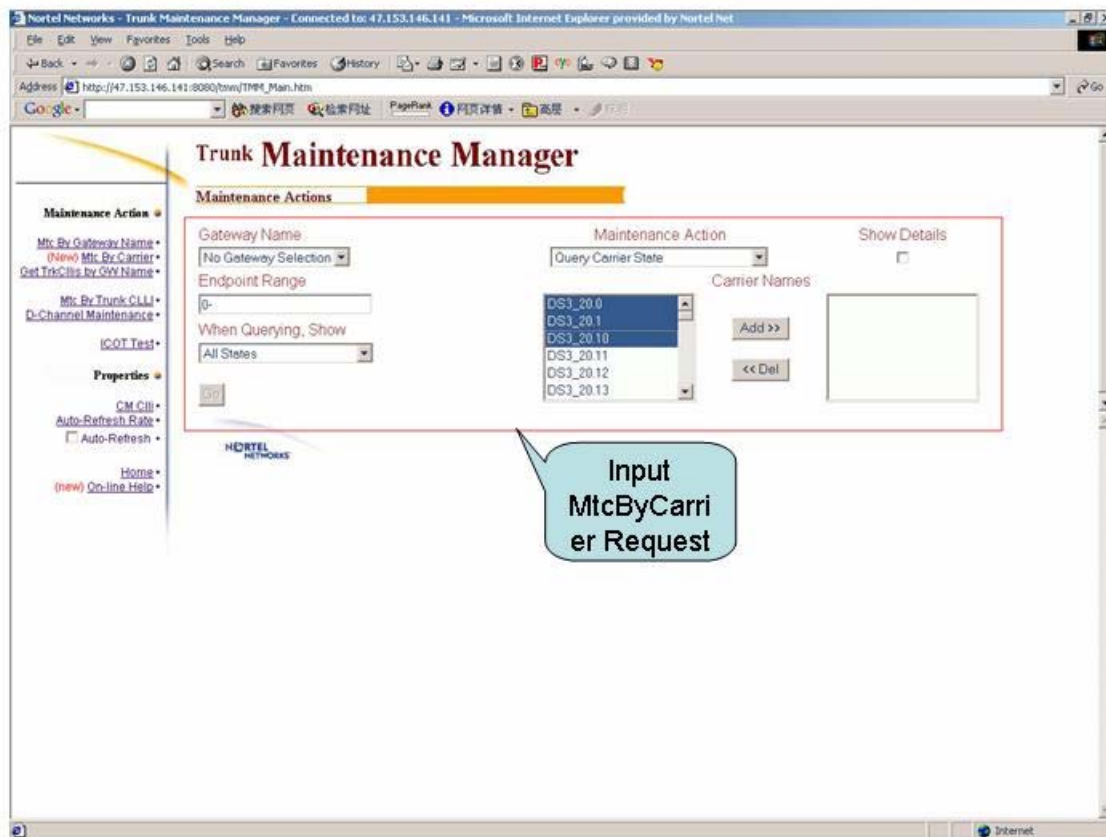
A new link “Mtc By Carrier” will be added on TMM main web page. (See the following figure.)

Mtc By Carrier link



After the link “Mtc By Carrier” is clicked, a web page as shown here will be displayed.

Prompt for Mtc By Carrier request



For a valid request of “MtcByCarrier”, one and only one gateway should be defined, one and only one action should be defined and at **least** one carrier should be selected.

If no carrier is selected it will post all the carriers.

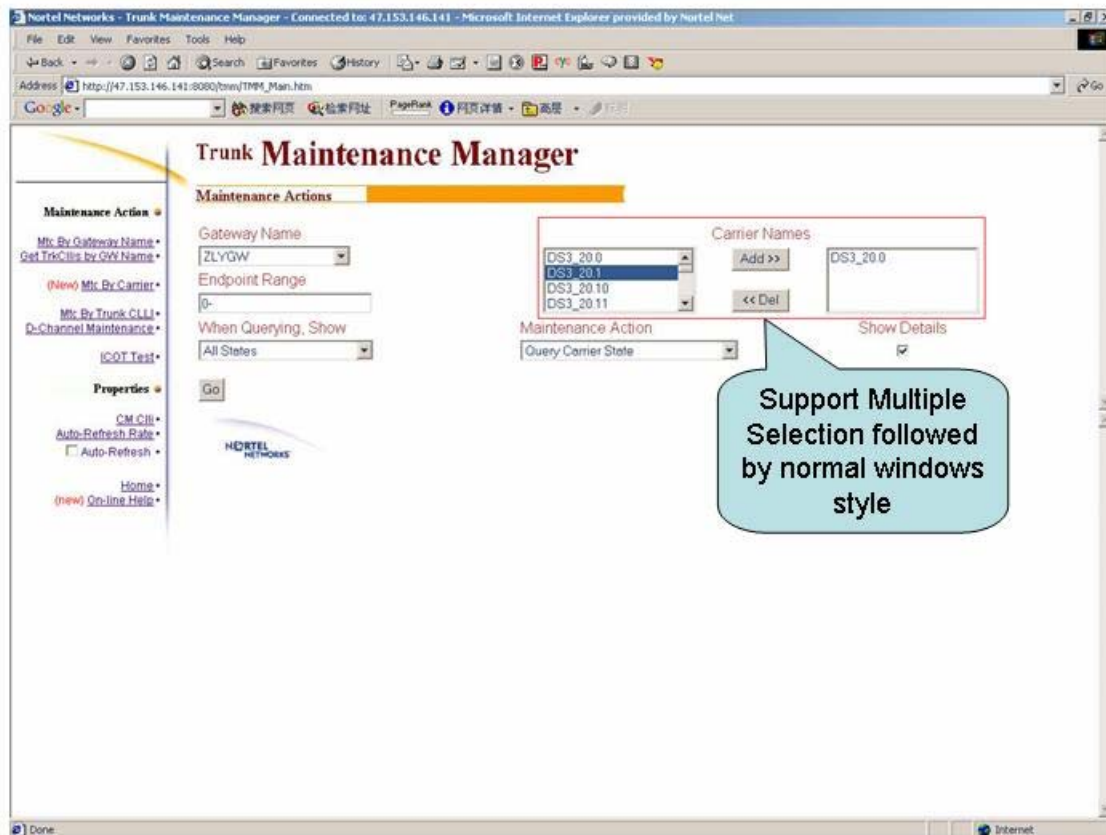
The gateway will be selected from drop list named “Gateway Names”. the action will be selected from drop list named “Maintenance Action”. The carrier will be selected from list box. After one item in the list box is highlighted, click button “Add” or “Del” to add or remove carriers from request input. Multiple selection with normal Windows style is supported. (For example, shift+mouse button, or ctrl+mouse button.) (See the following three figures.)

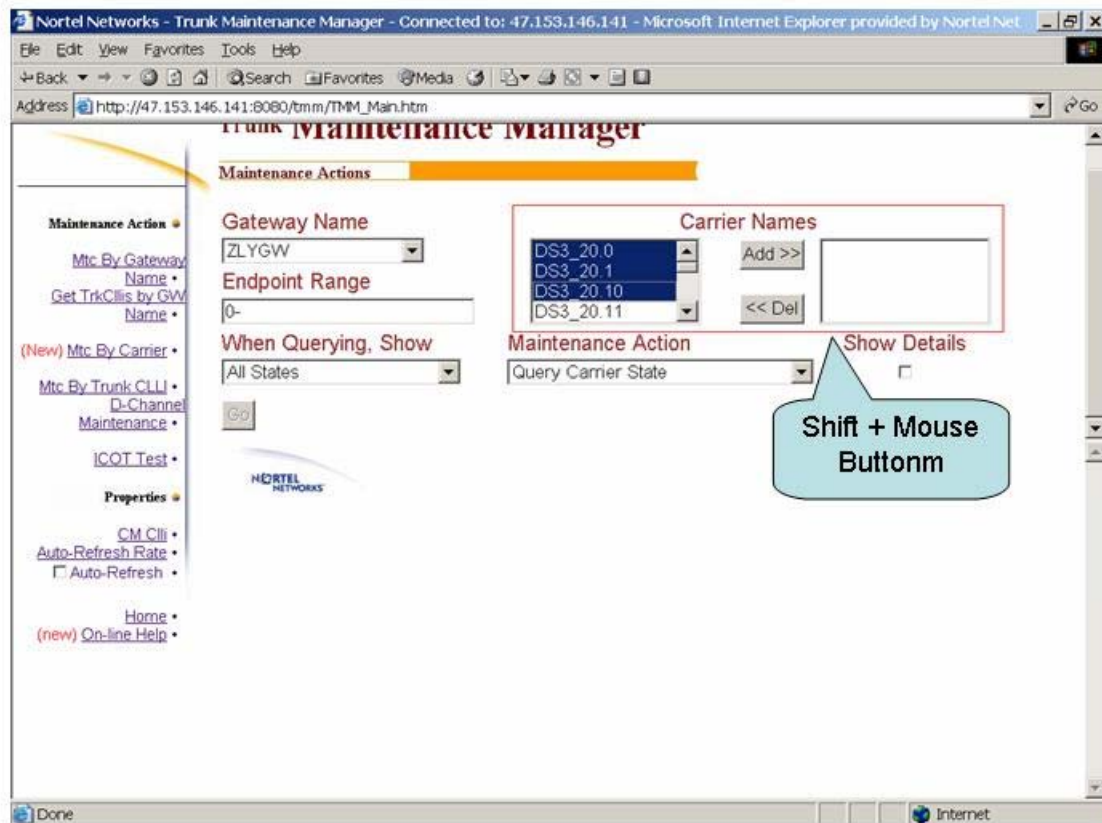
There are several options for the request “MtcByCarrier”.

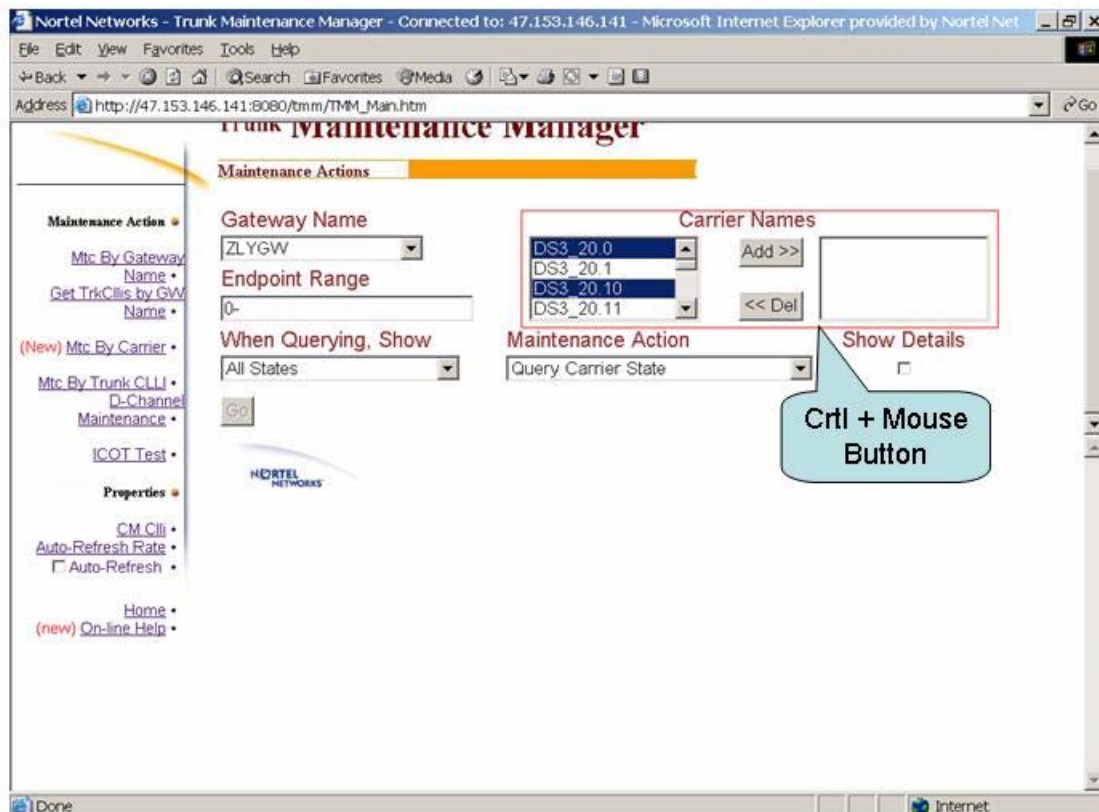
- “Endpoint Range”, its default is “0-”.

- “States Filter” which can be selected from the drop list “When Querying, Show”, its default is “All States”.
- “Show Details” which can be set by setting check box “Show Details”, its default is “false”.

Multiple selection permitted



Multiple selection with Shift + click

Multiple selection with Ctrl + click

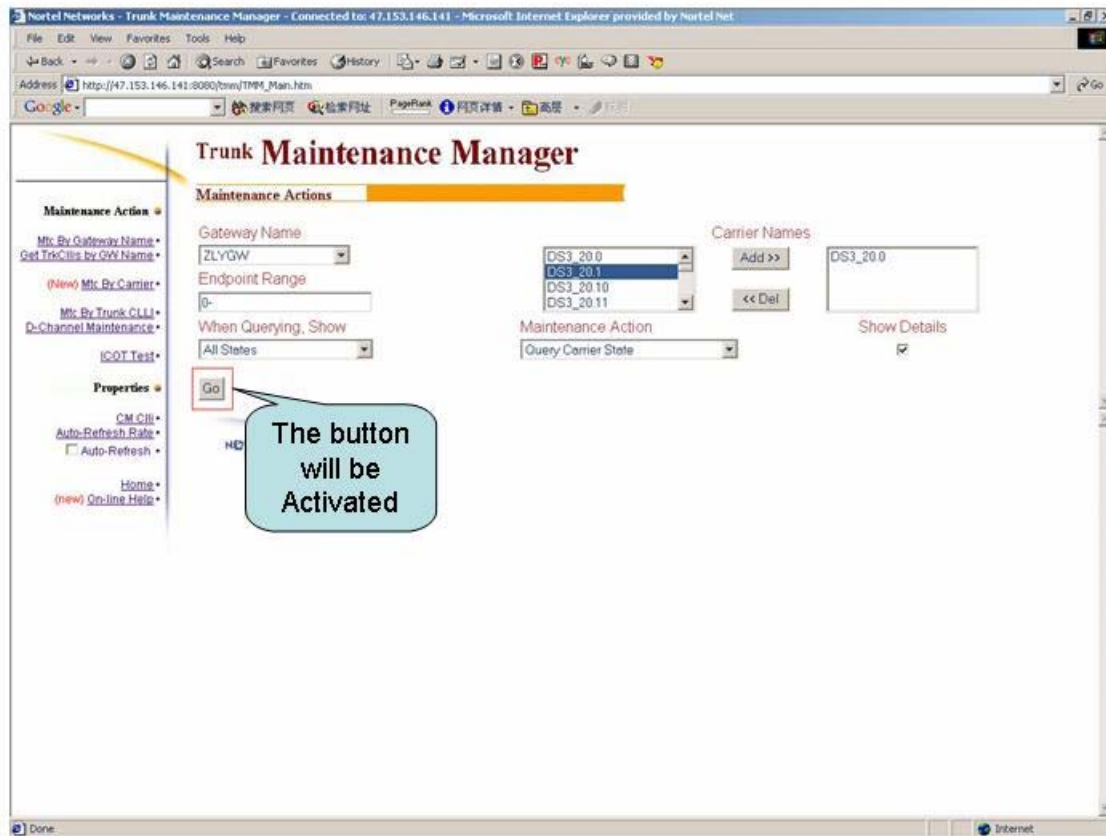
After gateway and carriers are defined, the button “go” will be activated. (See the following figure). After the button “go” is clicked, the corresponding response will be displayed.

Currently, six commands are supported by “MtcByCarrier” as illustrated in the six figures that follow.

- The response for the command “Query Carrier State”
- The response for the command “Post Carrier”
- The response for the command “Busy Carrier”
- The response for the command “Return Carrier to Services”
- The response for the command “Force Release Carrier”
- The response for the command “Installation Busy Carrier”

If the command failed, the error messages will be displayed. Please refer to “Error message for failed command” on page 528.

The “Go” button is activated



Response to “Query Carrier State”

Nortel Networks - Trunk Maintenance Manager - Connected to: 47.153.146.141 - Microsoft Internet Explorer provided by nortel.net

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites History

Address http://47.153.146.141:8080/tmm/TMM_Main.htm

Google 搜索网页 搜索网址 PageRank 网页评级 高层

Trunk Maintenance Manager

Maintenance Action

- Mix By Gateway Name
- Get TrkCltts by GW Name
- (New) Mix By Carrier
- Mix By Trunk CLLI
- D-Channel Maintenance
- ICOT Test

Properties

- CM Ctl
- Auto-Refresh Rate
- ☐ Auto-Refresh
- Home
- (new) On-line Help

Maintenance Actions

Gateway Name: ZLYGW

Endpoint Range: 0-

When Querying, Show: All States

Go

Carrier Names

DS3_20.0
DS3_20.1
DS3_20.10
DS3_20.11

Add >>

<< Del

DS3_20.0

Maintenance Action: Query Carrier State

Show Details ☒

Gateway Name: ZLYGW Node Number: 74 Filtered by State: ALL Endpoint Range: 1-25

Summary of Endpoints

Total Endpoints 25
INB 25

Endpoint Number	State
1	INB
2	INB
3	INB
4	INB

Done Internet

Response to “Post Carrier”

The screenshot shows the 'Trunk Maintenance Manager' web interface in a Microsoft Internet Explorer browser. The browser's address bar shows the URL: http://47.153.146.141:8080/tmm/TMM_Main.htm. The page title is 'Trunk Maintenance Manager'.

Maintenance Actions

Gateway Name: ZLYGW
 Endpoint Range: 0-
 When Querying, Show: All States
 Maintenance Action: Post Carrier
 Go

Carrier Names

DS3_20.0
 Add >>
 DS3_20.0
 << Del

Properties

CM CLI
 Auto-Refresh Rate
☐ Auto-Refresh
 Home
 (new) On-line Help

Total Endpoints

Total Endpoints 25
 UNKNOWN 1
 INB 24

Endpoint Number	State	Connected To	Direction	Signaling	PM Type	PM Number	Endpoint Name	Trunk CLLI	Trunk Member	PM Carrier	PM TimeSlot	Trunk Type
1	INB		2W	ISD ISD	GWC_NODE	6	DS3_20.0.1	T0	1	0	1	PRI
2	INB		2W	ISD ISD	GWC_NODE	6	DS3_20.0.2	T0	2	0	1	PRI
3	INB		2W	ISD ISD	GWC_NODE	6	DS3_20.0.3	T0	3	0	1	PRI
4	INB		2W	ISD ISD	GWC_NODE	6	DS3_20.0.4	T0	4	0	1	PRI
5	INB		2W	ISD ISD	GWC_NODE	6	DS3_20.0.5	T0	5	0	1	PRI
6	INB		2W	ISD ISD	GWC_NODE	6	DS3_20.0.6	T0	6	0	1	PRI
7	INB		2W	ISD ISD	GWC_NODE	6	DS3_20.0.7	T0	7	0	1	PRI

Last Refreshed: Tue Jul 22 15:53:45 UTC+0800 2003

Response to “Busy Carrier”

The screenshot displays the 'Trunk Maintenance Manager' web application in a Microsoft Internet Explorer browser. The interface includes a left-hand navigation menu with options like 'Maintenance Action', 'Properties', and 'Home'. The main content area is titled 'Maintenance Actions' and contains several input fields and buttons. The 'Gateway Name' is set to 'ZLYGW', 'Endpoint Range' is '0-', and 'When Querying, Show' is 'All States'. The 'Carrier Names' list includes 'DS3_20.0', 'DS3_20.1', 'DS3_20.10', and 'DS3_20.11'. The 'Maintenance Action' dropdown is set to 'Busy Carrier (BSY)'. A 'Go' button is present. Below the input fields, a summary box shows 'Summary of Endpoints' with 'Total Endpoints 25', 'INB 1', and 'MB 24'. At the bottom, a table lists the endpoints and their states.

Endpoint Number	State
1	MB
2	MB
3	MB
4	MB

Response to “Return Carrier to Services”

Nortel Networks - Trunk Maintenance Manager - Connected to: 47.153.146.141 - Microsoft Internet Explorer provided by nortel.net

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites History

Address http://47.153.146.141:8080/trunk/TMP1_Main.htm

Google 搜索网页 搜索网址 PageRank 网页评级 高层

Trunk Maintenance Manager

Maintenance Actions

Maintenance Action

- Mix By Gateway Name
- Get TrkClist by GW Name
- (New) Mix By Carrier
- Mix By Trunk CLLI
- D-Channel Maintenance
- ICOT Test

Properties

- CM CUI
- Auto-Refresh Rate
- ☐ Auto-Refresh
- Home
- (new) On-line Help

Gateway Name: ZLYGW

Endpoint Range: 0-

When Querying, Show: All States

Go

Carrier Names

DS3_20_0
DS3_20_1
DS3_20_10
DS3_20_11

Add >>

<< Del

DS3_20_0

Maintenance Action: Return Carrier to Service (RTS)

Show Details ☒

Gateway Name: ZLYGW Node Number: 74 Filtered by State: ALL Endpoint Range: 1-25

Summary of Endpoints

Total Endpoints 25
PMB 24
INB 1

Endpoint Number	State
1	PMB
2	PMB
3	PMB
4	PMB

Done Internet

Response to “Force Release Carrier”

Nortel Networks - Trunk Maintenance Manager - Connected to: 47.153.146.141 - Microsoft Internet Explorer provided by nortel.net

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites History

Address http://47.153.146.141:8080/trunk/TMP1_Man.htm

Google 搜索网页 搜索网址 PageRank 网页评级 高层

Trunk Maintenance Manager

Maintenance Action

- Mix By Gateway Name
- Get Trunk Lines by GW Name
- (New) Mix By Carrier
- Mix By Trunk CLLI
- D-Channel Maintenance
- ICOT Test

Properties

- CM CLLI
- Auto-Refresh Rate
- ☐ Auto-Refresh
- Home
- (new) On-line Help

Maintenance Actions

Gateway Name: ZLYGW

Endpoint Range: 0,1,2,3,4,5,6,7,8,9

When Querying, Show: All States

Go

Carrier Names

DS3_20_0
DS3_20_1
DS3_20_10
DS3_20_11

Add >> << Del

DS3_20_0

Show Details ☒

Maintenance Action: Force Release Carrier (FRLS)

Gateway Name: ZLYGW

Node Number: 74

Filtered by State: ALL

Endpoint Range: 1-1,2-2,3-3,4-4,5-5,6-6,7-7,8-8,9-9

Summary of Endpoints

Total Endpoints 9
MB 9

Endpoint Number	State
1	MB
2	MB
3	MB

Done Internet

Response to “Installation Busy Carrier”

The screenshot displays the 'Trunk Maintenance Manager' web application in a Microsoft Internet Explorer browser. The interface includes a left-hand navigation menu with options like 'Maintenance Action', 'Properties', and 'Home'. The main content area is titled 'Maintenance Actions' and contains several input fields and buttons for configuring maintenance actions. Below these fields, a summary of endpoints is shown, followed by a table of endpoint numbers and their states.

Maintenance Actions

Gateway Name: ZLYGW
Endpoint Range: 0-
When Querying, Show: All States
Carrier Names: DS3_20.0, DS3_20.1, DS3_20.10, DS3_20.11
Maintenance Action: Installation Busy Carrier (BSY INB)
Show Details: ☒

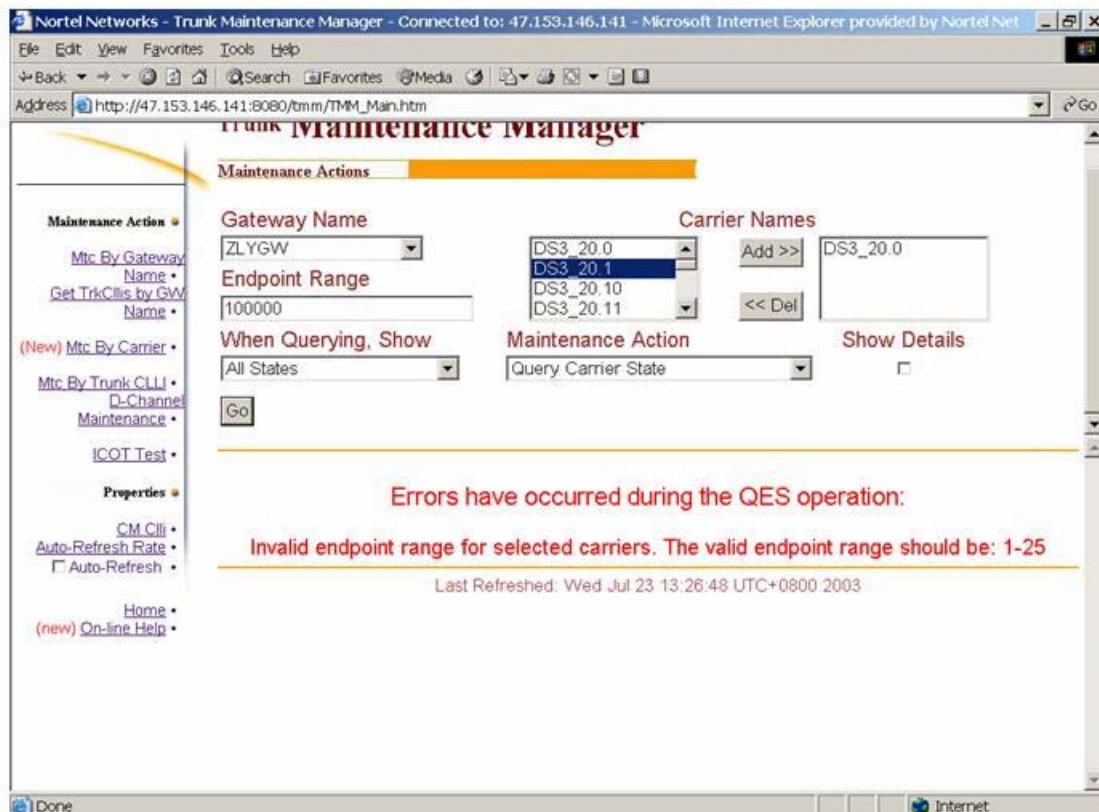
Go

Gateway Name: ZLYGW Node Number: 74 Filtered by State: ALL Endpoint Range: 1-25

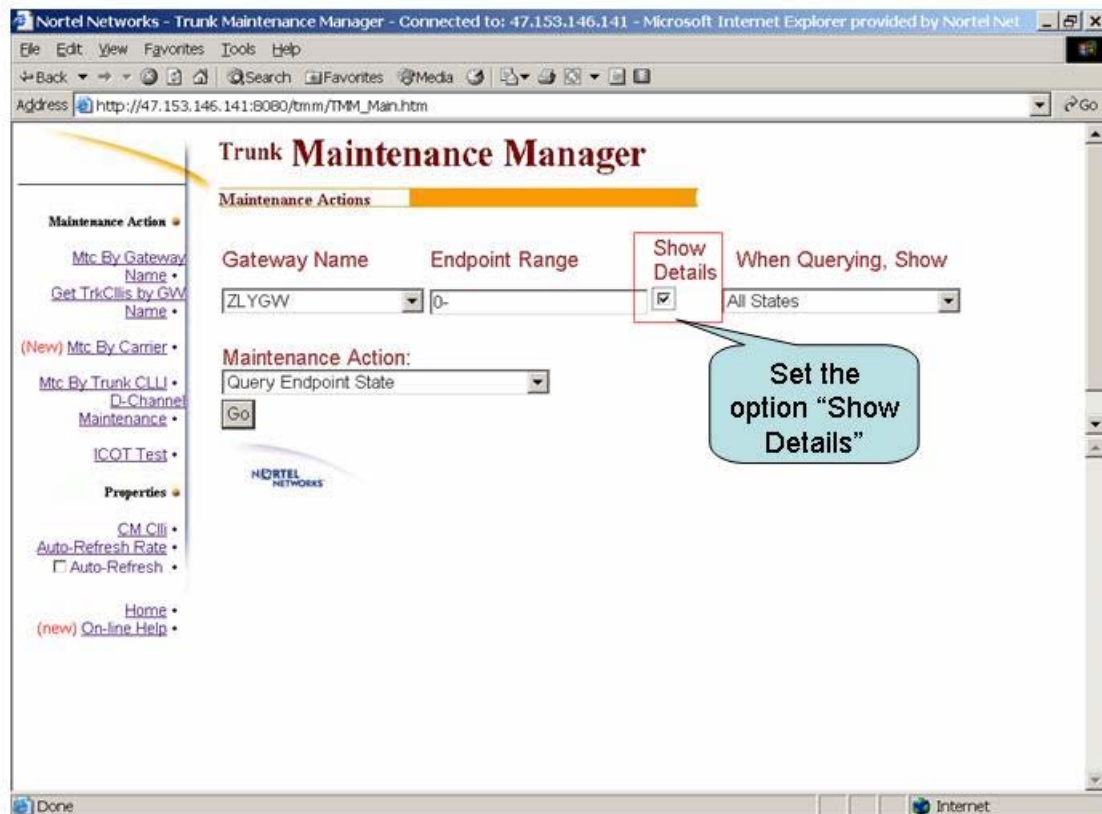
Summary of Endpoints

Total Endpoints 25
PMB 15
INB 1
MB 9

Endpoint Number	State
1	MB
2	MB
3	MB
4	MB

Error message for failed command**Show trunk types in post result set**

For the command “Post By Gateway” with the option “Show Details” to be set as seen in the following figure, the corresponding response will include trunk type. Please refer to “Trunk Type response” on page 530.

“Show Details” option set

Trunk Type response

Trunk Maintenance Manager

Maintenance Actions

Gateway Name: ZLYGW Endpoint Range: 0- Show Details: ☒ When Querying, Show: All States

Maintenance Action: Post Endpoints

Go

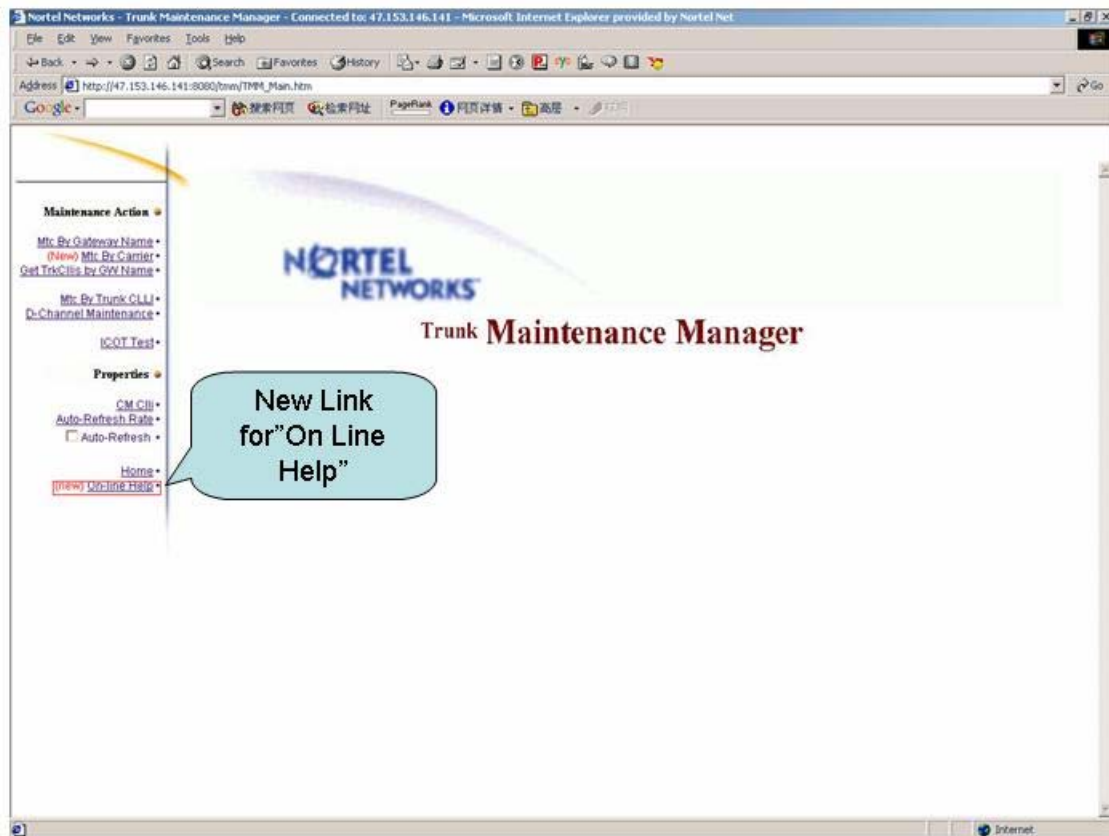
Total Endpoints 1104
UNKNOWN 46
INB 1058

Endpoint Number	State	Connected To	Direction	Signaling	PM Type	PM Number	Endpoint Name	Trunk CLLI	Trunk Member	PM Carrier	PM TimeSlot	Trunk Type
1	INB		2W	ISD ISD	GWC_NODE	6	DS3_20.0.1	T0	1	0	1	PRI
2	INB		2W	ISD ISD	GWC_NODE	6	DS3_20.0.2	T0	2	0	1	PRI
3	INB		2W	ISD ISD	GWC_NODE	6	DS3_20.0.3	T0	3	0	1	PRI
4	INB		2W	ISD ISD	GWC_NODE	6	DS3_20.0.4	T0	4	0	1	PRI
5	INB		2W	ISD ISD	GWC_NODE	6	DS3_20.0.5	T0	5	0	1	PRI
6	INB		2W	ISD ISD	GWC_NODE	6	DS3_20.0.6	T0	6	0	1	PRI
7	INB		2W	ISD ISD	GWC_NODE	6	DS3_20.0.7	T0	7	0	1	PRI

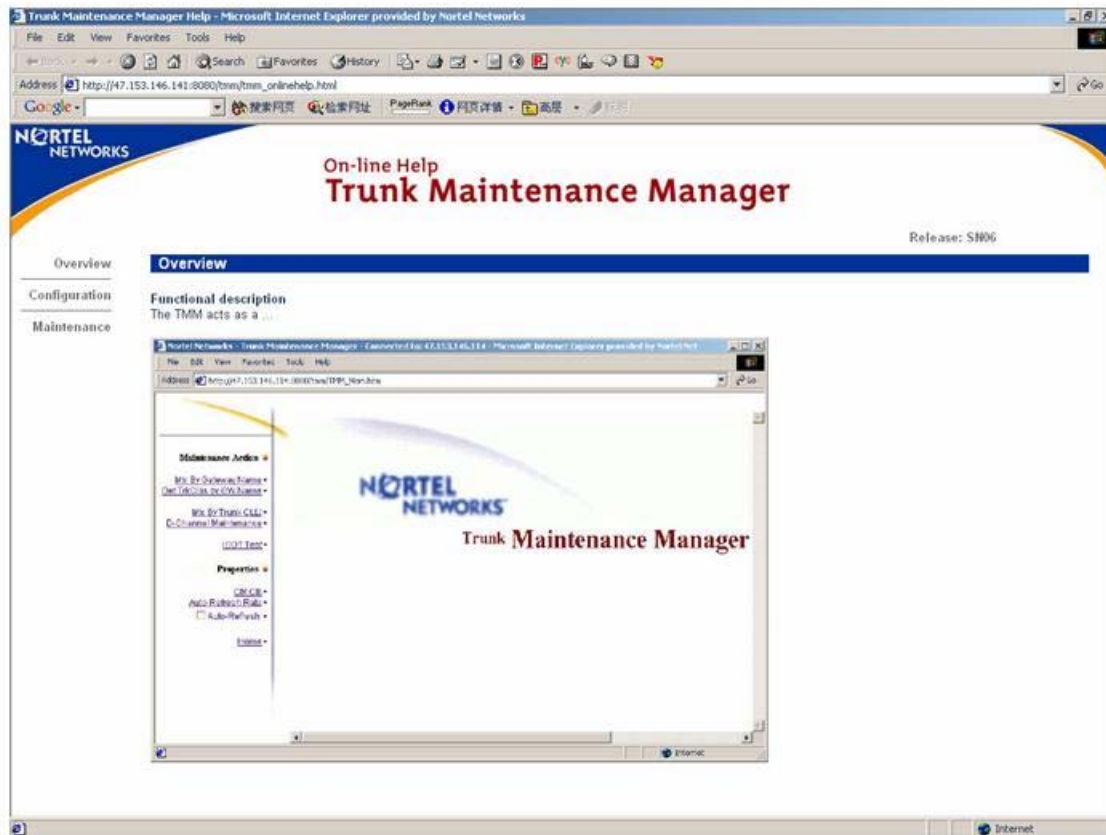
Last Refreshed: Tue Jul 22 15:49:17 UTC+0800 2003

Adding TMM Help

A new link will be added on TMM web page (see the following figure). After the link is clicked, a help window including help web page will be popped out (see “Online Help web page” on page 532).

Online Help link

Online Help web page



Hardware Requirements or Dependencies

Not Applicable.

Software Requirements or Dependencies

Not Applicable.

Limitation and Restrictions

Not Applicable.

Interactions

Not Applicable.

Applicable customer facing sections

Fault Management

Logs

N/A____

Alarms

N/A____

Configuration

Data Schema	N/A___
User Interface	X___
Element Management	N/A___
Security	X___
Service Order	N/A___
Office Parameters	N/A___

Accounting (includes AMA billing)N/A___

Performance (includes operational measurements) N/A___

Glossary

Not Applicable.

Appendix A

This document “TMM_A0002585_Commands_Responses_Errors.fm” on <http://ptm> describes the changes being made to the interface via OSSGate by activity A00002585 in SN07. Please refer to document “TMM_A0002585_Commands_Responses_Errors.fm” for all examples of changes.



SN07 Feature Deltas

Product = CS 2000

A00002741 -- Supernode Billing Application Base Real Time Billing Robustness (Succession on DMS)

Excerpts from the Design Description

Purpose

This activity robustifies SBA Base RTB to auto recover from downstream and network connectivity problems once the issues are resolved. This functionality will be optionalized. As well, the activity addresses many other deficiencies tracked by CRs and other means.

Problem Symptoms

Each item of functionality to be considered by this activity is grouped below, along with a summary explanation for the item.

1. Deletion/modification of underlying schedule tuple:

Problem Description: The billing stream Schedule tuple configuration is shared by both Outbound file transfer and the RTB Destination configuration. If the schedule tuple is removed or certain fields are modified while the corresponding RTB Destination is InSv, the RTB Destination would fail ungracefully.

Solution Description:

- i. This activity displays a message to the user asking him to OffL and delete any possible corresponding RTB Destination before modifying/deleting the associated Schedule tuple if the protocol of the tuple is RFTPW.
- ii. Also, RTB will now check for the current schedule tuple every transfer event irrespective of whether failure has occurred or not. If an active file is being transferred by RTB, and the schedule tuple is deleted or the protocol changed, the current active file will continue

to transfer until it is closed as is the case currently. If another active file is opened, RTB will move to SYSB state as is the behavior now.

2. Auto Recovery: “Test File transfer” and “Temp File renaming on DPMS”:

Problem Description: In order for RTB to recover from a user-defined maximum number of consecutive outages in connectivity between the SDM and the DPMS, manual intervention was required (i.e. have to BSY/RTS RTB Destination in billmtc) in order to resume real time transfer of future open billing files to the DPMS.

Also, a Temporary open file (with suffix.tmp) exists on the DPMS to collect the billing data sent by RTB. Whenever there was a LAN failure or when SDM/ Downstream processor reboots, this open file was not complete nor properly named. Its corresponding file on the SDM is moved from Open to ClosedNotSent (CNS) directory, and renamed. Thus, when RTB resumed service, a new open file was transferred and thus a new.tmp file was created on the DPMS. Thus there would be two.tmp files at the DPMS.

Solution Description:

- i. Enhancements are made to RTB such that after the maximum consecutive number of failures for a Destination, it will move to ISTB state to denote that RTB will initiate an autorecovery process.

When the above is encountered, it then starts a monitoring operation consisting of FTPing a test file (of size 10MB, named as NetworkTest) to the DPMS test file directory, and analyzing the response to figure out if the test transfer was successful, or in case of error, if it was due to a network issue or a non-network issue.

Below are the 2 resulting scenarios:

–If it is a non-network issue, RTB will sleep until a new file is open on the SDM and then resume its INSV state.

–If it is a network issue, RTB will try the operation again until it succeeds 3 consecutive times or until a non-network issue is detected, in which case the previous stated behavior above for this case is followed.

The location of the test files on the downstream can be configured through RMI (BILLMTC).

- ii. Enhancements are made such that whenever RTB resumes operation after an outage, the <filename>.tmp file on the downstream (for the associated stream/destination configuration) will be renamed to <filename>.partial before opening a new.tmp file. The location of this partial file is configurable through RMI (BILLMTC).

Both the test file transfer and partial file renaming functionality are one combined auto-recovery option (which applies to any/all configured RTB Destinations), which can be turned ON or OFF.

If the user sets the option to OFF, manual intervention will be required to return to service the RTB Destination after the configured maximum # of consecutive network failures occurs. In this case, RTB will go to SYSB state, and manual intervention is required to ever get out of this state, as is the behavior now.

3. Interoperability between RTB and base SBA status:

Problem Description: RTB behavior is heavily dependent on the status of base SBA resources such as the stream state, and the application status of SBA. RTB fails ungracefully when base SBA stream or application states change.

Solution Description:

- i. The RTB Destination will check the underlying stream status before executing the transfer event. If it is not INSV, a designlog and custlog will be raised, and the transfer will not be executed.
- ii. Whenever SBA is restarted, RTB will check the previous state for each RTB Destination and will bring the Destination INSV if it was previously INSV or ISTB or SYSB at the time of SBA application shutdown.

Limitations and restrictions

- There already exists a limitation on SBA, which is the following: Multiple schedule tuples must not be configured (across OR within SDMs) sharing the same 'remote destination IP', 'remote directory', 'file format' (DIRP), and 'File_Extension.' If this is not respected, collisions between billing filenames may result. This feature adds more of a limitation based on the above, which is the following: Multiple schedule tuples must not be configured (across OR within SDMs) sharing the same 'remote destination IP' and 'remote directory', and where there exists at least 1 RTB Destination configuration (on any SDM) based upon one of these underlying schedule tuple configurations. If this is not respected, and the Auto-recovery option is turned ON, then one transfer may remove files owned by another transfer.
- A new limitation exists if the Auto-recovery option is turned ON. Multiple RTB Destinations must not be configured (across OR within SDMs) with the same 'partial file location' OR the same 'test file location' on the DPMS. If this is not respected, collisions between files may result.

Definitions & Abbreviations

Acronym	Expansion
CNS	Closed Not Sent
FTP	File Transfer Protocol
MIB	Management Information Base
RMI	Remote Maintenance Interface
RTB	Real Time Billing
SBA	SuperNode Billing Application
DPMS	Data Processing and Management System
CM	Computing Module
SDM	SuperNode Data Manager

Product = CS 2000

A00002744 -- SBA: Automatic Recovery File Closure (Succession on DMS)

Description

If the core SBA application is unable to send billing data to the SDM SBA applications, core SBA changes its state to backup mode. In backup mode, the core stores billing data in backup storage. Once communication resumes between the core SBA and SDM SBA, the core SBA will transition from backup mode to recovery mode. During recovery, the core SBA will send the current billing data and the stored backup billing data to the SDM SBA. SDM SBA will open separate files to store the current data and the billing data recovered from backup storage. Once all billing data has been recovered from backup storage, core SBA will transition from recovery mode to normal mode.

For each billing stream configured in SBA, its corresponding billing files can be configured to be rotated based on elapsed time since the file was opened. The crafts person must specify a maximum file size and a maximum number of records for each billing file. In addition to these facilities for file closure, this feature brings in a mechanism to close the recovery file as soon as the SBA core transitions from recovery mode to normal mode, irrespective of the file closure criteria.

Hardware Requirements or Dependencies

None.

Software Requirements or Dependencies

- SuperNode Billing Application (SBA) is installed and InSv.
- Billing configured on the CM.

Limitations and restrictions

None

Interactions

None

Applicable customer facing sections

Existing logs will be retained. No new logs are introduced as part of the feature.

Fault Management

Logs N/A

Alarms N/A

Configuration

Data Schema N/A

User Interface N/A

Element Management N/A

Security N/A

Service Order N/A

Office Parameters N/A

Accounting (includes AMA billing) N/A

Performance (includes operational measurements) N/A

Glossary

Term	Description
Automatic Message Accounting	Telcordia specification for accounting records.

Term	Description
Automatic Message Accounting Data Networking System (AMADNS).	System for transferring accounting records from a generating system to application systems. Comprises a Data Server component and a Data Processing and Management System (DPMS) component.
CDR	Call Detail Record
Data Processing and Management System (DPMS)	System for receiving accounting records from Data Servers and processing the records as required for transfer to application systems.
data server	Component that collects accounting records from a generating system.
Digital Multiplex System (DMS)	DMS core Digital telephone switch
Device-Independent Recording Package (DIRP)	file format file format used by SBA to store billing records, based on the DIRP billing file format on the DMS core
File Transfer Protocol (FTP)	application protocol for transferring files via Internet Protocol (IP)
generating system	Component that generates accounting records, such as the DMS core.
Generic Requirements (GR)	Telcordia specification document
Management Information Base (MIB).	In the context of this document, refers to the persistent data repository where SBA configuration information is kept. Individual values stored within the MIB are referred to as MIB values
Non-Computing module Load (NCL)	software load for components other than the DMS core; in the context of this document, software load for the SDM
outbound file transfer	SBA file transfer mode where SBA initiates the transfer of billing files to a downstream FTP server.
recovery file	A file on the SDM in which the SDM SBA saves the billing data recovered from the core SBA backup storage.
Supernode Billing Application (SBA)	Accounting collection data server that resides on the SDM. Implements the Data Server function of an AMADNS environment.
Supernode Data Manager (SDM)	Motorola FX computing node upon which resides Operations, Administration, Maintenance, and Provisioning applications / Fault, Configuration, Accounting, Performance, and Security management applications. SDM xxrefers to a given SDM NCL release, where xx is a two-digit number.
Reset EOS	Message from CM Indicating the end of a session.

Product = CS 2000

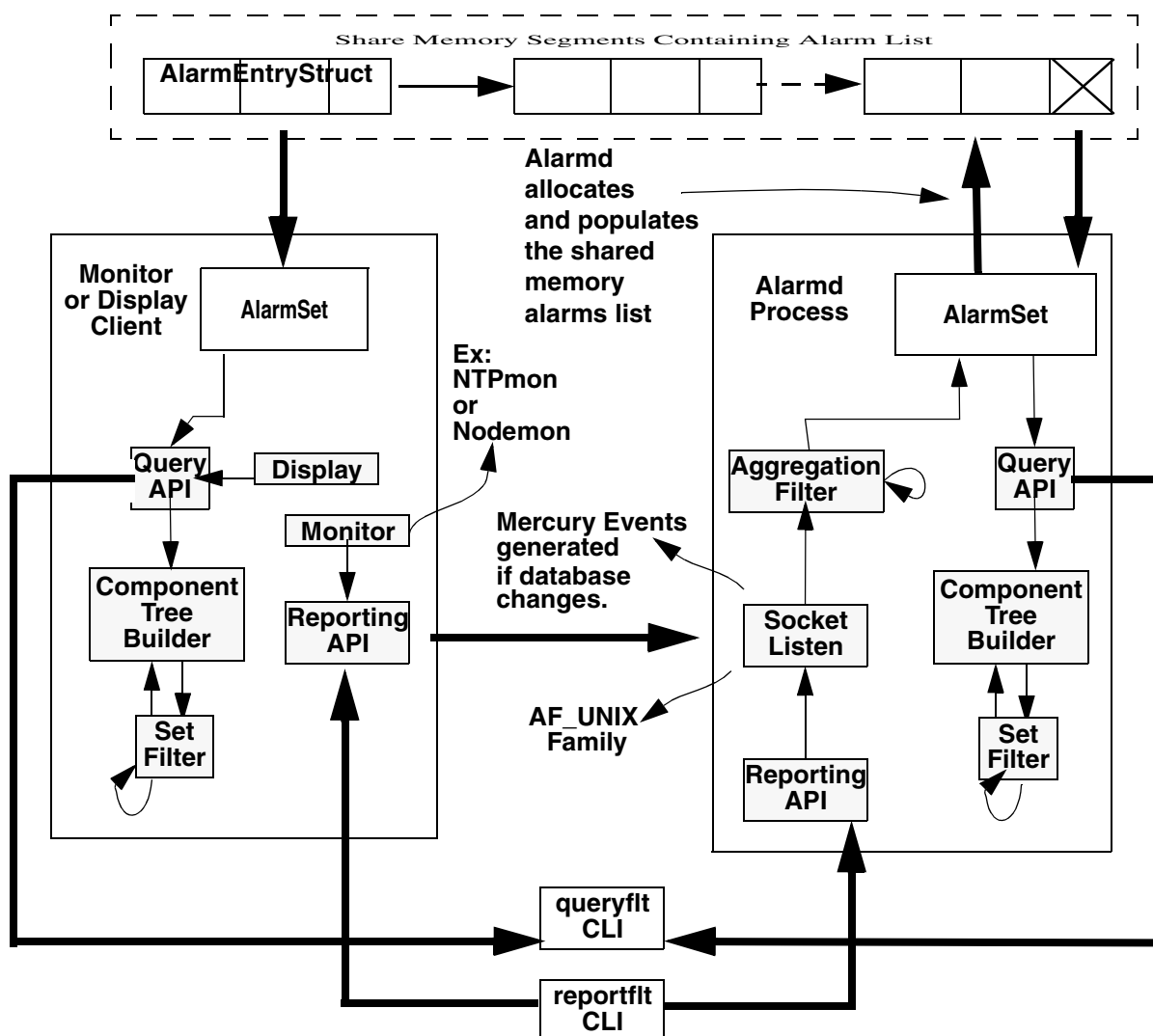
A00002757 -- NSDM Fault Management HA (Succession on DMS)

Functional Description

This feature provides a generic framework for centralizing fault information for the Next Generation SDM (CBM) product and for the SSPFS platform.

The mandate is to collect detailed fault information about components in the CBM cluster, maintain a list of current alarms, summarize the list in a hierarchical fashion, and report this information to clients in the desired fashion.

Alarmd Server/Client Process and Data Flow



User Interfaces

This feature will require changes to the QueryCBM command in the CBMMTC maintenance tool, as well as various Logs commands for respective CBMMTC levels.

Hardware Requirements or Dependencies

SSPFS defined platform.

Software Requirements or Dependencies

A00003617 - SSPFS Alarmd Integration will provide the light control API, and component monitors for this feature.

Limitations and restrictions

N/A

Interactions

A00003617 - SSPFS Alarmd Integration will provide system level monitors that will use the ReportingAPI part of this feature to record any alarms. It will also make use of the Query API in this feature to retrieve alarms stored in the Alarms Database.

A00002164 - The Application Manager (SAM) for HA will use the Reporting API part of this feature to record any alarms. It will also make use of the Query API in this feature to retrieve alarms stored in the Alarms Database.

Applicable customer facing sections

Fault Management

Logs __x__

Alarms _____

Configuration

Data Schema _n/a_

User Interface __x__

Element Management _n/a_

Security _n/a_

Service Order _n/a_

Office Parameters _n/a_

Accounting (includes AMA billing) _n/a_

Performance (includes operational measurements) n/a

Indicate with an X if you are completing the sections of the DDOC listed below. Indicate with “N/A” if these sections do not apply to this functionality.

Realtime n/a

Engineering Information x

Fault Management for A00002757

Fault management strategy

This feature provides functionality to a SSPFS Platform for the aggregation of Alarms into one database. Logs will be generated by the reporting entity when using the *Reporting API* to enter/update/clear alarms in the database.

Fault management tools and utilities

Two command line tools will be available to report and query faults contained in the *Alarm Database*.

The tools are called *queryflt*, and *reportflt*.

Logs

Explanation

Log Title: Report Alarm

Name: Report Alarm Log

Description:

This log is sent when requested by the entity that is reporting an alarm.

Event type: Customer Log

Format

```
_V2_~I=CBM~H=<hostname>~A=<application>~S=<seqNum>~~
<reportName><reportNum> NONE <eventType> <description>
      ComponentID: <componentID>
      Category: <categoryString>
```

Note: The *I=CBM* will be changed to reflect the currently defined network element name.

Field descriptions

Field	Value	Description
hostname	variable	Hostname of the cluster on which the log is being generated.
application	variable	Name of the application for which the alarm is raised.
seqNum	variable	Sequence number of the log being generated.
reportName	variable	The Customer Log report name (e.g.: CBM)
reportNum	variable	The Customer Log report number (e.g.: 300).
alarmLevel	variable	The alarm level for this alarm, one of: Cleared, Warning, Minor, Major, Critical, or Indeterminate.
eventType	variable	The Customer Log event type.
description	variable	Description for this particular alarm. Not describing the problem that happened, but describing what the alarm relates to or represents.
timeStamp	variable	This is the time at which the alarm was raised.
componentID	variable	This field is specified by the application to include the name of the component being alarmed (see definitions in section "1.7.4 Use of component name" on page 33 for details of how to specify this field).
categoryString	variable	The alarm category for this alarm.
probableCauseStr	variable	Probable cause information.
specificProblemStr	variable	Further qualifies the probable cause for this alarm.

Action

The action required is dependent on what the particular alarm report is. Any specific action will be described in the *description* field above.

Associated Operational Measurements or Performance Measurements

N/A

Additional information

Explanation

Log Title: Clear Alarm

Name: Clear Alarm Log

Description:

This log will be generated when a client clears an existing alarm in the alarms database managed by Alarmd.

Event type: Customer Log

Format

```
_V2_~I=CBM~H=<hostname>~A=<application>~S=<seqNum>~~
<reportName><reportNum> NONE <eventType> <description>
      ComponentID: <componentID>
      Category: <categoryString>
```

Note: The *I=CBM* will be changed to reflect the currently defined network element name.

Field descriptions

Field	Value	Description
hostname	variable	Hostname of the cluster on which the log is being generated.
application	variable	Name of the application for which the alarm is raised.
seqNum		Sequence number of the log being generated.
reportName	variable	The Customer Log report name (e.g.: CBM)
reportNum	variable	The Customer Log report number (e.g.: 300).
eventType	variable	The Customer Log event type.
description	variable	Description for this particular alarm. Not describing the problem that happened, but describing what the alarm relates to or represents.
componentID	variable	This field is specified by the application to include the name of the component being alarmed (see definitions in section “1.7.4 Use of component name” on page 33 for details of how to specify this field).
categoryString	variable	The alarm category for this alarm.

Action

No action required.

Associated Operational Measurements or Performance Measurements

N/A

Additional information

N/A

Explanation**Log Title: Alarm Summary****Name: Alarm Summary Log****Description:**

This log is sent periodically by Alarmd, to summarize the Alarms in the database managed by Alarmd.

Event type: Customer Log**Format**

```
_V2_~I=CBM~H=<hostname>  
  Timestamp: <timeStamp>  
  Minor: <minorCount>  
  Major: <majorCount>  
  Critical: <criticalCount>  
  Most Recent Minor: <MRMinorComponentID>  
  Most Recent Major: <MRMajorComponentID>  
  Most Recent Critical: <MRCriticalComponentID>
```

Note: The *I=CBM* will be changed to reflect the currently defined network element name.

Field descriptions

Field	Value	Description
hostname	variable	Hostname of the cluster on which the log is being generated.
timeStamp		
minorCount		
majorCount		
criticalCount		

Field	Value	Description
MRMinorComponentID		
MRMajorComponentID		
MRCriticalComponentID		

Action

N/A

Associated Operational Measurements or Performance Measurements

N/A

Additional information

N/A

Product = CS 2000**A00002766 -- Add Extension Registers for AMA OMs (Succession on DMS)*****Functional Description*****AMA OMs**

The ATTAMA OM group now has the maximum limit of 32 registers. Another group will be created to contain the extra extension registers. Only the extension registers for AMANS and AMUNANS will reside in the new ATTAMA2 OM group. The maximum register value for this group is now 32767 before it resets to 0. The extension register will allow capturing the number counter rollovers.

The new extension functionality will be implemented under SOC control. This will allow for controlled customer implementation and also provide the ability to disable the new extension if required.

The following shows the existing ATTAMA group along with the new ATTAMA2 group.

```
ATTAMA
CLASS:    ACTIVE
START:2002/12/24 11:45:00 TUE; STOP: 2002/12/24 11:56:30 TUE;
```

SLOWSAMPLES:	7 ;	FASTSAMPLES:	69 ;
AMORIGS	AMORIGS2	AMTRMT	AMTRMT2
AMNOTRMT	AMANS	AMRCSTPD	AMRCSTP2
AMLTSTPD	AMEDSTPD	AMNASTPD	AMRC411
AMLT411	AMED411	AMNA411	AMRC555
AMLT555	AMED555	AMNA555	AMRCTRRCR
AMLTTRCR	AMRCOTHR	AMLTOTHR	AMEDOTHR
AMNAOTHR	AMRCLONG	AMLTLONG	AMUNANS
AMRCSST	AMSST	AMDA555	AMDA411

0	0	0	0	0
	0	0	0	0
	0	0	0	0
	0	0	0	0
	0	0	0	0
	0	0	0	0
	0	0	0	0
	0	0	0	0
	0	0	0	0

ATTAMA2

CLASS: ACTIVE

START:2002/12/24 11:45:00 TUE; STOP: 2002/12/24 11:56:30 TUE;

SLOWSAMPLES: 7 ; FASTSAMPLES: 69 ;

AMANS2 AMUNANS2

0	0	0

Hardware Requirements or Dependencies

None

Software Requirements or Dependencies

The capabilities will be under SOC control.

This activity only impacts offices using the Bell Core AMA billing format.

Limitations and restrictions

None

Interactions

The existing OM groups will not be changed. The new groups will contain only new registers. The new OM groups are:

- ATTAMA2

Applicable customer facing sections

Fault Management

Logs

__N/A__

Alarms	__N/A__
Configuration	
Data Schema	__N/A__
User Interface	__N/A__
Element Management	__N/A__
Security	__N/A__
Service Order	__N/A__
Office Parameters	__N/A__
Accounting (includes AMA billing)	__N/A__
Performance (includes operational measurements)	__X__

Performance for A00002766

Performance management strategy

This feature provides the new OM group ATTAMA2.

Performance management tools and utilities

None

Performance Measurements (PM), Operational Measurements (OM), and stats

PM, OM, and stats format

N/A

OM Group ATTAMA2 (applies only to DMS)

OM description

OM Group ATTAMA2

The group ATTAMA2 is only pegged when the BAS00023 SOC is ON.

This group is used for register overflows from the OM group ATTAMA.

Release history update

The OM group is being provided new in the UCS20 release.

Registers

OM group registers display on the MAP terminal as follows:

```
ATTAMA2
CLASS:    ACTIVE
START:2002/12/24 11:45:00 TUE; STOP: 2002/12/24 11:56:30 TUE;
SLOWSAMPLES:    7 ; FASTSAMPLES:    69 ;
      AMANS2 AMUNANS2

      0          0          0
```

Group structure

This OM group provides 2 pre-defined tuples.

Associated OM groups

This OM group is used as register overflows for the OM group ATTAMA.

Associated functional groups

None

OM group registers logic flow chart

Refer to the comments in the Associated Register section.

Register (applies only to DMS)

Register description

AMANS2 - overflow for AMANS from group ATTAMA
AMUNANS2 - overflow for AMUNANS from group ATTAMA.

Register release history update

All the registers in this group are new in the UCS20 release.

Associated registers

ATTAMA.AMANS - ATTAMA2.AMANS2
ATTAMA.AMUNANS - ATTAMA2.AMUNAS2

The range of each of these registers is an decimal value of 0 - 32767.

When the ATTAMA register reaches its maximum value of 32767 and overflows, it increments the associated overflow register in group ATTAMA2. The ATTAMA register will then reset to 0 and resume incrementing.

The registers in the group ATTAMA2 indicate the number of times the associated register in group ATTAMA has overflowed. One peg in the ATTAMA2 register indicates 32767 pegs that were handled by the ATTAMA register.

Associated logs

None

Product = CS 2000**A00002822 -- UI Manager (Succession on DMS)*****Functional Description***

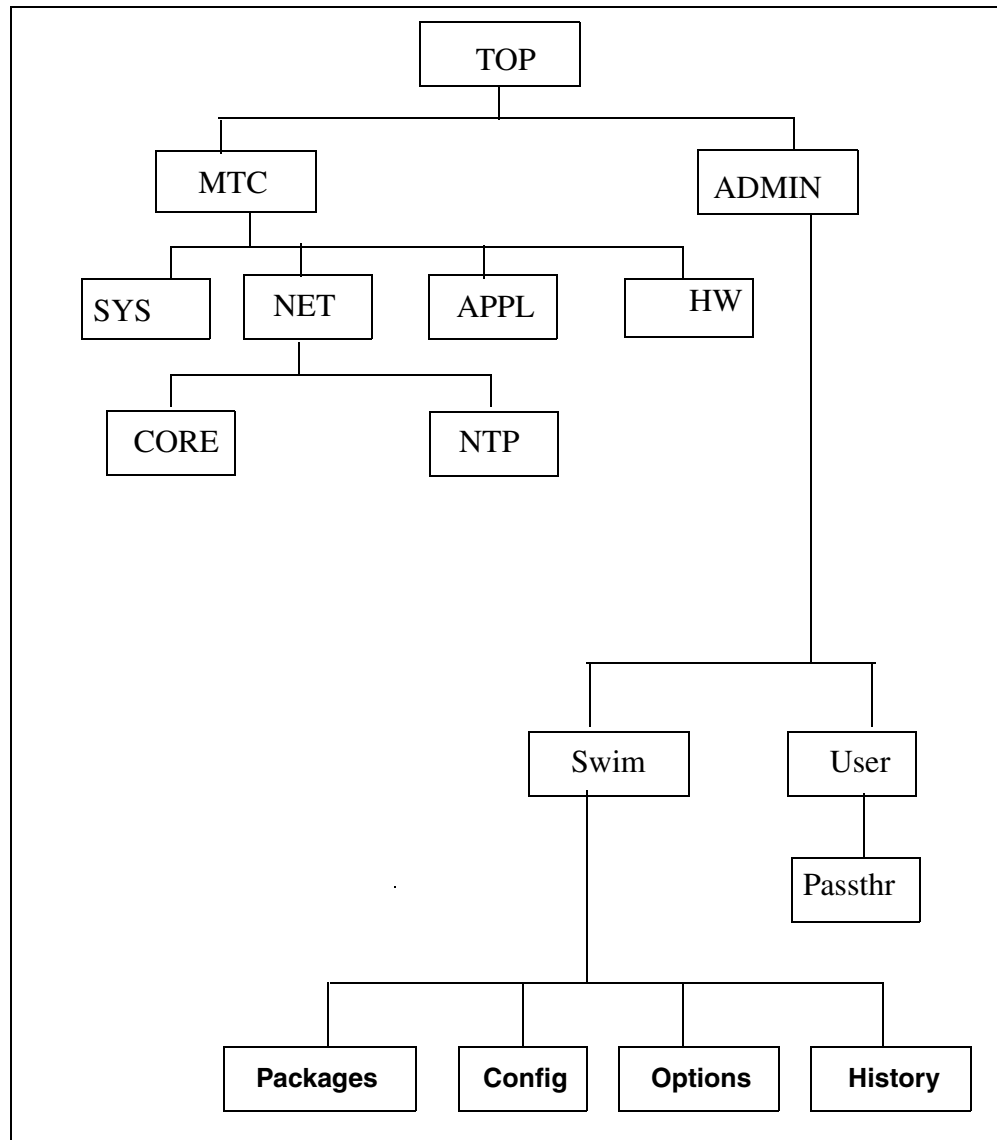
The User Interface Manager provides a user interface for local CBM maintenance, administration and system monitoring. The UI consolidates all of the primary maintenance operations under a single unified program which resembles the CM MAP interface.

The operations that can be accessed through the UI are divided into two categories; maintenance and system administration. Maintenance provides access and control over the CBM application software. System administration functions include CBM configuration, package installation/removal.

The UI provides input and output to a human operator. When a user selects an operation in the UI, a function contained in the appropriate maintenance subsystem is invoked.

The UI is organized into a system of screens. The screens are organized in a hierarchy, and each screen represents a functional area.

The UI functional structure is shown in the following figure. This is the intended view for CSEN07 (CBM) and is subject to changes as the product evolves.

UI functional structure.**Functionality**

The CBM screens are not identical to the MAP screens, but they retain the basic structure and input/output mechanisms as the MAP. Each CBM screen is divided into five areas: alarm banner, command list, output, clock, and input. A typical CBM screen is shown in the following figure.

```

          CBM Main Level Display
          CBM      MATE      NET      APPL      SYS      HW      CLI: SNM2
          ISTB     SysB      .        .        .        .      Host: pcarylrr
          M        M
CBMMtc
0  Quit
2  Mtc
3  Admin
4
5
6
7
8
9
10
11
12
13
14
15
16
17 Help
18 refresh
   root
Time 13:43  >

```

Alarm Banner

The top area (referred as I in the above figure) contains the current screen title and the CBM alarm banner. The alarm banner indicates the node state for the CBM and the state of the major CBM components. This area is updated dynamically, and appears on every CBM screen.

Command List

The area on the left is the CBM command menu (referred as II in the above figure). Commands available at the current level are listed in MAP style and the current level is displayed at the top of the list.

Output

The area on the right is the RMI output window (referred as III in the above figure). The information in this window can be either static or dynamic.

Clock

The CBM clock and current userid are displayed at the bottom left of the screen (referred as IV in the above figure). The clock is updated dynamically.

Input

The single line at the bottom right of the screen is used for CBM input (referred as V in the above figure).

Commands Available at 'All' Levels

The following commands are generally available at each level. The use of and output from these commands is essentially the same. They are:

1. **Quit:** Quits the current level and moves back to the previous one. You may specify the option ALL in order to exit the CBM from any level.
2. **Help:** Obtains help specific to the current level. If information on a specific command is desired you may type the command name as an option to get information pertaining to that specific command.
3. **Refresh:** If the screen display is corrupted, use refresh to force a redraw of the screen.

These commands will not be listed in the screen command descriptions later in this document.

CBM Main Level

The main menu breaks all functions into either the maintenance category, or the system administration category. Additional categories may be added in the future as needed.

There is no default output for this level other than the main banner.

Commands:

1. **Mtc:** Displays the SDM Maintenance Level (position 2 in the following figure).
2. **Admin:** Displays the SDM System Administration Level (position 3 in the following figure).

CBM Main Level Display

```

      CBM      MATE   NET    APPL   SYS    HW CLLI: SNM2
      IsTb     SysB    .      .      .      .      Host :pcarylrr
      M        M
CBMMtc
0 Quit
2 Mtc
3 Admin
4
5
6
7
8
9
10
11
12
13
14
15
16 LogQuery
17 Help
18 refresh
root
Time 13:43 >

```

CBM Maintenance Level:

The maintenance level is the highest level for maintenance related commands.

Commands:

1. Net: Displays the LAN Connectivity Level (position 3 in the following figure).
2. Appl: Displays the Software Application Status Level (position 4 the following figure).
3. Sys: Displays the Operating System s/w Status Level (position 5 in the following figure).
4. Hw: Displays the Hardware Status Level (position 6 in the following figure).

CBM Maintenance Level Display

CBM	MATE	NET	APPL	SYS	HW	CLLI:	SNM2
IsTb	SysB	.	.	.	.	ISTb	Host: pcarylrr
M	M						
Mtc							
0 Quit							
2							
3 Net							
4 Appl							
5 Sys							
6 Hw							
7							
8							
9							
10							
11							
12							
13							
14 QueryCBM							
15							
16							
17 Help							
18 refresh							
root							
Time 13:43							
>							

Net Connectivity Level

The net level shows the status indicator for the core heartbeat and NTP state. The status indicators displayed at this level are updated dynamically.

Commands:

1. Core: Go to core level (position 2 in the following figure).
2. NTP: Go to the NTP level. (position 5 in the following figure).

CBM Net Connectivity Level						
CBM	MATE	NET	APPL	SYS	HW	CLLI: SNM2
IstB	SysB	.	.	.	.	Host: pcarylrr
M	M					
Net						
0 Quit	Core Heartbeat State:	.				
2 Core	NTP State:	.				
3						
4 Logs						
5						
6 NTP						
7						
8						
9						
10						
11						
12						
13						
14 QueryCBM						
15						
16						
17 Help						
18 refresh						
root						
Time 13:43	>					

Core Level

The Core level shows the communication paths to the Core and it also monitors the state of that communication. Figure , on page 557 and Figure , on page 557 show the display for the Ethernet connected CBMs and the OC3 connected CBMs respectively. The command line equivalents of the command are shown in the following table.

Commands:

1. Add: Add a communication path to the Core.
2. Change: Change the values for the given communication path to the Core.
3. Delete: Delete the given communication path to the Core.

Core screen command line equivalents

UI Command	Command line equivalents
Add	No command line equivalents
Change	No command line equivalents
Delete	No command line equivalents

CBM Core Level (Ethernet Connected)

CBM	MATE	NET	APPL	Sys	HW	CLLI: SNM2
IsTb	SysB	.	.	.	.	Host: pcarylrr
M	M					

Core	Core
0 Quit	
2	<u># Communication Path</u> <u>State</u> <u>Core Addresses</u> <u>Node Address</u>
3	1 VIA ETHERnet . 10.101.8.196 10.101.8.96
4	
5 Logs	
6	
7	
8	
9	
10	
11	
12	
13	
14 QueryCBM	
15	
16	
17 Help	
18 refresh	
root	
Time 13:43	>

CBM Core Level (OC3 Connected)

CBM	MATE	NET	APPL	Sys	HW	CLLI: SNM2
IsTb	SysB	.	.	.	.	Host: pcarylrr
M	M					

Core	Core
0 Quit	
2	<u># Communication Path</u> <u>State</u> <u>Core Address</u> <u>Node Address</u>
3	1 VIA OC3 . 192.168.101.196 192.168.101.101
4	link 0: MTC_Open
5 Logs	link 1: Closed
6	
7	
8	
9	Note: link conditions are:
10	- Closed
11	- MTC_Open
12	- Open
13	
14 QueryCBM	
15	
16	
17 Help	
18 refresh	
root	
Time 13:43	>

NTP Level

The NTP level will synchronize the system clock. This level allows you to configure NTP daemon to synchronize the system clock with the NTP server(s)/peer(s). There are no command line equivalents commands for the NTP level.

CBM NTP Level

CBM	MATE	NET	APPL	SYS	HW	CLLI: SNM2
IsTb	SysB	.	.	.	.	Host: pcarylrr
M	M					
NTP						
0 Quit	NTP State: .					
2	Drift: 5.516					
3 Query	Info: NTP is synchronized.					
4 Logs	#	Hostname	Str	State	When	Poll Delay Offset Disp
5	1	zcarh09j	3	+	247	512 3.4 1.0 0.7
6	2	zcarh09m	2	*	168	512 3.4 3.3 0.2
7	NTP Nodes: 1 to 2 of 2					
8						
9						
10						
11						
12 Up						
13 Down						
14						
15						
16						
17 Help						
18 refresh						
root						
Time 13:43	>					

CBM Software Application Status Level

The Software Application Status Level shows the application status indicators. For each installed application, this level shows the application description and the current state. Application control is available on each of the installed application.

The status indicators displayed at this level are updated dynamically.

Commands:

1. Logs: Display application status logs (position 4 in the following figure).
2. Bsy: Issues a busy command to the application. Busying an application will run the stop script for that application, and will shutdown all associated processes (position 7 in the following figure). The parameter for this command is the application number (far left) or the GROUP keyword, which changes the overall state to ManB. Application that are Offline remain offline. The output for this command is displayed beneath the dynamic information (e.g. bsy 2).

3. **RTS:** Issues a Return To Service command to the application. Returning an application to service will run the data reformat script for that application, and will initiate all processes associated with that application (position 8 in the following figure). The parameter for this command is the application number (far left) or the GROUP keyword, which changes the overall state to InSv (In Service). The InSv state is represented by a dot “.”. The output for this command is displayed beneath the dynamic information.
4. **OffL:** Issues an Offline command to the application (position 9 in the following figure). The parameter for this command is the application number (far left) or the GROUP keyword, which changes the overall state to Offline. The applications themselves become ManB, and applications that are Offline remain Offline. The output for this command is displayed beneath the dynamic information in the following figure).

CBM APPL Level

CBM	MATE	NET	APPL	SYS	HW	CLLI: SNM2
ISTB	.	.	.	.	.	Host: pcarylrr
M	M					
Appl						
0 Quit	# Application					State
2	1 Table Access Service					.
3	2 OM Delivery					OffL
4 Logs	3 OM Access Service					ISTb
5	4 Log Delivery Service					ManB
6						
7 Bsy						
8 RTS						
9 OffL						
10						
11						
12 Up						
13 Down						
14 QueryCBM						
15						
16						
17 Help						
18 refresh						
root						
Time 13:43	>					

The command line equivalents of the commands under the appl level are shown in the following table:

APPL screen command line equivalent commands

UI Command	Command line equivalents
Bsy	appctrl --bsyl -b <appname> groupname>
Rts	appctrl --rts -r <appname> groupname>
Offl	appctrl --offl -o <appname> groupname>
QueryCBM flt	queryflt

UI Command	Command line equivalents
QueryCBM status	queryflt -s
Query flt mate	queryflt -m

CBM System Level

The CBM system level shows the status of operation system software parameters.

Commands:

Logs: Display the last events reported

QUERYCBM <flt, flt mate, status > : Commands are invoked as shown in the preceding table.

CBM SYS Level

CBM	MATE	NET	APPL	SYS	HW	CLLI: SNM2
IsTb	SysB	.	.	.	.	Host: pcarylrr
M	M					
Sys						
0 Quit						
2						
3						
4 Logs						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14 QueryCBM						
15						
16						
17 Help						
18 refresh						
root						
Time 13:43						>

CBM Hardware Status Level

The CBM hardware status level shows the hardware status indicators. The status indicators displayed at this level are updated dynamically.

Commands:

Logs: Displays the last event reported.

QueryCBM < flt, flt mate, status >: Commands are invoked as shown in [Table “Core screen command line equivalents” on page 556](#).

CBM Hardware Level

CBM	MATE	NET	APPL	SYS	HW	CLLI: SNM2
IsTb	SysB	.	.	.	.	Host: pcarylrr
M	M					
Hw						
0 Quit						
2						
3						
4 Logs						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14 QueryCBM						
15						
16						
17 Help						
18 refresh						
root						
Time 13:43						>

CBM Administration Level

The Admin level is the highest level for system administration commands. The commands available under system administration are dependent on the user id. The root user has full access to all commands. The maint class users are given only a subset of the system administration commands.

Commands:

1. Users: Enter the user administration level (position 4 in the following figure).
2. SWIM: Enter the software inventory management level (position 3 in the following figure).

```

                                CBM Admin Level
    CBM      MATE      NET      APPL      SYS      HW      CLLI:
    IsTb     SysB      .        .        .        .        Host: pcarylrr
    M        M
Admin
0 Quit
2
3 SWIM
4 User
5
6
7
8
9
10
11
12
13
14
15
16
17 Help
18 refresh
   root
Time 13:43  >
```

SWIM

The swim level of the CBM provides software inventory management. The SWIM level interface will show the product level information and the application status information.

Commands:

1. Packages: Enter the software packages level (position 2 in the following figure).
2. Config: Enter the software configuration level (position 6 in the following figure).
3. Options: Enter the options level (position 7 in the following figure).
4. History: Enter the software history level (position 8 in the following figure).

```

                                CBM SWIM Level
    CBM      MATE  NET  APPL  SYS  HW      CLLI: SNM2
    IsTb     SysB      .      .      .      .      Host: pcarylrr
    M        M

SWIM
0 Quit
2 Packages
3
4
5
6 Config
7 Options
8 History
9
10
11
12 Up
13 Down
14
15
16
17 Help
18 refresh
   root
Time 13:43  >

```

SWIM Packages Level

This level contains commands to list and remove installed software. It shows the list of packages which exist on the system. The software can be applied or removed from this level for maintenance purposes. The list columns include: a list index number representing the package in each row, the package name, instance or description, the version number which is currently installed, and the package status (APPLIED, PARTIAL or FAILED). The Status column was added to identify if the package has been APPLIED, if there is a NEWer instance (SDM/Nortel software only and mostly for lab environment) or if the package has NOT been APPLIED, no instance on the system. APPLIED packages versions are currently in use. PARTIAL packages are packages that had an error during installation and are only partially installed. PARTIAL and FAILED packages should be removed from the system. The Packages level is updated every 20 seconds or when you use the Refresh command. The Packages level is shown in Figure , on page 564 .

Commands:

1. Apply: Install the selected packages (position 2 in the following figure).
2. Select: Selects a package. A selected package appears highlighted within the software list. A selected entry can be deselected by selecting it again (position 7 in the following figure).
3. Remove: Remove software. This command can be used to remove software that is in any of the APPLIED, PARTIAL or FAILED states (position 8 in the following figure).

4. Search: Search the list for the given text, and reposition the list when a match entry is found (position 14 in the following figure).
5. Filter: Filter the list of software (position 15 in the following figure)
6. View: Toggle between showing the software description, the software package instance and the software package name (position 16 in the following figure).

CBM Packages Level

CBM	MATE	NET	APPL	SYS	HW	CLLI: SNM2																				
IsTb	SysB	.	.	.	.	Host: pcarylrr																				
M	M																									
Packages																										
0 Quit	Filter: sdm Interactive Mode: OFF																									
2 Apply	<table><tr><th>#</th><th>Package Description</th><th>Version</th><th>Status</th></tr><tr><td>1</td><td>RogueWave SourcePro Libraries</td><td>4.0.0.0</td><td>APPLIED</td></tr><tr><td>2</td><td>Platform Utilities</td><td>7.36.9.0</td><td>APPLIED</td></tr><tr><td>3</td><td>Table Access Service</td><td>7.36.9.0</td><td>APPLIED</td></tr><tr><td>4</td><td>SDM Billing Application</td><td>7.38.8.0</td><td>APPLIED</td></tr></table>						#	Package Description	Version	Status	1	RogueWave SourcePro Libraries	4.0.0.0	APPLIED	2	Platform Utilities	7.36.9.0	APPLIED	3	Table Access Service	7.36.9.0	APPLIED	4	SDM Billing Application	7.38.8.0	APPLIED
#	Package Description	Version	Status																							
1	RogueWave SourcePro Libraries	4.0.0.0	APPLIED																							
2	Platform Utilities	7.36.9.0	APPLIED																							
3	Table Access Service	7.36.9.0	APPLIED																							
4	SDM Billing Application	7.38.8.0	APPLIED																							
3																										
4																										
5																										
6																										
7 Select																										
8 Remove																										
9																										
10																										
11																										
12 Up																										
13 Down																										
14 Search																										
15 Filter																										
16 View																										
17 Help																										
18 refresh																										
root																										
Time 13:43 >																										

CBM Apply Level

The Packages Apply level shows a list of packages which exist on the source. The default source is automatically listed when entering the Apply level for the first time. The default source can be changed within the Options level. The list columns include: a list index number representing the package in each row, the package description, instance name or package name The current version listed beside every package is updated every 20 seconds or when you use the Refresh command. The command line equivalents are shown in [Table "SWIM screen command line equivalents" on page 565](#).

Commands:

1. Source: Choose a source directory from which to load packages.
2. Reload: Reload the list of packages from the current source.
3. Select: Selects a package. A selected package appears highlighted within the software list. A selected entry can be deselected by selecting it again.
4. Apply: Apply packages on this CBM

5. Upgrade: Upgrade all packages to the latest versions available on the source.
6. Search: Search the list for the given text, and reposition the list when a match entry is found.
7. Filter: Filter the list of software.
8. View: Toggle between showing the software description, the software package instance and the software package name

CBM Apply Level

CBM	MATE	NET	APPL	SYS	HW	CLLI: SNM2
IsTb	SysB	.	.	.	.	Host: pcarylrr
M	M					
Apply	Source: the directory /data/swd/sdm.					
0 Quit	Filter: OFF Interactive Mode: OFF					
2						
3						
4 Source						
5 Reload						
6						
7 Select						
8 Apply						
9 Upgrade						
10						
11						
12 Up						
13 Down						
14 Search						
15 Filter						
16 View						
17 Help						
18 refresh						
root						
Time 13:43	>					

SWIM screen command line equivalents

UI Command	Command line equivalents
Apply	pkgadd -d <full path to the package>
Remove	pkgrm <Package name >
Search	pkginfo -c <any matching string >

CBM Config Level

The Config level shows the list of applications which have configuration programs associated with them. Each configuration program can be executed by using the Config command. The Config level is updated every 20 seconds or when you use the Refresh command. The config level is shown in the following figure.

Commands:

1. **Select:** Selects a package. A selected package appears highlighted within the software list. A selected entry can be deselected by selecting it again.
2. **Config:** Configure packages
3. **Search:** Search the list for the given text, and reposition the list when a match entry is found.
4. **Filter:** Filter the list of software
5. **View:** Toggle between showing the software description, the software package instance and the software package name.

CBM Config Level

CBM	MATE	NET	APPL	SYS	HW	CLLI: SNM2
IsTb	SysB	.	.	.	.	Host: pcarylrr
M	M					
Config	Filter: OFF Interactive Mode: OFF					
0 Quit						
2	<u># Package Description</u> <u>Status</u>					
3	1 OM Delivery Configured					
4						
5						
6						
7 Select						
8 Config						
9						
10						
11						
12 Up						
13 Down						
14 Search						
15 Filter						
16 View						
17 Help						
18 refresh						
root						
Time 13:43	>					

User

The User level of the CBM provides administration of the CBM maint userid. The command line equivalents of Passthru level are shown in [Table "PassThru screen command line equivalents" on page 568.](#)

CBM User Level

CBM	MATE	NET	APPL	SYS	HW	CLLI: SNM2
IsTb	SysB	.	.	.	.	Host: pcarylrr
M	M					

User

0 Quit

2 Maintenance users

3 PassThru 1 maint

4

5

6

7

8

9

10

11

12

13

14

15

16

17 Help

18 refresh

root

Time 13:43 >

CBM PassThru Level

CBM	MATE	NET	APPL	SYS	HW	CLLI: SNM2
IsTb	SysB	.	.	.	.	Host: pcarylrr
M	M					

PassThru

0 Quit

2

3 UserName RealName Passthru Action FTP CM

4

5

6

7

8

9

10

11

12 Up

13 Down

14

15

16

17 Help

18 refresh

root

Time 13:43 >

PassThru screen command line equivalents

UI Command	Command line equivalents
Add	passthrcfg -m <username> -a realname=<real name> -a args=<telnet target>
Change	passthrcfg -c <username> -a realname=<new realname> -a args=<new target>
Delete	passthrcfg -d <username>

Hardware Requirements or Dependencies

None

Software Requirements or Dependencies

SDM base software is installed

Limitations and restrictions

None

Interactions

None

Applicable customer facing sections

Fault Management

Logs ☐ Y ☐Alarms ☐ Y ☐

Configuration

Data Schema ☐User Interface ☐ Y ☐Element Management ☐ NA ☐Security ☐ NA ☐Service Order ☐ NA ☐Office Parameters ☐ NA ☐Accounting (includes AMA billing) ☐ NA ☐

Performance (includes operational measurements) ____NA__

Indicate with an X if you are completing the sections of the DDOC listed below. Indicate with “N/A” if these sections do not apply to this functionality.

Realtime ____NA__

Engineering Information ____Y__

Glossary

Term	Description
CBM	Core(sucession) and Billing Manager
CM	Computing Module
MAP	Maintenance and Administration Position
UI	User Interface

Product = CS 2000

A00002858 -- SYSB Carrier (Succession on DMS)

Functional Description

Nortel's customers have expressed the desire to have a SysB carrier cause its SPM node to go ISTb under the PM banner. This would provide the telco a visual MAP alert that a carrier outage may be causing multiple trunk failures. Adding this capability would make SPM work like DTC. But most importantly, this feature will reduce the chance of long duration outages when the telco is not aware that a carrier problem is disrupting service. This feature will also reduce the chance of problems during a Panther upgrade since these types of carrier problems can prevent sparing on the OC3.

Feature A59036987 attempted to address this concern by adding the display of S/P/D/d/R under the TRKS banner.

Operation

There will be two new “triggers” that can cause a SPM node to go ISTb under the PM banner:

Trigger 1: Check SysB Carrier on OC3 RM

When one of the OC3's carriers goes SysB, which corresponds to a Bellcore state of OOS-AU-FAF (which is same as OC3 carrier state of IS-UPS-FAF).

FAF is FAcility Failure. Note that this trigger corresponds to “S/P/D/d” in the A59036987 feature. While the carrier is SysB, any of its trunks will be in the CFL condition and not able to bear traffic.

Here’s an example of the existing log that will be seen when a carrier goes SysB:

```
MSH706BM    * CARR511 JUN04 05:46:03 6200 SYSB CARRIER SPM  34
            CKT: 13  CarrName: SPM34_STS1P_1_VT15P_3_DS1P_3
            Carrier: STS1P  1 VT15P 15 DS1P  1
            Previous State: INSV
```

This trigger clears when the carrier is no longer SysB (e.g. CARR510 log when the carrier is RTSed and goes InSv).

For STM-1 international product, the trigger will occur when a STM-1 carrier goes SysB.

Trigger 2: Check RFI Alarm on STS3L Carrier

When one of the OC3’s InSv STS3L carriers has a RFI (Remote Failure Indication) alarm. Such an alarm can be caused by cutting the TX fiber on the OC3. Note that this trigger corresponds to “R” (for Remote alarm) in the A59036987 feature. Since OC3 sparing will not be allowed while the remote alarm condition is present on the line carrier, the OC3 is effectively in an E2 outage condition due to the loss of redundancy.

Here’s an example of the existing log that will be seen when a remote alarm is raised on a line carrier. Note that the carrier data in table MNHSCARR would have to set the RFI alarm as reportable (RFI MN RPT) for this log to be seen.

```
MSH8_03BM    * CARR310 APR18 10:27:41 3204 FLT  CARRIER SPM  41
            CKT: 178  CarrName: ATM_STS3L_SPM_41_CKT_178
            Carrier: RM      2 OC3S  0 STS3L  0
            Failure: RFI      Set
```

If the RFI alarm is set as NRPT (non-reportable) for the carrier, then the log will not be seen but the trigger will still occur. Note that the CI command:

```
MAPCI;MTC;TRKS;CARRIER;POST {carrier};LISTALM
```

will always show the presence of the alarm, independent of whether MNHSCARR sets the alarm as RPT or NRPT for the carrier.

This trigger clears when the RFI alarm clears (as reported by a CARR310 “RFI Clear” log).

For STM-1 international product, trigger will occur when a InSv STM1M carrier has a RFI alarm.

MAPCI PM Display

When one of these triggers occur, the new ISTb reason string will appear in the existing SPM300 log that occurs whenever a OC3 RM goes ISTb. See Log section below for details. The severity of this ISTb MAP alarm will be minor, so it won’t appear under the “1 SPM” display below.

Here’s how the MAP’s PM level will appear for the ISTb SPM when one of the above triggers has occurred. Note that the “S” under TRKS is part of an existing feature that indicates a section-level carrier (e.g. OCS3) is SysB.

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL				
.	.	.	.	1 SPM	.	.	S	.	.				
				SysB	ManB	OffL	CBsy	ISTb	InSv				
0 Quit		PM		0	0	0	0	1	177				
2 Post_		SPM		0	0	0	0	1	77				
3 ListSet													
4 ListRes		SPM	20	ISTb	Class: SMG4								
5 Trnsl													
6	Shlf0	SL	A	Stat	Shlf0	SL	A	Stat	Shlf1	SL	A	Stat	
7	-----	1	-	-----	CEM	1	8	A	ISTb	-----	1	-	-----
8	-----	2	-	-----	OC3	0	9	A	ISTb	-----	2	-	-----
9 OfClk	VSP	0	3	A InSv	OC3	1	10	I InSv	-----	3	-	-----	
10	VSP	1	4	A InSv	VSP	2	11	A InSv	-----	4	-	-----	
11 Disp_	-----	5	-	-----	VSP	3	12	A InSv	VSP	6	5	A InSv	
12 Next	-----	6	-	-----	VSP	4	13	A InSv	VSP	7	6	A InSv	
13 Select_	CEM	0	7	I InSv	VSP	5	14	A InSv	-----	7	-	-----	
14 QueryPM													
15 ListAlm													
16 Clock													
17 SPERFORM													
18 Upgrade_													

QUERYPM FLT Display

The telco can use this command:

MAPCI;MTC;PM;POST SPM ISTB;QUERYPM FLT REASON

to show what faults caused the SPM node(s) to become ISTb. If one of the SPM’s carriers has gone SysB, then the output will look like this:

```
>querypm flt reason
OC3 0 ISTb NonCritical faults:
Check SysB Carrier
```

CEM 0 ISTb NonCritical faults:

Check Carrier on OC3 RM

The “Check SysB Carrier” is a new reason that can cause a OC3 RM to go ISTb, which results in the CEM going ISTb, and hence the node ISTb. The “Check Carrier on OC3 RM” is a new ISTb reason for CEMs that will only occur when one (or both) of our two triggers have occurred.

For the STM1 product, CEM ISTb reason will appear as “Check Carrier on STM RM”.

If the 2nd trigger occurs (i.e. remote alarm on a line carrier), then the output will look like this:

>querypm flt reason

OC3 0 ISTb NonCritical faults:

Check RFI Alarm on STS3L Carrier

CEM 0 ISTb NonCritical faults:

Check Carrier on OC3 RM

The “Check RFI Alarm on STS3L Carrier” is the other new reason that can cause a OC3 RM to go ISTb.

For the STM1 product, the STM ISTb reason will appear as “Check RFI Alarm on STM1M Carrier” and the CEM ISTb reason will appear as “Check Carrier on STM RM”.

Note that our two new “triggers” are the only RM ISTb reasons that can also cause the Node to go ISTb.

LISTALM Display

The LISTALM command for the ISTb SPM will produce this output when one of the triggers has occurred. Note that it just reflects the Minor alarm reason that caused the node to go ISTb.

```
ListAlm: SPM 26 CEM 0
SEVERITY  ALARM  ACTION
-----
Critical  None
Major     None
Minor     ISTB    RPT
No_Alarm  None
```

Logs

When one of the new triggers occur, the existing CARRxxx log will occur as shown above. In addition, the existing SPM300 log will occur to show the OC3 RM has gone ISTb for one of the new ISTB text reasons. The severity of these SPM300 logs will be non-critical for each new reason.

Note: the maximum length for an ISTb reason string is 64 characters, so we can make the reasons longer if that would help.

Check SysB Carrier

This log will occur if one of the SPM's carriers goes SysB:

```
STEC207AM * SPM300 MAY30 15:57:33 4093 TBL Device Fault Report
Location   : SPM : 26   OC3 : 0
Status     : Alarm Raised
Problem Description: Non Critical
  7A: Check SysB Carrier
Action     : Refer to NTPs for Alarm Clearing Procedures.
Cardlist   :
  No Cardlist Available.
```

Check RFI Alarm on STS3L Carrier

This log will occur if one of the SPM's STS3L line carriers receives a RFI external alarm (e.g. due to TX fiber cut). Note that STS3L will be substituted with STM1M on STM1 nodes.

•

```
STEC207AM * SPM300 MAY30 15:57:33 4093 TBL Device Fault Report
Location   : SPM : 26   OC3 : 0
Status     : Alarm Raised
Problem Description: Non Critical
  7A: Check RFI Alarm on STS3L Carrier
Action     : Refer to NTPs for Alarm Clearing Procedures.
Cardlist   :
```

For the STM1 product, the 7A string above will instead appear as “Check RFI Alarm on STM1M Carrier”.

OC3 ISTb Log

If the OC3 RM was previously InSv when the trigger occurred, then the following SPM500 “Device State Change” log will occur when the OC3 transitions to ISTb. There are no changes to this log. Here’s an example:

```
STEC207AM * SPM500 MAY30 15:57:33 4194 INFO Device State Change
          Location: SPM : 26   OC3 : 0
          From      : InSv
          To        : ISTb
```

Node ISTb Log

If the SPM node was previously InSv when the trigger occurred, then the existing NODE500 “Node State Change” log will occur when the SPM node transitions to ISTb. There are no changes to this log. Here’s an example:

```
OLSC_SN06BT CM * NODE500 JUN04 15:14:16 1000 INFO Node State Change
Location: SPM 33 Unit 0
From:      InSv ( Connected, Active )
To:        ISTb ( Connected, Active )
```

Troubleshooting why SPM Node is ISTb

Determining which carrier caused the SPM Node to go ISTb depends on the type of reason given under QUERYPM FLT REASON:

Check SysB Carrier

Find which SPM is ISTb:

```
mapci;mtc;pm;post spm istb
```

then post the SysB carriers on the SPM:

```
trks;carrier;post spm {spm# from current post set} sysb
```

Then follow existing troubleshooting procedures for SysB SPM carriers.

Check RFI Alarm on STS3L Carrier

Find which SPM is ISTb:

```
mapci;mtc;trks;carrier;post spm istb
```

then post the line carriers on that SPM:

trks;carrier;post spm {spm# from current post set};next

The map will look something like this:

```

XAC      MS      IOD      Net      PM      CCS      Lns      Trks      Ext      APPL
SysBTh   .      NODLOG   .      1 SPM   .      .      232CCS   3Crit   .
          *C*      *C*      *C*

CLASS    ML    OS  ALRM  SYSB  MANB  UNEQ  OFFL  CBSY  PBSY  INSV
0 Quit   TRUNKS 176   0   95   201   0    0    0    88   0   746
2 Post_  HSCARR 203   0    5    3    0    0    0    63   0   753
3        STS3L
4        N CLASS SITE SPM RM  OC3S STS3L CKT STATE TR MA
5 Loop_  0 HSCARR HOST 12  0    0    0  89  INSV .S ..
6 Tst_   1 HSCARR HOST 12  1    0    0  90  INSV .. ..
7 Bsy_   2 HSCARR HOST 12  0    0    0  91  INSV .. ..
8 RTS_   3 HSCARR HOST 12  1    0    0  92  INSV .S m.
9 Offl_
10
11 Disp_
12 Next
13
14 Detail_
15 ListAlm_
16
17 Perfmon_
18
SIZE OF POSTED SET : 176
MORE...
```

The faulty line carrier will be the one with an alarm (e.g. “m”) under the “MA” column. Use LISTALM or PERFMON;PPQUERY to confirm the alarm. Then follow existing troubleshooting procedures for clearing alarms on a STS3L carrier. One thing to check for is a cut TX fiber on the OC3.

For the STM1 product, everything is the same except STM1M will appear instead of STS3L (and STM1R will appear instead of OC3S).

Hardware requirements

There are no new hardware dependencies introduced by this feature.

This feature will only work on TDM (legacy) SPM nodes (i.e. SPM and STM1). Anywhere that OC3 RM or STS3L carrier is referred to in this document for SPM, you can substitute STM RM or STM1M carrier when referring to a STM1.

Succession ATM/IP-based nodes (MG4K, IW, LSA, STS1) will **not** support this feature in the initial release.

Software Requirements or Dependencies

There are no new software dependencies introduced by this feature.

The feature will be “off” by default, but can be turned “on” by the customer.

This feature will impact Local CEM and RM loads for the SPM and STM1 products in the SN07/20 release, and will impact the SN07/20 (i.e. SHR20) Core load.

Limitations and restrictions

1. As stated above, the feature is only supported on TDM (legacy) SPM nodes, which includes the STM1.
2. Note that existing feature A59036987 will also show “P” for a ManB line carrier, whereas this new feature ignores any ManB carrier.
3. This feature will be “off” by default. An option will be provided (in Table OFCENG) for the customer to turn the feature “on” for all SPMs in the office. There will be no way to control the feature for individual SPMs. It is strongly recommended that the customer leave the feature “on” so they can avoid any long duration outages due to SPM carrier problems.
4. For the feature to be “on”, the new SN07/20 Core and Local loads must be running. If an upgrade is in progress where the customer is running the new SN07/20 Local loads but still has the pre-SN07/20 Core loads, then the feature will not activate until the new SN07/20 Core load is also running (e.g. after a No Restart SWACT).
5. While this feature is backwards compatible, it will not be forwards compatible when the feature is enabled. For example, telco can run the new SN07/20 Local load with an older Core load as described above in #4 (this is “backwards compatibility”), but telco cannot run the new SN07/20 Core load with an older Local load when the feature is turned “on” in the new Core load (via Table OFCENG). If forward compatibility is needed, the feature must be turned “off” in the new Core load.
6. When the feature is activated or deactivated via Table OFCENG, it will take up to 45 minutes for this change to propagate throughout the system. The user will be warned about this delay time when the change is made. The same amount of delay will be incurred when the telco first upgrades the Core to the new SN07/20 load via NoRestartSWACT.
7. The carrier alarm level in Table MNHSCARR will not have an impact on whether a specific carrier can cause the node to go ISTb. So even if the carrier is set to NRPT (Non-Reportable), if it drops SysB, then it will cause the node to go ISTb. Same with the remote alarm trigger.
8. It only takes a single SysB carrier on the SPM node (including one DS1P or E1P path carrier) to cause the node to go ISTb. Any ManB or OFFL carrier will not cause the node to go ISTb.
9. If both “triggers” are present on the same OC3/STM at the same time, then only the last one reported will be shown when QUERYPM FLT REASON is done. If the last trigger is cleared, then QUERYPM FLT REASON will show the first trigger (until the first trigger is also cleared).

Interactions

This new feature works very similar to the 17/SN04 A59036987 feature that reports “S/P/D/d” under TRKS banner for a SysB carrier and “R” for a line carrier with a remote alarm. There are **no** interactions between them. Note that “S/P/D/d/R” will continue to be displayed under the TRKS banner.

With both features operating concurrently, the telco will have more info available on the MAP display to isolate the carrier issue *if* there is only *one* node ISTb. If the PM banner shows “1 SPM”, then the telco will know this extra info by examining the right-most letter under the TRKS banner display:

1. **“S”**: telco will know that a SysB section carrier (OC3S, STM1R) has caused the SPM to go ISTb.
2. **“P”**: telco will know that a SysB line carrier (STS3L, STM1M) has caused the SPM to go ISTb. If “P” appears and there is no ISTb SPM, then we know there is a ManB line carrier on one of the SPMs. This ManB line carrier will prevent OC3 sparing so the SPM has a E2 loss of redundancy.
3. **“D”**: telco will know that a higher-level path carrier (STS1P, DS3P, VC4P) going SysB has caused the SPM to go ISTb.
4. **“d”**: telco will know that a lower-level path carrier (DS1P, VT15, VC12P, E1P, E1L) going SysB has caused the SPM to go ISTb.
5. **“R”**: telco will know that a InSv line carrier (STS3L, STM1M) with remote RFI alarm has caused the SPM to go ISTb.

The TRKS letters above (“S/P/D/d/R”) are shown in their priority order of precedence. This means that if a “S” and “D” fault exist concurrently, then the “S” precedes the “D” so only “S” is shown.

If *more than one* SPM is ISTb, then the telco will still know the highest level carrier severity, but won’t know which SPM it is on. For example, a “2 SPM” under PM banner and a “S” under TRKS banner means one SPM has a “S” fault and the other SPM has “S” or lower fault.

Applicable customer facing sections

Fault Management

Logs	__X__
Alarms	__N/A__

Configuration

Data Schema	__N/A__
User Interface	__X__
Element Management	__N/A__

Security	__N/A__
Service Order	__N/A__
Office Parameters	__X__
Accounting (includes AMA billing)	__N/A__
Performance (includes operational measurements)	__N/A__
Indicate with an X if you are completing the sections of the DDOC listed below. Indicate with “N/A” if these sections do not apply to this functionality.	
Realtime	__X__
Engineering Information	__N/A__

Fault Management for A00002858

Fault management strategy

The purpose of the “SPM Node ISTb for Carrier Outage” feature is to mark an SPM as ISTb so an indicator appears under the PM Map banner whenever one of these carrier faults appear:

1. Any of the SPMs carriers goes SysB.
2. Any of the SPM’s line carriers (STS3L or STM1M) has an RFI (Remote Failure Indicator) alarm.

The new steps for resolving these faults will be integrated into the existing Succession fault management documentation for troubleshooting SPM ISTb faults.

Note that the Functional Description section of this A00002858 feature provides an easier to follow format for troubleshooting these faults. The Configuration section documents the changes to the QUERYPM FLT REASON command. This Fault Management section documents changes to the impacted logs.

Fault management tools and utilities

No new tools. Existing tools used are MAPCI and LOGUTIL.

Logs

There are no new logs introduced by this feature, but some existing logs will act as triggers to cause the SPM node to go ISTb on the MAP, and there will be some modifications to existing logs.

CARR511 for SPM carrier going SysB

The CARR511 log is the first of the two new triggers than can cause the SPM node to get ISTb under the PM banner of the MAP display.

Explanation

Log Title: CARR511

Name: SYSB CARRIER SPM

Description: Generated when an SPM carrier changes state to SysB.

Event type: minor

Format

Existing log with no changes, so just showing an example:

```
MSH706BM * CARR511 JUN04 05:46:03 6200 SYSB CARRIER SPM 34
CKT: 13 CarrName: SPM34_STS1P_1_VT15P_3_DS1P_3
Carrier: STS1P 1 VT15P 15 DS1P 1
Previous State: INSV
```

Action

Follow the standard procedures for maintenance of a SysB SPM carrier.

Associated Operational Measurements or Performance Measurements

None

Additional information

CARR511 is generated when one of the OC3's carriers goes SysB, which corresponds to a Bellcore state of OOS-AU-FAF (which is same as OC3 carrier state of IS-UPS-FAF). FAF is Facility Failure. While the carrier is SysB, any of its trunks will be in the CFL condition and not able to bear traffic.

For STM-1 international product, this log will occur when a STM-1 carrier goes SysB.

CARR310 for SPM line carrier raising RFI alarm

The CARR310 log is the second of the two new triggers than can cause the SPM node to get ISTb under the PM banner of the MAP display.

Explanation

Log Title: CARR310

Name: FLT CARRIER SPM

Description: Generated when an SPM line carrier (STS3L or STM1M) raises an RFI (Remote Fault Indicator) alarm.

Event type: minor

Format

Existing log with no changes, so just showing an example:

```
MSH8_03BM * CARR310 APR18 10:27:41 3204 FLT CARRIER SPM 41
CKT: 178 CarrName: ATM_STS3L_SPM_41_CKT_178
Carrier: RM      2 OC3S      0 STS3L  0
Failure: RFI      Set
```

Action

Follow the standard procedures for maintenance of a SPM carrier fault.

Associated Operational Measurements or Performance Measurements

None

Additional information

The CARR310 log above is generated when one of the OC3's InSv STS3L carriers has a RFI (Remote Failure Indication) alarm. Such an alarm can be caused by cutting the TX fiber on the OC3. Note that this trigger corresponds to "R" (for Remote alarm) in the A59036987 feature. Since OC3 sparing will not be allowed while the remote alarm condition is present on the line carrier, the OC3 is effectively in an E2 outage condition due to the loss of redundancy.

If the RFI alarm is set as NRPT (non-reportable) for the carrier in Table MNHSCARR, then the log will not be seen but the trigger will still occur. Note that the CI command:

```
MAPCI;MTC;TRKS;CARRIER;POST {carrier};LISTALM
```

will always show the presence of the alarm, independent of whether MNHSCARR sets the alarm as RPT or NRPT for the carrier.

This trigger/log clears when the RFI alarm clears (as reported by a CARR310 "RFI Clear" log).

For STM-1 international product, trigger will occur when a InSv STM1M carrier has a RFI alarm.

SPM300 for SPM carrier going SysB

The existing SPM300 log will occur for a new reason: a OC3 carrier going SysB. The SPM300 log shows why a OC3 RM went ISTb.

Explanation

Log Title: SPM300

Name: Device Fault Report / Check SysB Carrier

Description: generated when an OC3 has no SysB carriers and one of its carriers goes SysB.

Event type: minor

Format

Existing log that now has a new text reason beside the “7A” row:

```
STEC207AM * SPM300 MAY30 15:57:33 4093 TBL Device Fault Report
Location : SPM : 26 OC3 : 0
Status : Alarm Raised
Problem Description: Non Critical
7A: Check SysB Carrier
Action : Refer to NTPs for Alarm Clearing Procedures.
Cardlist :
No Cardlist Available.
```

Action

See troubleshooting chapter of OPTFN section for how to determine which carrier caused this log to occur.

Associated Operational Measurements or Performance Measurements

None

Additional information

None

SPM300 for RFI Alarm on STS3L Carrier

The existing SPM300 log will occur for a new reason: RFI alarm occurring on a STS3L carrier. The SPM300 log shows why a OC3 RM went ISTb.

Explanation

Log Title: SPM300

Name: Device Fault Report / Check RFI Alarm on STS3L Carrier

Description: generated when a STS3L carrier experiences an RFI alarm.

Event type: minor

Format

Existing log that now has a new text reason beside the “7A” row:

```
STEC207AM * SPM300 MAY30 15:57:33 4093 TBL Device Fault Report
Location   : SPM : 26   OC3 : 0
Status     : Alarm Raised
Problem Description: Non Critical
    7A: Check RFI Alarm on STS3L Carrier
Action     : Refer to NTPs for Alarm Clearing Procedures.
Cardlist   :
```

Action

See troubleshooting chapter of OPTFN section for how to determine which carrier caused this log to occur.

Associated Operational Measurements or Performance Measurements

None

Additional information

None

Alarms

There are no new or changed alarms for this feature.

Related documentation

None

Configuration for A00002858**Hardware and Software Requirements**

Just need SN07/20 release or later in the Core and SPMs.

Initial Configuration

At the CI prompt:

ENGWRITE ON

TABLE OFCENG

POS SPM_NODE_ISTB_FOR_CARRIER_OUTAGE

Office/Subnet parameters (OP/SP) (CM & SESM)

Introducing OFCENG office parameter

SPM_NODE_ISTB_FOR_CARRIER_OUTAGE in the CM.

New/modified office/subnet parameters

Parm table	Parameter name	NEW/CHANGE D/DELETED/RE LOCATED	Domain (CM or Subnet Management)
OFCENG	SPM_NODE_ISTB_FOR_CARRIER_OUTAGE	NEW	CM

Parameter information

SPM_NODE_ISTB_FOR_CARRIER_OUTAGE

SPM Node ISTb under PM Map banner for carrier outage

Functional description

This parameter controls taking a SPM or STM-1 node ISTb under the PM Map banner whenever one of its carriers has an outage. The carrier outage can be 1) whenever any of the SPM's carriers goes SysB, or 2) whenever one of the SPM's line carriers (STS3L or STM1M) has a RFI (Remote Failure Indicator) alarm.

When the parameter is enabled ("Y"), any SPM carrier outage will cause an indicator under the PM banner that a SPM node has gone ISTb. When the parameter is disabled ("N"), carrier outages will never cause a SPM node to go ISTb.

The parameter is only supported on TDM Legacy nodes (SPM and STM-1), and has no impact on Succession nodes (MG4K, LSA, IW, STS-1).

Provisioning rules

Range information

Minimum	Maximum	Default
N	Y	N
It is strongly recommended that this parameter be enabled ("Y") so the telco craftperson will be alerted at the Map to any carrier outages that can disrupt service.		

Activation

Activation is immediate; no restart or manual action is required.

When the parameter is changed to "Y" to enable the feature, these warning messages will be seen:

WARNING: If pre-20 Local loads are running on Legacy SPM/STM

while this parm is YES, then carrier outages may occur.

WARNING: Activation takes up to 45 minutes to complete.

The first warning insures that user does not enable the feature when the local software to support it is not available. For the feature to work when enabled, the Core and Local must be running version 20 or later. If the Local is running 19 or earlier, then carrier outages can occur when the feature is enabled.

The second warning indicates that it can take up to 45 minutes for the change to be propagated to every SPM node, and the current SPM carrier outage status reflected under the Map PM banner.

Dependencies

None

Consequences

N/A

Verification

The only way to test this parameter is working is to turn it on, cause an outage, and confirm the Map reflects the outage. Since service would be disrupted, this is not recommended.

Memory requirements

No memory impact.

Parameter release history update

Added SPM_NODE_ISTB_FOR_CARRIER_OUTAGE parameter to Table OFCENG to control taking SPM node ISTb in the MAP whenever one of the SPM carriers has an outage.

Upgrade Impact**Dump and Restore**

No impact.

Element Management Upgrade

No impact.

Data schema (DS) (CM, MIBS, RDB)

No impact.

Service Orders (SO) (CM & SESM)

No impact.

Element Management

No impact.

Command interface changes

Two new ISTb reasons were added to the output of the existing QUERYPM FLT REASON command.

See the OPTFN section of this feature for good examples of how this command is used.

Directory: MAPCI;MTC;PM;POST SPM [spm#]**Directory description**

PM is an existing MAP level.

Accessing directory: MAPCI;MTC;PM;POST SPM [spm#]**Access to directory or MAP level and return to CI**

Example of how to access and quit the PM Map level for SPM 10:

```
mapci;mtc;pm;post spm 10
```

```
quit mapci
```

Command: QUERYPM FLT REASON

Command type: Listed MENU

Command target: All

Command availability: RES

Command description

The QUERYPM FLT REASON will show the reason an SPM is in the ISTb or SysB state. This feature adds the following new ISTb reasons:

Check SysB Carrier - non-critical fault that indicates the OC3 (or STM) RM has a carrier in the SysB state.

Check RFI Alarm on STS3L Carrier - non-critical fault that indicates the STS3L carrier on the OC3 (which OC3 specified below) has a RFI alarm.

Check Carrier on OC3 RM - non-critical fault that indicates a carrier on this OC3 has one of the two faults listed above.

Command syntax

QUERYPM command parameters and variables

Command	Parameters and variables
QUERYPM	existing
Parameters and variables	Description
FLT REASON	existing

Qualifications and warnings

None

Responses

There are two possible new responses for the QUERYPM FLT REASON command. Each is a status message visible on “All” systems.

Check SysB Carrier

```
>querypm flt reason
OC3 0 ISTb NonCritical faults:
Check SysB Carrier
CEM 0 ISTb NonCritical faults:
Check Carrier on OC3 RM
```

If this is the international STM-1 product, substitute “OC3” above with “STM”.

This ISTb status output indicates that one of the carriers on the OC3 (or STM) is in a SysB state.

Check RFI Alarm on STS3L Carrier

```
>querypm flt reason
```

```
OC3 0 ISTb NonCritical faults:
```

Check RFI Alarm on STS3L Carrier

```
CEM 0 ISTb NonCritical faults:
```

Check Carrier on OC3 RM

If this is the international STM-1 product, substitute “OC3” above with “STM” and “STS3L” with “STM1M”.

This ISTb status output indicates that one of the STS3L (or STM1M) carriers on the OC3 (or STM) has an RFI (Remote Fault Indicator) alarm.

MAP outputs with associated meanings and actions

Command: QUERYPM FLT REASON
RESPONSE: Check SysB Carrier Meaning: one of the carriers on the OC3 has gone SysB. System or user actions: see Troubleshooting chapter of the OPTFN section.
RESPONSE: Check RFI Alarm on STS3L Carrier Meaning: one of the STS3L carriers on the OC3 has an RFI alarm. System or user actions: see Troubleshooting chapter of the OPTFN section.

Example

See OPTFN section of this feature for examples of each scenario when these new responses can occur, and what the telco response should be in each case.

Security

No impact.

Configuration Walkthrough

Other than upgrading to the new SN07/20 release, no further action is required to provision this feature. The new SPM_NODE_ISTB_FOR_CARRIER_OUTAGE office parameter will be “on” by default, so this feature will start working right away.

Product = CS 2000

A00002901 -- Meet-Me Conference Enhancement (Succession on DMS)

Functional Description

Existing Meet-Me Conference allows users to have a conference call without the conference setup time required with most other conferencing features. A directory number and a time is given to all conferees before the conference takes place. The conferees dial the directory number at the chosen time and are entered into the conference. This enables the conferees to quickly get on with the conference.

The user begins a Meet-Me conference by dialing the designated Meet-Me number. The maximum number of participants for a given conference is established in datafill and is associated with the customer group by the SUPERCNF option in table CUSTHEAD. As of BCS-25 it is datafillable whether the first caller must be a member of the Meridian Digital Centrex (MDC) customer group family. In either case if the first caller is a trunk it must have disconnect supervision. Note that other participants in the conference do not necessarily have to be members of the MDC customer group or have disconnect supervision if they are on incoming trunks. Other participants may always access the conference locally or from remote locations over all types of incoming trunk facilities if the datafill in table MMCONF allows them. The first caller receives audible ringing tone until the arrival of the second caller. The conference begins with the arrival of the second caller to the Meet-Me number. Each new participant to arrive on the bridge is announced with an audible confirmation tone to all the current participants. For each customer group, the number of 6-port conference circuits required by Meet-Me Conference are allocated for a customer group in table CUSTENG, option CONF6C.

But in the existing Meet-Me Conference feature, there is no security protection function provided to the conference. If a conference is reserved and datafilled in table MMCONF, anyone who knows the conference bridge DN can dial this DN and start a conference. Also, when a conference is in progress, anyone can enter the conference if he/she knows the conference DN and the conference is not being locked by other conferees. This leak makes the conference unsafe. Because of the limitation of associating the maximum number of 6-port conference circuits to customer group, the number of conference that can be reserved in one customer group is restricted too.

To resolve above limitations and leaks, this feature provides an Enhanced Meet-Me Conference with security protection and other functionalities.

Feature Requirement

Enhanced Meet-Me Conference service on CS2Kc provides a conference bridge which conference participants can enter by dialing a specific DN.

Conference is divided into 2 types: scheduled or timeless. A scheduled conference is the conference that predetermines conference date/time, conference elapsed time so that only within the reserved period of time could the conference be started. Scheduled conference has two sub-type: periodicity and non-periodicity conference type. The user can specify a scheduled conference as a periodically effective reserved conference, what means this conference is reserved with start date/time and elapsed time and the reservation can become effective daily/weekly/monthly. If the scheduled conference is reserved as non-periodicity, the reservation will get effective only once. With timeless conference, the conference DN is reserved timeless. Conference can be started whenever it is needed.

Conference participants are classified into 2 categories: chair-person and invited participants. Chair-person is the conference organizer, only one chair-person exists in one conference. Invited participants are the others invited to join the conference. The number of invited participants can be up to (N-1) per conference where N is the maximum number of conferees allowed in one conference session, it can be from 3 to 30. The chair-person and the invited participants are not necessarily subscribers from CS2Kc. The chair-person and the invited participants can dial into the conference from a IBN line and a CISUP/CTUP/SIP-T trunk.

Conference is secured by assigning conference password for all participants and chair-person. The chair-person and invited participants will have different passwords. The different passwords are the only means to distinguish the roles of chair-person and invited participants while conferees set up their calls to conference. These two password can not be the same. They are datafilled by the operator, and they are visible to operator. Please refer to section 2.2.3 for detail description.

It is optional for the conference organizer whether to let the conference starts without a chair-person. If so, the conference is allowed to start only after the chair-person arrives the conference. Otherwise, the conference can start when any conferee arrives.

In the case that the conference must start after the chair-person arrives, all invited participants arrives the conference before the chair-person will be given an announcement to declare that the chair-person has not arrived and the conference has not started. After that, the invited participants will be given music and placed on hold. When the chair-person arrives, the on-hold participants will be placed into the conference.

In the case that allows the participants enter no matter whether chair-person has arrived, the situation is simpler. When a conferee arrives (if this is a timeless conference or it is in the reserved time of a schedule conference), just place him/her into the conference.

All conferees can have the conference through the conference bridge. In the progress of conference, if a new conferee enters the conference, all online conferees will hear a short ringing tone for announcing the arrival. Another short ringing tone will provide to the existing conferees if a conferee has disconnected. After at least two conferees have arrived and been placed into, the conference can really start.

Another option is given based on the status of the chair-person. The conference organizer can choose whether the conference will go on after the chair-person has disconnected while the conference is being reserved. If this option is set to TRUE, the conference can continue after the chair-person has disconnected from the conference. If this option is set to FALSE, the conference will end while the chair-person drops off even though there are still other conferees online.

For scheduled conference, System should play alarm tone or announcement to participants when time is expired before N minutes. (N is provisionable, e.g N=5 minutes.)

Every call into the conference DN should be mutual control or calling-party control. If a conference participant drops off, the corresponding conference port is automatically released.

Once the Enhanced Meet-Me Conference service is provisioned, it is available to the conference participants at any time, until the service provision is removed. However, the service provision can NOT be removed while the conference is still on.

Conference Provision

Enhanced Meet-Me Conference can be provisioned in a new table EMMCDATA with these aspects:

- Conference bridge DN
- Conference reservation type -- timeless, scheduled or periodicity conference
- Conference Date, Start Time, Elapsed Time. (If the conference type is timeless, this provision information is disable)
- Max number of ports available for the conference
- Invited participant password
- Chair-person password

- Quick start option: whether to allow the conference start if the chair-person has not entered
- ID of the Greeting to conference participants: operator can datafill a default greeting for each conference. If the customer has specific requirement for the greeting, and if software and hardware resource are enough, the operator can datafill a specific greeting for the customer. But this functionality is not guaranteed.
- Audio group number for playing music.
- System should play alarm tone to participants when time is expired before N minutes. N can be provisionable. (If the conference type is timeless, this provision information is disable.)
- Allow_to_continue option: whether to allow the conference to continue after the chair-person drops off
- Billing option: whether to generate a specific billing record for the conference

The provision capability is provided by a table EMMCDATA. The operator can datafill this table for each reserved conference session. The datafill examples of scheduled conference and timeless conference are shown below:

Datafill Example of Table EMMCDATA

TABLE: EMMCDATA

LKEY RESERVE SIZE CHRPSWD PARTPSWD QUICK GREETING AUDIOGRP ENDALARM CONTINUE BILLING

28 801 9998 TIMELESS 6 111111 222222 Y EMMC1 AUDIO12 6 N N

28 801 9996 SCHEDULE NONPERIOD 2003 12 11 08:00 120 6 111111 222222 N EMMC1

AUDIO12 5 N N

28 801 9995 SCHEDULE DAILY 2003 12 02 19:00 300 6 111111 222222 N EMMC1

AUDIO12 6 N N

28 801 9994 SCHEDULE WEEKLY 2003 08 14 20:30 240 6 111111 222222 N EMMC1

AUDIO12 5 N N

Note: The key filed LKEY is composed of SNPA, OFCCODE and STNCODE (which form the bridge DN). The filed RESERVE denotes the reservation type of the conference.

The first tuple shows an example of timeless conference with bridge DN 28 8019998. The user can start a conference at any time from this bridge DN. The timeless conference type is denoted in the filed RESERVE with "TIMELESS".

The second tuple of in this example is a scheduled conference which provides a conference bridge DN 28 8019996. This conference can support up to six conferees to arrives. It starts at 8:00 am on Dec. 11, 2003 and carries through

for 120 minutes. The schedule information is denoted by the field RESERVE with “SCHEDULED NONPERIOD 2003 12 11 08:00 60”. During this period of time, anyone with correct password can enter the conference if the number of the online conferees has not exceeded conference size (in this example, it is 6). This conference session allows the conference to start before the chairperson arrives. It will play a greeting (denoted by EMMCOMPA) to all conferees when they arrives. It allows the conference continue after chairperson disconnects from conference and it will generate a separate billing record for this conference session. Field ENDALLARM denotes that five minutes before the expired time of this conference (10:00 am), an alarm tone will be given to remind the conferees.

The third tuple is also a scheduled conference and it is reserved for periodically used. It is denoted in field RESERVE with “SCHEDULED DAILY 2003 12 02 10:00 300”. The users can use this conference bridge at 19:00 for 5 hours each day from Dec. 02, 2003 until this tuple is removed by the operator.

The size of this table is up to 8192.

When datafilling a tuple in table EMMCDATA, a corresponding tuple is datafilled in table DNINV to make this feature can be triggered via dialling the conference bridge DN. A new feature name EMMC is defined for this feature. Figure , on page 592 shows an example of traver from a line 82220008 to bridge DN 8015555 (the second conference datafilled in Figure , on page 591).

Traver Example of Triggering Enhanced Meet-Me Conference Feature

```
>traver 1 8010008 8019000 b
TABLE IBNLINES
HOST 00 0 00 08 0 DT STN IBN 8010008 CSGRPTA 0 2 28 (FNT) $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE IBNFEAT
TUPLE NOT FOUND
TABLE CUSTSTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
INAP Origination Attempt TDP: no subscribed trigger.
INAP Info Collected TDP: no subscribed trigger.
```

```

TABLE NCOS
CSGRPTA 2 0 0 CSXLTA ( ACR Y)$
TABLE CUSTHEAD: CUSTGRP, PRELIMXLA, CUSTXLA, FEATXLA, VACTRMT, AND DIGCOL
CSGRPTA NXLA CSXLTA FEATXLA 0 CSDIG
TABLE DIGCOL
CSDIG 8 POTS N
TABLE IBNXLA: XLANAME CSXLTA
TUPLE NOT FOUND
Default from table XLANAME:
CSXLTA
      (NET N N 0 N NDGT N Y GEN (LATTR CSXLTA 842_NPRT_2 NLCA_NILLA_2) $ $)$ F
TABLE DIGCOL
NDGT specified: digits collected individually
TABLE LINEATTR
CSXLTA IBN NONE NT 1 0 NILSFC 0 PX CSXLTA NIL 00 CSXLTA CS_NIL $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
842_NPRT_2 NSCR 842 NPRT NONE N $ $
TABLE RATEAREA
NLCA_NILLA_2 NLCA NIL NILLATA $
TABLE PXHEAD
CSXLTA SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                        8019000
TABLE PXCODE
CSXLTA 801 801 CONT ( MM 7 7) ( CLASS NATL) ( XLT OFC CSTERMTA) ( LNET NATL1) ( MZONE 1)$
TABLE OFCHEAD
CSTERMTA SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                        8019000
TABLE OFCCODE
CSTERMTA 801 801 RTE ( MM 3 9) ( DEST 801) ( CLASS LCL) ( LNET NATL1) ( MZONE 1)$
TABLE: OFCRTE
KEY: CSTERMTA 801
. T OFRT 801
. . TABLE OFRT
. . 801 T IBNRTE 801
. . . TABLE IBNRTE
. . . 801 DN 28 801 N 0 4
. . . . TABLE TOFCNAME

```

```
. . . . 28 801 $
. . . . TABLE DNINV
. . . . 28 801 9000 FEAT EMMC 28 801 9000
TABLE DNFEAT
TUPLE NOT FOUND
. . . . TABLE DNATTRS
. . . . TUPLE NOT FOUND
. . . . TABLE DNGRPS
. . . . TUPLE NOT FOUND
. . . . EXIT TABLE IBNRTE
. . . . EXIT TABLE OFRT
EXIT TABLE OFCRTE
INAP Info Analyzed TDP: no subscribed trigger.
INAP Route Select Failure TDP: no subscribed trigger.
INAP Termination Attempt TDP: no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 FEATURE                288019000                ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 BUSY

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

Conference Processing

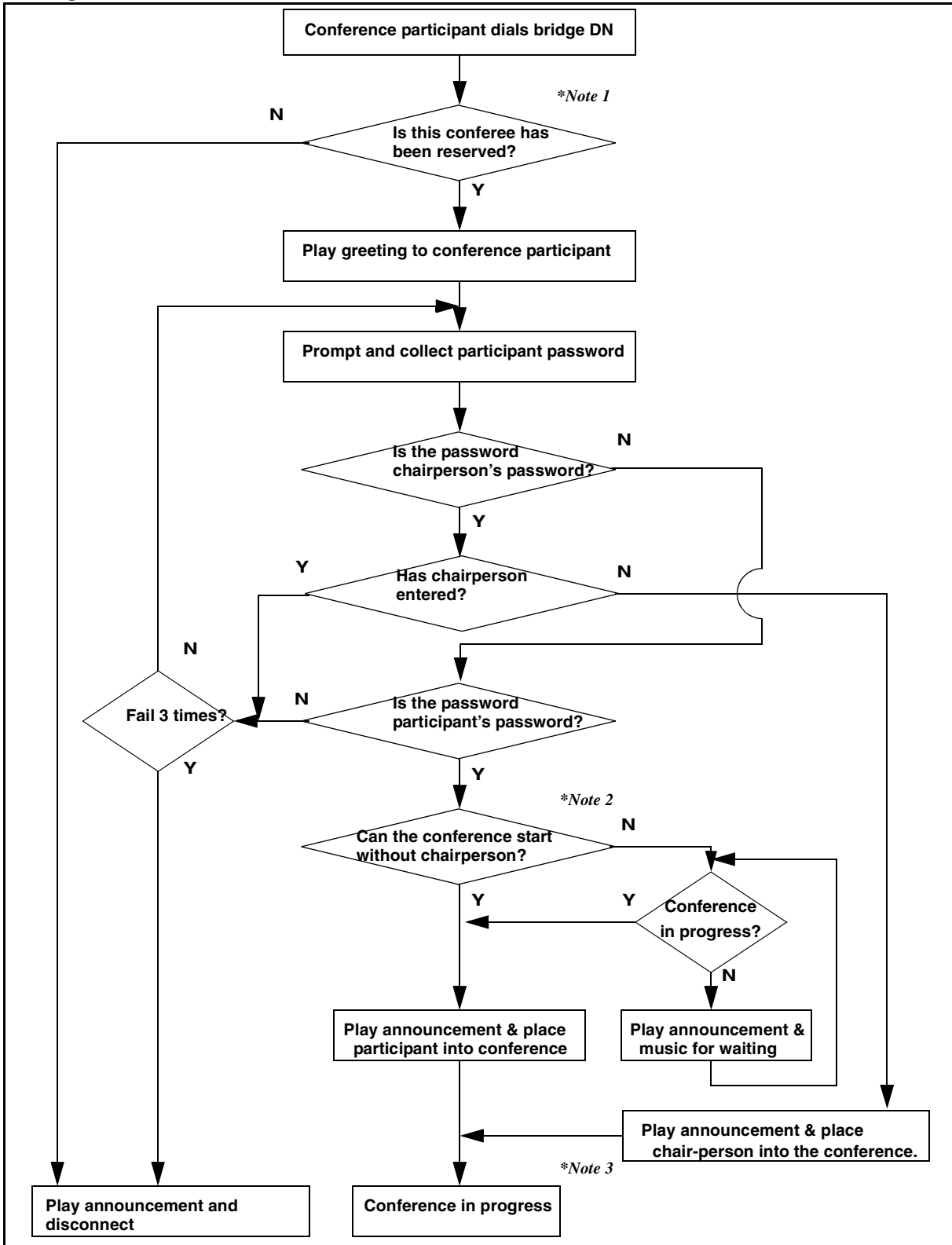
The conference should be protected to prevent any accidental or malicious invader. This function is implemented by assigning conference password for all invited participants and specific chair-person password. During dialling phase, after dialling conference bridge DN, all conferees (invited participants and chair-person) are required to input passwords. Only the ones having inputted correct passwords are guaranteed to enter the conference. Conferees are guided by prompt and announcements when they dialling password. Conferees need input password once in dialling process if a correct password is inputted. Their roles are identified by passwords.

During the dialling process, some announcement are provided to guide the user how to execute following steps. The user can bypass the announcement by directly dialling any key. These announcements are:

- Greeting to welcome the user arrives the conference. This greeting can be datafilled on a per conference basis. So different conference may have different greeting.
- Prompt for collecting conferee's password.
- Prompt for reminding the user has inputted wrong password and to input again.
- Prompt for welcoming the chair-person enters the conference.
- Prompt for welcoming an invited participant enters the conference.
- Prompt for welcoming an invited participant but to place this participant on hold because the chair-person has not entered.
- Prompt for reminding the user has made some error and will be disconnected from the conference.

With the scheduled conference type, before N minutes to the end time (N is datafilled in field ENDALARM in table EMMCDATA), an announcement will play to all participants that the conference will end in N minutes.

The dialling conference DN and password process are shown in the following figure.

Dialling Process

Note: 1. If the conference type is scheduled and the dialling date/time is within the reserved conference start date/time and elapsed time, or the conference type is timeless, we think that the conference has been reserved.

Note: 2. Whether a conference can start without a chair-person is controlled by datafilling a quick start option for each conference session.

Note: 3. Under following two circumstance, we think that the conference is in progress: I. The chair-person has entered the conference. II. If the conference session has quick start option, an invited participant is the first conferee and is allowed to entered the conference.

After the conferee gets through the password verification and enters the conference, a conference port is allocated for this conferee. He/She will occupy one port of 6-port conference circuit mounted of CTM/MTM on TDM side or a member of UAS on IP side. The hardware resource will not be freed until the conferee drops off. If the conference reaches the maximum allowed size specified in table EMMCDATA, further call attempts will receive busy treatment. Until a conferee disconnects and thereby provides a vacant port on the conference, further user is allowed to enter. If the conference is under maximum size but it is unable to attach hardware resource, the user will receive NOSC treatment.

During conference processing, each new participant arriving on the bridge is announced with an audible confirmation tone to all the current participants. Similarly, A burst of dial tone is provided each time a conferee leaves the conference. When all conferees are dropped from the conference, all the conference circuits are freed. It is datafillable whether the conference will end after the chair-person disconnects.

For scheduled conference, an alarm tone will be played to all participants when elapsed time will be expired in N minutes. N is a number that When the predetermined elapsed time expires, the conference ends and all conferees (chair-person and invited participants) disconnect from the conference. For the timeless conference, the conference can keep on till all conferees drop off, no elapsed time limitation.

Conference Billing

When the billing option is datafilled, a billing record is generated for each session of the conference, and only one record is generated.

The billing record includes the following:

- Conference start date/time: the time that the first participant enters the conference if quick start option is set to TRUE, or when the chair-person is placed into the conference if quick start option is set to FALSE.

- Conference end time: the time all the participants have dropped off
- Conference port usage: the maximum number of ports used during the conference session. This is not the conference allowed size datafilled in the table, but the maximum actual used ports in conference progress.
- Conference bridge DN

According to different datafill of field QUICK in table EMMCDATA for different conference, conference start date/time have different definitions. If this field is set to TRUE, which means the conference can start without the chair-person entering, conference start date/time record the date and time when the first conferee enters the conference, no matter this conferee is a chair-person or an invited participant. If this field is set to FALSE, which means the conference can only start after the chair-person enters, conference start date/time record the date and time when the chair-person enters the conference.

Conference end time always records the time when the last conferee drops off from the conference.

A conference session denotes the period of time from conference start time to conference end time. In a scheduled conference, if all conferees drops off, it is considered that this conference session has completed. If the time hasn't expired, any user can still start the conference. But it will be thought as a new conference session. For each conference session, only one billing record is generated. And the billing record is only associated with this conference session.

Conference port usage records the maximum number of ports used during a conference session, i.e. the maximum number of online conferees at the same time during a conference session.

Conference bridge DN should also appear in the billing record.

One thing should be noticed, the control of generated billing record is per conference base, but not per conference session base. That means the field BILLING in table EMMCDATA can only control the generation of the billing record to the conference datafilled in the same tuple. If this conference has multi conference sessions, all sessions will (or will not) generate the billing records according to the filed BILLING.

An ama log will be generated as the billing record for each conference session. This ama log contains a structure code (the structure code can be selected from x0510, x0511, x0512, x0513 or x0514) and a module code (612) to record billing information. MC612 is appended to the structure code. The conference bridge DN is stored in the structure code, the other information are stored in the module code. One ama log is to be generated for one conference session.

The following figure is an example of a billing record, the module code 612 is appended to the structure code 40514.

An Example of Billing Record of a Conference Session

```
>calldump full
*
HEX ID: AA
STRUCTURE CODE: 40514C
CALL CODE: 006C STATION PAID
SENSOR TYPE: 036C DMS 100F
SENSOR ID: 0250250C
REC OFFICE TYPE: 036C DMS 100F
REC OFFICE ID: 0250250C
DATE: 30827C AUGUST 27, 2003
TIMING IND:
  TIMING GUARD FLAG 0 UNUSED
  SHORT CLD PARTY OFF-HOOK IND 0 UNUSED
  LONG DUR/SERV PTY CAPABILITY IND 0 UNUSED
  UNUSED 0
  UNUSED 0C
STUDY IND:
  STUDY TYPE A 0 UNUSED
  STUDY TYPE B 2 NETWORK COMPLETION
  STUDY TYPE C 0 UNUSED
  TEST CALL IND 0 UNUSED
  UNUSED 0
  ORIG/TERM NANP NUM IND 0 UNUSED
  OPERATOR SERV IND 0C UNUSED
CLD PTY OFF-HK: 0C CLD OFF-HOOK DETECTED
SERVICE OBSERVED: 0C NONE
OPER ACTION: 0C ANI, CUSTOMER DIALED CALL
SERVICE FEATURE: 000C OTHER
SIG DIGITS NEXT FIELD: 010C
ORIG OPEN DIGITS 1: FFFFFFFF
ORIG OPEN DIGITS 2: FFFFFFFF
ORIGINATING CHARGE INFO: FFFF
DOMESTIC/INTL INDICATOR: 1C DOMESTIC
SIG DIGITS NEXT FIELD: 007C
EXT TERM OPEN DIGITS 1: 000000008015555C
EXT TERM OPEN DIGITS 2: FFFFFFFFFFFFFFFF
CONNECT TIME: 1707089C 17:07:08.9
ELAPSED TIME: 000000026C 000000:02.6
COMPLETION INDICATOR: 001C COMPLETED: ANSWERED
MODULE CODE: 612C EMMC
GENERIC DIGITS STRING 1: 308271706128000C
GENERIC DIGITS STRING 2: 308271707086003C
MODULE CODE: 000C FINAL MODULE
```

The conference bridge DN is stored in the filed 'EXT TERM OPEN DIGITS 1' as 000000008015555c. In the module code 612 appended to the structure code, filed 'GENERIC DIGITS STRING 1' records the conference start date/time: 17:06:12.8 on Aug., 27, 2003. Field 'GENERIC DIGITS STRING

2' records the conference end date/time: 17:07:08.6 on Aug., 27, 2003 and the maximum ports used during this conference session: 3 ports.

Hardware Requirements or Dependencies

This feature uses conference circuits provide by six-party conference card on TDM side or UAS on IP side to implement conference bridge.

Software Requirements or Dependencies

N/A

Limitations and restrictions

- All changes to the conference bridge DN and other information should be done through table EMMCDATA. Any other method of changing the DN is not supported.
- The hardware resource in the switch is not guaranteed enough to support all reserved conference at the same time. If a large conference is supported by a UAS on CS2Kc, it is not possible to guarantee with absolute certainty that sufficient UAS ports will always be available to allow additional persons to join the conference. If an additional person tries to join a large conference at a time when a UAS port is not available, the system provides treatment (a reorder tone) to the user and leaves the existing conference intact. Same thing will happen on TDM side.
- Touch tone commands should be provided to the chair-person and invited participants to implement specific control to the conference. To provide touch tone commands, DTMF tone must be able to be detected during talking phase in a call. But implementing DTMF tone detection needs a lot of development effort, so touch tome commands functionality will leave as a potential function of this feature in the future.
- When a subscriber is being included in an Enhanced Meet-Me Conference, all flash activation/deactivation feature is forbidden.
- Multiple Appearance Directory Number (MADN) is forbidden while a subscriber is being included in the conference.

Interactions

- If these features have been activated (Three Way Call, Attendant Console, Station Controlled conference, Preset Conference, Directed Call Pickup, Call Forward, Simring) on a subscriber, it is not allowed to terminate on Enhanced Meet-Me Conference bridge DN.
- If a conferee has the call forward busy (CFB) feature, calls to the conferee are forwarded during the conference.
- 3-way call and call waiting will be disable if a user is in conference progress.

- When a subscriber is being included in an Enhanced Meet-Me Conference, feature Calling Number Delivery Blocking (CNDB), Calling Number Blocking (CNB), Calling Name and Number Blocking (CNNB) is allowed.

Applicable customer facing sections

Fault Management

Logs ☐ N/A ☐

Alarms ☐ N/A ☐

Configuration

Data Schema ☐ X ☐

User Interface ☐ N/A ☐

Element Management ☐ N/A ☐

Security ☐ N/A ☐

Service Order ☐ N/A ☐

Office Parameters ☐ N/A ☐

Accounting (includes AMA billing) ☐ X ☐

Performance (includes operational measurements) ☐ N/A ☐

Indicate with an X if you are completing the sections of the DDOC listed below. Indicate with “N/A” if these sections do not apply to this functionality.

Realtime ☐ N/A ☐

Engineering Information ☐ N/A ☐

Glossary

Term	Description
DN	Directory Number
EMMC	Enhanced Meet-Me Conference
UAS	Universal Access Server

Reference

- a. AMA Formatter User’s Guide
- b. BR0781FN - Call Forwarding Remote Activation

Appendix

Datafill Example of UAS

To achieve proper audio node maintenance, the CM needs to know the number of conference and announcement terminals supported to allow this to be dynamically modified when needed.

TABLE SERVSINV

SRVSNAME SRVRNAME NUMTERMS OPTIONS

AUD 1 GWC 96 2048 (3PORT 30) (6PORT 30) (ANNC 100) \$

TABLE CLLI

CLLI ADNUM TRKGRSIZ ADMININF

UASCF6P 219 30 UAS_6_CONFERENCE

Example of Datafilling Conference Circuit on TDM Side

Enhanced Meet-Me Conference is based on six-way conferences. The example for datafilling conference circuit with a CTM card on TDM side is shown below:

TABLE CLLI

CLLI ADNUM TRKGRSIZ ADMININF

CF6P 110 20 6_CONF

TABLE PADDATA

PADKEY PAD1TO2 PAD2TO1

CONF CONF 0 0

TABLE TMINV

TMNM FRTYPE FRNO SHPOS FLOOR ROW FRPOS LKDATA EQPEC LOAD EXEC S CTMLOC

CTM 0 TME 0 32 1 BB 0 0 10 6 0 1X81AA MTMKA02 MTMEX SINGLE_CARD MTM 1 10

```
TABLE CONF6PR
CNFCKTNO EXTRKNM TMTYPE TMNO TMCKTNO CARDCODE PADGRP
-----
0 0 CTM 0 24 1X81AA CONF
```

Datafill Example of Announcements

The datafill sequence for announcements is different on TDM side and IP side. The following example shows the datafill sequence with EDRAM announcements (TDM side) and UAS announcements (IP side).

```
TABLE ANNAUDID                                %% Only for UAS announcements
PHRASEKY AUDID
-----
EMMCGREE1 1210
EMMCPSWD  1211
EMMCREINPUT 1213
EMMCCHAIR 1214
EMMCINVITED 1215
EMMCERROR 1216
EMMCHELD 1217
```

```
TABLE DRAMPHRS                                %% Only for EDRAM announcements
DRAM PHRSNAME PHRASENO BLOCK LENGTH RECORDED
-----
0 EMMCEGREE 25 2 6 Y N 11
0 EMMCPSWD 26 2 5 Y N 17
0 EMMCREINPUT 27 2 5 Y N 22
0 EMMCCHAIR 28 2 3 Y N 27
0 EMMCVITED 29 3 6 Y N 5
0 EMMCERROR 30 3 4 Y N 11
0 EMMCHELD 31 3 5 Y N 16
```

```
TABLE CLLI
CLLI ADNUM TRKGRSIZ ADMININF
-----
EMMCDEFAULT 345 10 EMMC_DEFAULT_GREETING
EMMCANN 478 10 EMMC_ANNOUNCEMENT
```

TABLE ANNS

CLLI ANNARCH TRAFSNO CYTIME MAXCYC DATA

EMMCDEFAULT NETWK 0 10 2 STND Y 30

EMMCANN NETWK 0 3 1 EMMC 10

TABLE ANNMEMS

ANNMEM HDWTYPE CARD MEMINFO

EMMCDEFAULT 0 UAS AUD 0 AUD 0

%% This is for UAS announcements

EMMCDEFAULTL 1 DRAM DRA (1 DTM 1 1)

%% This is for EDRAM announcements

EMMCANN 0 DRAM DRA (0 DTM 2 1)

%% This is for EDRAM announcements

EMMCANN 1 UAS AUD 0 AUD 1

%% This is for UAS announcements

TABLE ANNPHLST

ANNPHKEY PHSLIST

EMMCDEFAULT 1 (EMMCEGREE) \$

%% for EDRAM announcements

EMMCDEFAULT 0 (EMMCGREE1) \$

%% for UAS announcements

EMMCANN 1 (LANGUAGE 1) (EMMCPSWD) \$

EMMCANN 2 (LANGUAGE 1) (EMMCREINPUT) \$

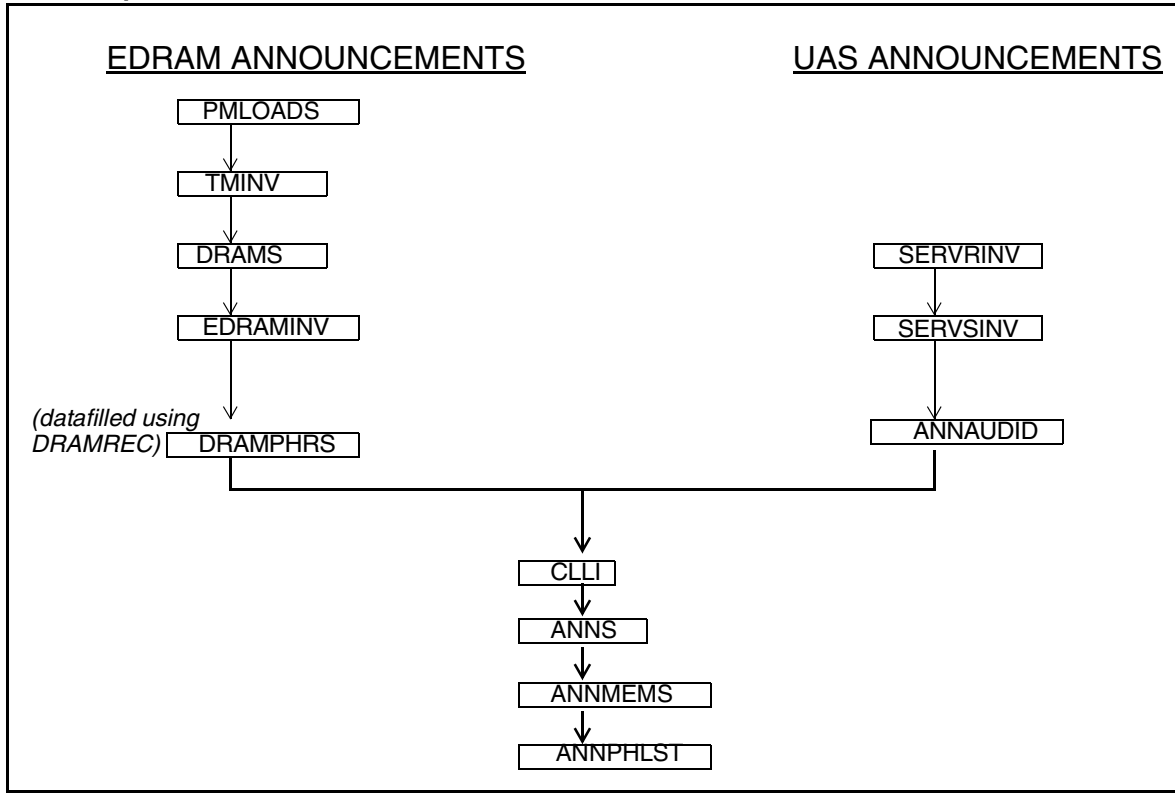
EMMCANN 3 (LANGUAGE 1) (EMMCCHAIR) \$

EMMCANN 4 (LANGUAGE 1) (EMMCINVITED) \$

EMMCANN 5 (LANGUAGE 1) (EMMCERROR) \$

EMMCANN 6 (LANGUAGE 1) (EMMCHELD) \$

The datafill above that is not designated specific for EDRAM or UAS announcements is for both types.

Datafill sequence of announcements**Datafill Example of Music**

The music playing for the held participant is defined with a new audio group, the datafill example is shown below:

```

TABLE AUDIO
AUDIOKEY ROUTES
-----
AUDIO10 EMMC (MUSIC MUSIC1 0)
  
```

Configuration for A00002901**Hardware and Software Requirements**

NA

Initial Configuration

NA

Office/Subnet parameters (OP/SP) (CM & SESM)

NA

Upgrade Impact

NA

Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
EMMCDATA	NEW	NEW

Table/MIB/Remote Database Schema information

Name: EMMCDATA

Functional description

This table is used for Enhanced Meet-Me Conference provisioning.

Usage sequence and implications (CM Only)

N/A.

Size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
EMMCDATA	0	8192	

Fields/OIDs

The following table lists fields/OIDs for EMMCDATA.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
LKEY	New		see subfields	EMMC table Key, this field consists of subfields SNPA, OFCCODE and STNCODE
		SNPA	serving_numbering_plan_area	area code of a DN
		OFCCODE	ofccode_digit_register	office code of a DN
		STNCODE	stncode_digit_register	station code of a DN

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RESERVE	New	RESERVED	see subfields SCHEDULE or TIMELESS	The reservation type of the conference: timeless or schedule. Selector. If the conference is reserved for the user to have a conference at any time, then enter TIMELESS and datafill no refinement is this field. If the conference is reserved for the user to have conference only at specific time, then enter SCHEDULE and datafill refinements SCHEDULE, STARTDAT, STARTTIM and ELAPSED.
SIZE	New	N/A.	numeric {3 TO 30}	Conference size. Specify the maximum allowed conferees in this conference.
CHAIPSWD	New	N/A.	6 digits code	Chair-person's password. Enter the 6 digit length password.
PARTPSWD	New	N/A.	6 digits code	Invited Participant's password. Enter the 6 digit length password. This password can not be the same as the one of chair-person's.
QUICKST	New	N/A.	Y or N (boolean)	Quick Start option. If the conference can start without the chair-person, enter Y. With this datafill, all participants enter before the chair-person will be placed on hold. If the conference must start with the chair-person entering, then enter N.
GREETING	New	N/A.	alphanumeric {a maximum of 16 characters}	Enter the CLLI name of the announcement defined for the greeting of this conference.
AUDIOGRP	New	N/A.	audio group	Enter the audio group name of the music which will be played while an invited participant is to be held.
ENDALARM	New	N/A.	{1 TO 10}	numeric range

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CONTINUE	New	N/A.	Y or N (boolean)	Continue option. Enter Y if the conference can continue after the chair-person leaves. If the conference should drop after the chair-person leaves, Enter N.
BILLING	New	N/A.	Y or N (boolean)	Billing option. Enter Y for generating conference specific AMA log. Enter N for no specific AMA log generation.

RESERVED = SCHEDULE

If the entry in subfield is SCHEDULE, datafill refinement as described below.

Table field descriptions when RESERVED = SCHEDULE

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
		SCHEDULE	DAILY, WEEKLY, MONTHLY or NONPERIOD	Scheduled type of the conference. This field denotes the scheduled type of the conference being reserved. If the conference is reserved to be used during a specific time for each day, enter DAILY. If the conference is reserved to be used during a specific time and is able to be used on one day of each week, enter WEEKLY. If the conference is reserved to be used during a specific time and is able to be used on one day of each month, enter MONTHLY. If the conference is reserved to be used during a specific time and is only for once, enter NONPERIOD.
		STARTDAT	yyyymmdd	Conference start date. Enter the start date of this conference (year, month and day).
		STARTTIM	hhmm	Conference start time. Enter the start time of this conference (hours and minutes).

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
		ELAPSED	1 to 9999	Conference elapsed time. Enter the predefined elapsed time of this conference (in minutes).

Datafill example

The following example shows sample datafill for table EMMCDATA.

TABLE: EMMCDATA

LKEY RESERVE SIZE CHRPSWD PARTPSWD QUICK GREETING AUDIOGRP ENDALARM CONTINUE BILLING

131 830 1000 SCHEDULE NONPERIOD 20030810 0930 60 6 111111 222222 Y EMMCOMPA AUDIO10 5
Y N

131 801 5555 TIMELESS 10 111111 222222 N EMMCOMPB AUDIO10 0 Y Y

131 830 2000 SCHEDULE DAILY 20030810 1130 60 6 111111 222222 Y EMMCOMPA AUDIO10 5 Y Y

Table release history update

New table EMMCDATA is added.

Supplementary information

N/A.

Translation verification other tools

N/A.

Product = CS 2000**A00002960 -- Originator Identification Screening (Succession on DMS)*****Functional Description***

This feature allows customers to block call terminations to certain ISUP EANT trunks when the Charge Number (CN) or Calling Party Number (CPN) identifiers are not available. The intent of this new functionality is to allow only calls with one of the originating identifiers to complete over certain ISUP EANT trunks. All other calls will advance to the next trunk in the route list.

Please refer to the following sections for additional information:

- “SOC Control: UTRS0011” on page 610
- “Table TRKOPTS: ORIGIDSCR” on page 610.
- “Call Processing” on page 610

SOC Control: UTRS0011

The new SOC order code UTRS0011, UCS Orig ID Screen, is introduced by this feature. When UTRS0011 is IDLE calls will not be blocked on any ISUP EANT trunks when the CPN or CN is not present. The new ORIGIDSCR option in Table TRKOPTS can be datafilled when SOC is IDLE. When UTRS0011 is ON certain calls can be blocked. For more information see “Call Processing” on page 610.

The functionality introduced by this feature has been patched in older releases under password activated patch ATM51. During ONP processes UTRS0011 will have STATE set to ‘ON’ if the old side has patch ATM51 applied and activated. Otherwise, the SOC is set to IDLE.

Table TRKOPTS: ORIGIDSCR

A new trunk group option, ORIGIDSCR, is introduced in Table TRKOPTS for ISUP EANT trunks only. This allows the customer to specify which ISUP EANT trunks perform originator identification screening. For more information see “Call Processing” on page 610.

Table TRKOPTS Examples

TABLE: TRKOPTS

TRK1 ORIGIDSCR ORIGIDSCR

When an attempt to add ORIGIDSCR to a trunk other than EANT type or an MF EANT trunk the following error message is generated by table control:

TABLE: TRKOPTS

*** ERROR - ORIGIDSCR can only be assigned to EANT ISUP trunks.

When an attempt to add ORIGIDSCR to an incoming trunk the following error message is generated by table control:

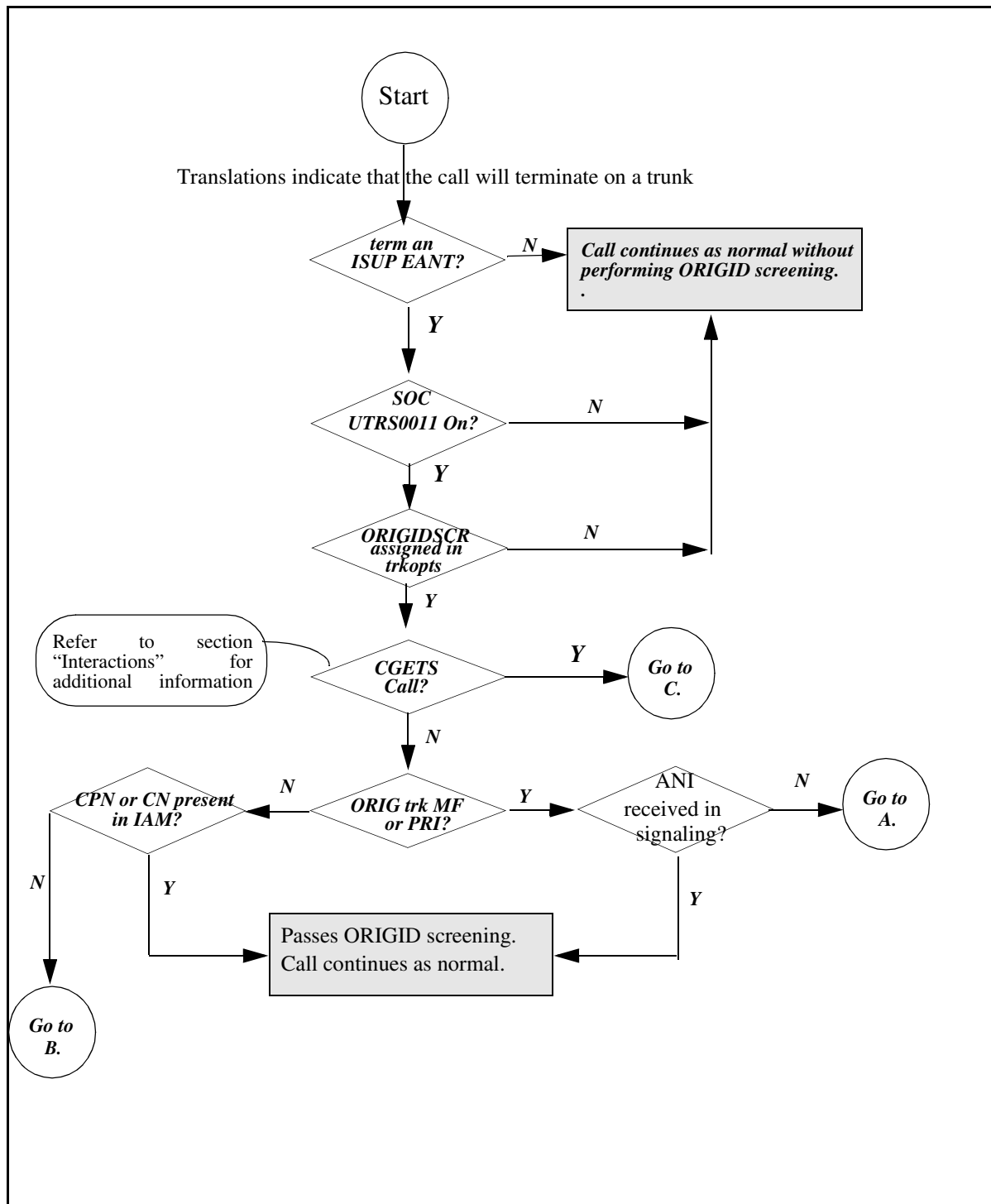
TABLE: TRKOPTS

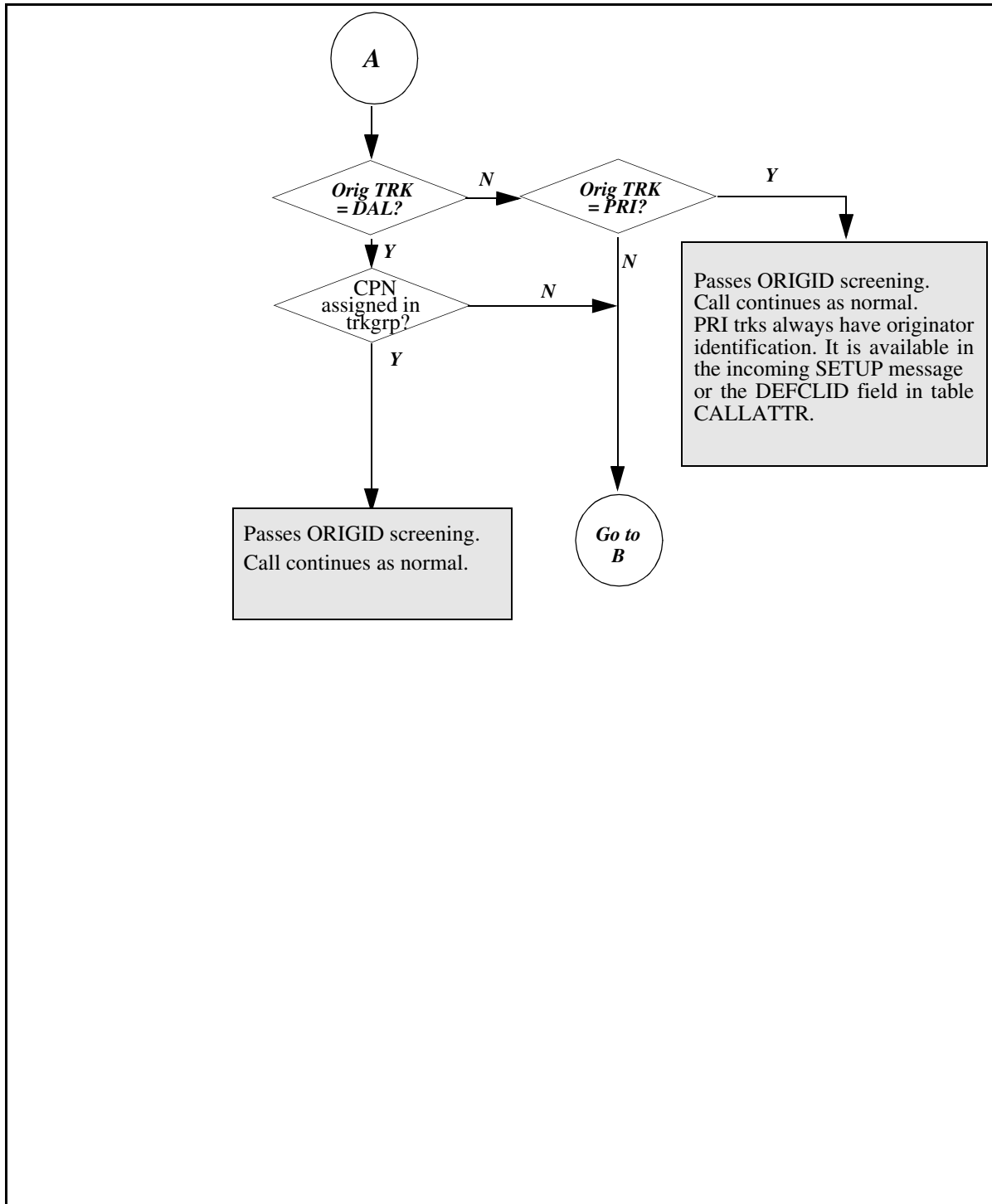
*** ERROR - ORIGIDSCR can not be assigned to Incoming trunks.

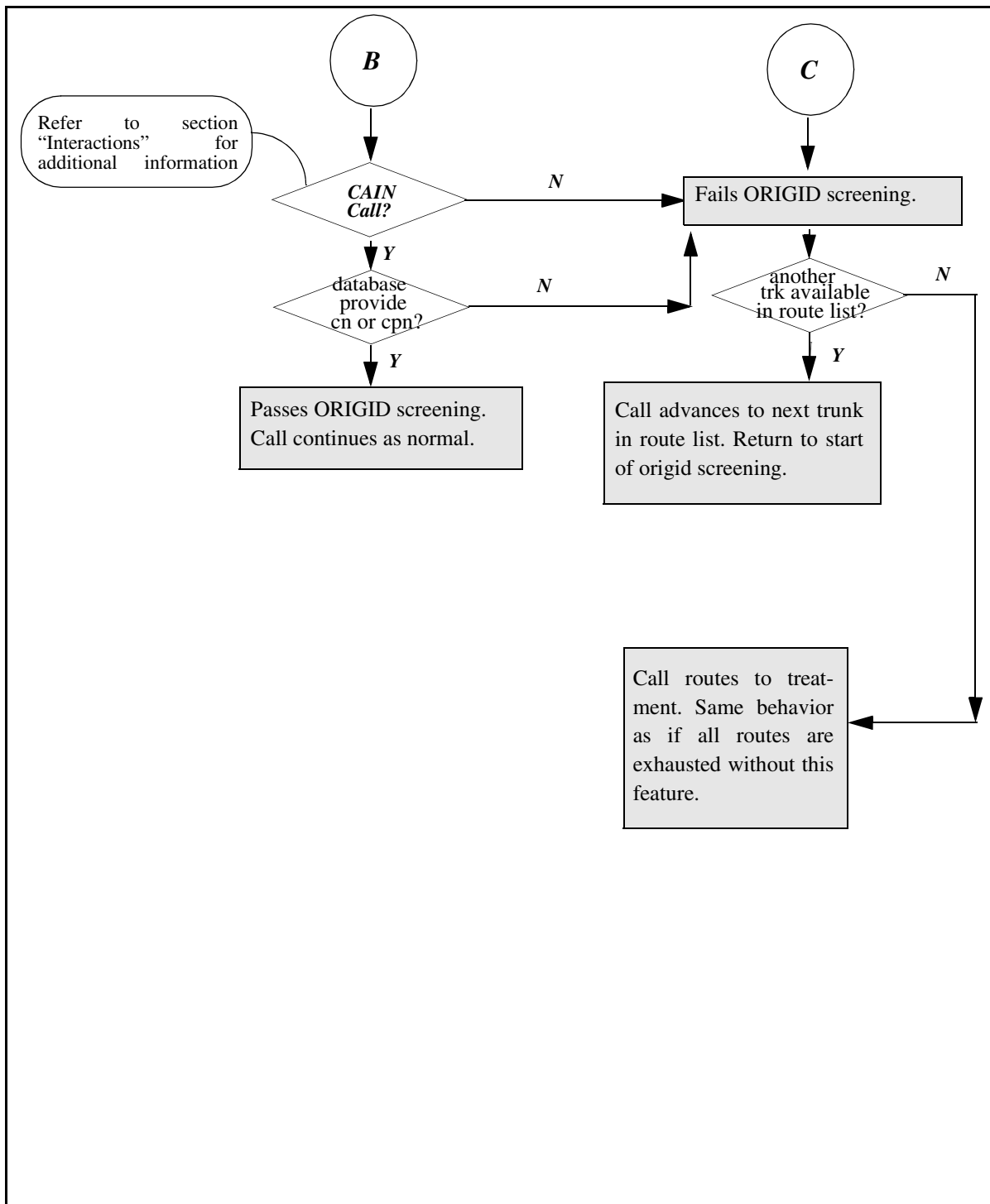
Call Processing

Call processing is enhanced to block call terminations on ISUP EANT trunks when ORIGIDSCR is assigned in Table TRKOPTS if the CN or CPN is not available from the incoming signaling or originator datafill. This feature is also controlled by SOC UTRS0011. Starting on page 611 is a detailed flow chart that describes the behavior of this feature.

Originator Identification Screening Flow Chart



Originator Identification Screening Flow Chart - PART A

Originator Identification Screening Flow Chart - PART B

Hardware Requirements or Dependencies

None.

Software Requirements or Dependencies

None.

Limitations and restrictions

The new option ORIGIDSCR in Table TRKOPTS can only be assigned to 2w or outgoing ISUP EANT trunks. ORIGIDSCR can not be assigned to incoming ISUP EANT trunks.

This feature does not support interaction with Dynamically Controlled Routing (DCR.).

Interactions

Blocking of ANI delivery

This feature only considers if the CPN or CN is available from the incoming signaling or originator datafill. It does not consider if the originator or terminator has blocked delivery of this information in datafill. Therefore, the blocking of information has no impact on this feature. It is possible for originator screening to pass but the outgoing IAM to not contain CN or CPN because of one of the blocking features. Examples are:

Table RTEATTR	Datafill in Table RTEATTR can block sending out CPN, CN, and other parameters. It can also include CPN, CN, or other parameters.
IMT trunks: Table TRKGRP	Datafill in Table TRKGRP for IMT trunks can block sending out the CPN or CN with field CPIXFER.
EANT trunks: Table TRKGRP	Datafill in Table TRKGRP for EANT trunks can block sending out the CPN or CN with option TMANIDLK.
Tables ANISCUSP & UNIPROF	Datafill in both tables can block sending out the CPN or CN with field ANIDELV.

CAIN

CAIN calls can receive a CPN or CN from the SCP. If CPN and CN are not available from the incoming trunk then CAIN calls must check if the database supplied them.

Assume that SOC UTRS0011 is ON and the route determined by CAIN translations provides two possible trunks, TRK1 and TRK2. Only TRK1 has

the new ORIGIDSCR option assigned in Table TRKOPTS which is discussed in “Table TRKOPTS: ORIGIDSCR” on page 610. Neither incoming signalling nor the originator datafill provided the CPN or CN but CPN or CN was supplied by the database so the call can terminate on TRK1. If the CAIN database had not supplied CN or CPN the call would route advance to TRK2.

CGETS

This feature does not support the termination of CGETS calls on trunks with ORIGIDSCR assigned. If a CGETS call attempts to route over a trunk that has this feature activated it will always route advance.

Applicable customer facing sections

Fault Management

Logs ___N/A___

Alarms ___N/A___

Configuration

Data Schema ___X___

User Interface ___N/A___

Element Management ___N/A___

Security ___N/A___

Service Order ___N/A___

Office Parameters ___N/A___

Accounting (includes AMA billing) ___N/A___

Performance (includes operational measurements) ___N/A___

Realtime ___X___

Engineering Information ___X___

Glossary

ANI	Automatic Number Identification
CAIN	Carrier Advanced Intelligent Network
CGETS	Carrier Government Emergency Telecommunications System
CPN	Calling Party Number parameter of IAM
CN	Charge Number parameter of IAM

DAL	Dedicated Access Line
DCR	Dynamically Controlled Routing
EAEO	Equal Access End Office
EANT	Equal Access Network Trunk
IAM	Initial Address Message of the SS7 signalling
ISUP	Integrated Services digital network User Part
MF	Multi-Frequency
PRI	Primary Rate Interface
SOC	Software Optionality Control

Configuration for A00002960

Hardware and Software Requirements

In order to perform originator identification screening SOC UTRS0011 must be ON and the terminating ISUP EANT trunk must have ORIGIDSCR assigned in Table TRKOPTS.

Initial Configuration

This feature only impacts calls that terminate on ISUP EANT trunk.

Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

Upgrade Impact

Dump and Restore

No special steps are required.

Element Management Upgrade

N/A

Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
TRKOPTS	Changed	New

Table/MIB/Remote Database Schema information

Name: TRKOPTS

TRunK OPTionS

Functional description

A new trunk group option, ORIGIDSCR, is introduced in Table TRKOPTS for ISUP EANT trunks only. This allows the customer to specify which ISUP EANT trunks perform originator identification screening introduced by this feature.

Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

Current datafill order unchanged.

Size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TRKOPTS	0	131072	Dynamically Allocated

Fields/OIDs

The following table lists fields/OIDs for TRKOPTS impacted by this feature.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTION	Changed	Refinement	ORIGIDSCR refinement is added	New option is ORIGINator IDENTificaton SCreening.

Datafill example

The following example shows sample datafill for table TRKOPTS.

Table TRKOPTS Examples

TABLE: TRKOPTS

TRK1 ORIGIDSCR ORIGIDSCR

When an attempt to add ORIGIDSCR to a trunk other than EANT type or an MF EANT trunk the following error message is generated by table control:

TABLE: TRKOPTS

*** ERROR - ORIGIDSCR can only be assigned to EANT ISUP trunks.

When an attempt to add ORIGIDSCR to an incoming trunk the following error message is generated by table control:

TABLE: TRKOPTS

*** ERROR - ORIGIDSCR can not be assigned to Incoming trunks.

Table release history update

Added option ORIIDSCR option for ISUP EANT trunks. This allows the customer to specify which ISUP EANT trunks perform originator identification screening.

Supplementary information

None

Translation verification other tools

Table TRKOPTS is not displayed in TRAVER.

Service Orders (SO) (CM & SESM)

N/A

Software optionality control (SOC)

SOC

SOC option name:	UCS ORIG ID SCREEN
SOC option title:	Yes
SOC option control type:	usage
New SOC option?	Yes
SOC option order code	UTRS0011
Option defined in DRU:	UCS

SOC

Affected products:	SN07

Element Management

N/A

Command interface changes

N/A

Security

N/A

Configuration Walkthrough

In order to perform originator identification screening SOC UTRS0011 must be ON and the terminating ISUP EANT trunk must have ORIGIDSCR assigned in Table TRKOPTS.

Product = CS 2000**A00002966 -- Base Re-architecture Phase 2 (Succession on DMS)*****Functional Description (FN)***

The feature is a follow-up to Base Re-architecture Phase 1 which re-architected the SDM platform software to decouple the AIX specific software from the common base software and port it from AIX compiler to open sourced GCC compiler. The common base software can be compiled across multi-platforms, such as AIX, Sun, and be used by SDM and CBM products.

The following major functions are expected to be ported from the SDM to the CBM in the feature:

- **Passthru users using SSH/telnet:** this functionality enables customers to access the Core/CM by logging in the CBM through telnet/SSH client software. The user will be automatically forwarded to the Core/CM or the destination configured for the user. No command can be initiated on the CBM by passthru class users. The user interface for managing the passthru users is described in the FN of the feature A00002822 - User Interface Manager for CBM.
- **Restrict shell for maint class users:** all maint class users on the CBM are using the restrict shell to meet security requirement. It uses pretty much the same mechanism as in the SDM except that unix standard man pages are used instead of SDM-own fashioned help command. The user interface for

managing the maint class users is described in the FN of the feature A00002822 - User Interface Manager for CBM.

- **Cbmgather tool:** an equivalent platgather tool, which is called cbmgather, is developed on the CBM. The difference from platgather is that the cbmgather doesn't collect the platform specific information, such as splitmode related log, FXgather, etc.

In addition to the porting work, the following new enhancements to the SDM or/and the CBM are expected to be completed in the feature:

- Add querytape subcommand in the apply level of sdmmtc for the SDM to retrieve the version information from the specified tape. It has the following syntax:

```
querytape <dat0 | dat1 >
```

dat0: tape drive in the domain 0

dat1: tape drive in the domain 1

The help information can be obtained through the help subcommand in the apply level.

- Add a new option to platgather/cbmgather to specify number of days' logs to be collected in order to accommodate some special need when the entire custlog and designlog files are expected to be collected. The new option looks like as follows:

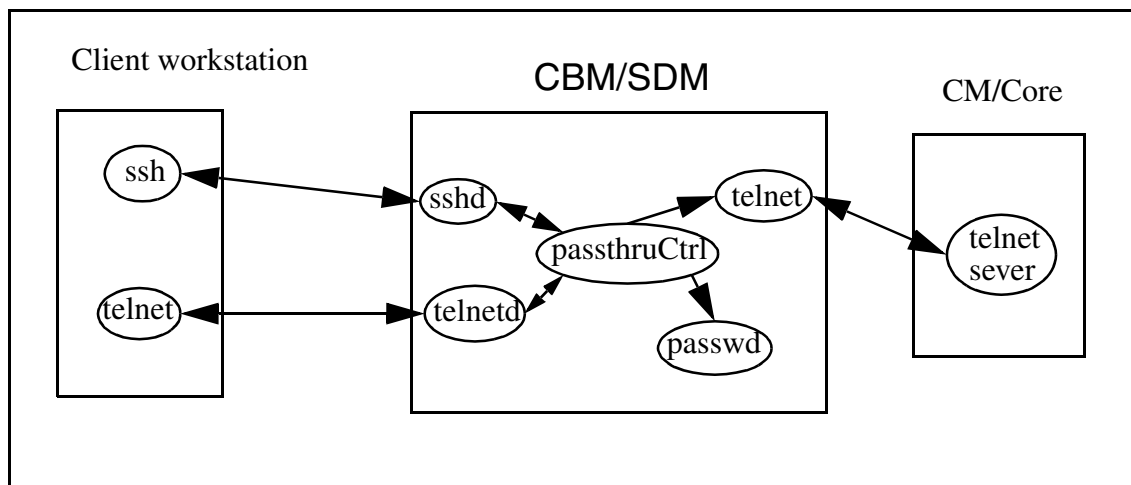
```
platgather -n <# of days' log> for the SDM
```

```
cbmgather -n <# of days' log> for the CBM
```

Where the number ranges from 1 to 7.

- Provide the capability for the passthru users themselves to change their own passwords for the SDM and the CBM. The functionality is requested from our customers and will eliminate the need of administrative users to change the passwords for the passthru users when they want.

The following figure shows how the passthru users work on the CBM/SDM.

Functional behavior diagram for passthru users using telnet/ssh

- List, add, change and modify the passthru users through the command line tool - passthru.

Hardware Requirements or Dependencies

SSPFS platform hardware and FX

Software Requirements or Dependencies

SSPFS platform software and SDM

Limitations and restrictions

Passthru users don't support the slicing on the CBM in the current release

Interactions

NA

Applicable customer facing sections

Fault Management

Logs

__N/A__

Alarms

__N/A__

Configuration

Data Schema

__N/A__

User Interface

__N/A__

Element Management

__N/A__

Security	__N/A__
Service Order	__N/A__
Office Parameters	__N/A__
Accounting (includes AMA billing)	__N/A__
Performance (includes operational measurements)	__N/A__

Glossary

Term	Description
CBM	Core and Billing Manager
CM	Computing Module
SDM	Supernode Data Manager

Product = CS2000

A00002979 -- Panther Electronic Software Delivery (Succession on DMS)

Functional Description

The PMUPGRADE DMS tool is part of the PANTHER initiative to automate the peripheral module (PM) software upgrade process for DMS switches. PM software upgrades are tedious and time consuming for Nortel customers, usually performed over several off-hour maintenance shifts. PANTHER's goals with respect to the PM software upgrade process are to:

- simplify
- reduce interval
- reduce cost
- improve quality

The purpose of this feature (Feature Number: A00002979) is to update and verify the unreleased CSP10 feature SD0910 so that it is able to be safely released and sustained in the current TDM and Succession environments. This is necessary to ensure the proper working of this feature with the new products and functionality that have been introduced since SD0910 was originally developed (e.g. SPM, XA-Core, etc.)

The purpose of the original CSP10 feature SD0910 is to supplement the PMUPGRADE tool for the electronic delivery of PM upgrade files to the DMS switch. Electronic software delivery (ESD) will contribute to interval and cost reduction of the PM upgrade process. This will allow Nortel customers to deploy new services and conform to changing regulatory requirements in a timely fashion and at a reasonable cost.

The PM upgrade process consists of three phases:

- administration of the new PM upgrade release files (PM load files, PM patch files, and the PM patch cross-reference file) by the PMUPGRADE tool
- production of a recommended PM upgrade plan by the PMUPGRADE tool
- execution of this upgrade plan by the SWUPGRADE PM tool

Feature SD0910 was designed to supplement the PMUPGRADE tool to support the electronic delivery of new PM upgrade files to the DMS switch during the file administration phase of the PM upgrade. The PMUPGRADE design component which deals with physical DMS volumes and files is extended to handle connections to remote FTP volumes. The traditional tape delivery of PM upgrade files remains fully supported by PMUPGRADE. Electronic software delivery helps reduce the need for site access to the DMS switch by customer personnel during the PM upgrade process. This promotes remote activation and supervision of the PM upgrade process.

Feature Limitations

Panther does not handle electronic software delivery of DMS-Core load files. Only PM loads and patches are handled by Panther. However, it is possible to manually transfer DMS-Core load files via FTP when initiating the file transfer from the DMS.

Secure File Transfer (SFT - NTP 297-5051-304 “SuperNode Data Manager Secure File Transfer User Guide” for more information) is currently not supported to transfer files between the DMS-Core and SDM when the file transfer is initiated from the DMS-Core. Therefore, in order for Panther ESD to access the SDM remote FTP volumes, the SDM will need to support normal or anonymous FTP protocol.

Hardware Requirements or Dependencies

None

Software Requirements or Dependencies

None

Limitations and restrictions

The electronic software delivery capabilities provided to PANTHER by features SD0910 and A00002979 is only supported on DMS switches which have TCP/IP connectivity via a SDM.

Interactions

None.

Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema _____

User Interface X

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

Glossary

Term	Description
CSP	Communications Services Platform
DMS	Digital Multiplexing System
ESD	Electronic Software Delivery
FTP	File Transfer Protocol
PANTHER	PM upgrade automation initiative
PM	Peripheral Module
PMUPGRADE	DMS tool for PM upgrade automation (file administration and upgrade planning phases)
SDM	SuperNode Data Manager
SPM	Spectrum Peripheral Module

Term	Description
SWUPGRADE PM	DMS tool for PM upgrade automation (upgrade execution phase).
TDM	Time Division Multiplexing
XA-Core	Extended Architecture Core

Configuration for A00002979

Hardware and Software Requirements

Initial Configuration

Office/Subnet parameters (OP/SP) (CM & SESM)

Upgrade Impact

Data schema (DS) (CM, MIBS, RDB)

Service Orders (SO) (CM & SESM)

Software optionality control (SOC)

Element Management

Command interface changes

Directory: PMUPGDIR

Directory description

The PMUPGRADE CI allows users to prepare and plan for the upgrade of peripherals in the office.

Accessing directory: PMUPGDIR

Access to directory or MAP level and return to CI

To access PMUPGDIR from the CI environment, enter >PMUPGRADE

To return to the CI environment, enter >quit

Command: SET

Command type: NON-MENU

Command target: All

Command availability: RES

Command description

The LOADDISTRIB and PATCHDISTRIB options of the SET command are extended to support electronic software delivery via FTP as described below.

A complete description of the SET command can be found in the “Commands” subsection of the “Overview of automated update process” section of the following NTP:

*North American DMS-100 Peripheral Module Software Release
Document, NTP 297-8981-599*

Command syntax

SET command parameters and variables

Command	Parameters and variables
SET	<Set options> <new values>
Parameters and variables	Description
<Set options>	LOADDISTRIB: The source of the load files to be copied. PATCHDISTRIB: The source of the patch files to be copied.
<new values>	ftp://<SDM_IP_address><directory_location>

Qualifications and warnings

None.

Responses

The LOADDISTRIB and PATCHDISTRIB options of the SET command will allow the crafts person to specify remote FTP volumes as PM load and patch distribution volumes.

The name of a **remote FTP volume** looks like:

```
ftp://<SDM_IP_address><directory_location>
```

where **<SDM_IP_address>** designates the IP address of the SDM containing the PM upgrade files to be copied, and **<directory_location>** designates where on the SDM the PM upgrade files are stored.

SET LOADDISTRIB and PATCHDISTRIB

MAP outputs with associated meanings and actions

Command
<pre>>SET LOADDISTRIB 'ftp://<SDM_IP_address_1><directory_location_1>' The current PMUPGRADE settings are: Load File Distribution: ftp://<SDM_IP_address_1><directory_location_1> Load File Destination: S00DPMLOADS Patch File Distribution: S00T ISN Patch Destination: SFDEV XPM Patch Destination: SFDEV Confirmation: ON IncludeLoads: ExcludeLoads: >SET PATCHDISTRIB 'ftp://<SDM_IP_address_2><directory_location_2>' The current PMUPGRADE settings are: Load File Distribution: ftp://<SDM_IP_address_1><directory_location_1> Load File Destination: S00DPMLOADS Patch File Distribution: ftp://<SDM_IP_address_2><directory_location_2> ISN Patch Destination: SFDEV XPM Patch Destination: SFDEV Confirmation: ON IncludeLoads: ExcludeLoads:</pre>
Meaning: The crafts person has requested PMUPGRADE to set the load distribution volume and patch distribution volume to be remote FTP volumes. System or user actions: PMUPGRADE sets the load distribution volume and patch distribution volume as requested, and displays the new settings. Note: Because of DMS command interpreter restrictions, the remote FTP volumes must be enclosed in single quotes as shown in the example above.

Example

Usage examples for SET command

Description of task	The crafts person request PMUPGRADE to set the load distribution volume and patch distribution volume to be remote FTP volumes.
Command: MAP response:	>SET LOADDISTRIB 'ftp://10.1.2.3/NA08/pm-loads' The current PMUPGRADE settings are: Load File Distribution: ftp://10.1.2.3/NA08/pm-loads Load File Destination: S00DPMLOADS Patch File Distribution: S00T ISN Patch Destination: SFDEV XPM Patch Destination: SFDEV Confirmation: ON IncludeLoads: ExcludeLoads: >SET PATCHDISTRIB 'ftp://10.1.2.3/NA08/pm-patches' The current PMUPGRADE settings are: Load File Distribution: ftp://10.1.2.3/NA08/pm-loads Load File Destination: S00DPMLOADS Patch File Distribution: ftp://10.1.2.3/NA08/pm-patches ISN Patch Destination: SFDEV XPM Patch Destination: SFDEV Confirmation: ON IncludeLoads: ExcludeLoads

Command: START

Command type: NON-MENU

Command target: All

Command availability: RES

Command description

The FILECOPY phase of the START command is extended to support electronic software delivery via FTP as described below.

A complete description of the START command can be found in the “Commands” subsection of the “Overview of automated update process” section of the following NTP:
North American DMS-100 Peripheral Module Software Release Document,
NTP 297-8981-599

Command syntax

START command parameters and variables

Command	Parameters and variables
START	<Start phases>
Parameters and variables	Description
<Start phases>	FILECOPY: Will copy load files and patches required to upgrade the peripherals on the switch.

Qualifications and warnings

None.

Responses

Remote FTP volume login

MAP outputs with associated meanings and actions

Command
<pre>>START FILECOPY Please enter the username and password for the remote FTP volume: ftp://<IP_address_1><directory_location_1> Username? <username_1> Password? <password_1> Please enter the username and password for the remote FTP volume: ftp://<IP_address_2><directory_location_2> Username? <username_2> Password? <password_2></pre>
Meaning: The crafts person has requested PMUPGRADE to begin the FILECOPY phase of the PM upgrade process. The FILECOPY phase of the START command will allow the crafts person to copy PM load and patch files from remote FTP volumes to the destination volumes on the DMS switch. System or user actions: Because the load distribution volume and patch distribution volume are remote FTP volumes, PMUPGRADE prompts the crafts person to supply usernames and passwords. The crafts person enters the usernames and passwords for the remote FTP volumes. Notes: Up to two retries will be provided by PMUPGRADE for the username and password prompts in case the original supplied values are not valid.

Example

Usage examples for START command

Description of task:	
Command: MAP response:	>START FILECOPY Please enter the username and password for the remote FTP volume: ftp://10.1.2.3/NA08/pm-loads Username? nortel-esd Password? <password> Please enter the username and password for the remote FTP volume: ftp://10.1.2.3/NA08/pm-patches Username? nortel-esd Password? <password>

Security

Configuration Walkthrough

Product = CS 2000

A00003073 -- SimRing Deny Redirection (SRDR) (Succession on DMS)

Functional Description (FN)

SimRing is a terminating end office feature. It resides in the Pilot DN's terminating end office and allows a user defined group of up to five DN's to be alerted simultaneously when a specific member (pilot DN) of this group is called. The SimRing group is comprised of a single Pilot DN (PDN) and up to 4 Non-Pilot Member DN's (NPMDN's or MDN's). The first alerted DN that answers the call is connected to the calling party, and the other alerted DN's are released.

This feature, SimRing Deny Redirection (SRDR), enhances SimRing by providing an optional method to allow a SimRing call to forward based only on the Pilot DN's call forwarding options. The NPMDN's are not allowed to forward the call. Without this option the NPMDN's behavior is unchanged, i.e.,

they are allowed to forward based on the call forwarding options on the NPMDN.

Hardware Requirements or Dependencies

No new hardware dependencies are introduced by this feature.

Software Requirements or Dependencies

Redirection Framework.

Limitations and restrictions

1. The NPMDN's terminating switch must not forward a call which has been marked as having been previously forwarded five (5) times.

This feature relies on the terminating switch of the NPMDN to adhere to the following standards by not forwarding a call which has already been forwarded five times.

— GR-586-CORE, *LSSGR: Call Forwarding Subfeatures (FSD 01-02-1450)*

3.1.1.2.A *Subfeature Construction and Assignment* CFDA: The sequential forwarding limit is five.

— TR-NWT-000972, *Call Forwarding Subfeatures: Switching System Requirements Using Signaling System No. 7 (SS7)*

3.1.1.4.D *Sequential Forwarding* Within the SS7 network or tandem SS7 networks the total number of all (intra and inter-switch) forwardings for each call should be limited. A count of the number of sequential forwardings is kept in the Redirection Counter field in the Redirection Information parameter.

3.1.3.1 *Sequential Forwarding Limit Reached* When the call ... has already been forwarded five times which is the sequential CF limit ... the call should not be forwarded...

2. SRDR is not compatible with a NPMDN terminating end office that uses any overflow or redirection that ignores the redirection/sequential-forwarding counter (for example RCF).
3. SRDR is not compatible with any SCP query/response which results in the modification of the redirection count.

For example, after the PDN-NPMDN call leg leaves the PDN's office, it is possible for an SSP (i.e., a tandem office in the network or the NPMDN's terminating office) to query an SCP and receive a message, `analyze_route` for example, with instructions for the SSP to reset the redirection count.

4. For inter-office PDN-NPMDN call legs, SRDR is supported when the connection between the Pilot DN's office and the NPMDN's office is ISUP all the way, PRI all the way, or ISUP/PRI interworking. It is not supported for any other network topology.
5. For inter-office PDN-NPMDN call legs, the existing office parm REDIRECTION_FRAMEWORK in table OFCVAR must be set to Y.
6. SRDR is not compatible with AIN, i.e. if AIN trigger is added to the NPMDN member calls to the pilot of the SimRing will be forwarded even though the SRDR is set to "N".
7. SRDR is not compatible with the following features when NPMDN and forwarded to DN are in the same office:
 - RCF (Remote Call Forwarding)
 - LOD (Line Overflow to Directory number)
 - LOR (Line Overflow to Route)
 - SCMP (Series Completion)
 - DNH (Directory Number Hunt)
 - KSH (Key Short Hunt)

Interactions

1. For the PDN-NPMDN leg, when member_dn_redir_allowed is set to NO, the call is made to look as if five redirections have taken place. Therefore, subsequent AIN queries on the PDN-NPMDN leg will include redirection parameters.
2. For calling number delivery, the EBS NPMDN will display the pilot DN and No Ans Fwd as the redirecting DN/reason when the pilot and NPMDN are in the same customer group but in separate offices connected over an ISUP IBN trunk.
3. If the Simring Redirection bool is set to 'NO' on a Simring group that has member DNs that route via ISUP/PRI trunk to a business set agent capable of displaying a REASON, then that set will display a REASON of Call Forward Don't Answer along with the calling party ID. With the Simring Redirection bool set to 'YES' the display of the terminating business set will not display a REASON of Call Forward Don't Answer.

Applicable customer facing sections

Fault Management

Logs _____n/a_____

Alarms _____n/a_____

Configuration

Data Schema	___x___
User Interface	___n/a___
Element Management	___n/a___
Security	___n/a___
Service Order	___x___
Office Parameters	___n/a___
Accounting (includes AMA billing)	___n/a___
Performance (includes operational measurements)	___n/a___
Realtime	___x___
Engineering Information	___x___

Glossary

Term	Description
DNH	Directory Number Hunt
EBS	Electronic Business Set
KSH	Key Short Hunt
LOD	Line Overflow to Directory number
LOR	Line Overflow to Route
MDN	Member Directory Number
NPMDN	Non Pilot Member Directory Number
PDN	Pilot Directory Number
RCF	Remote Call Forwarding
SCMP	Series Completion
SCP	Service Control Point
SimRing	Simultaneous Ringing
SRDR	SimRing Deny Redirection feature
SSP	Service Switching Point

Configuration for A00003073

Hardware and Software Requirements

SimRing Deny Redirection feature requires Redirection Framework.

No new hardware is required.

Initial Configuration

Set existing redirection_framework office parm to Y.

```
TABLE: OFCVAR
PARMNAME  PARMVAL
-----
REDIRECTION_FRAMEWORK Y
```

Office/Subnet parameters (OP/SP) (CM & SESM)

No office parameter is added or modified by this feature.

Upgrade Impact

Dump and Restore

Reformat Procs will be written to deal with table KSETFEAT and IBNFEAT changes during ONP. The new added field (REDIRECTION) will have the default value of “ALLOWED”. This will ensure that the existing SimRing feature in the switch will work the same as before.

Element Management Upgrade

N/A

Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
IBNFEAT	changed	unchanged
KSETFEAT	changed	unchanged

Table/MIB/Remote Database Schema information**Name: IBNFEAT****Functional description**

This feature adds a Redirection subfield to the SimRing line option datafilled in table IBNFEAT. When this option has a value of Not_allowed on a SimRing pilot DN then the resultant NPMDN legs are not allowed to call forward.

Usage sequence and implications (CM Only)

Current datafill order unchanged.

Size

Current table size is unchanged.

Fields/OIDs

The following table lists the new subfield for SimRing line option in IBNFEAT.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
Redirection	NEW	none	allowed /not_allowed	SimRing Deny Redirection Allowed assigned to this subfield of simring group option indicates that NPMDN terminators with active call forwarding are allowed to redirect calls. Not_Allowed assigned to this subfield of simring group option indicates that NPMDN terminators are not allowed to call forward.

Datafill example

The following example shows sample datafill for table IBNFEAT line option SimRing.

```

TABLE: IBNFEAT
>
>list
LEN DNNO DF FEATURE DATA
-----
HOST 01 0 00 00 0 SIMRING SIMRING 0 ACT FALSE $
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
FEATURE: SIMRING
>
GRPKEY: 0
>
STATE: ACT
>
REDIRECTION: ALLOWED
>not_allowed
PIN: $
>
TUPLE TO BE CHANGED:
HOST 01 0 00 00 0 SIMRING SIMRING 0 ACT NOT_ALLOWED $

```

Table release history update

A subfield, Redirection, added to the SimRing group option.

Supplementary information

None.

Translation verification other tools

Not applicable.

Name: KSETFEAT**Functional description**

This feature adds an Redirection subfield to the SimRing line option datafilled in table KSETFEAT. When this option has a value of Not_allowed on a SimRing pilot DN then the resultant NPMDN legs are not allowed to call forward.

Usage sequence and implications (CM Only)

Current datafill order unchanged.

Size

There is no change to the table size.

Fields/OIDs

The following table lists fields/OIDs for KSETFEAT.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
Redirection	NEW	none	allowed /not_allowed	SimRing Deny Redirection Allowed assigned to this subfield of simring group option indicates that NPMDN terminators with active call forwarding are allowed to redirect calls. Not_Allowed assigned to this subfield of simring group option indicates that NPMDN terminators are not allowed to call forward.

Datafill example

The following example shows sample datafill for table KSETFEAT line option SimRing.

```

TABLE: KSETFEAT
>list
FEATKEY FEATURE KVAR
-----
ISDN 1 1 SIMRING SIMRING 1 ACT ALLOWED $
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
FEATURE: SIMRING
>
GRPKEY: 1
>
STATE: ACT
>
REDIRECTION: ALLOWED
>not_allowed
PIN: $
>
TUPLE TO BE CHANGED:
ISDN 1 1 SIMRING SIMRING 1 ACT NOT_ALLOWED $

```

Table release history update

A subfield, SRDR, added to the SimRing group option.

Supplementary information

None.

Translation verification other tools

Not applicable.

Service Orders (SO) (CM & SESM)**Service order change details****LCC and options****New commands**

This activity adds a new option “REDIRECTION” to the existing SimRing group commands. The commands that can be used to datafill SimRing are the standard ADO, DEO, CHF, EST, ADD, and DEL commands. The following table describes what the new prompt is for each of the ServOrd commands.

Command	Prompting
ADO	• Redirection • PIN
DEO	• No new prompt
CHF	• state • Redirection • PIN
EST	• NPMDNs • State • Redirection • PIN
ADD	• No new prompt
DEL	• No new prompt

How service order commands are presented

No new commands added

ExampleCommand prompts

The system prompts for EST and CHF commands are shown in order of their appearance.

How service order options are presented

Description

For SimRing, EST and CHF commands are changed in order to have the new “REDIRECTION” option. Other than that crafts person will not see any other changes.

Example

Example of the EST command in prompt mode

```
>est
SONUMBER:  NOW  3 7 16 AM
>
GROUPTYPE:
>simring
SIMRING_PILOT_LEN_OR_DN:
>6213510
SIMRING_MEMBER_DN:
>6213511
SIMRING_MEMBER_DN:
>$
SIMR_STATE: INACT
>act
REDIRECTION:
>allowed
SIMR_PIN:
>123
COMMAND AS ENTERED:
EST NOW 3 7 16 AM SIMRING 6213510 ( 6213511 ) $ ACT ALLOWED 123
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
```

Example of the EST command in no-prompt mode

```
est $ simring 6213510 6213511 $ act allowed 123 y y
```

Example of the CHF command in prompt mode

```
>chf
SONUMBER:  NOW  3 7 16 AM
>
DN_OR_LEN:
>6213510
OPTION:
>simring
SIMR_STATE: INACT
>act
REDIRECTION:
>allowed
SIMR_PIN:
>123
OPTION:
>$
COMMAND AS ENTERED:
CHF NOW 3 7 16 AM 6213510 ( SIMRING ACT ALLOWED 123 ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
COMMAND AS ENTERED:
EST NOW 3 7 16 AM SIMRING 6213510 ( 6213511 ) $ ACT ALLOWED 123
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
MACHINES ARE OUT OF SYNC, SERVICE ORDERS NOT ALLOWED
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
SHOULD ORDER BE DONE ANYWAY? (Y OR N)
>y
```

Example of the CHF command in prompt mode

```
chf $ 6213510 simring allowed 123 $ yy
```

Option prompts

System prompts for Redirection field of SimRing option

Prompt	Valid input	Description	Areas affected by prompt
REDIRECTION	ALLOWED	NPMDN with active call forwarding are allowed to redirect calls.	This change only affects NPMDNs with active call forwarding (CFA, CFD, CFB)
	NOT_ALLOWED	NPMDN with active call forwarding are not allowed to forward calls.	

Line class code compatibility

No change to SimRing option / LCC compatibility.

Redirection compatibility to LCC

Line class code	Compatible?
N/A	
1FR-1MR	Yes/No

Assignability

Redirection option is SimRing group option.

Option prerequisites

Redirection option is part of the SimRing group option and can not be added to any lines.

Notes

n/a

Feature identification

n/a

SERVORD+ Exceptions

n/a

Software optionality control (SOC)

No new SOC is introduced by this feature.

Element Management

Not applicable.

Command interface changes**Command: QSIMR**

This feature modifies the display of QSIMR. It adds an indication that Redirection is allowed/not allowed on the SimRing group.

Security

This feature does not impact security.

Configuration Walkthrough

See “Service Orders (SO) (CM & SESM)” on page 639 for configuration details.

Product = CS 2000**A00003273 -- NGSS Application Maintenance (PT-IP)**

The FN for this feature document is located in activity A00003933. The A00003933 document contains the FN for the Session Server project.

A00003277 -- SP2000 Logs, Alarms, OMs, Subsystem (PT-IP)

Documentation for this activity can be found in activity A00003393.

A00003279 -- Load Balancing (PT-IP)

Documentation for this activity can be found in A00003933.

Product = CS 2000**A00003371 -- SESM Common Inventory Data Consolidation (PT-IP, UA-IP, IAW, IAC)*****Functional Description***

This feature introduces a Common Inventory data schema and eliminates redundant data. It provides for creation of new components and modification of a number of existing components summarized as follows:

- a new centralized inventory database schema in Oracle representing network element data and its relationships (logical and physical associations) with other entities in the system.
- a new JDBC-based API that allows applications to add, modify, remove, and retrieve inventory information from the schema.
- a new event notification and registration component for applications to register for data addition/deletion/modification events.
- an new inventory schema upgrade infrastructure for supporting upgrades from one release of the inventory schema to another.
- Modification of all relevant applications in the SESM package to use the new common inventory, including the elimination of the NETWORK and PROXY schema data. Affected applications are: GWC Manager, UAS Manager, Alarm Manager, Proxy Agent, Data Engine, NetworkView, Service Broker, Line Provisioning, Trunk Provisioning, LMM, Cs2kCfgMgr, V52CfgMgr ProfileManager and TMM.

Part of the effort in providing this feature includes generation of IEM compliant customer logs. This is the only customer visible aspect of this feature and is captured in an accompanying Fault management document.

Hardware Requirements or Dependencies

NA

Software Requirements or Dependencies

NA

Limitations and restrictions

NA

Interactions

NA

Applicable customer facing sections

Fault Management

Logs

___X___

Alarms

___N/A___

Configuration

Data Schema

___N/A_

User Interface	___N/A___
Element Management	___N/A___
Security	___N/A___
Service Order	___N/A___
Office Parameters	___N/A___
Accounting (includes AMA billing)	___N/A___
Performance (includes operational measurements)	___N/A___

Fault Management for A00003371

Fault management strategy

The Common Inventory and Data Consolidation A00003371 feature is focused on the CMT network element data and database access. As such, new customer logs will be generated to notify the system operators of noteworthy database access events as per the Nortel standard document:

Log reporting Rules and guidelines

DIS Ref: IEMPG DIS No: AF01 Release: Standard

All Logs created apply the principles and comply with the formats specified in the standard. Also nomenclature or identifiers already in use will be used where possible.

Note that none of the logs created initiate operator actions. The event being logged are failures to obtain a database connection. These can occur when a resource limit has been exceeded, when a database password is changed or when the database server has stopped or restarted.

The following identifies the general format of the CS2M database access Logs created by this activity.

The general format for all logs is given in the next subsection. Specific Logs are defined further on in this document.

Log Header Formats

The SCC2 log header is organized as follows:

<severity> <minute> <LogName/Num> <sequence number> <logtype>
<device type> <Event Label>

For Nortel Standard format, the header is organized as follows:

<CM CLI> <severity> <logname/num> <mmdd hh:mm:ss> <sequence number> <logtype> <device id> <Event Label>

Where:

Severity is NOA

Minute or mmdd hh:mm:ss is minutes of the day or month, day, hour, minute

LogName/Num is CMTxxx where xxx is in the range 600 - 799

Sequence Number is number internally generated

LogType is INFO

Device Type is SESM

Event Label describes the event that occurred

Log Body Format

The body of logs will be the same for both Nortel and SSC2 formats:

Location: SSPFS=hostname

Information: <Detected problem>

Time: <MMM dd hh:mm:ss YYYY>

Component Id: Database

Specific Problem: <Specific problem>

Description: <short text description>

Fault management tools and utilities

Not applicable

Logs

Database Stopped Log

Log Title:DB600

Formats

NTSTD log format:

RTP2 DB600 SEP23 17:25:00 0401 INFO DB Connection Error

Location: SSPFS=wnc0s0jd

Information: I/O error, the database did not respond

Time: SEP23 17:25:00 2003

Component Id: Database, GWCEM User

Specific Problem: I/O error was detected when attempting to get a database connection.

Description: Transient error detected. The database maybe stopped for administrative actions. Investigate when this log occurs repeatedly.

Log Field descriptions

Field	Value
Category	Information
Severity	NOA
LogName	DB
LogNumber	600
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	INFO
Device ID	DB
EventLabel	Connection Error
Location	SSPFS=hostname
Information	I/O error, the database did not respond
Day Time Year	MMMdd hh:mm:ss YYYY
Component Id	Database, user id
SpecificProblem	I/O error was detected when attempting to get database connection.
Description	Transient error detected. The database maybe stopped for administrative actions. Investigate when this log occurs repeatedly.

Explanation

This Log is generated when an attempt to allocate a database connection encounters an I/O error. These errors can occur when the database has been stopped momentarily for administrative purposes. A few occurrences of this log is informational. Continuous occurrences within a 15 minutes or a half hour should be investigated to insure these errors are attributable to specific authorized administrative actions.

Action

Monitor for multiple occurrences within a 15 minutes or a half hour for the same "Component Id".(Note: It is expected that a Log will be generated for multiple different "Component Ids".) If this is detected investigate to insure

these errors are attributable to specific authorized administrative actions. If these are occurring and are not caused by administrative activity then verify the database on the SSPFS machine identified is functioning normally.

Database Connection Closed Log

Log Title:DB601

Formats

NTSTD log format:

RTP2 DB601 SEP23 17:25:00 0401 INFO DB Connection Error

Location: SSPFS=wnc0s0jd

Information: Database connection closed, stale connections will refresh.

Time: SEP23 17:25:00 2003

Component Id: Database, GWCEM User

Specific Problem: A closed or stale database connection was detected, all stale connections will be refreshed.

Description: Transient error detected. Investigate when a threshold is exceeded in a short time.

Log Field descriptions

Field	Value
Category	Information
Severity	NOA
LogName	DB
LogNumber	601
Day Time	mmdd hh:mm:ss
Sequence Number	sequential log number
EventType	INFO
Device ID	DB
EventLabel	Connection Error
Location	SSPFS=hostname
Information	Database started, stale connections were refreshed
Day Time Year	MMdd hh:mm:ss YYYY
Component Id	Database, user id
SpecificProblem	A closed or stale database connection was detected, all stale connections were refreshed.

Log Field descriptions

Field	Value
Description	Transient error detected. Investigate when a threshold is exceeded in a short time

Explanation

This Log is generated when an attempt to allocate a database connection encounters detects that the connection is already closed. These errors can occur when the database has been stopped momentarily and then again started. A single occurrence of this log is informational. Multiple occurrences within a 15 minutes or a half hour for the same "Component Id" should be investigated to insure these errors are attributable to specific authorized administrative actions.

Action

Monitor for multiple occurrences within a 15 minutes or a half hour for the same "Component Id".(Note: It is expected that a Log will be generated for multiple different "Component Ids".) If this is detected investigate to insure these errors are attributable to specific authorized administrative actions. If these are occurring and are not caused by administrative activity then verify the SSPFS machine identified is functioning normally.

Database Password Changed Log

Log Title:DB602

Formats**NTSTD log format:**

RTP2 DB602 SEP23 18:25:00 0402 INFO DB Connection Error

Location: SSPFS=wnc0s0jd

Information: User password has changed

Time: SEP23 17:25:00 2003

Component Id: Database, GWCEM User

Specific Problem: Invalid password was detected on a database connection, the new password is now in use for this database user.

Description: Transient error detected. When a threshold is exceeded in a short time, investigate to insure security violations or unauthorized access are not the cause.

Log Field descriptions

Field	Value
Category	Information
Severity	NOA

Log Field descriptions

Field	Value
LogName	DB
LogNumber	602
Day Time	mmdd hh:mm:ss
Sequence Number	sequential log number
EventType	INFO
Device ID	DB
EventLabel	Connection Error
Location	SSPFS=hostname
Information	I/O error, stale connections were refreshed
Day Time Year	MMdd hh:mm:ss YYYY
Component Id	Database, user id
SpecificProblem	Invalid password was detected on a database connection, the new password is now in use for this database user.
Description	Transient error detected. When a threshold is exceeded in a short time, investigate to insure security violations or unauthorized access are not the cause.

Explanation

This Log is generated when an attempt to allocate a database connection encounters an invalid password error. These errors can occur when the database log in password for a database user is changed. A single occurrence of this log is informational. Multiple occurrences within a 15 minutes or a half hour should be investigated.

Action

Monitor for multiple occurrences within a 15 minutes or a half hour. If this is detected investigate to insure these errors are attributable to authorized security actions to change the database password and not due to security violations or unauthorized system access.

Database Maximum Sessions Log

Log Title:DB603

Formats

NTSTD log format:

RTP2 DB603 SEP23 18:45:00 0403 INFO DB Connection Error

Location: SSPFS=wnc0s0jd

Information: Maximum database sessions limit reached

Time: SEP23 17:25:00 2003

Component Id: Database, GWCEM User

Specific Problem: Maximum database sessions active was detected on an attempt to create a database connection.

Description: Transient error detected. When a threshold is exceeded in a short time, reconfiguration of the database's limits maybe required.

Log Field descriptions

Field	Value
Category	Information
Severity	NOA
LogName	DB
LogNumber	603
Day Time	mmdd hh:mm:ss
Sequence Number	sequential log number
EventType	INFO
Device ID	DB
EventLabel	Connection Error
Location	SSPFS=hostname
Information	Maximum database sessions limit reached
Day Time Year	MMdd hh:mm:ss YYYY
Component Id	Database, user id
SpecificProblem	Maximum database sessions active was detected on an attempt to create a database connection.
Description	Transient error detected. When a threshold is exceeded in a short time, reconfiguration of the database's limits maybe required.

Explanation

This Log is generated when an attempt to allocate a database connection encounters maximum database sessions exceeded error. These errors can occur when an unusual event has occurred that caused sustained high levels of system activity. A single occurrence of this log is informational indicating that database resources may need reconfiguration. Multiple occurrences within a 15 minutes or a half hour should be investigated.

Action

Monitor for multiple occurrences within a half hour or an hour. If this is detected notify the database or system administrator. A possible solution is increase the value of the SESSIONS initialization parameter.

Database Maximum Processes Log

Log Title:DB604

Formats**NTSTD log format:**

RTP2 DB604 SEP23 18:45:00 0403 INFO DB Connection Error

Location: SSPFS=wnc0s0jd

Information: Maximum database processes limit reached

Time: SEP23 17:25:00 2003

Component Id: Database, GWCEM User

Specific Problem: Maximum database processes was detected on an attempt to create a database connection.

Description: Transient error detected. When a threshold is exceeded in a short time, reconfiguration of the database's processes limit maybe required.

Log Field descriptions

Field	Value
Category	Information
Severity	NOA
LogName	DB
LogNumber	604
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	INFO
Device ID	DB
EventLabel	Connection Error
Location	SSPFS=hostname
Information	Maximum database processes limit reached
Day Time Year	MMMdd hh:mm:ss YYYY
Component Id	Database, user id
SpecificProblem	Maximum database processes limit reached

Log Field descriptions

Field	Value
Description	Transient error detected. When a threshold is exceeded in a short time, reconfiguration of the database's processes limit maybe required.

Explanation

This Log is generated when an attempt to allocate a database connection encounters maximum database processes exceeded error. These errors can occur when an unusual event has occurred that caused sustained high levels of system activity. A single occurrence of this log is informational indicating that database resources may need reconfiguration. Multiple occurrences within a 15 minutes or a half hour should be investigated.

Action

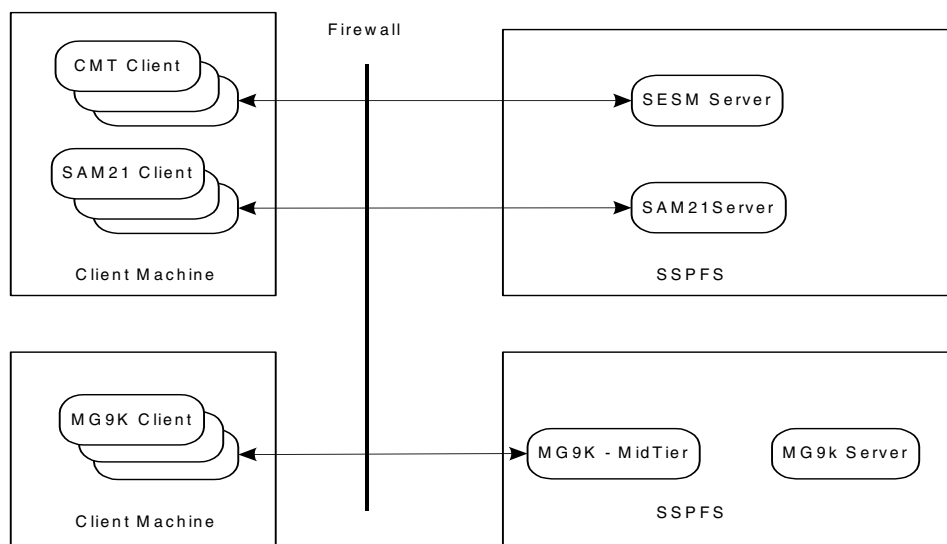
Monitor for multiple occurrences within a half hour or an hour. If this is detected notify the database or system administrator. A possible solution is increase the value of the PROCESSES initialization parameter.

Related documentation

Log Reporting Rules and Guidelines DIS Ref: IEMPG DIS No: AF01 Release: Standard

Product = CS 2000**A00003454 -- Secure and Firewall Compatible CS2M and UE9KEM Client GUI Communication (PT-IP, UA-IP, IAW, IAC)*****Functional Description***

The primary purpose for this feature is to facilitate firewall protection for traffic for the Succession OAM&P GUI Client/Server communication, the Succession GUI's will work even with the addition of a firewall in the customer network. Along with sending the data through a firewall, the data will also be encrypted.

Purpose of A00003454

This was done with the addition of a SOCKS proxy on the client and server machines. The Succession GUI's will send all messages to a SOCKS proxy listening on a specific port on the client machine. The client SOCKS proxy will send all the messages to a SOCKS proxy listening on a specific port on the server machine.

There are two things that have customer impact.

1. Configuring the client and server ports.
2. Starting, stopping, and getting the status of the SOCKS proxy on the server machine.

The applications that are covered with this activity include the CMT, SAM21 EM, and MG9K EM GUI's.

Configuration

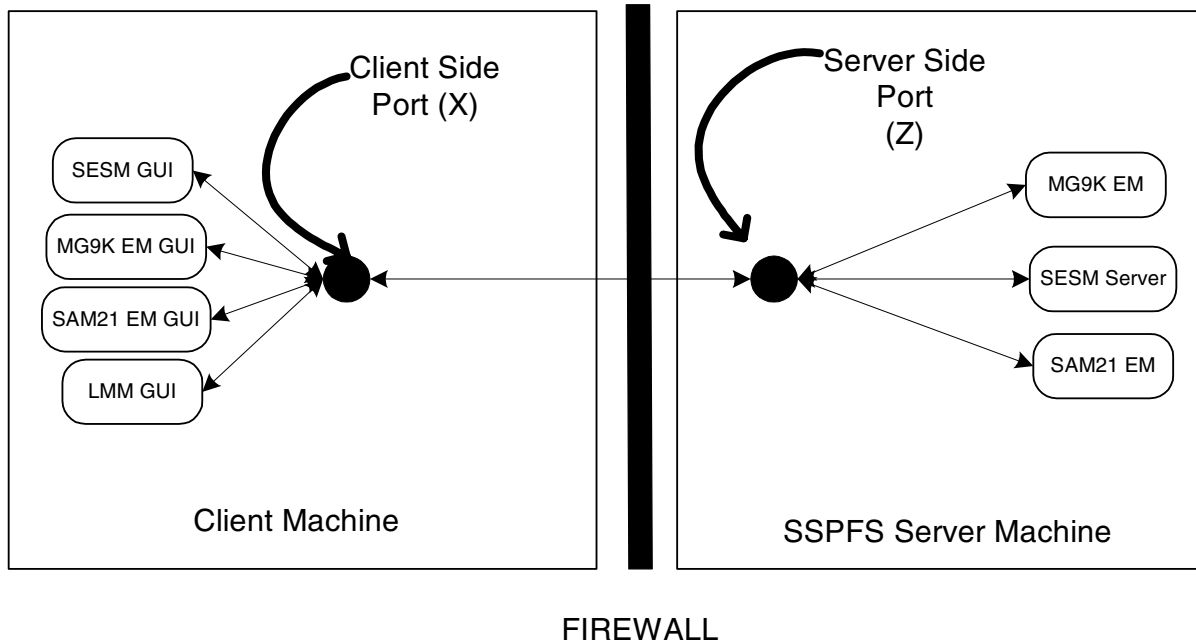
There is one changed command the customer will use to configure this feature, the *cli* command. The function that will be added is to configure the port and to list the currently used ports.

- A port on the SSPFS server machine used to receive all requests from clients.
- A port on the client machine that concentrates all requests from the client to the server.
- A port on the client machine to receive all the requests from the Succession GUI applications.

The following figure depicts the ports configured. Each of the ports has a default value. If the default value is acceptable, it is not necessary to configure

the ports with the `cli` command. If the default value is not the value required, the `cli` command is used to change these ports.

Ports configured



The port configuration takes place on each SSPFS server the SOCKS software is used on. The SSPFS machines that would require configuration are those that contain the GUI's covered by this feature.

As shown, the Server Side Port, referenced as Z will be configured using the `cli` command. This is the port that requests from all client machines will be concentrated to. If a firewall is in place, the Server Side port Z must be opened to allow these messages through. The default value for this port is 10080. It is recommended that port 10080 is used, but if it is necessary to change, the software on the server machine will ensure there are no port collisions on the SSPFS machine by verifying that the port is not in file `/etc/services`. All SSPFS server machines must configure this to the same value.

The Client Side port, referenced as X will also be configured using the `cli` command. Upon startup of the client machines, the Succession GUI will connect to that port. This port is an internal port used only on the client machine. There is no firewall configuration necessary. All SSPFS machines must be configured to the same value. The default value for this port is 10080 and may be configured to a different value.

Consistent configuration of ports

The ports configured through the offices must be configured consistently across all offices in the network. If the ports are not configured consistently, the GUI's will not function correctly. See the troubleshooting section for information on incorrect behavior.

Port conflicts on server side

The ports on the server side will be added to the file `/etc/services`. If the port is already bound into `/etc/services`, the configuration will not be allowed. The list of ports in `/etc/services` is not exhaustive, and the customer should know the site-specific configuration of the SSPFS ports.

Note that in the MG9K case, the database host machine (as defined in the `DB_HOST` variable) must be upgraded to SN07 before the MG9K Midtier.

Start and Stop of server component

There is a new command added to start, stop, and restart the server side component that is listening on the Server Side port.

If the `cli` command is used to change the Server Side Port, the change takes effect immediately, as the the SOCKS server on the SSPFS machine is restarted.

Impacts to restarting SOCKS server

If the server side component is reconfigured or restarted, the clients GUI's covered by this feature will need to be restarted. Also, the following servers on the SSPFS where the SOCKS proxy is restarted will need to be restarted as well.

- MG9K Mid-Tier
- SAM21 EM
- Notification Service
- SESMSservice
- NPM
- PSE

Starting and stopping the SOCKS process using *servman*

The command `servman` will be use to start, stop, and query the status of the SOCKS server.

If the SOCKS server is stopped and then started, the Succession servers running on the same SSPFS machine will need to be restarted. The GUI clients that are active and communicating with the server will also need to be restarted.

Starting the SOCKS server

```
servstart SOCKS
```

```
SOCKS server successfully started
```

If servstart SOCKS does not work the following error will be displayed.

The SOCKS server could not be started due to the port <port number> is already in use. Verify the port is not configured for another use.

Stopping the SOCKS server

```
servstop SOCKS
```

```
SOCKS server successfully stopped
```

Querying the SOCKS server

```
servquery -status -group SOCKS -v
```

```
SOCKS server RUNNING
```

If the SOCKS server is not running the result will be:

```
SOCKS server STOPPED
```

Hardware Requirements or Dependencies

There are no new hardware requirements added with the introduction of this feature.

Software Requirements or Dependencies

There are no new software requirements or dependencies added by this feature.

Limitations and restrictions

The Client Side ports as shown in Figure on page 656 must be free for the Succession GUI's shown to operate.

The Server Side port as shown in Figure on page 656 must be opened on a firewall that supports stateful packet inspection.

Reconfiguration of Server Side port requires server side Socks Proxy restart, EM restart, and client application restart.

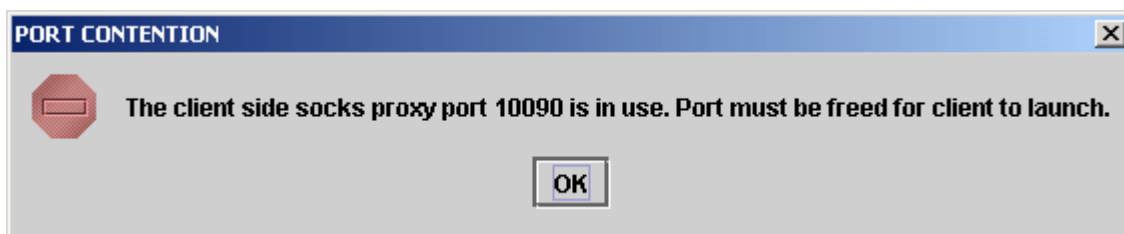
Troubleshooting

At times, there may be configuration errors which cause port contention on the client machine or servers configured with different ports. In both these cases a failure by the client to launch or connect will be encountered.

Client Port Binding Error

If the port on the client machine is already bound to another process then the client GUI will fail to start. If the port is already bound to another process, and the client will not start successfully, the following dialog to show there is a problem with a port contention:

Dialog specifying port contention upon startup on the client machine



The solution to this is to free the port in the client machine. Depending upon what type of client machine used, the solution will differ. Closing the application will free the port.

Server Configuration Errors

If there are server side configuration differences between offices there will be a failure of the GUI to connect to the server machine. If office A is configured for the server to listen on port 10080, and office B is configured for the server to listen on port 10090. If there are only GUI's launched to communicate with either office A or office B, there will be no problems. If GUI's are launched to communicate with both office A and B, then there will be a failure to communicate with one of the offices. The GUI that is launched to communicate with one office, say office A will work. If there are other GUI's launched to communicate with office A, those will also work. If there is a GUI launched to communicate with office B, those communications will fail.

The recourse to solving this problem is to verify if there is in fact a configuration error. If there is a configuration error, there are two ways to get the GUI's to launch correctly.

Re-Launch GUI's

If the GUI to server B, as described in the previous section needs to be launched, and the desire is to not reconfigure the server, the GUI's launched that are communicating with office A need to be closed.

After all the GUI's have been closed, re-launch the GUI to office B.

Re-Configure server

Reconfiguring the server is the best solution to this problem. Configure all the server side ports to the same value on all offices. Please see the CN section to determine how to reconfigure the server side ports.

Server side SOCKS Proxy not running

If the Socks Proxy is not running on the server side, the following dialog will be displayed.

Dialog specifying server side socks proxy is not running



Interactions

Launch sequence

When launching a Succession GUI, the succession GUI outline will launch and a new dialog will be shown. This dialog is shown so the user knows that the Client Side Socks Proxy is being launched.

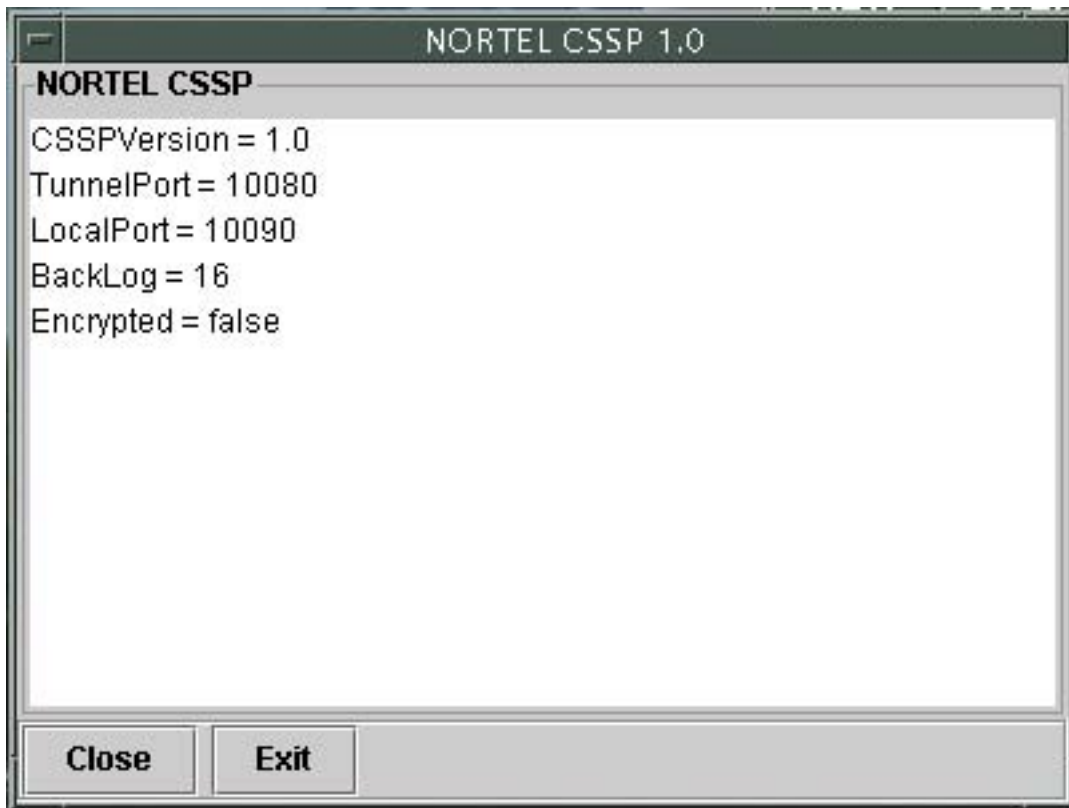
Dialog shown when Client Socks Proxy is being launched



When launching an application after starting this feature, the user will be prompted to allow a new Java Web Start application unrestricted access to the client machine, prior to launching a Succession GUI as follows:

Added Security Warning dialog when starting Succession GUI's

The client side SOCKS proxy has a small GUI that automatically opens up at the start of the first client application on the client machine. The GUI will automatically minimise itself, but may be opened to see parameters of the connection. The client side SOCKS proxy may be terminated also from this GUI by hitting the 'Exit' button. Note that hitting the 'Close' button only re-minimises the GUI; it does not terminate the client side SOCKS proxy. Note that the parameters cannot be changed; they are shown for reference only. The following figure shows an example of the GUI.

Nortel Client Side SOCKS Proxy GUI***Configuration for A00003454*****Hardware and Software Requirements**

There are no special hardware or software requirements.

Configuration

The initial configuration of this package is completed as part of the installation.

Following is an example of getting to the SOCKS configuration using *cli*. All following examples will presume the SOCKS configuration was successfully navigated to.

Starting the SOCKS configuration

```
>/opt/nortel/NTsocks/cli
```

```
Command Line Interface
```

```
1 - View
```

2 - Configuration

3 - Other

X - exit

select - 2

Configuration

1 - NTP Configuration

2 - Apache Proxy Configuration

3 - DCE Configuration

4 - OAMP Application Configuration

5 - CORBA Configuration

6 - IP Configuration

7 - DNS Configuration

8 - Syslog Configuration

9 - Database Configuration

10 - NFS Configuration

11 - Bootp Configuration

12 - Restricted Shell Configuration

13 - Succession Element Configuration

14 - chg_tz (Change Timezone)

15 - login_session_timeout (Login Session Timeout Configuration)

16 - snmp_poller (SNMP Poller Configuration)

X - exit

select - 13

Succession Element Configuration

- 1 - SAM21EM Application Configuration
- 2 - NPM Application Configuration
- 3 - PSE Application Configuration
- 4 - OMPUSH Application Configuration
- 5 - SOCKS Configuration

X - exit

select - 5

SOCKS Configuration

- 1 - SOCKS configuration tool

select - 1

The changes of the server side port is a disruptive action. If the server side port is changed, the SOCKS server and all dependant applications must be restarted.

SOCKS ports in all offices must be configured the same. Misconfiguration will cause EMS clients to not function.

Proceed with caution.

Successful configuration of the SOCKS ports using default values.

Enter the port the Server side SOCKS Proxy will listen on. Value must be

within [1025 - 65535]. default value 10080.

Current value 10080[?,q]

Is port 10080 acceptable? [y] [y,n,?,q] y

Enter the port the Client side SOCKS Proxy will listen to client requests. Value must be within [1025 - 65535]. default value 10080.
Current value 10080.[?,q]

Is port 10080 acceptable? [y] [y,n,?,q] y
Ports Successfully configured

Entering a non-default value for both the server and client ports.

Enter the port the Server side SOCKS Proxy will listen on. Value must be within [1025 - 65535]. default value 10080.
Current value 10080 [?,q] 2334

Is port 2334 acceptable? [y] [y,n,?,q] y

Configuring the SOCKS server side port requires a restart of the SOCKS server and all dependent applications, are you sure you want to change the configuration? [y] [y,n,?,q] y

The SOCKS server and dependent applications must be restarted to take effect.

Enter the port the Client side SOCKS Proxy will listen to client requests. Value must be within [1025 - 65535]. default value 10080 [?,q] 3445

Is port 3445 acceptable? [y] [y,n,?,q] y

Clients already running Succession GUI's must be restarted to use this new port, are you sure you want to change the configuration? [y] [y,n,?,q] y

Ports Successfully Configured

Entering invalid port ranges for both server and client ports

Enter the port the Server side SOCKS Proxy will listen on. Value must be within [1025 - 65535]. default value 10080 [?,q] 111

Invalid entry:Value must be within [1025 - 65535]

Enter the port the Server side SOCKS Proxy will listen on. Value must be within [1025 - 65535]. default value 10080 [?,q] 65555

Invalid entry:Value must be within [1025 - 65535]

Enter the port the Server side SOCKS Proxy will listen on. Value must be within [1025 - 65535]. default value 10080 [?,q] 45544

Is port 45544 acceptable? [y] [y,n,?,q] y

Configuring the SOCKS server side port requires a restart of the SOCKS server and all dependent

applications, are you sure you want to change the configuration? [y] [y,n,?,q] y

The SOCKS server and dependent applications must be restarted to take effect.

Enter the port the Client side SOCKS Proxy will listen to client requests. Value must be within [1025 - 65535]. default value 10080 [?,q] 111

Invalid entry:Value must be within [1025 - 65535]

Enter the port the Client side SOCKS Proxy will listen to client requests. Value must be within [1025 - 65535]. default value 10080 [?,q] 55555

Invalid entry:Value must be within [1025 - 65535]

Enter the port the Client side SOCKS Proxy will listen to client requests. Value must be within [1025 - 65535]. default value 10080 [?,q] 4536

Is port 4536 acceptable? [y] [y,n,?,q] y

Clients already running Succession GUI's must be restarted to use this new port, are you sure you want to change the configuration? [y] [y,n,?,q] y

Ports Successfully Configured

Product = CS2000

A00003459 -- GWC Lifecycle: SSC & Application Datasync Support (UA-IP)

Functional Description

This activity covers a part of the SSC re-architecture work. It has four main design components:

- Add new alarm for succession SYSB line.
- Generate a new log when the above alarm is raised/cleared.
- Add a new pm sublevel for LGRP and
- Raise alarm when there are LGRPs in SYSB state.

New alarm for SYSB lines

This alarm will only be supplied to Succession office. The class of the alarm (MINOR, MAJOR, or CRITICAL) will be displayed in the system status display area under the header Lns of the mapci display (i.e. under Lns header of mapci;mtc). Here is the map window:

```

XAC      MS      IOD      Net      PM      CCS      Lns      Trks      Ext      APPL
.         .         .         .         .         .      LGRP      .         .         .
                        *C*

MTC
0 Quit
2
3 MTCNA
4 SRSTATUS
5 BERP
6 CAPACITY
7
8
9 XAC
10 MS
11 IOD
12 Net
13 PM
14 CCS
15 Lns
16 Trks
17 Ext
18 APPL
YD
Time 10:56 >

```

Currently, the alarm for Lns has four types: CUT, DF, HAZ, PSPD. Accordingly, the alarm is displayed using the following characters for the combination of alarms of the same severity:

- { 1}: 'CUT '
- { 2}: One of the following diagnostic failure alarms: 'Diag', 'Fac ', 'SDiag', ...

{ 3}: 'CT DF'
 { 4}: 'HZD '
 { 5}: 'HZ CT'
 { 6}: 'HZ DF'
 { 7}: 'H C D'
 { 8}: 'PSPD '
 { 9}: 'CT PS'
 {10}: 'PS DF'
 {11}: 'C P D'
 {12}: 'HZ PS'
 {13}: 'H C P'
 {14}: 'H P D'
 {15}: 'HCPD '

With the new addition of SYSB alarm, the following character display will be used to indicate the multiple alarms occurring at a given time:

New alarm display

	CUT	DF	HAZ	PSPD	SYSB
'SYSB '					X
'CT SB'	X				X
'DF SB'		X			X
'CD SB'	X	X			X
'HZ SB'			X		X
'CH SB'	X		X		X
'DH SB'		X	X		X
'CDHSB'	X	X	X		X
'PS SB'				X	X
'CP SB'	X			X	X
'DP SB'		X		X	X
'CDPSB'	X	X		X	X
'HP SB'			X	X	X
'CHPSB'	X		X	X	X
'DHPSB'		X	X	X	X
'CDHPS'	X	X	X	X	X

The alarm will only be applied to succession lines (excluding ABI) in the entire office. The severity of the alarm is based on the alarm thresholds, which are set independently. A new office parameter **SYSBALARM** will be created in table OFCVAR. The new office parameter will have a default value { 10, 20, 30 } which will be set at IPL time and will survive all restarts.

AlmStat at the LTP level will be changed to display and modify the threshold of SYSBALARM. The new display of this command without parameter will look like the following:

OFFICE TOTALS

OFFICE LINE FAILURE TOTALS

	OFFICE CURRENT	OFFICE MINOR	OFFICE MAJOR	OFFICE CRITICAL
Ext Diag Fail (D)	1	10	20	30
Facility Fault (F)	0	10	20	30
Short Diag Fail (S)	0	10	20	30
Needs Ext Diag (N)	0	10	20	30
Set Missing (MSET)	0	10	20	30
Card Missing (MCARD)	7	100	150	200
Shower Queue (QUEUE)	0	100	150	200
Major ICMOLINE(IMAJ)	0	100	150	200
Minor ICMOLINE(IMIN)	0	100	150	200
Loop Sig Set (LSET)	0	100	150	200
Loop Sig Card(LCARD)	0	100	150	200
TCM sync loss (T)	0	100	150	200
Loop Performance (P)	0	100	150	200
Major CPERROR (CMAJ)	0	5	10	15
Minor CPERROR (CMIN)	0	5	10	15
Major RapidMSG(OMAJ)	0	10	20	30
Minor RapidMSG(OMIN)	0	10	20	30
Utility Card (U)	0	100	150	200
State = PLO (PSPD)	6	10	20	30
State = HAZ (HAZARD)	0	0	1	10
State = SYSB (SYSB)	6	10	20	30

.....

where 6 in this example is the total number of SysB lgrp lines in the office.

Use the following command to change the SYSB threshold:

AlmStat SYSB minor_value major_value critical_value

The input values must be in ascending order, or the command will be rejected. User could also change the threshold via table OFCVAR, but a warning will be displayed on the MAP: "WARNING: This parameter should only be changed using the ALMSTAT command at the LTP".

This alarm can be disabled by changing the threshold to (0 0 0) via table control on table ofcvar. Again, a warning message will be displayed for this action.

New log for SYSB line alarm

A new log LINE 811 will be generated when the alarm is raised or cleared. The format of the log will be as below:

RTP7 *** LINE 811 DEC01 17:45:14 2000 THR LNS ALARM

Category: Communications

Cause: thresholdCrossed

Severity: CRITICAL

ThresholdID: SYSB_LINES

RTP7 ** LINE 811 DEC01 17:45:14 2000 THR LNS ALARM

Category: Communications

Cause: thresholdCrossed

Severity: MAJOR

ThresholdID: SYSB_LINES

RTP7 * LINE 811 DEC01 17:45:14 2000 THR LNS ALARM

Category: Communications

Cause: thresholdCrossed

Severity: MINOR

ThresholdID: SYSB_LINES

RTP7 LINE 811 DEC01 17:45:14 2000 THR LNS ALARM

Category: Communications

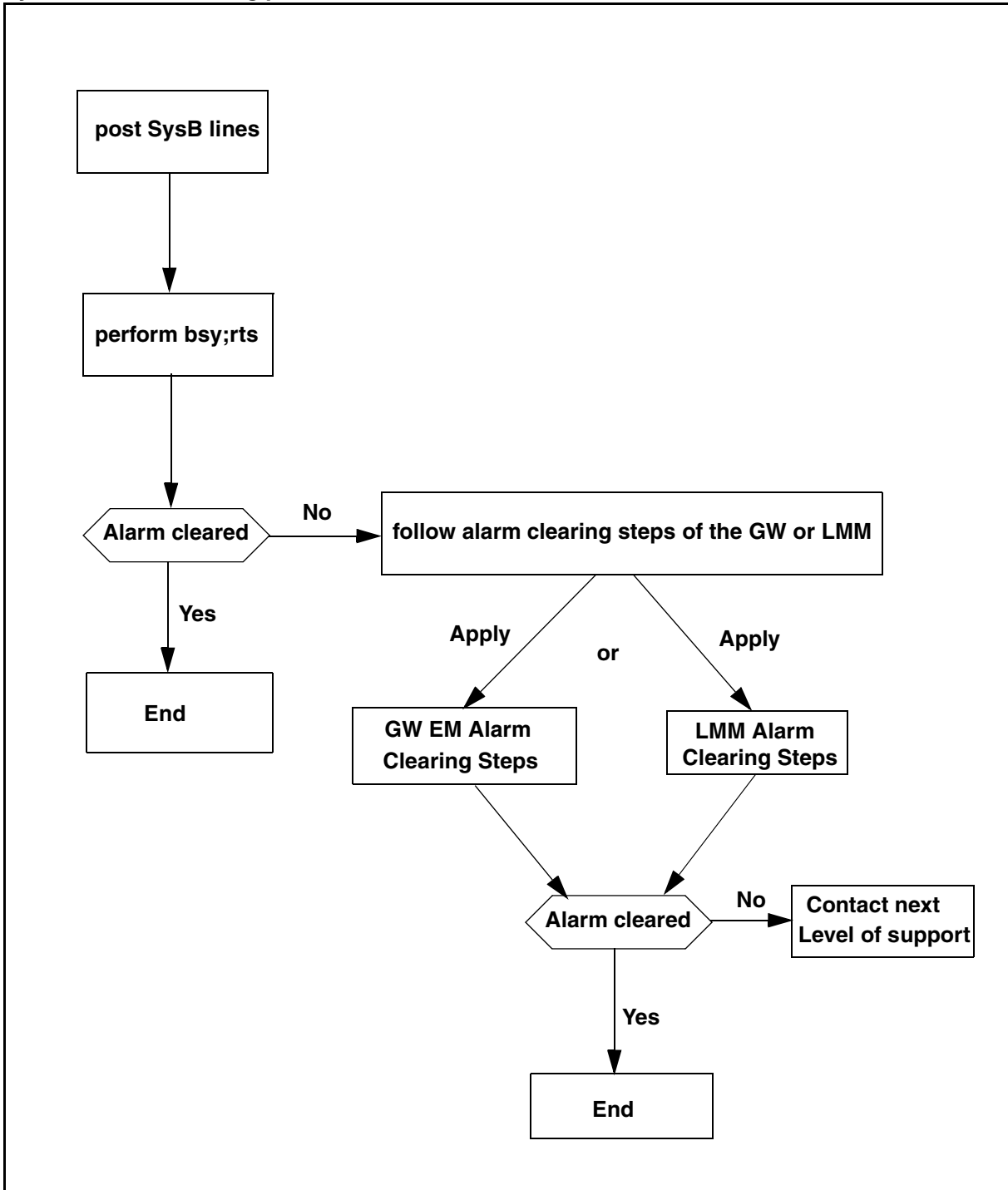
Cause: thresholdCrossed

Severity: CLEAR

ThresholdID: SYSB_LINES

SysB lns alarm clearing procedures

Please refer to the summary flowchart depicted in the following figure to clear the SysB Lns alarm:

SysB line alarm clearing procedures

Note: For MG9K, the alarm clearing procedures are documented in A00005016.

LGRP maintenance

This feature will provide a new lgrp maintenance support on the core. The following lists the work items to be done:

- lgrp pm map interface support to allow user to post lgrp nodes and perform maintenance action against the posted lgrp node
- lgrp SysB alarm support
- support for new lgrp map maintenance commands: bsy, rts, offl and QueryPM

New pm map level for lgrp

User will be able to post LGRP under the PM maintenance level. The map window is very similar to other LCDs:

```

XAC      MS      IOD      Net      PM      CCS      Lns      Trks      Ext      APPL
.         .         .         .         2lgrp    .         .         .         .         .
          *C*
LGRP      SysB    ManB    OffL    CBsy    ISTb    InSv
0 Quit          PM        4        0        0        0        0        0
2 Post_        LGRP      2        0        0        0        0        0
3 Listset
4          LGRP: LG    00 0      SysB      Links_OOS: Cside 0
5
6          POST:
7 Bsy
8 Rts
9 OffL
10
11 Disp_
12 Next
13
14 QueryPM
15
16
17
18
  YD
Time 09:05 Pref>

```

The state of the posted lgrp will be displayed, so does the total numbers of LGRPs in each state.

Command Bsy, Rts, and Offl can only be issued for the large node lgrp (i.e. only for a lgrp of S type).

Bsy command

Command Bsy will send a man_bsy message to GWC. The map will wait for an ACK from gwc with 5 second timer. Upon receiving man_bsy message, GWC will disable the heartbeat between MG9K and GWC, and send an man_bsy_ack message back to the core. Upon receiving the ACK, Bsy

command will kill all the calls and change the node state to ManB. If timeout occurs, the core will send bsy force request to gwc and change the node state to ManB.

Bsy nowait command will also be supported. This command does the same thing as Bsy command but user gets the prompt back immediately.

This command can only be issued on a node state of OFFLINE, SYSTEM BUSY, or INSERVICE.

Rts command

Command Rts will send man_rts message to gwc and wait for an ACK. Upon receiving man_rts message from the core, gwc will reenable the heartbeat between MG9K and GWC, and send man_rts_ack (if service-change-disconnected message is received from MG9K) back to the core.

If man_rts_ack message is received, the map process will handle it as tid-idle message is received (i.e. change the state to Insv and send down the line state table to gwc, etc). Map display will be updated accordingly.

If 90-second timeout occurs, a “TIMEOUT ON WAIT FOR REPLY FROM GWC” message will be displayed on the map and no state change will occur.

Rts force command will do the same thing as Rts, except that it does not wait but immediately change the node state to SysB.

Rts nowait command allows the user to get the prompt back immediately.

Rts force nowait command does the same thing as Rts force.

Rts command can only be issued on a ManB state.

Offl command

Command Offl will take the lgrp posted to unequipped state. It can only issued from ManB state.

Note: The lgrp node state will be set to OFFL (like most of the PM nodes are) after the node provisioning. User will need to perform manual action in order to bring the node into service.

QueryPM command

Command QueryPM will show the posted LGRP node data information:

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.	2lgrp	.	.	.	.	.
				C					
LGRP				SysB	ManB	OffL	CBsy	ISTb	InSv
0 Quit		PM		4	0	0	0	0	0

```

2 Post_      LGRP      2      0      0      0      0      0
3 Listset
4      LGRP: LG    01 0      SysB      Links_OOS: Cside  0
5
6      QueryPM
7 Bsy      PM Type: LGRP  PM No: 81  Int. No: 1  HOSTNN: 72
8 Rts      Cside Host Name: GWC  6
9 OffL     Cside Host IP:  172.16.112.56
10      FrmType  Flr    RowPos  FrmPos  ShlfPos
11 Disp_    MG9F      2      ZZ      3      0
12 Next
13
14 QueryPM
15
16
17
18
    YD
Time 09:12 Pref>

```

New pm alarm for LGRP

The new alarm will be displayed under the PM banner and will be raised when there are LGRP nodes that are in SysB (machine busy).

The severity of this alarm will follow the rule of existing PM alarms: If the number of SysB lgrp exceeds 10 percent of the total pm in the office of all types, set the alarm class to CRITICAL. Otherwise, set the alarm to MAJOR if there is at least one SysB lgrp. The alarm will be cleared only when the state of all lgrp nodes is changed to other state (via Bsy or Offl command).

lgrp alarm clearing procedures

The most common reason of lgrp sysb alarm is due to OOS (Out of Service) of MG9K or due to state mismatch between the lgrp node in the core and the MG9K VMG the lgrp represents. User should use the alarm clearing procedure in A00005015 as the guide for clearing the alarm. If none of them clears the sysb alarm in the core, call GNPS for next level support.

Hardware Requirements or Dependencies

N/A

Software Requirements or Dependencies

N/A

Limitations and restrictions

N/A

Interactions

N/A

Applicable customer facing sections

Fault Management

Logs ☒

Alarms ☒

Configuration

Data Schema ☒

User Interface ☒

Element Management ☐

Security ☐

Service Order ☐

Office Parameters ☒

Accounting (includes AMA billing) ☐

Performance (includes operational measurements) ☐

Glossary

Term	Description
New term	Definition
LMM	Line Maintenance Manager
GW	Gateway

References

1. “New VMG Out of Service Alarm”, A00005016MG9000_FM.fm
2. “CS2000 Line Test for MG9000 Lines” A00001888 in FMDOC

Configuration for A00003459

Hardware and Software Requirements

N/A

Initial Configuration

N/A

Office/Subnet parameters (OP/SP) (CM & SESM)

New/modified office/subnet parameters

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management)
OFCVAR	SYSBALARM	NEW	CM

Parameter information**SYSBALARM**

System Busy Line Alarm

Functional description

Provides thresholds for sysb line alarm. It has three values: minor_threshold, major_threshold, critical_threshold. The unit of the threshold is Lines. Lns alarm under mapci;mtc will be updated when there is a threshold crossing over the threshold.

Provisioning rules

The default value of SYSBALARM is { 10, 20, 30 }. It can be changed via mapci;mtc;lns;ltp;almStat command:

AlmStat SYSB minor_value major_value critical_value.

To disable the alarm, user needs to use table OFCVAR change command to set the threshold values to {0, 0, 0}. User cannot use AlmStat command to disable the alarm.

Memory requirements

No memory impact.

Upgrade Impact

N/A

Data schema (DS) (CM, MIBS, RDB)

N/A

Service Orders (SO) (CM & SESM)

N/A

Software optionality control (SOC)

N/A

Element Management

N/A

Command interface changes

Directory: LGRP

Directory description

LGRP can be posted under mapci;mtc;pm level. This directory will display the lgrp name, state info. User can also Bsy, Rts, Offl, and QueryPM the lgrp node.

Accessing directory: mapci;,mtc;pm

Access to directory or MAP level and return to CI

To access lgrp CO10 20 0, type

mapci;mtc;pm;post lgrp CO10 20 0

Command: Bsy

Command type: Listed MENU

Command target: SUPERNODE

Command description

To change the lgrp state to ManB.

Command syntax

This command takes no parameter.

Qualifications and warnings

None

Responses

MAP outputs with associated meanings and actions

Command
<RESPONSE>: The state of the lgrp posted will be changed to ManB
System or user actions:
Example: bsy
Meaning: To busy out the posted lgrp node
System or user actions:
If response is received from gwc, the lgrp state is changed to ManB and 'Bsy is successful' is displayed on the map. Otherwise, no state change will occur and "TIMEOUT ON WAIT FOR REPLY FROM GWC" message will be displayed on the map.

Command: Bsy force**Command type:** Listed MENU**Command target:** SUPERNODE**Command description**

To change the lgrp state to ManB immediately.

Command syntax**Qualifications and warnings**

None

Responses**MAP outputs with associated meanings and actions**

Command
<RESPONSE>: The state of the lgrp posted will be changed to ManB
System or user actions:
Example: bsy nowait
Meaning: To busy out the posted lgrp node while getting the CI prompt back immediately
System or user actions:
The lgrp state is changed to ManB and user gets the prompt back immediately.

Command: Offl**Command type:** Listed MENU**Command target:** SUPERNODE**Command availability:****Command description**

To change the lgrp state to Offl.

Command syntax

This command takes no parameter.

Responses

MAP outputs with associated meanings and actions

Command
<RESPONSE>: The state of the lgrp posted will be changed to Offl
System or user actions:
Example: Offl
Meaning: To Offl the posted lgrp node
System or user actions:
The lgrp state is changed to Offl and 'Offl is successful' is displayed on the map.

Command: Rts

Command type: Listed MENU

Command target: SUPERNODE

Command availability:

Command description

To change the lgrp state to Insv. It sends a message to GWC to activate the messaging between GWC and MG9K. Upon receiving the service-change-disconnected message from MG9K, GWC will send a message to the core. The state of the lgrp involved will then be changed to InSv.

Command syntax

user can issue rts, rts force, rts nowait, and rts force nowait. rts nowait allows the user to get the CI prompt back immediately. rts force also allows the user to get the CI prompt back immediately, but it sets the lgrp node state to SysB.

Command: Rts force

Command type: Listed MENU

Command target: SUPERNODE

Command availability:

Command description

To try to change the lgrp state to Insv without waiting for response from GWC. man-rts-mtc message will be sent to GWC. The state of the lgrp posted will be changed to SysB initially and will stay if no response is received from GWC.

It GWC responds to the lgrp_man_rts after it receives the service-change-disconnected message from MG9K, The core will change the lgrp node state to InSv from SysB and all the map will be updated.

Command: QueryPm

Command type: Listed MENU

Command target: SUPERNODE

Command availability:

Command description

To display the LGRP node data information.

Command syntax

This command takes no parameter.

Responses

MAP outputs with associated meanings and actions

Command
<RESPONSE>: The state of the lgrp posted will be changed to SysB
System or user actions:
Example: Rts
Meaning: To Rts the posted lgrp node
System or user actions:
The lgrp state is changed to SysB and 'Rts is successful' is displayed on the map.

Security

N/A

Configuration Walkthrough

N/A

Product = CS2000

A00003485--ISUP 200,000 Ports Trunk Support (PT-IP)

Description

ISUP 200K Ports Trunk Support

This feature increases the limit on the size of table C7TRKMEM for a standalone SSP from 165,000 tuples to a maximum of 200,000 tuples.

The constraints which will allow table C7TRKMEM to realize an increased maximum number of tuples from 165,000 to 200,000 are:

- Switch is a stand-alone SSP.
- Universal Signaling Platform.

If an attempt to exceed the above maximum of 200,000 tuples is made, a pre-existing error message is printed which states that the number of tuples in table C7TRKMEM is at the supported limit.

When ISUP, PRI, DPT, and PTS ports are provisioned the total ports for the SSP can not be above 200,000 total trunk ports.

EPUTIL

EPUTIL is a CI tool in the CM(Type EPUTIL on the CI prompt to access the tool) tool which allows a user to capture and display maintenance messages sent from the GWCs to the CM. This tool has been available as a lab-only tool until now. This feature will make this tool field ready.

Given below is a list of the various commands that will be available to the user in EPUTIL.

1. **EPTRACE:** This is the main test tool available to the user. It provides the user with commands to turn ON/OFF the trace, display the captured messages etc. Given below is a list of the sub-commnads available at this level:
 - a. **SELECT:** Allows the user to select a node for the trace. The user has an option of selecting all nodes or a specific node.
 - eg SELECT ALL : selects all nodes
 - SELECT GWC <GWC NO> : selects the specified GWC

Note : A maximum of seven nodes can be selected at a given time(applicable only when specific nodes are being selected)
 - b. **REMOVE:** Allows the user to remove a selected node. The user can remove all nodes, or can remove a specific node
 - eg REMOVE ALL : removes all selected nodes
 - REMOVE GWC <GWC NO> : removes the specified GWC
 - c. **START:** Starts the TRACE
 - d. **STOP:** Stops the TRACE

- e. **LIST**: Lists all the captured bundle messages
 e.g., **LIST ALL** : Lists all the captured messages
 LIST GWC <GWC NO> : Lists all the captured messages
 for the specified GWC
- f. **SHOW**: Shows the details regarding the specified bundle message

The following figure displays a sample output for the **SHOW** command

Sample Display for **SHOW** command

```
*****
Msg Received at: 2004/01/13 11:14:47.206 TUE.
GWC Number: 80(0x0050), Node Number: 28(0x001C)
Bundle Count: 3, (0x0003)
Sequence No: 6, (0x0006)

Individual Messages
=====

Message 1 <==
Received from Node 28(0x001C)
Terminal Number: 801 (0x0321), CPID: CKT ETSIV2OG 1
Individual message type: um_car (0x0003)
Carrier Event:tid_cflt(0x0003) Amount: 3(0x0003)

Message 2 <==
Received from Node 28(0x001C)
Terminal Number: 804 (0x0324), CPID: CKT ETSIV2IC 1
Individual message type: um_car (0x0003)
Carrier Event:tid_cflt(0x0003) Amount: 3(0x0003)

Message 3 <== Received from Node 28(0x001C)
Terminal Number: 807 (0x0327), CPID: CKT ETSISPAREOG 1
Individual message type: um_car (0x0003)
Carrier Event:tid_cflt(0x0003) Amount: 3(0x0003)
*****
```

- a. **STATUS**: Displays the current status of the TRACE(displays whether the TRACE is ON/OFF, and all the GWCs selected for the TRACE).
 - b. **COUNT**: Displays the total number of messages captured
 - c. **HELP**: Provides the user with the list and a brief description of all available commands at the EPTRACE level
1. **EPPTABLE**: Displays the details regarding all the processes in the input handler. The details include the Process ID, the In Use Queues and the Mailbox ID
 2. **FQTABLE**: Lists the free queues

3. **NODEMAP**: Displays the node to process mapping
4. **HELP**: Provides the user with the list and a brief description of all available commands at the EPUTIL level

Hardware Requirements or Dependencies

This increased limit of table C7TRKMEM can only be realized for Succession offices with Universal Signaling Platform is being used as SS7 network interface.

Software Requirements or Dependencies

None

Limitations and restrictions

ISUP 200K Ports Trunk Support

- Support of only 64k of trunks being transferred during upgrades in the states, INB, RES, or MB.
- When ISUP, PRI, DPT, and PTS ports are provisioned the total ports for the SSP can not be above 200,000 total trunk ports.

EPUTIL

- A maximum of 1024 messages can be captured by EPUTIL if the trace is turned on for all GWCs. In case the trace is turned on for specific nodes, then a maximum of 512 messages can be captured for each of the selected nodes.
- EPUTIL captures the messages at the input handler, and hence turning on the trace might have some real time impact. It is recommended that this tool be used at off-peak hours
- EPUTIL does not keep track of all the users that are logged into the tool simultaneously. Care should be taken when multiple users use this tool.

Interactions

None

Applicable customer facing sections

Fault Management

Logs __NA__

Alarms __NA__

Configuration

Data Schema __NA__

User Interface __NA__

Element Management	__NA__
Security	__NA__
Service Order	__NA__
Office Parameters	__NA__
Accounting (includes AMA billing)	__NA__
Performance (includes operational measurements)	__NA__

Glossary

Term	Description
USP	Universal Signaling Platform
CM	Central Module
GWC	Gateway Controller

Product = CS2000

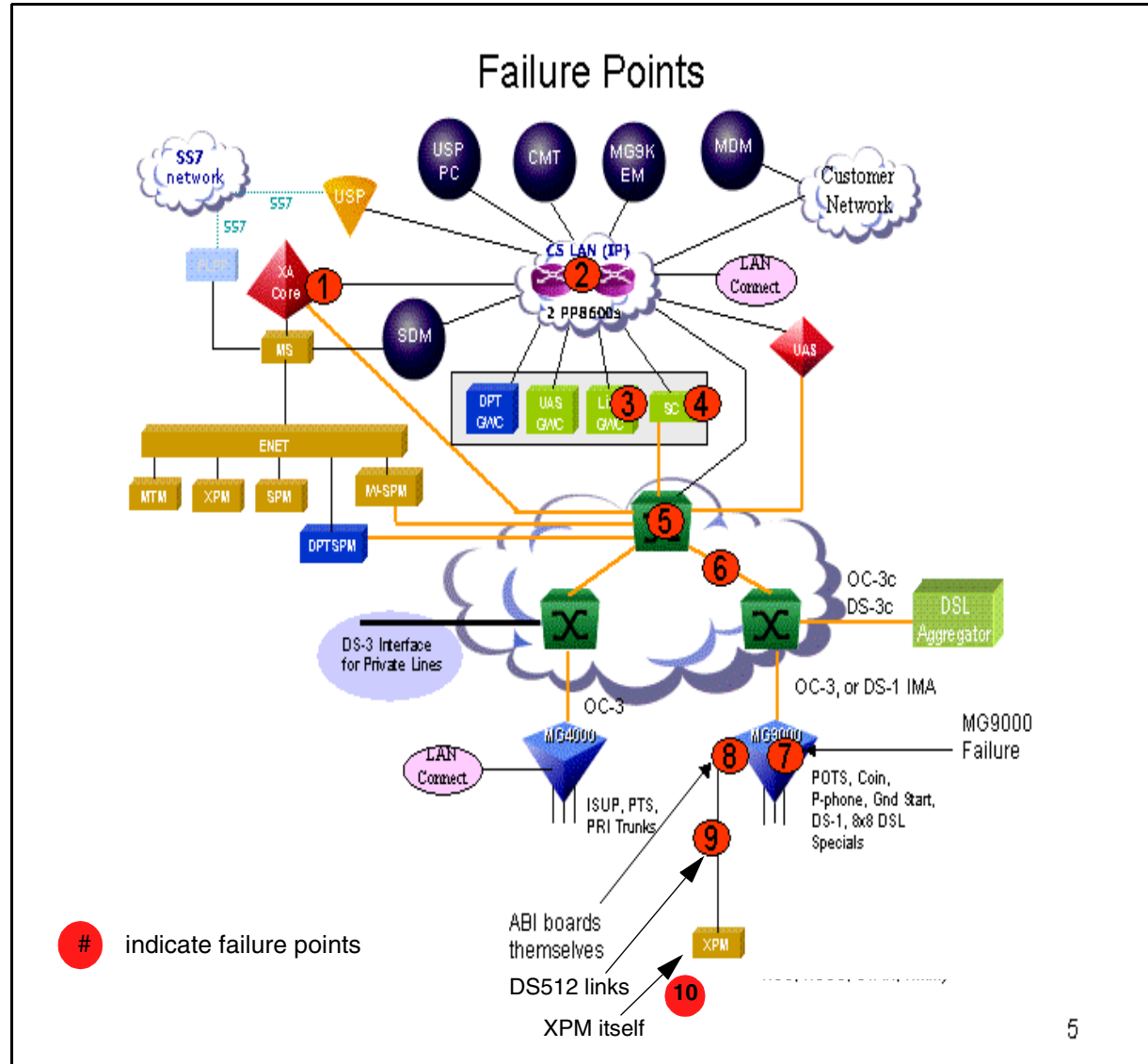
A00003486 -- Gateway Location information (UA-IP)

Functional Description

The purpose of this feature is to provide physical location data for MG9K gateways which host only ABI XPMs to aid in the determination and ultimately the resolution of ABI XPM and line troubles on the Core where applicable.

Currently, these service-impacting failures can occur in many different points in the Succession networks. Please refer to the following figure.

Succession Networks Failure Points



The ability to identify MG9Ks involved in the ABI configurations and their lines and their physical location was not easily determined.

This feature will aid in identifying the failure points detectable by the Core by providing necessary and accurate location data. Then using this newly provisioned data to correctly report and identify problem areas in the form of Logs, OMs, and Mapci commands.

In order to provide these new functionalities, the customer will see changes in the following areas:

- operation of Table LTCINV

- introduction of new Table GATWYINV
- display of the QueryPM command for ABI XPMs

Table LTCINV

The impact to this table consists of moving most of the ABI gateway information out of the EXTDS512 option and replacing it with a key to the ABI gateway information provisioned in table GATWYINV. For details on what/how this is provisioned, refer to [“Table LTCINV Database Schema information” on page 691](#).

Table GATWYINV

This is a new table on the Core designed to house gateway related information. The term gateway in this context has a flexible meaning. Gateway could refer to the physical gateway, where the hardware and call processing entity are the same. Gateway could also refer to a logical gateway, where the hardware contains many call processing entities each of which are considered a gateway. Therefore the meaning you choose depends on the construction of the “gateway”.

For our more experienced DMS customers, provisioning of “gateways” in this table does not result in node creation, even though the name “INV” might suggest otherwise. Therefore the maintenance and management of the gateway is still performed from the Element Manager.

For details on what/how this table is provisioned, refer to [“Table GATWYINV Database Schema Information” on page 695](#).

ABI QueryPM

The impact to this command is a change in the amount of data displayed as a result of issuing the command. The command itself has not changed. For details on how this functionality has changed, refer to [“Map Level: QUERYPM MAPCI command” on page 700](#).

Hardware Requirements or Dependencies

There is no hardware dependencies required to execute this feature.

Software Requirements or Dependencies

This feature requires the Core load to be a Succession load. Specifically Succession release SN07 or later.

Limitations and restrictions

The new GATWYINV table will not have flow through provisioning in this release. There are plans to have flow through for this table in a future release.

For our more experienced DMS customers, provisioning of “gateways” in this table does not result in node creation, even though the name “INV” might

suggest otherwise. Therefore the maintenance and management of the gateway is still performed from the Element Manager.

As is the current functionality today, flow through provisioning for this ABI Gateway and its corresponding location information is not available in this release. There are plans to have this ABI gateway data flow through in the future.

Although the new GATWYINV table is being designed for many different types of Gateways, for this initial SN07 release, only ABI gateways are allowed to be provisioned.

As is the currently functionality today of table LTCINV, the ability to change the hosting GWC once provisioned in the new GATWYINV table is not allowed.

Interactions

The following are the feature interactions for this feature:

- Features which this feature is dependent on:
 - none
- Features which are dependent on this feature:
 - A00004430 - ATM SVC ATM606 logs

This feature possibly will need access to the Location information to format logs accurately.
- Features which have an interaction with this feature:
 - A00003490 - Network Change and ABI XPM Migration

This feature plans to allow change to GWC host and ABI IP address data. This data will be moving to the new GATWYINV table and this functionality will have to be addressed from the new table.
 - A00002380 - ABI ESA Logs

This feature is possibly changing the Mapci levels for ABI. This may impact ABI QueryPM and ABI Link Mtc which is being impacted by this feature.

Applicable customer facing sections

Fault Management

Logs ___n/a___

Alarms ___n/a___

Configuration

Data Schema ___X___

User Interface	___X___
Element Management	___n/a___
Security	___n/a___
Service Order	___n/a___
Office Parameters	___n/a___
Accounting (includes AMA billing)	___n/a___
Performance (includes operational measurements)	___n/a___
Real-time	___X___
Engineering Information	___X___

Glossary

Term	Description
VMG	Virtual Media Gateway - this is a logical representation of a gateway.
ABI XPM	An XPM which is provisioned in table LTCINV with the optional attribute EXTDS512. These XPMs are physically connected to MG9K Gateways via a DS512 interface.

Configuration A00003486

Hardware and Software Requirements

The changes provided by this feature will allow the customer to physically identify ABI configured hardware components hosting ABI lines from the Core when trouble shooting their network. This enables quick problem resolutions. These Core changes provide:

- MG9K Frame/Shelf physical location data for MG9Ks hosting ABI lines
- Changes to the Mapci QueryPM application to make use of this data

Therefore the following hardware needs to be in place prior to exercising the software provided by this feature. The software is exercised by provisioning the physical location data of these hardware components:

- A typical ABI configuration

Software Requirements:

- SN07 Succession Core load or later

Initial Configuration

As a provisioning component of the Succession program, much of this functionality performs as designed without the hardware being in place. However, to provision actual physical location data, the provisioning of the configurations mentioned in section should be installed.

Once the hardware is installed and the software is available, provisioning of the physical location data can begin. The ABI Gateway and its location data is provisioned in table GATWYINV. This is a new table as of SN07. The steps to perform the provisioning are described in section “Data schema (DS) (CM, MIBS, RDB)” on page 690.

Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable.

Upgrade Impact

Dump and Restore

Table GATWYINV will use the existing data transfer “TabXfr” mechanism available to all Table Control tables to preserve its data during an upgrade. Because this is a new table as of SN07, there will be no data to preserve.

Due to the changes to table LTCINV for the ABI XPM tuples, data preservation for these tuples will occur when upgrading from any prior release which could contain ABI XPM datafill (SN05 or later) to the SN07 release. This means entries will be created in table GATWYINV when processing table LTCINV to preserve the ABI XPM datafill. Because the new GATWYINV table has much more configuration information available than what is provisioned against the ABI XPMs, much of the data will be defaulted. Therefore, once the upgrade is complete, the customer is expected to modify the newly created data in table GATWYINV to provide more accurate information than could possibly be provided during the upgrade.

Element Management Upgrade

Not applicable.

Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
LTCINV	Changed	Unchanged
GATWYINV	New	New Table Control

Table LTCINV Database Schema information

Name: LTCINV

Long Table Name: Line Trunk Controller INventory

Functional description

Table LTCINV contains the inventory data, except P-side link assignments, for various host peripheral module (XPM) types. This feature will only impact ABI XPM tuples. The change impacts the datafill associated with the ABI (EXTDS512) option. The change is to move most of the option datafill to table GATWYINV and replace the data with a key to the ABI gateway. Please refer to “Table LTCINV changed field descriptions” on page 692.

Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

1. Table SERVRINV - GWC datafill, no change
2. Table SERVSINV - AUD datafill, no change
3. Table GATWYINV - New table, Gateway datafill. Dependencies on both SERVRINV and SERVSINV.
4. Table LTCINV - Dependency on GATWYINV for ABI XPM tuples
5. Table SERVCONN - ATM server connection datafill, no change

Size

No change in the maximum number of tuples for table LTCINV.

Table LTCINV size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
LTCINV	0	210	Memory is automatically allocated in increments of 10 XPMs at a time up to a maximum of 210 tuples.

Fields

The following table lists impacted fields for Table LTCINV.

Table LTCINV changed field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTATTR	Changed	Modified the EXTDS512 refinement, add 1 new subfield and deleted 4 existing subfields	GTWY_HOST (added)	New field, This field contains the data which points to an entry in the new GATWYINV table. Made up of two sub-fields: GWTYPE GW_TYPE GWNO {0 TO 1023}
			NE_NBR (deleted)	GW_NETWORK_ELEMENT_NUMBER_RANGE - This field is deleted. The data is now available in table GATWYINV.
			ABI_SLOT_NBR (deleted)	ABI_SLOT_RANGE - This field is deleted. The data is now available in table GATWYINV.
			IPADDR (deleted)	TABLE OF 4 {0 TO 255}'s - This field is deleted. The data is now available in table GATWYINV.
			GWC_HOST (deleted)	Made up of two sub-fields: PMTYPE PM_TYPE PMNO {0 TO 255} - This field is deleted. The data is now available in table GATWYINV.

Datafill example

The following example illustrates the changed prompting sequence for the EXTDS512 option in table LTCINV.

Prompting sequence for the modified option EXTDS512

```

>add lgc 1 7 lgci 0 32 1 D 33 6x02na qlil6at pots potsex keyset ksetex $ $ msg6x69 isp +
16 $ northaa sx05aa $ sx05aa $ 0 sxfwaj01
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y

OPT_ATTR:
>asdfd
*** ERROR ***
ASDFD
|
TYPE OF OPT_ATTR IS LTCINV_OPT_ATTR
OPT_ATTR:
>asdfd
*** ERROR ***
ASDFD
|
TYPE OF OPT_ATTR IS LTCINV_OPT_ATTR
TYPE IS LTCINV_OPT_ATTR {CCS7,STRBBF,STRDTRE,STRN5,FSTR2,PCM30,NX64,METER,
                        FLS,OC,FDCP,EXTDS512}

OPT_ATTR:
>extds512
SITE:
>cary
>GTWY_HOST
>ABI 5
>$
PEC6X40:
>6X40FA

... << continue with normal datafill for LTCINV >>

```

The following figure shows the changes to the OPTATTR field with the new gateway field ranges for the optional refinement EXTDS512.

Range Values for new Gateway PM datafill in option EXTDS512

```

>table ltcinv
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: LTCINV
>range optattr
18 OPTATTR          LTCINV_OPT_ATTR_VECTOR
TYPE IS LTCINV_OPT_ATTR_VECTOR VECTOR OF UP TO 12 MULTIPLES WITH
    OPT_ATTR          LTCINV_OPT_ATTR REFINEMENTS:
    {EXTDS512}        MULTIPLE WITH
        SITE          CHAR_VECTOR VECTOR OF UP TO 16 CHAR'S
        GTWY_HOST      GW_KEY  MULTIPLE WITH
            GWTYPE      GW_TYPE
            GWNO         {0 TO 1023}
    OTHERWISE          LTCINV_OPT_ATTR_NIL_DATA

```

The following figure provides a view of the successfully added tuple with the new Gateway data fields for option EXTDS512.

Sample LTCINV Tuples with new Gateway fields for option EXTDS512

```
>table ltcinv
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: LTCINV
LTCNAME ADNUM FRTYPE FRNO SHPOS FLOOR ROW FRPOS EQPEC LOAD EXECTAB CSLNKTAB OPTCARD
TONESET PROCPEC EXTLINKS E2LOAD OPTATTR PEC6X40 EXTINFO
-----
LGC 1 1002 LTEI 2 19 1 CC 2 6X02NA QLI17AY1 (POTS POTSEX) $ (4 0)(4 1)(4 2)(4 3) $
(MSG6X69) $ NORTHAM SX05AA $ SX05AA $ 0 SXFWAE08 (EXTDS512 CARY ABI 5) $ 6X40FA N

SMA2 2 1009 LTE 1 51 2 E 31 MX85AB QLI17AY1 (POTS POTSEX) $ (4 4) (4 5)(4 6) (4 7) $
(UTR6) (MSGMX76 HOST ) (ISP 4) $ NORTHAM AX74AA AX74AA 0 SXFWAE08
(EXTDS512 GRNR ABI 120) $ 6X40AC N
```

Table release history update

SN07 Feature A00003486: Available in the Core with the SN07 or later release.

Modified field: OPTATTR:

- add 1 new subfield for the EXTDS512 refinement and deleted 4 existing subfields for the EXTDS512 refinement. For more information see “Table LTCINV changed field descriptions” on page 692.

Supplementary information

Limitations:

- LTCINV - since the impacted fields apply to ABI XPMs, they can only be datafilled on tuples with the EXTDS512 option.

ONP Upgrade to SN07:

- During the upgrade to SN07, tuples will be auto populated in table GWCINV. This is required to preserved any existing datafill in table LTCINV for tuples with the EXTDS512 option. There will be new fields which will be assigned a nil value, refer to GW 0006 Figure on page 699. It is expected that the user will correct this to more accurate data after the ONP is completed.

Translation verification other tools

Table LTCINV does not impact translations. Therefore TABAUDIT is the tool used to verify the contents of table LTCINV. The following figure shows the output from TABAUDIT when it is used to verify LTCINV.

Sample Tabaudit output for Verifying Table LTCINV Datafill

```

>tabaudit
TABAUDIT:
>include ltcinv

>execute
-----
|                TABAUDIT STATUS                |
|-----|
The following tables are included:
    table LTCINV (91)

The following tables are excluded:
    From table VERSIONS (0)                to table SERVRINV (90).
    From table MGCINV (92)                 to table IPINV (299).
    From table X75INFO (301)               to table INWATNPA (1426).

Please confirm ("YES", "Y", "NO", or "N"):
>yes
Creating TABAUDIT summaryfile: SUMMARY$MAP on SFDEV.
Starting DMS data verification ...
Table LTCINV: New table control.
    Completed tuple checking.
    SUMMARY: Tbl LTCINV: tuples checked 2, passed 2, failed 0.
Data verification is completed.

```

Table GATWYINV Database Schema Information**Name: GATWYINV**

Long Table Name: Gateway Inventory

Functional Description

Table GATWYINV is where gateway configuration information is provisioned. Provisioning gateways in this table does not allocate IOUI nodes of any kind. For this release, this table contains configuration information only (no nodes) involving gateways. The term “gateway” could either mean a physical gateway or logical gateway, it depends on the actual “gateway” in question.

Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

1. Table SERVRINV - GWC datafill, no change
2. Table SERVSINV - AUD datafill, no change
3. Table GATWYINV - New table, Gateway datafill. Dependencies on both SERVRINV and SERVSINV.
4. Table LTCINV - Dependency on GATWYINV for ABI XPM tuples

Size

The maximum number of tuples is 32767 for this table GATWYINV. Currently limited to 1024 (0-1023) for only ABI gateways for SN07.

Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
GATWYINV	0	32767	Memory is automatically allocated in increments of 32 tuples at a time up to 32767. The multiple of 32 allows for an exact allocation of store to accommodate the maximum number of tuples.

Fields

Table GATWYINV new field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GTWYPMNO	New	2 Subfields: GWTYPE GWNO	GW_TYPE - only valid SN07 value is "ABI". GW_NO - {0 - 1023} - any valid number in this range.	Two part Key: GW_TYPE - This is the type of the gateway as defined on the Core. GW_NO - This is the unique external number of the gateway.
GTWYPRFL	New	n/a	An enumerated list of gateway profiles consisting of Alpha-numeric Characters. Examples:MG9KITP, MG9KABI, PVG. only valid SN07 value is MG9KABI.	The name of the profile for the gateway. The profile provides a way to assign a finer level of granularity (as opposed to GW_TYPE) to specify specific gateway behaviors.
GTWYNAME	New	n/a	32 Alphanumeric characters.	The name of the gateway, could be upper and lower characters with special characters.
GTWYADDR	New	n/a	IPADDR Table of 4 {0 TO 255}	The IP address of the gateway. For this release this could be either the Callp address or Mtce address.(aka CIPOA address)
GTWYCSPM	New	3 Subfields: SITE_ID PMT EXT_PMNO	4 Alphanumerics PM_TYPE - any valid PM type. {0 TO 255} - any valid number in this range.	SITE_ID: The physical Site of the Hosting Gateway Controller. Site name must be defined in table SITE. The only valid value for SN07 is HOST. PM_TYPE - This is a valid PM type of the cside host XPM. This could be any valid PM type but generally will be a GWC. PMNO - The unique external number of the cside host Gateway Controller.

Table GATWYINV new field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GTWYOPTS	New	Refinement GTWYLOC with 8 fields.	GTWY_SITE (4 alpha numerics)	SITE_NAME: The physical site of the gateway. Valid values are verified against entries in table SITE. Example datafill 'CARY'.
			FRAME_TYPE	FRAME_NAME - existing data dictionary type. The unique frame type. Example datafill, MG9Ks have a frame type of 'MG9F'.
			FRAME_NUMBER {0 - 511}	FRAME - existing data dictionary type. The unique number given to a frame within an Office.
			FLOOR_POSITION {0 TO 99}	FLOOR_POS - existing data dictionary type. The unique floor with a unique Site (generally a building).
			ROW_POSITION {A,B,C...X,Y,Z,AA, BB,CC...XX,YY,ZZ}	ROW_POS - existing data dictionary type. The unique row within a floor.
			FRAME_POSITION {0 TO 99}	FRAME_POS - existing data dictionary type. The unique frame position within a row.
			SHELF_POSITION {0 TO 77}	SHELF_POS - existing data dictionary type. Traditionally, this is the bolt hole position as measured in inches from the floor up. For MG9K shelves, it should be equal to the Shelf Number as specified in the Lgrp Key. The unique shelf position within a specific frame.
			GW_CARD_SLOT_NB R {0-50}	SLOT_NO - existing data dictionary type. This is the slot number for a card. The SN07 use if for the ABI card slot.

Table GATWYINV new field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GTWYOPTS (continued...)	New	ELMGR with 1 field.	GTWY_NE_NBR {0-999}	GW_NETWORK_ELEMENT_NUMBER_RANGE - existing data dictionary type. This is the network element number assigned when the gateway is added via the MG9K-EM. 0 is the NIL value.

Datafill Example

The following figure provides a view of a successfully added tuples with the location and element manager options. Note that other gateway types other than ABI are shown, this is just example data. Only ABI gateways are supported in SN07.

Sample GATWYINV Tuples with Options

```
>table gatwyinv
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: GATWYINV
GTWYPMNO      GTWYPRFL      GTWYNAME      GTWYADDR      GTWYCSPM      GTWYOPTS
-----
GW 0          MG9KITP      CARY-000-0-0  47 142 14 65  GWC 15 (GTWYLOC CARY MG9F 15 2 C 3 0
0) (ELMGR 43) $

GW 6          MG9KITP      AUTO_DISC      192 2 45 87  GWC 10 (GTWYLOC APEX MG9F 0 0 ZZ 99
77 8) (ELMGR 32) $

ABI 9          MG9KABI      EXPM10          192 1 23 184  GWC 15 (GTWYLOC APEX MG9F 12 3 C 2
0 18) (ELMGR 61) $

GW 15         PVGPRF      PVGGW-5         147 142 172 45  GWC 20 (GTWYLOC GRNS OTHR 5 1 E 4
0 0) $

GW 4          CICMPRF      CICM-10         148 124 67 34  GWC 16 (GTWYLOC WKFT OTHR 4 1 B 7
0 6) $
```

Table release history update

Release SN07, feature A00003486: Initial release of this new table GATWYINV.

Supplementary information

ONP Upgrade to SN07:

- During the upgrade to SN07, tuples will be auto populated in table GWCINV. This is required to preserved any existing datafill in table LTCINV for tuples with the EXTDS512 option. There will be new fields which will be assigned a nil value, refer to GW 0006 Figure on page 699. It is expected that the user will correct this to more accurate data after the ONP is completed.

Translation verification other tools

Table GATWYINV does not impact translations. TABAUDIT is the tool used to verify the contents of table GATWYINV. Examples will be provided once the new table is functioning.

Service Orders (SO) (CM & SESM)

Not Applicable.

Software optionality control (SOC)

Not Applicable.

Element Management

Not Applicable.

Command interface changes**Map Level: QUERYPM MAPCI command**

The QUERYPM command is used to query miscellaneous information about the currently posted XPM at the PM level of the MAP. This feature modifies the legacy QUERYPM command by displaying an additional screen to the default QUERYPM command (without arguments) which reflects the following ABI MG9K:

- Site
- Floor
- Row Position
- Frame Position
- Frame Type
- Frame Number
- Shelf Number
- ABI Slots
- Network Element Number
- ABI card IP address

Note: New output only occurs if the posted XPM is an ABI XPM.

Current QUERYPM for ABI XPM

Current QueryPM Display for ABI XPMs

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.	.	.	.	.	.	.
LGC				SysB	ManB	OffL	CBsy	ISTb	InSv
0 Quit		PM		0	0	0	0	0	20
2 Post_		LGC		0	0	0	0	0	2
3 ListSet									
4 ABILink	LGC		1 InSv	Links_OOS: CSide	0	, PSide	0		
5 Trnsl_	Unit0:	Inact	Insv						
6 Tst_	Unit1:	Act	Insv						
7 Bsy_	SITE	ABISlots	NE						
8 RTS_	GRNR	04/05	6						
9 OffL									
10 LoadPM_									
11 Disp_									
12 Next									
13 SwAct									
14 QueryPM									
15									
16									
17 Perform									
18									
TEAM01									
Time 03:47	>								

Modified QUERYPM for ABI XPM

Modified QueryPM Display for ABI XPMs

XAC	MS	IOD	Net	PM	CCS	LnS	Trks	Ext	APPL
.	.	.	.	.	.	.	.	.	.
SMA2				SysB	ManB	OffL	CBsy	ISTb	InSv
0 Quit		PM		0	0	0	0	0	20
2 Post_		SMA2		0	0	0	0	0	2
3 ListSet									
4 ABILink	SMA2	2 InSv	Links_OOS: CSide	0	, PSide	0			
5 TrnsL_	Unit0:	Inact	Insv						
6 Tst_	Unit1:	Act	Insv						
7 Bsy_	MG9K Information:								
8 RTS_	Site	Flr	RPos	Bay_id	Shf	Description	Slots	NE	IP Address
9 OffL	GRNR	01	CC02	MG9F	002	GW	0004	01/05	6 47 142 133 45
10 LoadPM_	floor								
11 Disp_		rowpos			shelfnbr				
12 Next		framepos		frametype	framenbr				
13 SwAct									
14 QueryPM									
15 DCH									
16									
17 Perform									
18 ISG									
Time 12:33									
>									

gw_type+gw_no
 ABI slots
 Network Element NBR
 ABI Card IP address

Accessing directory: LGCDIR

Access to directory or MAP level and return to CI

To access the LGCDIR from the CI environment, enter:

```
>mapci;mtc;pm;post <<XPM #>>;querypm
```

To return to the CI environment, enter quit mapci.

Command: <command name>

Not Applicable.

Security

Not Applicable.

Configuration Walkthrough

Not Applicable.



SN07 Feature Deltas

Product = CS 2000

A00003487 -- Tri-modal Provisioning, Logs and OMs (UA-IP)

Functional Description

Note that this Functional Description covers all the SN07 Trimodal Call Server Features:

- a00003488: TriModal Call Signaling and Connectivity
- a00003662: TriModal Call Server Bridge Maintenance
- a00003509: TriModal Support for Lawful Intercept
- a00003947: TriModal Logs and OMs
- a00003948: TriModal GWC EM

Description

Prior to SN07, the CS2000 call server had very limited knowledge about the packet bearer network. Only a single packet bearer network was supported along with the legacy ENET bearer network. Individual agents were associated with a bearer network based upon the connectivity of the node that hosted the agent. For example, a trunk member that was assigned to a DTC would be associated with the legacy ENET bearer network. A trunk member that was assigned to either a GWC or an MG4K would be associated with the packet bearer network. Since both the GWC and the MG4K tag their hosted agents as 'packet bearer network', the core connectivity cannot distinguish between the various types of packet bearer networks are available (i.e., IP, AAL1, AAL2). This is the basis for the CS2000 call server restriction that it can only support a single packet bearer network prior to SN07.

Feature Functionality

In the SN07 release, work is being started in the CS2000 Call Server to support multiple bearer networks. These bearer networks include both the legacy ENET bearer network and up to seven additional packet bearer networks.

In the SN07 release, a bearer network framework is implemented but full integration of all possible supported configurations will not be supported in this release. In SN07, the focus will be on supporting three bearer networks¹:

- ENET
- AAL1 packet network
- IP packet network

The main focus in SN07 is to support a Universal Access (UA)- AAL1 and a Universal Access (UA) - IP configuration with a single CS2000 Call Server. In addition, there are requirements to support some limited Carrier Hosted Services (CHS) functionality as well (i.e., H.323 and Media Call Server 5200 (MCS5200)).

Interworking between the UA-AAL1 and UA-IP configurations in a multi-bearer network configuration is supported in SN07. However, interworking with the CHS agents is limited in SN07. In SN07, there is no support for interworking between the H.323 gateway (using a Media Portal) and the IP IW SPM. For this reason, a loop around trunk, hosted by a PVG on the CHS bearer network and hosted by a PVG in the UA IP bearer network or an MG4K in the UA AAL1 bearer network or an SPM/DTC in the ENET network, must be used to provide connectivity between the H.323 GW and all other agents on the CS2000 Call Server.

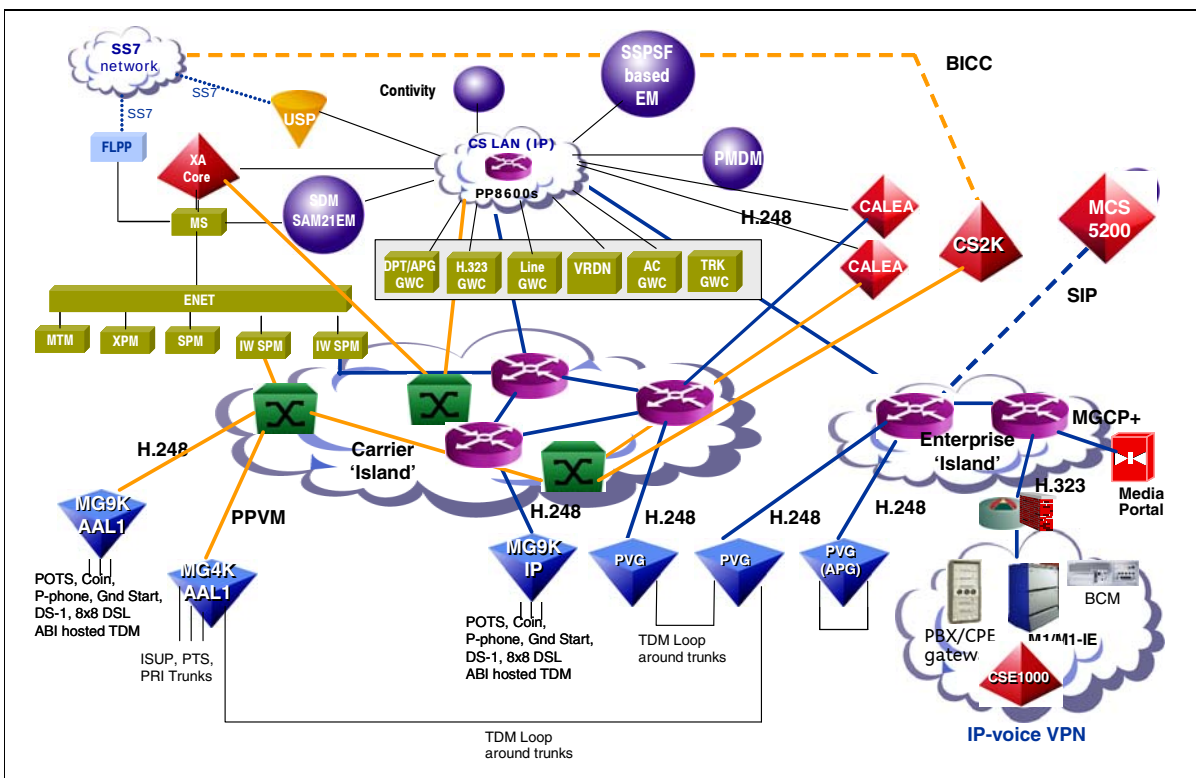
The following list provides a view of the limitations associated with H.323 calls in this configuration:

- Multiple billing records generated - A call from an H.323 agent to an MG9000 AAL1 native line would be represented as two calls in the CS2000 call server, each generating its own billing record.
- H.323 agent access to announcements - Since there is no announcements accessible to the CHS IP network (i.e., no IP IW bridge supported), announcements cannot be played to the H.323 agent. Any CS2000 Call Server services will not be able to use announcements and any treatments will have to be configured to 'release with cause' and the announcement would be provided by the enterprise bearer network.
- H.323 agent access to conferencing - Since there is no conference circuits accessible to the CHS IP network (i.e., no IP IW bridge supported), conferencing services cannot be supported to the H.323 agent.
- H.323 agent access to test trunk facilities - Since there is no test trunk circuits accessible to the CHS IP network (i.e., no IP IW bridge supported), trunk tests cannot be supported to the H.323 gateway.

1. AAL2 packet networks are not going to be tested in a multi-bearer network configuration, but there is nothing to block this type of bearer network from being configured.

A diagram of the network topology is shown in the following figure.

SN07 supported multi-bearer network topology



In SN07, the following gateways and packet agents are supported in the multi-bearer network configuration.

Gateways and packet agents supported in SN07

Bearer Network	Gateway	Agents
ENET	None ^a	supported SN07 legacy peripherals which includes both lines and trunk

Gateways and packet agents supported in SN07

Bearer Network	Gateway	Agents
ATM AAL1 (UA)	MG4000	ISUP trunks PTS trunks PRI trunks BICC DPT trunks
	GWC ^b	BICC DPT trunks
	MG9000	POTS lines Pphone lines Coin lines Ground Start lines
	MG9000 with ABI	supported SN07 ABI peripherals which includes both lines and trunk
	DPT SPM	BICC DPT trunks
IP (UA)	PVG (for loop-around trunk access only for support of H.323)	ISUP trunks PRI trunks
	MG9000	POTS lines Pphone lines Coin lines Group Start lines
	MG9000 with ABI	supported SN07 ABI peripherals which includes both lines and trunk
IP (CHS)	PVG (for loop-around trunk access only for support of H.323)	ISUP trunks PRI trunks
	GWC ^c	SIP-T DPT trunks
	H.323 GWs (Cisco, Westel, BCM, M1)	PRI trunks

a. There are no 'gateways' support on the ENET. However, there is a list of supported legacy peripherals for Succession Call Servers. This list remains unchanged by this feature.

b. Not a true bearer gateway. This is included to illustrate the support for BICC DPT trunk.

- c. Not a true bearer gateway. This is included to illustrate the support for SIP-T DPT trunk support.

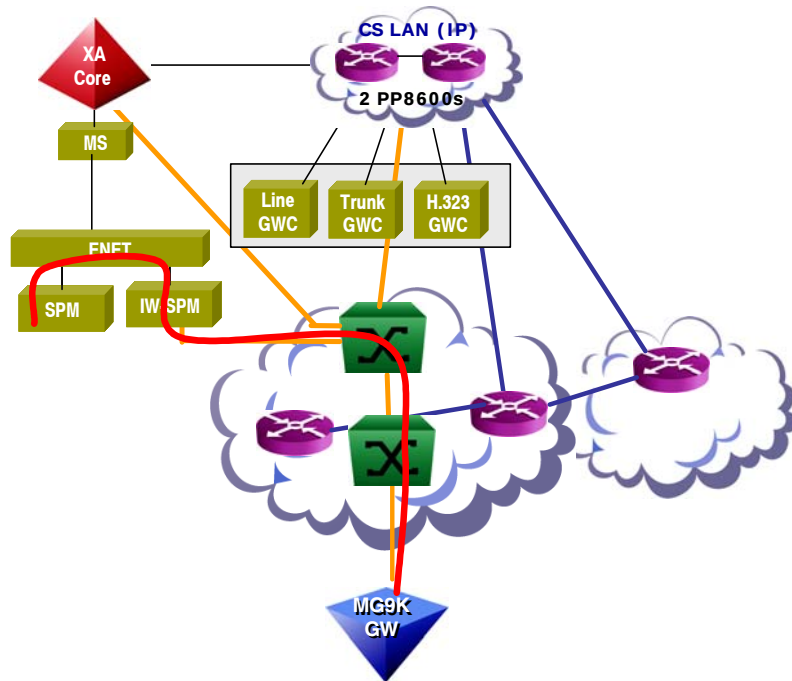
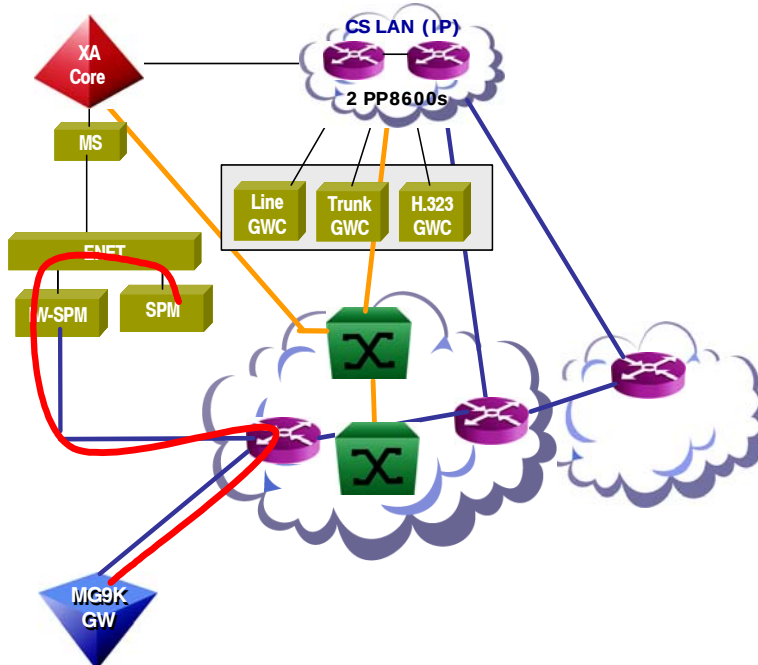
Connectivity between the supported bearer networks is accomplished by using IW SPM bridges. The CS2000 Call Server is modified to allow support of both the ATM AAL1 based IW SPM and the IP based IW SPM at the same time. Prior to SN07, the CS2000 Call Server could only support one type of IW SPM. A single IW bridge pool was supported. In SN07, support for multiple bridge pools is introduced.

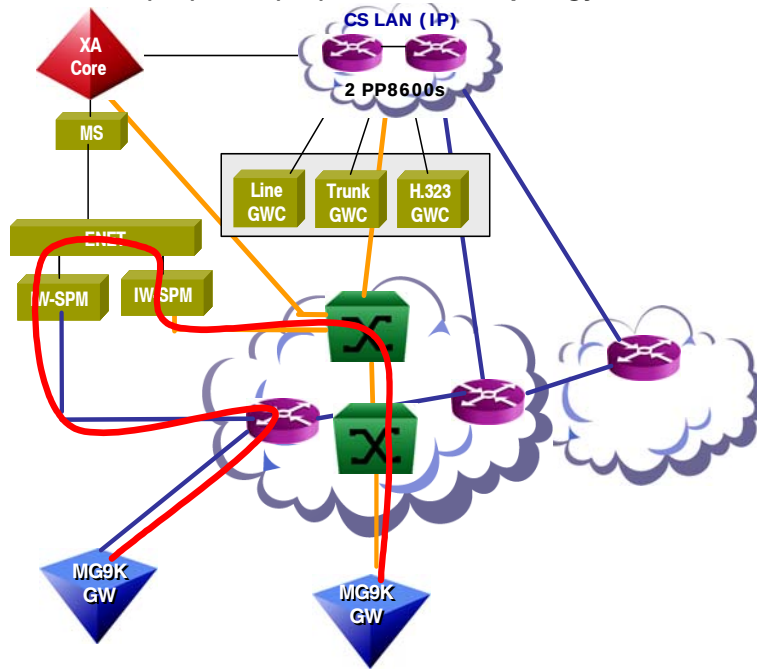
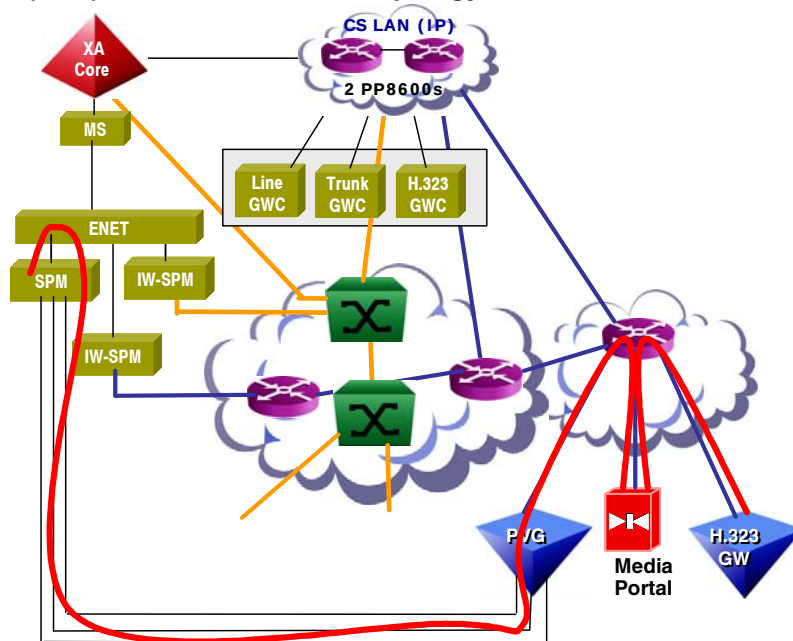
Control is given to the Succession customer to configure how the supported bearer networks in the CS2000 Call Server connect to each other. This is controlled by provisioning the types of interworking bridges needed to connect one bearer network to another. The interworking bridges available in SN07 are the following:

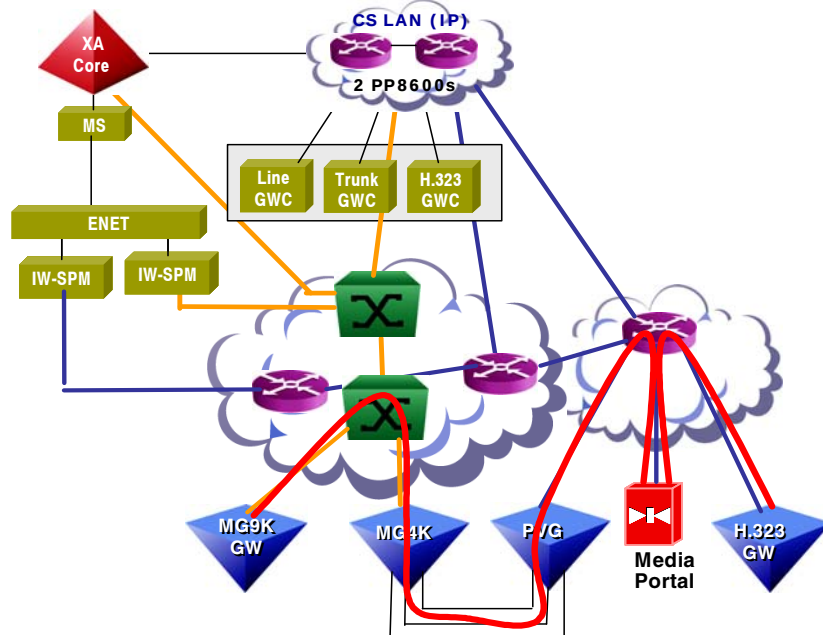
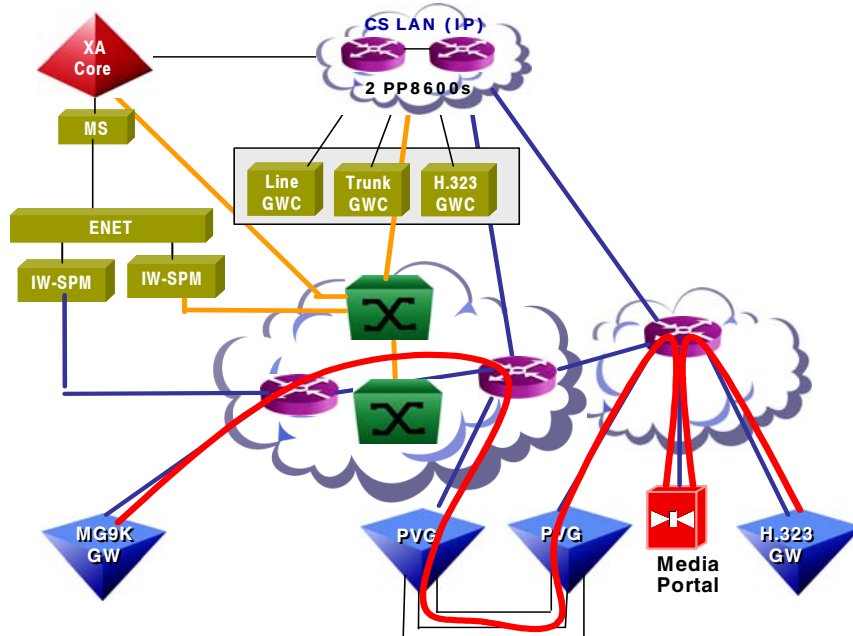
- IW SPM AAL1 - connects an AAL1 bearer network to the ENET
- IW SPM IP - connects an IP bearer network to the ENET

Prior to SN07, Succession configurations used the IW SPM AAL1 to connect an AAL1 bearer network to the ENET and used the IW SPM IP to connect an IP bearer network to the ENET. This is still supported in SN07 with multi-bearer network support. In this multi-bearer network configuration, a connection between an AAL1 bearer network and an IP bearer network will use two IW bridges (i.e., 1 IW SPM AAL1 and 1 IW SPM IP using the ENET to connect the two packet bearer networks). The following figures illustrate the connection topologies².

2. Note that these figures are logical representations and are not meant to imply physical connectivity of the bearer networks.

ATM AAL1 (UA) to ENET connection topology**IP (UA) to ENET connection topology**

ATM AAL1 (UA) to IP (UA) connection topology**IP (CHS) to ENET connection topology**

IP (CHS) to ATM AAL1 (UA) connection topology**IP (CHS) to IP (UA) connection topology**

The following areas will be addressed in more detail in the following sections:

- Bearer network and connectivity provisioning
- Multiple bearer network support in the GWC EM
- Core connectivity connection management
- IW Bridge management
- OAMP changes on the CS2000 Call Server
- Lawful Intercept
- Service circuit support
- Groups with members in multiple bearer networks
- Trunk selection (like network selection)
- DPT (BICC and SIP-T) interworking including audible ringing support
- Translations and Routing changes
- USP messaging
- ECAN across multiple bearer networks
- Voice quality
- ONP
- Capacity

Bearer network and connectivity provisioning

The purpose of the provisioning changes are to allow bearer networks to be defined and associated to individual agents. Once this is accomplished, there are rules created that define which bearer networks can connect to each other and how that connection is accomplished.

When the CS2000 Call Server is requested to make a connection between two endpoints, it needs to know the bearer network associated with each endpoint. If this model were followed for provisioning, then each line and trunk member datafill would have to include an indication of the bearer network. This level of provisioning is cumbersome and very repetitive in most cases. For this reason, a hierarchical model is used in SN07. An assumption is made that a node (either an SPM node or a line/trunk GWC) supports one and only one bearer network. This allows the bearer network to be associated with the node and then this information is applicable to all the endpoints associated with that node. In other words, the bearer network for the endpoint is derived from the bearer network of the node that hosts the endpoint. Note that endpoints that are hosted on legacy peripherals which are then hosted on MG9000 ABI, will derive their bearer network from the GWC that hosts the MG9000 ABI.

There is one exception to the above behavior and it is in the area of DPT trunk support. Given the dynamic endpoint association that is made between the hosting node and the DPT trunk member, GWCs configured as DPT GWCs will not have an associated bearer network at the node level. The bearer network is associated with the DPT trunk group. The DPT endpoint obtains its associated bearer network from the DPT trunk group that is associated to it on a call-by-call basis.

The following provisioning changes are made by this activity:

- Bearer network definition
- Bearer network node association
- Bearer network DPT trunk group association
- IW bridge pool definition
- IW bridge pool assignment
- Bearer network connectivity

Bearer network definition

A new table is introduced (Table BEARNETS) that defines the bearer network and the bearer fabric associated with this bearer network. The key to the table is a bearer network index. This index is needed to make it easy to change the bearer network name (i.e., without having to delete and re-add the entry). Index 0 is always reserved for the ENET tuple, if it exists.

The OPTIONS field in this table identifies an optional bearer network characteristics. In SN07, the following options are supported:

- Default packet network - specifies the default packet bearer network in the office. This is used during the ONP process as well as an endpoint bearer network designation if a node-based bearer network cannot be determined.

Table BEARNETS supports up to eight bearer networks in the CS2000 Call Server. Refer to the Configuration section for more details on Table BEARNETS.

Table BEARNETS example datafill

TABLE: BEARNETS				
NETIDX	BNETNAME	DISPLAY	FABRIC	OPTIONS
NET 0	TDM_ENET	ENET	ENET	\$
NET 1	NET_AAL1	ATM	AAL1	(PACKET_NETWORK_DEFAULT) \$
NET 2	NET_IP	IP	IP	\$
NET 3	NET_AAL2	AAL2	AAL2	\$

Bearer network node association

Association of the bearer network is done at the node level in the CS2000 Call Server. In order to minimize table changes and to provide minimal impact to DMS legacy offices, legacy peripheral nodes do not require an explicit association to the 'ENET' bearer network. This will be assumed in within the CS2000 Call Server.

However, any node that hosts packet bearer network endpoints requires that the bearer network be associated with the node. This is applicable to the following nodes:

- GWC (Table SERVINV) - GWCs host many types of endpoints: lines and trunks)
- MG4K (Table MNNODE)
- DPT SPM (Table MNNODE)

Table SERVINV is modified to include a new field BEARNETS. This field lists all the supported bearer networks associated with the GWC. In SN07, only one entry for this field is supported, which would always be marked as the default=Y. This information is populated by the GWC Element Manager when a GWC is defined in SN07. Refer to the Configuration section for more details on Table SERVINV.

Table SERVINV example datafill

TABLE: SERVINV									
SERVNAME	SERVADDR	SERVEXEC	SERVRTONE	BEARNETS	SERVROPTS				

GWC 0	IP 47 192 48 24	(POTS POTSEX)		(KEYSET KSETEX)	\$				
NORTHAA	(NET_AAL1 Y)	\$	\$						

Table MNNODE is modified for 'SMG4' class of SPMs (i.e., MG4Ks) to include a new field BEARNETS. This field lists all the supported bearer networks associated with the MG4K. In SN07, only one entry for this field is supported, which would always be marked as the default=Y. Refer to the Configuration section for more details on Table MNNODE.

Table MNNODE example datafill - MG4K

```

TABLE: MNNODE
NODEKEY ALIAS      NODEINFO
-----
SPM 1      SPM_1      SMG4 0 SYNC LINE 50
(COT 60) (DTMF 60) (ECAN 60) (TONESYN 60) (MF 60) $ (SYSB CR
RPT) (MANB MJ RPT) (ISTB MN RPT) (SYSBNA CR RPT) (MANBNA MJ
RPT) (COTLOW MN RPT) (DTMFLOW MN RPT) (ECANLOW MN RPT) (MFLOW
MN RPT) (CMRLOW MN RPT) (TONESLOW MN RPT) (SMG4CN MJ RPT)
(PATCHFAIL MJ RPT) (ATMBCN CR RPT) (STE3HLD MJ RPT) (STE3HLD24
CR RPT) (SMCHLD MF RPT) (SMCHLD24 CR RPT) (SPMSRMNTD MN RPT)
(LOCUR MJ RPT) (TMCFAIL CR RPT) $ $ N 0 $ N N (NET_AAL1 Y) $

```

Table MNNODE is modified for 'IW' class of SPMs whose DPT_INFO indicates a DPT SPM (i.e., DPT SPMs) to include a new field BEARNETS. This field lists all the supported bearer networks associated with the DPT SPM. In SN07, only one entry for this field is supported, which would always be marked as the default=Y. Refer to the Configuration section for more details on Table MNNODE.

Table MNNODE example datafill - DPT SPM

```

TABLE: MNNODE
NODEKEY ALIAS      NODEINFO
-----
SPM 1      SPM_1      IW 1 SYNCH INTERNAL 15 (DTMF 60) (ECAN
60) (TONESYN 60) $ (SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT)
(SYSBNA CR RPT) (MANBNA MJ RPT) (DTMFLOW MN RPT) (ECANLOW MN RPT)
(TONESLOW MN RPT) (PATCHFAIL MJ RPT) (ATMBCN CR RPT) (SMCHLD MF
RPT) (SMCHLD24 CR RPT) $ DPT_ONLY (NET_AAL1 Y) $
(SPMCEIDX 0)$

```

Bearer network DPT trunk group association

DPT trunk groups require an association to the bearer network. Changes are made to Table TRKOPTS where the DPT trunk groups are defined. As part of this change, it was decided to change the option used to indicate a DPT trunk group. The DPT application is removed from the DYNAMIC option. A new DPT option is created to define a DPT trunk group. This new option contains a field to designate the associated bearer network. Other application users for the DYNAMIC option remain unchanged. Refer to the Configuration section for more details on Table TRKOPTS.

Table TRKOPTS example datafill

```

TABLE: TRKOPTS
OPTKEY      OPTINFO
-----
DPTTRK DPT      DPT BICC NET_AAL1 1
SIPTRK DPT      DPT SIPT NET_IP N MGC2 PROF MGCTWO Y
OCTRK    DYNAMIC  DYNAMIC ISUP IP IP OC

```

IW bridge pool definition

A framework is needed to allow multiple bridge pools to be defined in the CS2000 Call Server. This framework is intended to support any type of bridge that may be used to connect two bearer networks together.

In SN07, there is only one bridge type supported, the core-managed IW SPM bridge. In defining a bridge pool of this type, the two bearer networks that this bridge can connect together are specified. Other types of bridges may require additional information to be defined.

The bridge pool name is first defined in Table CLLI. Note that the number of members in the CLLI is not applicable to the bridge pool. New table NETBRDGE is created to define the bridge pool and its type. Refer to the Configuration section for more details on Table NETBRDGE.

Table CLLI and Table NETBRDGE example datafill

```

TABLE CLLI
CLLI      ADNUM  TRKGSIZ      ADMININF
-----
ENET_TO_AAL1  321    0      ENET_TO_AAL1_BRIDGE_POOL
ENET_TO_IP    322    0      ENET_TO_IP_BRIDGE_POOL

TABLE: NETBRDGE
BRDGCLLI   TYPE      DISPLAY BEARNETS
-----
ENET_TO_AAL1  CORE_BRDGE  E-A1    (TDM_ENET NET_AAL1) $
ENET_TO_IP    CORE_BRDGE  E-IP    (TDM_ENET NET_IP)  $

```

IW bridge pool assignment

Once a bridge pool has been defined, the individual IW SPM bridge nodes needs to be associated with a bridge pool. Table MNNODE is modified for 'IW' class of SPMs whose DPT_INFO indicates an IW SPM (i.e., not a DPT SPM) to include a new field BRDGCILLI. This field lists all the supported bridge pools associated with the IW SPM. In SN07, only one entry for this field is supported. Refer to the Configuration section for more details on Table MNNODE.

Table MNODE example datafill - IW SPM

```

TABLE: MNODE
NODEKEY ALIAS NODEINFO
-----
SPM 1 SPM_1 IW 1 SYNCH INTERNAL 15 (DTMF 60) (ECAN
60) (TONESYN 60) $(SYSB CR RPT) (MANB MJ RPT) (DTMFLOW MN RPT)
(ECANLOW MN RPT) (TONESLOW MN RPT) (PATCHFAIL MJ RPT) (ATMBCN
CR RPT) (SMCHLD MF RPT) (SMCHLD24 CR RPT) $ BRDG_ONLY
(ENET_TO_AAL1) $ (SPMECIDX 0)$

```

Bearer network connectivity

Now that the bearer networks have been defined and the bridge pools have been defined, the next step is to define the connectivity rules between the bearer networks. An assumption is made that a connection between two endpoints on the same bearer network will always be allowed to proceed. The rules being discussed here apply only to a connection request made between two endpoints that are associated with different bearer networks. These rules answer the following questions:

- Can a bearer network connect to another bearer network?
- What bridge pool or bridge pools are used to support a connection between two bearer networks?
- With trunk groups that support members in multiple bearer networks, what order, within trunk group member selection, should the bearer networks be attempted

Two new tables are created to allow the customer to provide answers to these questions. Table NETPATH provides a set of bridge pool combinations. These can be thought of as ‘connectivity routes’ and assist in answering the second question posed above. Note that it is possible to create a NETPATH entry that contains more than one bridge pool which would instruct connectivity to obtain multiple bridges for the connection. Note that this is also possible to create a NETPATH entry that contains no bridge pools which would instruct connectivity to allow the connection to proceed with no bridges needed.³

Table NET2NET allows the customer define which bearer networks connect to other bearer networks, the order that trunk group member selection uses and what ‘connectivity route’ should be used (i.e., points to an entry in Table NETPATH). If there are no connecting networks specified in Table NET2NET, then a connection request from that bearer network to any other bearer network will be denied. Refer to “Trunk selection (like network selection)” on page 738 for more information on using the bearer network ordering in Table NET2NET.

3. The customer may use this option when there are two bearer networks that have the same fabric. No bridge is needed to connect the two bearer networks.

Refer to the Configuration section for more information on Tables NETPATH and NET2NET.

Table NETPATH example datafill

TABLE: NETPATH			
PATHIDX	NETBRDGE		

0			\$
1	(ENET_TO_AAL1)		\$
2	(ENET_TO_IP)		\$
3	(ENET_TO_AAL1)	(ENET_TO_IP)	\$

Table NET2NET example datafill

TABLE: NET2NET			
BNETNAME	CONNETS		

TDM_ENET	(NET_AAL1 1)	(NET_IP 2)	\$
NET_AAL1	(TDM_ENET 1)	(NET_IP 3)	\$
NET_IP	(NET_AAL1 3),	(TDM_ENET 2)	\$

Multiple bearer network support in the GWC EM

As described in the previous section, the bearer network needs to be associated with the GWC. New GWCs are added using the GWC Element Manager (EM). Information input using the GWC EM GUIs is then automatically updated in CS2000 Call Server tables (such as Table SERVINV).

Prior to SN07, the GWC EM supported only one packet network. Characteristics about that packet bearer network were defined and associated with all the GWCs in the office.

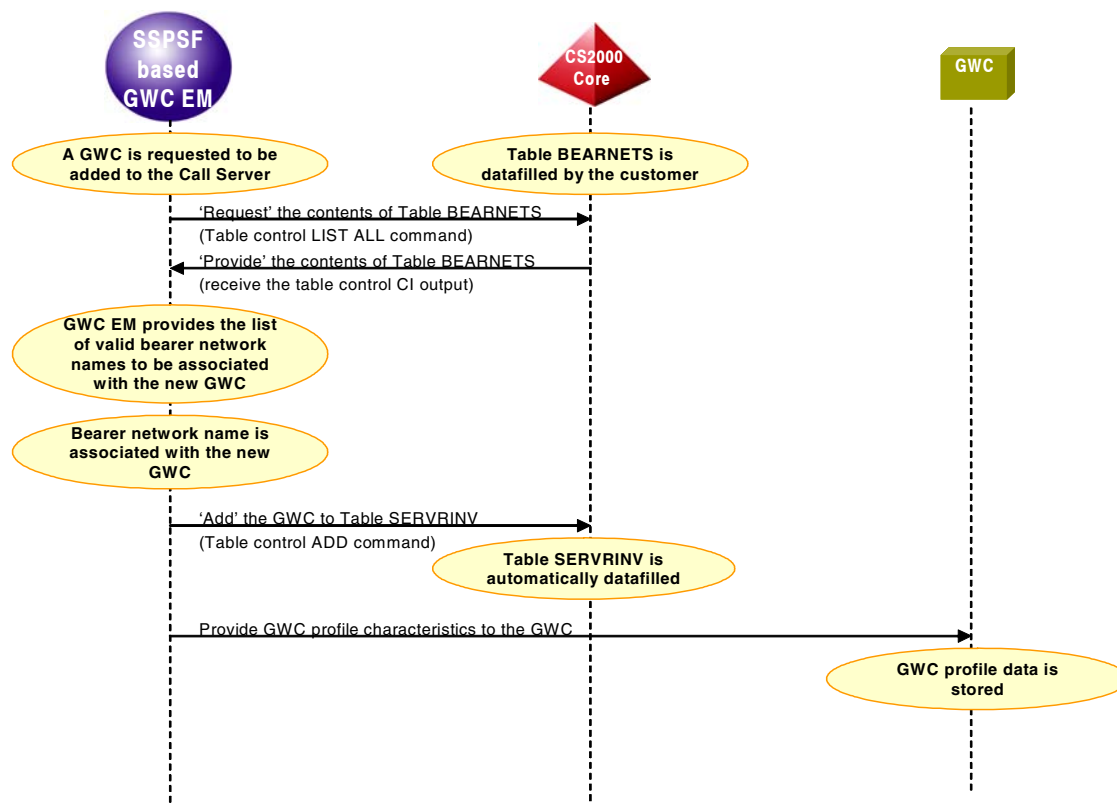
In SN07, changes are made to the GWC EM to support multiple bearer networks. These changes involve the following:

- Support the provisioning of multiple bearer network codec profiles.
 - Display bearer network codec profile on GWC-EM GUI.
 - Add bearer network codec profile from GWC-EM GUI.
 - Delete bearer network codec profile from GWC-EM GUI.
 - Change bearer network codec profile from GWC-EM GUI.
- Support the specification of a bearer network and a bearer network codec profile for each GWC.
 - Display the bearer network and network codec profile of each GWC on GWC-EM GUI.

- Associate the bearer network and network codec profile with one GWC when adding GWC node from GWC-EM GUI.
- Change the associated bearer network codec profile of one GWC node from GWC-EM GUI.
- Support population of the selected bearer network in the CS2000 Call Server table SERVINV

The following figure illustrates the steps involved in flowing the data from the GWC EM to the CS2000 Call Server. Refer to the Configuration section for more information on the GWC EM GUI screens that are available in SN07.

GWC EM flow through provisioning for bearer network



Core connectivity connection management

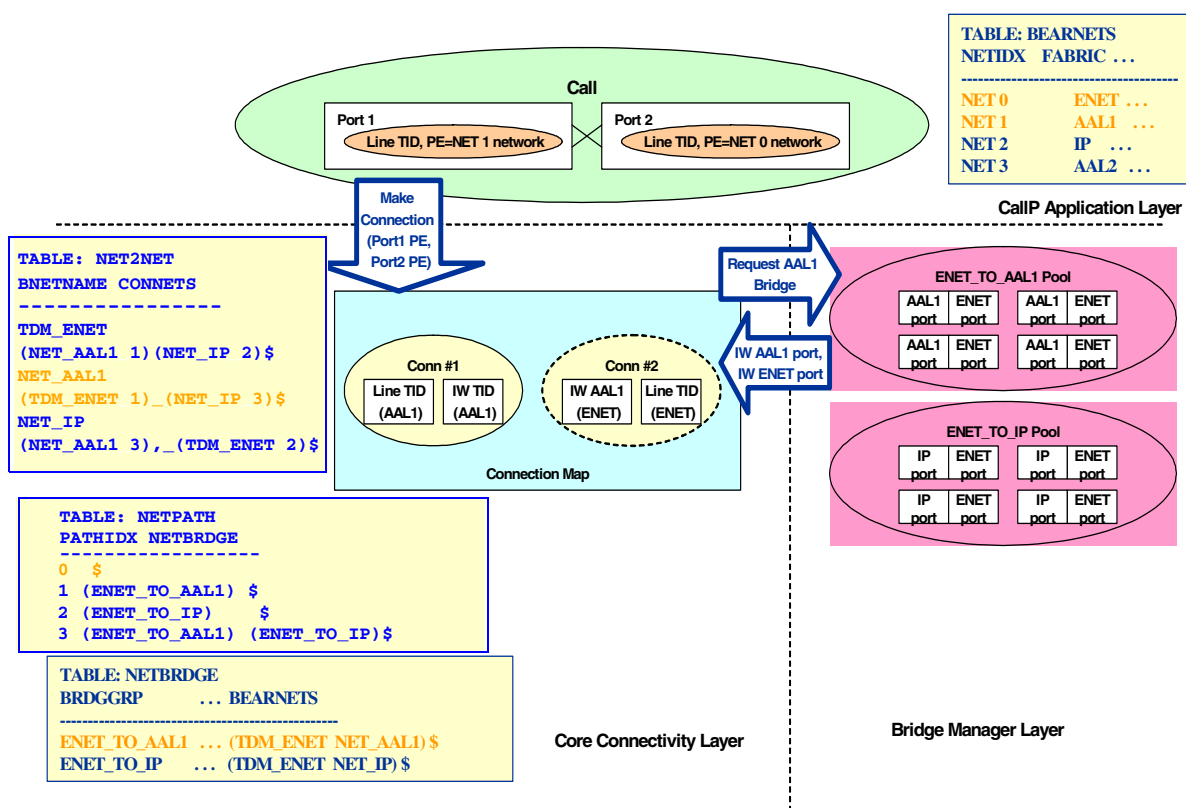
Core connectivity is a function in the CS2000 Call Server that handles connection requests that are made from the CallP and Services applications. Prior to SN07, core connectivity processed requests to make a connection between endpoints. Endpoints were designated as being 'internal' (i.e., connected to the ENET) or 'external' (i.e., connected to the packet bearer

network). Core connectivity knew that if a request was made to connect and 'internal' endpoint to an 'external' endpoint, then an IW bridge was needed. It would request a bridge from the office-wide IW bridge pool.

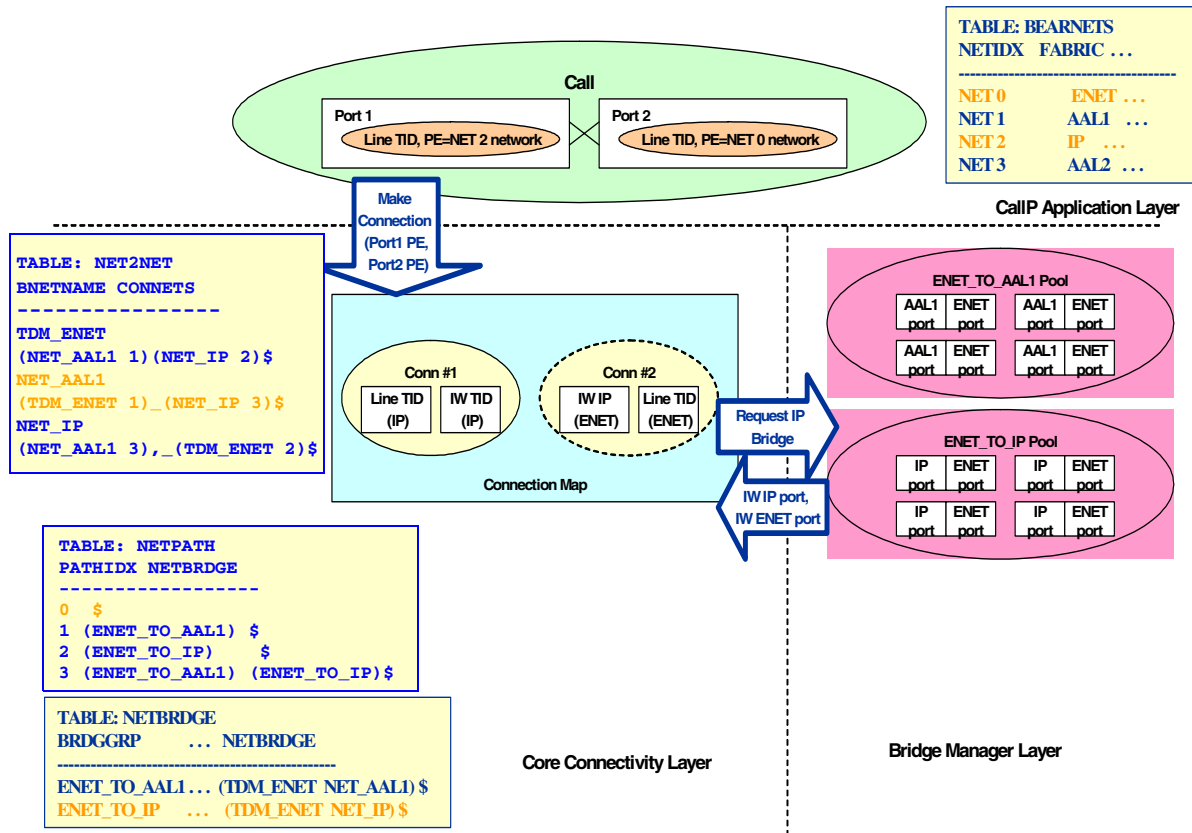
In SN07, core connectivity is changed to support multiple bearer networks and multiple bridge pools. Rather than making assumptions that a bridge from a bridge pool is needed to make a connection, core connectivity references tables NET2NET and NETPATH when a connection between two unlike bearer networks is requested. If these tables indicate that a connection should not be made, then core connectivity denies the connection request to the CallP application. The CallP application would then route the call to a Network Blocking (NBLH) treatment causing the call to not be completed.

The following figures provide examples on how core connectivity uses the datafill to process a connection request from the CallP application.

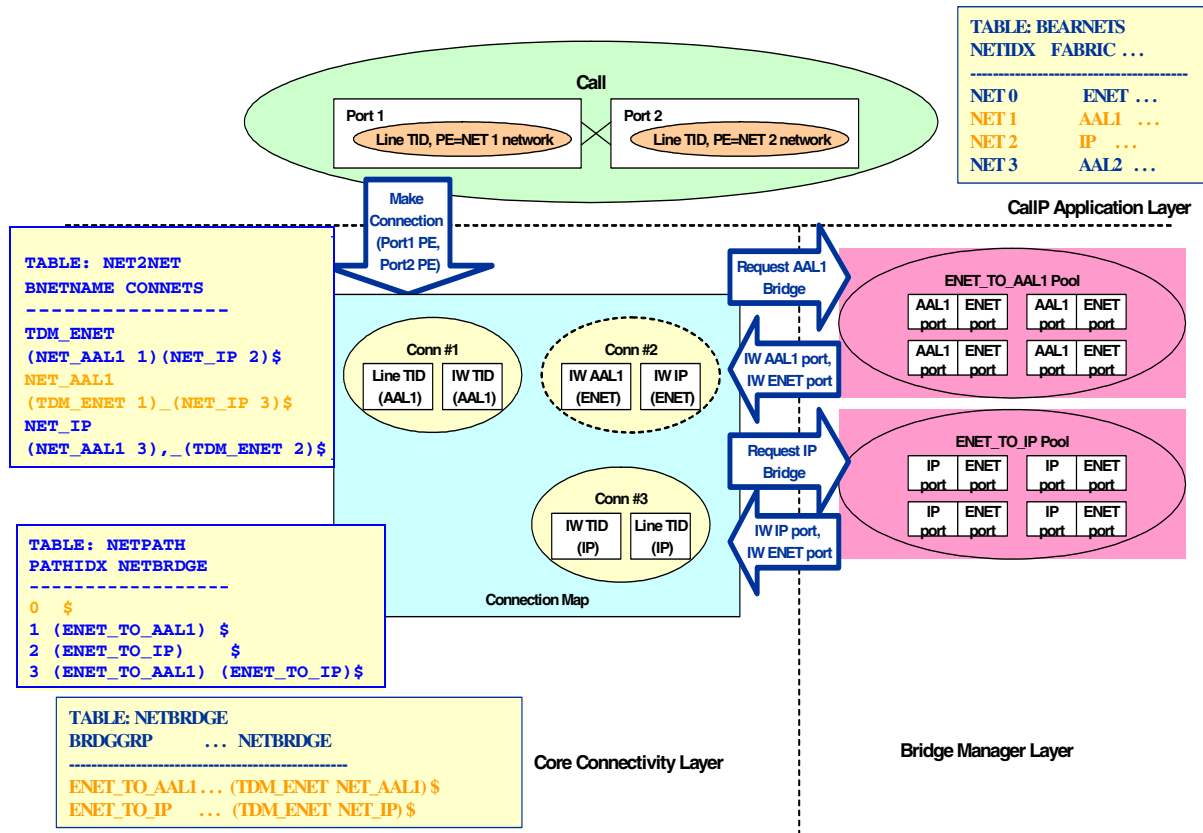
ATM AAL1 (UA) to ENET connection request



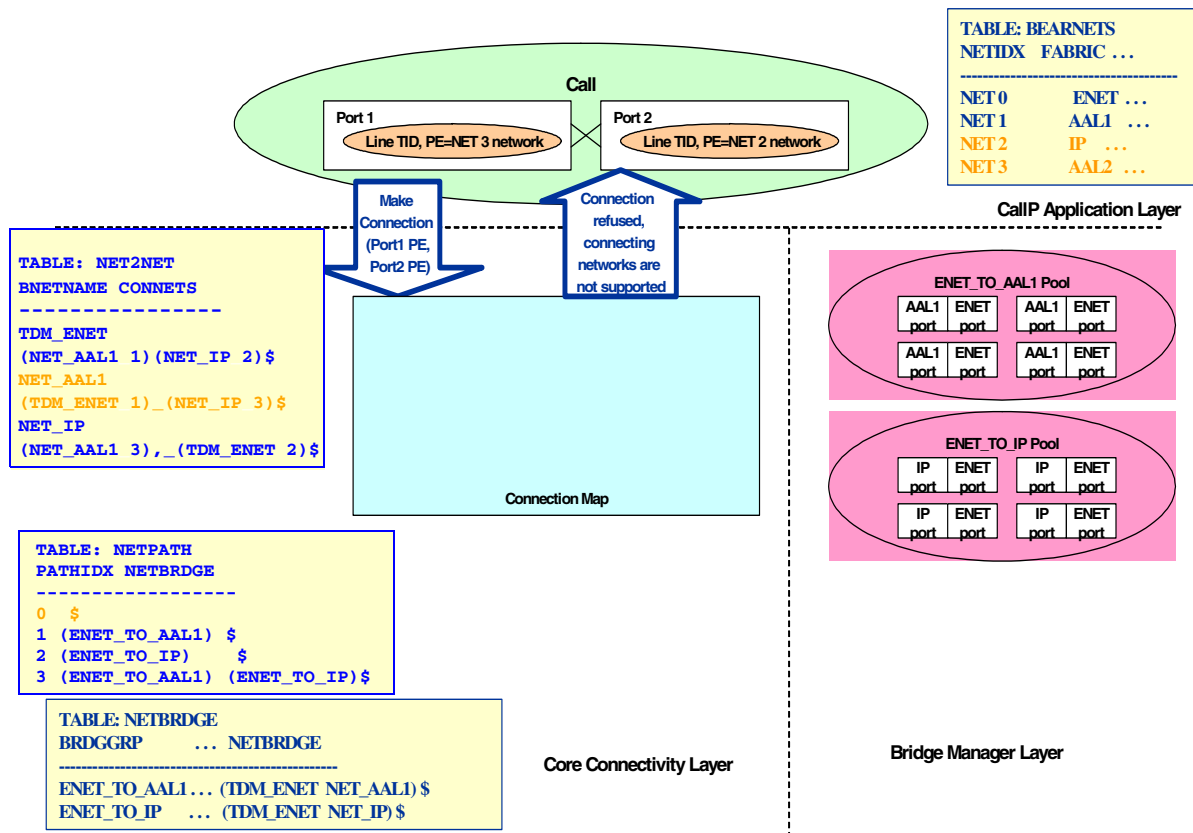
IP (UA) to ENET connection request



ATM AAL1 (UA) to IP (UA) connection request



ATM AAL2 to IP (UA) connection request



Core connectivity supports a set of connection operations. All of the possible connection requests that the CallP application may request in support of the services supported on the CS2000 Call Server map to one of these connection operations.

- Make a connection
- Break a connection
- Hold a connection
- Restore a connection
- Move a connection

These connection operations can be performed multiple times on a single call depending upon the services that are invoked. Each time a connection operation is performed, the connectivity datafill is consulted to determine how the connection map should be modified. IW bridges may be added or removed to maintain the most optimized connection topology for the call.

The following is an example of a 3-way call. The originating line (A) is on the AAL1 bearer network. The first terminating line (B) is on the IP bearer network and the second terminating line (C) is on the ENET network.

Example 3-way call

Step	Description	Connectivity Operation	Connection Map
1	'A' calls 'B'	Make connection	Connection 1 : active 'A' endpoint (NET_AAL1) - Bridge #1 endpoint (NET_AAL1) Connection 2 : active 'B' endpoint (NET_IP) - Bridge # 2 endpoint (NET_IP) Connection 3 : active - Bridge #1 endpoint (ENET) - Bridge #2 endpoint (ENET)
2	'A' flashes and puts 'B' on hold	Hold connection	Connection 1 : held 'A' endpoint (NET_AAL1) - Bridge #1 endpoint (NET_AAL1) Connection 2 : held - TO endpoint (NET_IP) - Bridge # 2 endpoint (NET_IP) Connection 3 : freed - Bridge #1 endpoint (ENET) - Bridge #2 endpoint (ENET)
3	'A' calls 'C'	Move connection	Connection 1 : active 'A' endpoint (NET_AAL1) - Bridge #1 endpoint (NET_AAL1) Connection 2 : held - TO endpoint (NET_IP) - Bridge # 2 endpoint (NET_IP) Connection 4: active - Bridge #1 endpoint (ENET) 'C' endpoint (ENET)

Example 3-way call

Step	Description	Connectivity Operation	Connection Map
4	'A' flashes and connects to 'B' and 'C'. A conference circuit is obtained on the MTM.	Move connection	Connection 1 : active 'A' endpoint (NET_AAL1) - Bridge #1 endpoint (NET_AAL1) Connection 2 : active - TO endpoint (NET_IP) - Bridge # 2 endpoint (NET_IP) Connection 4: freed - Bridge #1 endpoint (ENET) 'C' endpoint (ENET) Connection 5: active - Bridge #1 endpoint (ENET) - CF3P(0) endpoint (ENET) Connection 6: active - Bridge #2 endpoint (ENET) - CF3P(1) endpoint (ENET) Connection 7: active 'C' endpoint (ENET) - CF3P(2) endpoint (ENET)
5	All parties disconnect	Break connection	Connection 1 : freed 'A' endpoint (NET_AAL1) - Bridge #1 endpoint (NET_AAL1) Connection 2 : freed - TO endpoint (NET_IP) - Bridge # 2 endpoint (NET_IP) Connection 5: freed - Bridge #1 endpoint (ENET) - CF3P(0) endpoint (ENET) Connection 6: freed - Bridge #2 endpoint (ENET) - CF3P(1) endpoint (ENET) Connection 7: freed 'C' endpoint (ENET) - CF3P(2) endpoint (ENET)

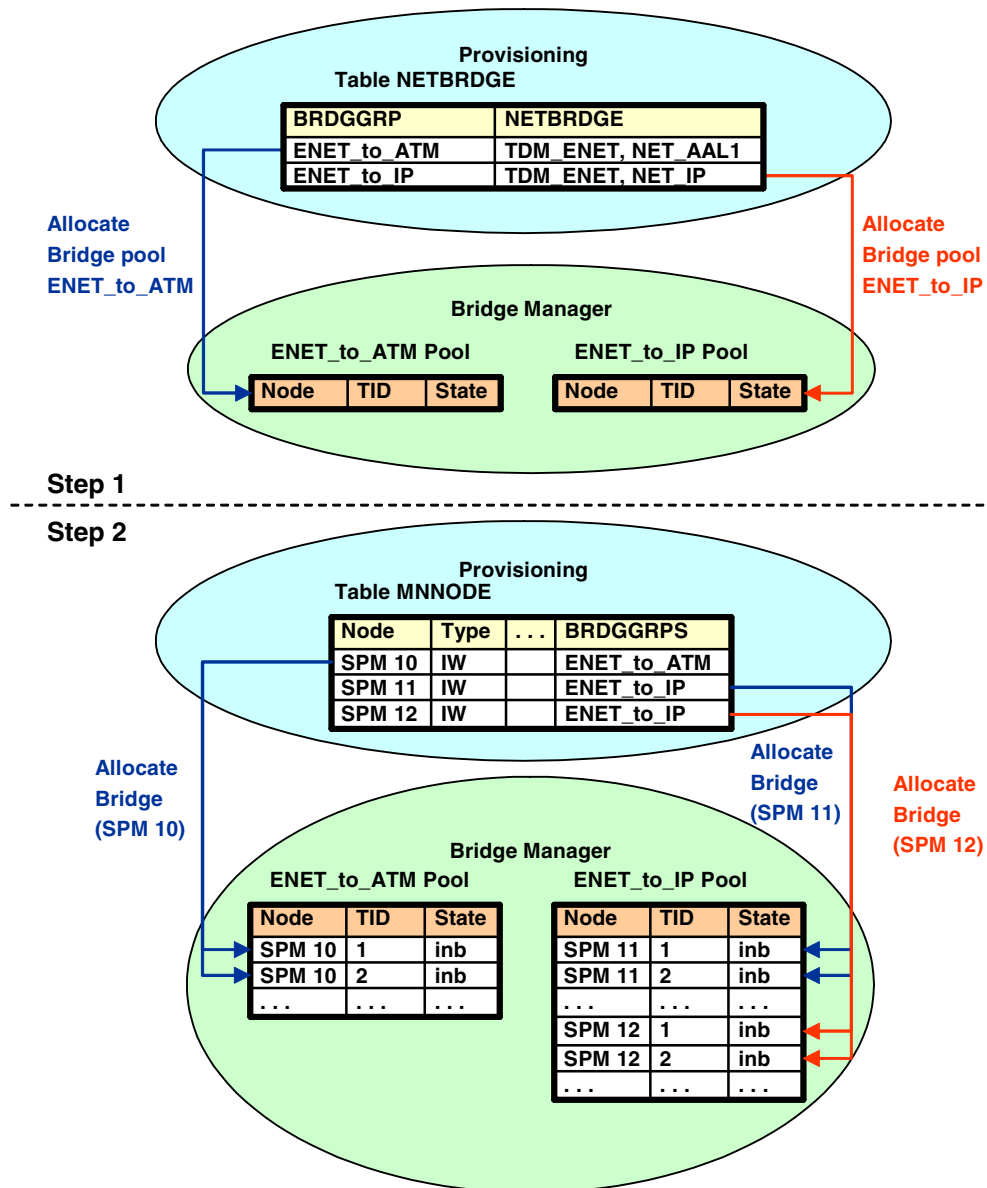
IW Bridge management

IW bridge management is a function in the CS2000 Call Server that manages the pool of IW SPM bridges. Prior to SN07, a single, office-wide pool of available IW bridges was managed by this utility. Each IW bridge node is composed of four groups of 504 bridge endpoints each. When an IW bridge

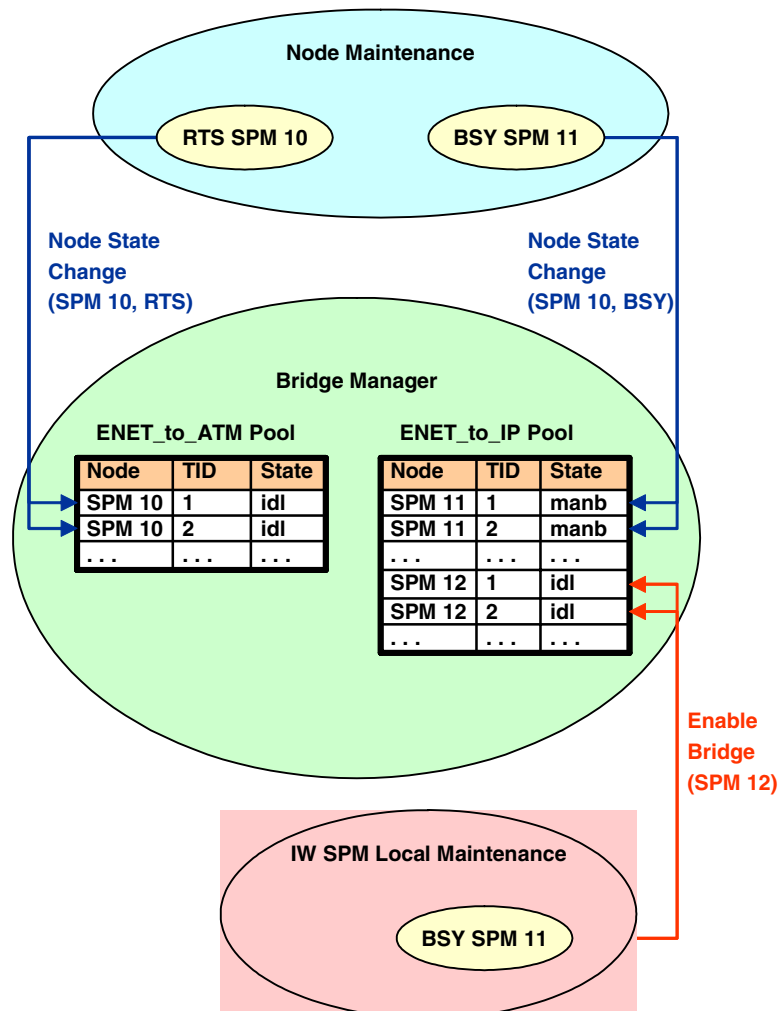
node was provisioned in Table MNNODE, a set of four groups of 504 endpoints were added to the bridge pool. As the group of 504 endpoints was brought into service, these endpoints became available for Core Connectivity to use. The bridge manager function interfaced with maintenance and Core Connectivity to manage the set of available IW bridge endpoints in the office.

In SN07, the office-wide, single bridge pool is changed to support multiple bridge pools in a single CS2000 Call Server. A bridge pool is created when it is datafilled in Table NETBRDGE and the first IW SPM node is defined in that bridge pool in Table MNNODE. Additional individual IW bridge nodes are added (still in the 4 groups of 504 endpoints each) as they are provisioned in Table MNNODE against the newly created bridge pool.

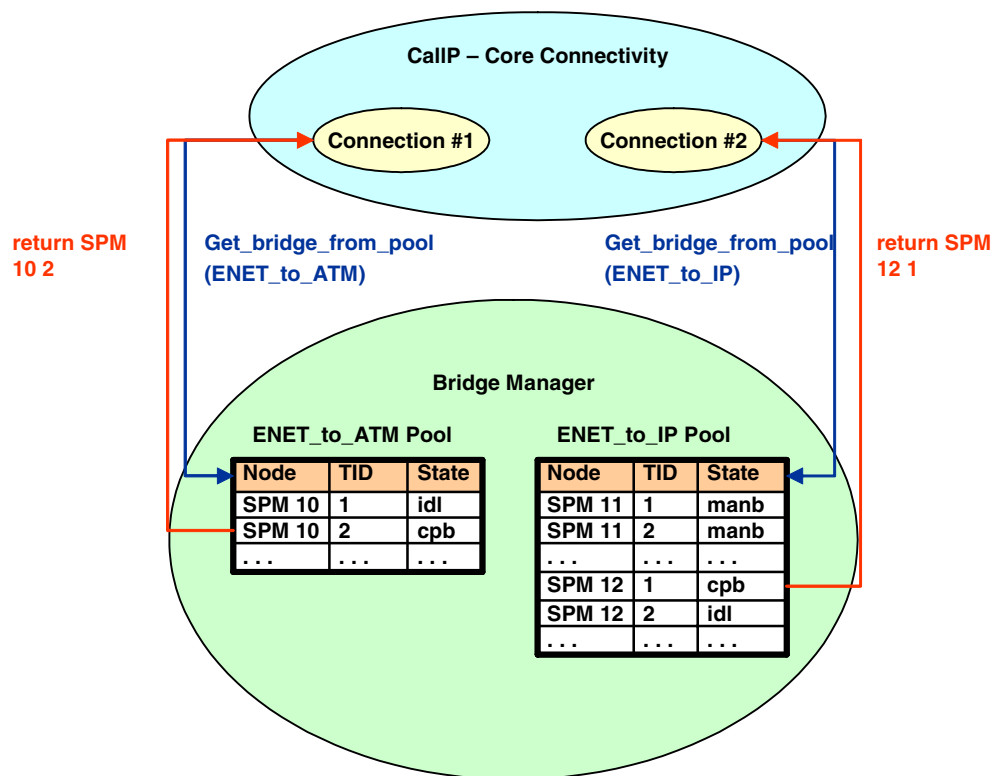
IW bridge pool creation



Once the bridge pools are created through provisioning, the individual IW bridge nodes are brought into service. This causes the nodes in the associated bridge pool to become available for use.

IW bridge maintenance

With idle IW bridge endpoints available in their associated bridge pools, the Bridge Manager can respond to requests from Core Connectivity to get a bridge. If more than one bridge is needed for a connection request, the Core Connectivity makes a request for each bridge needed.

IW bridge request**OAM changes on the CS2000 Call Server**

OAM changes associated with the support of multiple bearer networks are limited in SN07. It is recognized that many additional requirements should be implemented and will be addressed in a future release.

In SN07, this feature does address the following areas:

- IW bridge OAM
- Trunk group OAM
- DPT OAM
- Office-wide usage OAM

Since many of these changes have impacts to customer OSSMINE interfaces, the activation of these changes is controlled by a new office parameter, MULTINET_DISPLAY_ACTIVE. Setting this parameter to 'Y' allows these changes to be visible. Setting this parameter to 'N' hides these changes. Note that this parameter does not impact the ability to support call connections between multiple bearer networks.

IW bridge OAM

In SN07 with the support of multiple bridge pools, changes are made to the IWB 800 series logs. These logs are generated to monitor the usage thresholding of the bridge pools in the office. When office parameter MULTINET_DISPLAY_ACTIVE is set to 'Y', then a new information line is output indicating the associated bridge pool that is causing the generation of the log. Refer to the Fault Management section of the document for more information.

IWB 800 log example

```
RTP7 ** IWB800 SEP17 12:16:55 6600 1st Threshold Exceeded
The number of interworking bridges in use has
exceeded 70 percent of all bridges in the pool.
Total number of IW bridges: 2016
Number of available IW bridges: <NN>
Bridge Pool: <bridge pool CLI from Table NETBRDGE>
```

In addition to the modified IWB 800 logs, the existing OM group IWB is modified to provide a set of registers for each bridge pool that is defined in Table NETBRDGE. In addition to the registers that were present in the OM group prior to SN07, additional call type usage registers are added. IWB contains registers to monitor the following usage information:

- Number of attempts to get a bridge from the associated pool
- Number of failures to get a bridge from the associated pool
- Number of get bridge aborts from the associated pool
- Number of attempts to free a bridge from the associated pool
- Number of failures to free a bridge from the associated pool
- Number of free bridge aborts from the associated pool
- Indicates when the number of 'in use' bridges exceeds 70% of the total bridges in the associated pool
- Indicates when the number of 'in use' bridges exceeds 90% of the total bridges in the associated pool
- Indicates when the number of 'in use' bridges falls below 65% of the total bridges in the associated pool
- Indicates when the number of 'in use' bridges falls below 85% of the total bridges in the associated pool
- Number of times a bridge from the associated pool was used to connect to a test facility

- Number of times a bridge from the associated pool was used to connect to an announcement or conference facility
- Number of times a bridge from the associated pool was used to connect to a line
- Number of times a bridge from the associated pool was used to connect to a trunk

Refer to the Performance Management section of the document for more details.

Note that the value of MULTINET_DISPLAY_ACTIVE office parameter does not impact the availability of this OM group. It is always available in SN07.

Trunk group OAM

With support for multiple bearer networks, a trunk group can be configured to have members in multiple bearer networks. The existing TRK and TRNK2 OM groups only provide data on a per trunk group basis. When office parameter MULTINET_DISPLAY_ACTIVE is set to 'Y', then new OM groups (TRK2NET1 and TRK2NET2) are created to provide a per trunk group and per bearer network view of the trunk group usage.

OM group TRK2NET1 contains the same set of registers that existing OM group TRK contains. It contains registers to monitor the following usage information:

- Automatic congestion control
- Invalid or no automatic number identification (ANI)
- Number of calls answered
- Automatic number identification (ANI) office failure
- Number of successful connections
- Network management reroutes
- Glare
- Answer messages sent and received on incoming trunks
- Answer messages sent and received usage on incoming trunks
- Total incoming attempts
- Incoming failures
- Invalid authorization code
- Maintenance busy usage
- Maximum busy circuits

- Total outgoing attempts
- No answer on trunk (timed out)
- Number of overflows, all trunks busy
- Answer messages sent and received on outgoing trunks
- Outgoing failures
- Outgoing matching failures
- Pre-route abandons
- System busy usage
- Number of tandem calls
- Total usage
- Traffic busy usage

OM group TRK2NET2 contains the same set of registers that existing OM group TRNK2 contains. It contains registers to monitor the following usage information:

- Number of calls answered (extension from TRK2NET1)
- Number of successful connections (extension from TRK2NET1)
- Network management reroutes (extension from TRK2NET1)
- Total incoming attempts (extension from TRK2NET1)
- Total outgoing attempts (extension from TRK2NET1)
- System busy usage (extension from TRK2NET1)
- Number of tandem calls (extension from TRK2NET1)
- Total usage (extension from TRK2NET1)
- Traffic busy usage (extension from TRK2NET1)

DPT OAM

In providing support for multiple bearer networks, a requirement to support both BICC and SIP-T DPT protocols in the same office was also requested. Prior to SN07, the DPT OM groups did not indicate the associated DPT protocol.

In SN07, when office parameter MULTINET_DISPLAY_ACTIVE is set to 'Y', then the following changes are made:

- Provide an office-wide, per-protocol DPT performance summary
- Provide a per-DPT node, per-protocol DPT performance summary

A new OM group (DPTOFCP) is created to provide an office-wide, per-DPT protocol performance summary. This group is modeled after the DPTOFC OM group and contains the same set of registers. Two DPT protocols are supported: BICC and SIP-T. The following registers are included per protocol:

- Get DPT terminal attempts
- Get DPT terminal failures
- Get DPT optimized terminal failures
- DPT terminal usage
- DPT terminal usage high water mark
- DPT port depletion

Changes are made to the existing DPTNODE OM group. This OM group provides a per-DPT node performance summary. In SN07, each DPT node can only support one DPT protocol. For example, a DPT capable MG4K node can only support BICC. DPT GWC nodes can support either BICC or SIP-T but not at the same time. When MULTINET_DISPLAY_ACTIVE is set to 'Y', additional information is added to the DPTNODE OM group to display the following additional information:

- DPT protocol
- For SPM-type nodes, the associated bearer network and SPM node type are also displayed⁴

Office-wide usage OAM

With support for multiple bearer networks, it is a requirement to be able to monitor the performance of the traffic over each bearer network. The existing OFZ and OFZ2 OM groups only provide an office-wide view. When office parameter MULTINET_DISPLAY_ACTIVE is set to 'Y', then new OM groups (OFZ2NET1 and OFZ2NET2) are created to provide a per bearer network view of office traffic.

OM group OFZ2NET1 contains the same set of registers that existing OM group OFZ contains. It contains registers to monitor the following traffic information for each bearer network defined in Table BEARNETS:

- Incoming trunk subscriber abandoned calls
- Incoming trunk switch abandoned calls
- Incoming trunk calls routed to an announcement
- Incoming trunk calls routed to a tone
- Incoming trunk calls to lock-out

4. DPT GWCs are considered bearer independent, so the associated bearer network is not included for DPT GWCs.

- Incoming trunk calls to outgoing trunk calls
- Incoming trunk calls to terminating line calls
- Lines manual busy
- Number of incoming trunk calls
- Number of originating line calls
- Originating line switch abandoned calls
- Originating line calls routed to an announcement
- Originating line calls to lock-out
- Originating line calls to outgoing trunk calls
- Originating line calls routed to a tone
- Originating line calls to terminating line calls
- Outgoing trunk match failures
- Outgoing trunk network attempts
- Outgoing trunk original seize failures
- Outgoing trunk retrial match failures
- Outgoing trunk retrial seize failures
- Terminating line blocked
- Terminating line match failures
- Terminating line network attempts

OM group OFZ2NET2 contains the same set of registers that existing OM group OFZ2 contains. It contains registers to monitor the following traffic information for each bearer network defined in Table BEARNETS:

- No circuits available on business network trunks
- No circuits available on inward dial trunks
- No circuits available on intermachine trunks
- No circuits available on intertoll trunks
- No circuits available on local tandem trunks
- No circuits available on offnet trunks
- No circuits available on connect trunks
- No circuits available on toll completing trunks
- No circuits available on circuit trunks
- No circuits available on all other trunks

- Calls routed to GNCT treatment
- Switch originated partial dial calls
- Switch originated calls to permanent signal treatment

Lawful Intercept

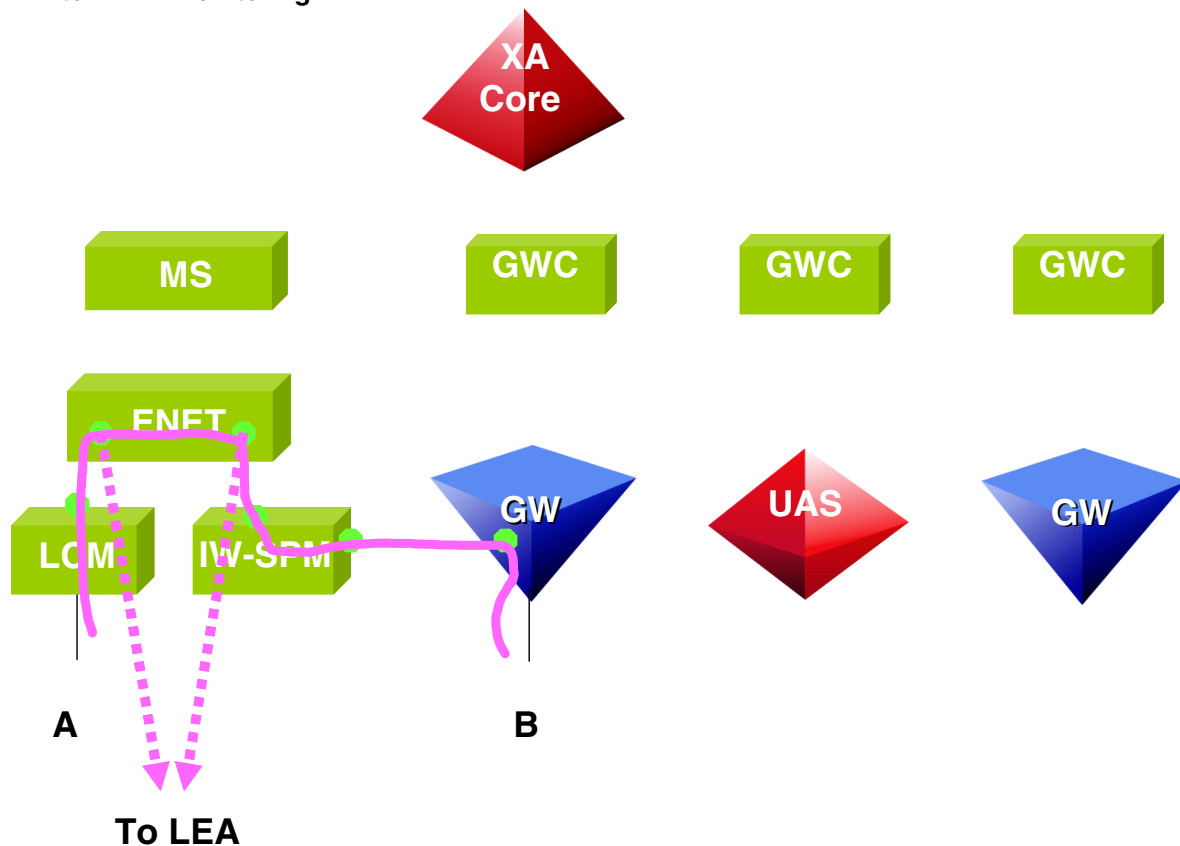
Lawful Interception is the ability to perform call monitoring on selected agents. Call monitoring includes:

- Call Data monitoring - reporting details about monitored calls (e.g. time of the call, dialled digits, parties involved, etc.)
- Call Content monitoring - delivery of both sides of a monitored conversation to law enforcement

With support for multiple bearer network in a single CS2000 Call Server, lawful intercept must provide the ability to do Call Content monitoring on all required call types and all supported bearer connections. Previous to SN07, Call content monitoring was supported for the following call types:

- ENET-to-ENET: replicas are attached to the primary ENET pathends which broadcast the transmit of each endpoint (legacy monitoring)

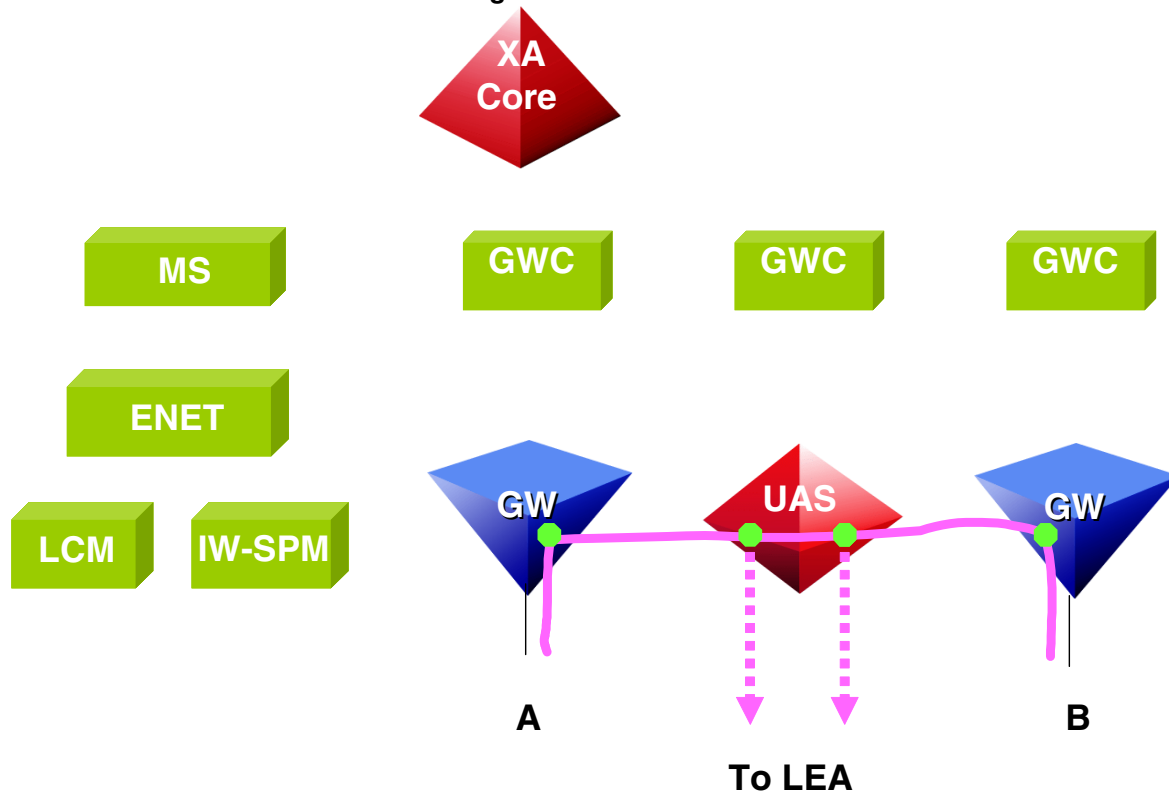
ENET-to-ENET Monitoring



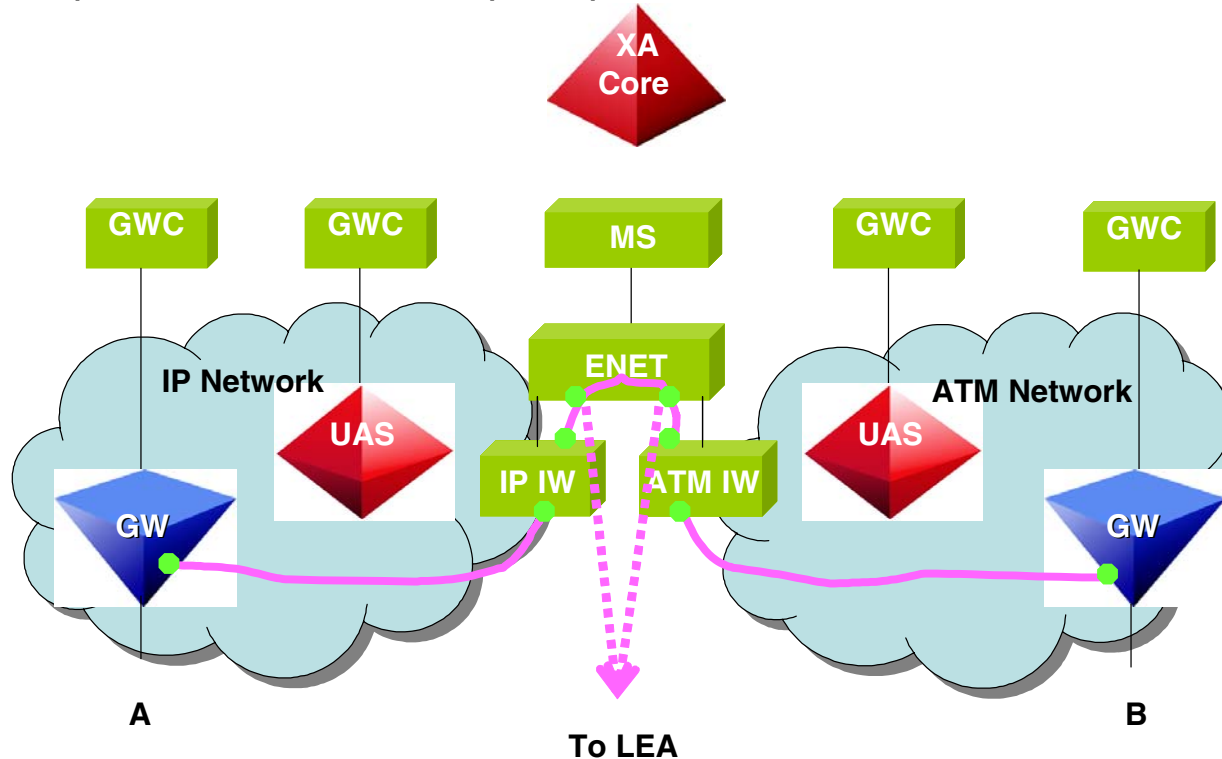
- IP-to-IP: primary call is tandemed through a Centralized Replicator (CR) to which replicas are attached. This functionality is known as Bearer Channel Tandeming (BCT).
- AAL1-to-AAL1: when BCT is active, the same strategy is used as in IP-to-IP calls. If not, then broadcast connections are attempted. This works for Packet Trunking - AAL1 solutions where the only AAL1-to-AAL1 calls involve MG4Ks which support broadcast connections.

- **AAL1-to-AAL1:** when BCT is active, the same strategy is used as in IP-to-IP calls. If not, then broadcast connections are attempted. This works for Packet Trunking - AAL1 solutions where the only AAL1-to-AAL1 calls involve MG4Ks which support broadcast connections.

IP-to-IP or AAL1-to-AAL1 BCT Monitoring



In SN07, there are no impacts to the replication models that are used to lawful intercept. Since the connection model for supporting a packet bearer network 1 to packet bearer network 2 connection involves using 2 IW SPM bridges, lawful intercept will use the ENET-to-ENET model to perform replication. Also, there is no impact to the connections made to the Law Enforcement Agency (LEA). A single interface is supported for all the replication methods. Refer to the following figure for an example connection with lawful intercept.

Multiple bearer network lawful intercept example

In summary, this means that in a CS2000 Call Server that supports three bearer networks (ENET, AAL1 and IP), that the following replication points will be used:

- ENET
 - for ENET-to-ENET calls
 - for AAL1-to-IP calls
 - for ENET-to-AAL1 calls
 - for ENET-to-IP calls
- UAS IP
 - for IP-to-IP calls
- UAS AAL1
 - for AAL1-to-AAL1 calls⁵

Service circuit support

Service circuits include specialized components needed to support the following:

5. If the call involves only 2 MG4Ks, then the UAS is not needed (MG4Ks can broadcast the bearer path). But if an MG9K is involved, then the UAS is required.

- Announcements
- Conferencing
- Line and trunk test facilities

Each Succession configuration provides support for these service circuits in different ways. The following table provides a view of how these components are supported prior to SN07.

Pre-SN07 service circuit support

Succession Configuration	Service Circuit Type	Service Circuit Support
PT-AAL1	announcements	ENET-based MTM
	conferencing	ENET-based MTM
	line/trunk test facilities	ENET-based MTM
UA-AAL1	announcements	ENET-based MTM
	conferencing	ENET-based MTM
	line/trunk test facilities	ENET-based MTM
PT-IP (XA Core)	announcements	ENET-based MTM and/or UAS (IP) ^a
	conferencing	ENET-based MTM and/or UAS (IP) ^b
	line/trunk test facilities	ENET-based MTM
PT-IP (CS2Kc)	announcements	UAS (IP or AAL2)
	conferencing	UAS (IP or AAL2)
	line/trunk test facilities	UAS (IP or AAL2) with Sage box
UA-IP (XA Core)	announcements	ENET-based MTM and/or UAS (IP)
	conferencing	ENET-based MTM and/or UAS (IP)
	line/trunk test facilities	ENET-based MTM
UA -IP (CS2Kc)	announcements	UAS (IP)
	conferencing	UAS (IP)
	trunk test facilities	UAS with Sage box
	line test facilities	AccessCare

a. Directed terminations for announcements is used if both platforms are present. ENET originating agents use the announcements on the MTM and IP originated agents use announcements on the UAS.

b. Directed terminations for conferencing is used if both platforms are present. ENET requesting agents use the conference ports on the MTM and IP requesting agents use conference ports on the UAS.

In SN07, in order to support multiple bearer networks and multiple service circuit platforms, then the director terminations function would have to be changed to take into account multiple packet bearer networks. This work is not being done in SN07. This means that only a single platform for providing announcements, conferencing and test facilities is supported in a multiple packet bearer network configuration. Since full service circuit functionality is provided when using the MTM as the platform, this is the configuration that is supported. This means that all packet bearer networks must allow connectivity to the ENET network in order to obtain announcements, conference ports and test facilities. If this network connectivity is not in place, then services that requires these facilities will fail.

Groups with members in multiple bearer networks

The CS2000 Call Server maintains line group types and trunk group types. These groups are comprised of individual members. Here are some examples of these groups:

- Centrex customer group
- Hunt group
- MADN group
- Trunk group

There is no restriction in place to require that all the members of the line group types be associated with a single bearer network. For example, a hunt group can members in all supported bearer networks. There are connectivity implications to consider in the case. In order to ensure seamless group functionality among all its members, then the associated bearer networks must be able to connect to each other (i.e., Table NET2NET must indicate connectivity between the bearer networks). If connectivity is not fully supported, then some group services may fail.

There is no restriction in place to require that all the members of a trunk group be associated with a single bearer network. Refer to the next section for more details on like network selection for trunk groups.

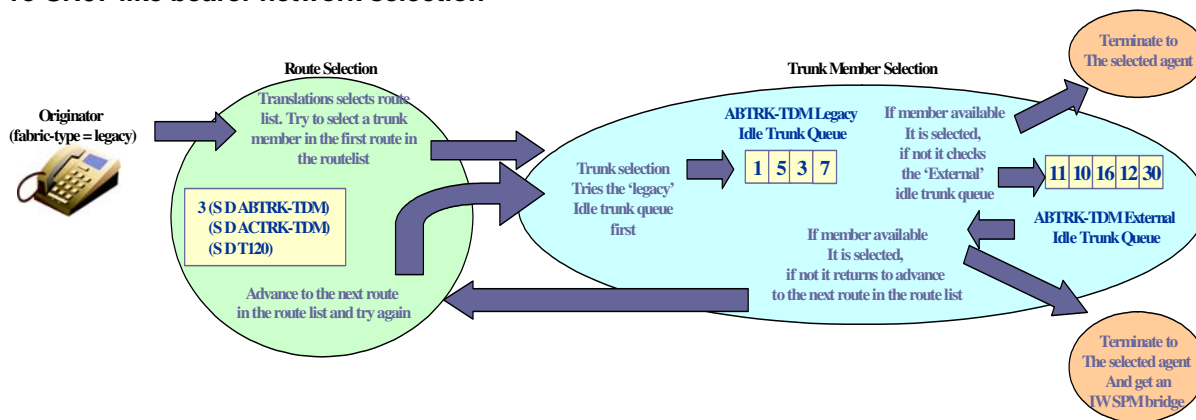
Trunk selection (like network selection)

Prior to SN07, the CS2000 Call Server tried to optimize bearer network connections by trying to select a trunk member whose bearer network matched the bearer network of the originating agent. Since there were only two bearer networks supported ('internal' and 'external'), the trunk selection utility internally maintained an idle trunk queue for each of the two bearer networks. When a request was made to select a trunk member, the trunk selection utility would determine the bearer network of the originating agent and then traverse the 'matching' bearer network's idle trunk queue looking for an available trunk member. If a member was found, it would be selected and returned to CallP

which would then request that a connection be made to that selected member (note that this connection would not require an interworking bridge).

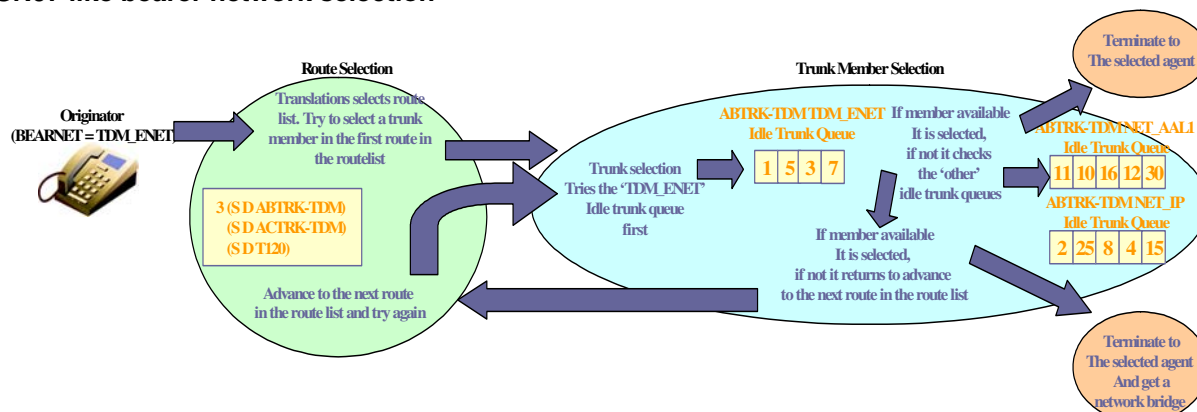
If it did not find a member, it would search the 'other' bearer network's idle trunk queue looking for an available trunk member. If a member was found, it would be selected and returned to CallP which would then request that a connection be made to that selected member (note that this connection would require an interworking bridge). If both queues are checked and no available member can be found, then the request is returned with an indication that the call should advance to the next route in the route list.

Pre-SN07 like bearer network selection



In SN07, the trunk selection utility is changed to support multiple bearer networks (i.e., more than two). When a request was made to select a trunk member, the trunk selection utility determines the bearer network of the originating agent and then traverses the 'matching' bearer network's idle trunk queue looking for an available trunk member. If a member was found, it would be selected and returned to CallP which would then request that a connection be made to that selected member (note that this connection would not require an interworking bridge).

If it did not find a member, it would search the 'next' bearer network's idle trunk queue looking for an available trunk member. The 'next' bearer network is determined by the order that the connecting bearer networks are datafilled in Table NET2NET. If a member was found, it would be selected and returned to CallP which would then request that a connection be made to that selected member (note that this connection would require an interworking bridge). If it did not find a member, it would continue searching its idle trunk queues in the Table NET2NET bearer network order until it either found an available member or exhausted all of its bearer networks. If all bearer networks are exhausted, then the request is returned with an indication that the call should advance to the next route in the route list.

SN07 like bearer network selection

The following is an example trunk selection request.

- Originating agent's bearer network = NET_AAL1
- Table NET2NET datafill
 - NET_AAL1 -> (TDM_ENET 0) (NET_IP 2)
- Terminating trunk group has members in all three bearer networks

The following is the order that the trunk selection utility will try to find an available trunk member:

1. Trunk group members in the NET_AAL1 bearer network
 - This is first because this is the originator's bearer network.
2. Trunk group members in the TDM_ENET bearer network
 - This is second because it is the first entry in Table NET2NET.
3. Trunk group members in the NET_IP bearer network
 - This is third because this is the second entry in Table NET2NET.

DPT (BICC and SIP-T) interworking including audible ringing support

Providing support for both BICC and SIP-T DPT protocols in the same CS2000 Call Server impacts the following areas:

- DPT terminal selection
- DPT audible ringing support

DPT terminal selection

The algorithm for determining which node to host a DPT trunk call differs for BICC and SIP-T. Now that both are supported in the same CS2000 Call Server, this feature must ensure that both function properly.

Changes are needed for the BICC DPT terminal selection algorithms to make sure the bearer network of the hosting DPT capable node matches the bearer network of the DPT trunk group that was selected in translations.

The following table defines the algorithms for each protocol.

DPT protocol algorithms

DPT Protocol	Direction	Algorithm
SIP-T	outgoing	CS2000 Call Server selects the next available GWC node that is provisioned to support SIP-T (Tables SERVRLINV and SERVSINV). Note that the bearer network of the DPT trunk group does not factor into the selection process.
SIP-T	incoming	The VRDN GWC selects the next available GWC node that is provisioned to support SIP-T (Tables SERVRLINV and SERVSINV). The VRDN GWC builds its list of available SIP-T GWCs because the SIP-T GWCs register with it. BICC GWCs do not register with the VRDN GWC.
BICC	outgoing	CS2000 Call Server tries to put the DPT trunk on the most optimized BICC DPT capable node. BICC DPT capable nodes include the following: • BICC GWCs (bearer network independent) • MG4Ks (with an associated bearer network) • DPT SPMs (with an associated bearer network) If the originating agent is on the MG9K, then a BICC GWC is selected. Note that the bearer network of the DPT trunk group does not factor into the selection process because BICC GWCs can support any bearer network. If the originating agent is on the MG4K, then that same MG4K is selected provided the bearer network of the DPT trunk group matches the bearer network of the MG4K. If the bearer network of the DPT trunk group does not match the bearer network of that same MG4K, then terminal selection will try the BICC GWC (since it is bearer network independent) first, then it will try to get another MG4K that does support the DPT trunk group's bearer network. If the originating agent is on a legacy peripheral, then the DPT SPM is selected (if present) provided the bearer network of the DPT trunk group matches the bearer network of the DPT SPM. If the bearer network of the DPT trunk group does not match the bearer network of any DPT SPM in the office, then terminal selection will try the BICC GWC (since it is bearer network independent) first, then it will try to get any MG4K that does support the DPT trunk group's bearer network.

DPT protocol algorithms

DPT Protocol	Direction	Algorithm
BICC	incoming	Prior to SN07, the CS2000 Call Server attempts to initially put the DPT terminal on an MG4K for message normalization and then will move it to the most optimized location based upon what agent the call terminates to. The reason for doing this was to provide a hosting node that had the ability to play tones and collect digits in the case where a service was invoked prior to digit translations and line/trunk termination. In SN07, the CS2000 Call Server continues to place the DPT terminal on an MG4K or DPT SPM for normalization. However, this MG4K/DPT SPM's associated bearer network must now match the bearer network of the incoming BICC DPT trunk group. If no match can be found, then the call is sent to a BICC GWC to be normalized. Note that this leaves no place to support tones and digit collection for those services that may be invoked prior to agent termination. Once the DPT call is normalized, the CS2000 Call Server attempts to optimize the location of the DPT context based on the terminating agent in the call. If the terminating agent is on an MG9K, then the DPT context is moved to a BICC GWC. Note that the bearer network of the BICC DPT trunk group does not factor into the optimization process because BICC GWCs can support any bearer network. If the terminating agent is on an MG4K, then the DPT context will be moved to that MG4K provided the bearer network of the terminating agent's MG4K matches the bearer network of the BICC DPT trunk group. If it does not match, then the DPT context remains where it is (i.e., where it was normalized). If the terminating agent is on a legacy peripheral, then the DPT context will be moved to a DPT SPM (if present) provided the bearer network of the DPT SPM matches the bearer network of the BICC DPT trunk group. If a DPT SPM cannot be found, then the DPT context is moved to a BICC GWC and an IW SPM bridge from the associated bridge pool is used to connect the bearer network of the DPT trunk group and the legacy peripheral. If a BICC GWC is not present, then the call remains where it is (i.e., where it was normalized) and an IW SPM bridge from the associated bridge pool is used.

DPT audible ringing support

The means for providing audible ringing on egress DPT trunk calls differs based upon the DPT protocol being used. Now that both protocols are support in the same CS2000 Call Server, care is taken to ensure that audible ringing functions properly in all scenarios, including bearer network interworking scenarios.

On an incoming DPT SIP-T trunk call where the DPT SIP-T trunk is asked to apply audible ringing, the DPT SIP-T trunk uses Remote Bearer Control (RBC) to ask the originating call server to apply the audible ringing tone on its

behalf. On an incoming DPT BICC trunk, the DPT BICC trunk uses Bearer Channel Proxy - No-Anchor (BCP-NA) to ask the terminating gateway to apply audible ringing back towards the originating call server. The following table illustrates the scenarios and how audible is applied.

DPT audible ringing scenarios

Originating Agent	Terminating DPT Agent	How audible ringing is applied
Line (TDM_ENET)	DPT BICC (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
Trunk (TDM_ENET)	DPT BICC (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
Line (NET_AAL1)	DPT BICC (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
Trunk (NET_AAL1)	DPT BICC (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
Line (NET_IP)	DPT BICC (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
Trunk (NET_IP)	DPT BICC (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
Line (TDM_ENET)	DPT SIP-T (NET_IP)	RBC request may be received. Audible ringing is applied on the IP IW SPM towards the ENET
Trunk (TDM_ENET)	DPT SIP-T (NET_IP)	RBC request may be received. Audible ringing is applied on the IP IW SPM towards the ENET
Line (NET_AAL1)	DPT SIP-T (NET_IP)	RBC request may be received. Audible ringing is applied on the IP IW SPM towards the ENET
Trunk (NET_AAL1)	DPT SIP-T (NET_IP)	RBC request may be received. Audible ringing is applied on the IP IW SPM towards the ENET
Line (NET_IP)	DPT SIP-T (NET_IP)	RBC request may be received. Audible ringing is applied on the Line GW towards the line agent
Trunk (NET_IP)	DPT SIP-T (NET_IP)	RBC request may be received. Audible ringing is applied on the Trunk GW towards the trunk agent
DPT BICC (NET_AAL1)	Line (TDM_ENET)	BCP-NA used to ask the AAL1 IW SPM to apply audible ringing towards the AAL1 network
DPT BICC (NET_AAL1)	Trunk (TDM_ENET)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
DPT BICC (NET_AAL1)	Line (NET_AAL1)	BCP-NA used to ask the MG9K to apply audible ringing towards the AAL1 network
DPT BICC (NET_AAL1)	Trunk (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.

DPT audible ringing scenarios

Originating Agent	Terminating DPT Agent	How audible ringing is applied
DPT BICC (NET_AAL1)	Line (NET_IP)	BCP-NA used to ask the AAL1 IW SPM to apply audible ringing towards the AAL1 network
DPT BICC (NET_AAL1)	Trunk (NET_IP)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
DPT SIP-T (NET_IP)	Line (TDM_ENET)	BCP-NA used to ask the IP IW SPM to apply audible ringing towards the IP network. If it cannot accommodate the request, the RBC is used to ask the originating call server to play audible ringing.
DPT SIP-T (NET_IP)	Trunk (TDM_ENET)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
DPT SIP-T (NET_IP)	Line (NET_AAL1)	BCP-NA used to ask the IP IW SPM to apply audible ringing towards the IP network. If it cannot accommodate the request, the RBC is used to ask the originating call server to play audible ringing.
DPT SIP-T (NET_IP)	Trunk (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
DPT SIP-T (NET_IP)	Line (NET_IP)	BCP-NA used to ask the line gateway to apply audible ringing towards the IP network. If it cannot accommodate the request, the RBC is used to ask the originating call server to play audible ringing.
DPT SIP-T (NET_IP)	Trunk (NET_IP)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.
DPT BICC (NET_AAL1)	DPT SIP-T (NET_IP)	RBC request may be received. Audible ringing is applied on the IP IW SPM towards the ENET
DPT SIP-T (NET_IP)	DPT BICC (NET_AAL1)	Not in the CS2000 Call Server. Audible ringing is applied in the next call server.

Translations and Routing changes

With support for multiple bearer networks, there is an assumption that calls should remain on the same bearer network as much as possible. Given this assumption, the following changes are made in SN07:

- Routing based upon the bearer network
- TRAVER modifications to support multiple bearer networks

Routing based upon the bearer network

Prior to SN07, the PKT conditional route selector allowed the customer to force routing between the ENET and the packet bearer network. In SN07, this selector is replaced by two new conditional route selectors:

- FABRIC

- BEARNET

The FABRIC conditional route selector replaces the PKT conditional route selector. During translations and routing, the fabric of the originating agent's bearer network is examined and determines the next route in the route list. This allows the customer to explicitly keep a call on a particular bearer network fabric. During the ONP to SN07, the FABRIC selector replaces any PKT selectors found.

The BEARNET conditional route selector is new in SN07. During translations and routing, the originating agent's bearer network is examined and determines the next route in the route list. This allows the customer to explicitly keep a call on a particular bearer network.

Refer to the Configuration section of the document for additional information.

Conditional routing example datafill

TABLE: OFRT

```
-----
100 (CND FABRIC ENET ST 200) (CND FABRIC AAL1 ST 201)
    (CND FABRIC IP ST 202) $
101 (CND BEARNET TDM_ENET ST 200) (CND BEARNET NET_AAL1 ST 201)
    (CND BEARNET NET_IP ST 202) $
```

TRAVER modifications to support multiple bearer networks

In order to support the new conditional route selectors described above, changes are needed in TRAVER to provide the correct route selection. In SN07, TRAVER needs to determine either the fabric or the bearer network of the originating agent.

If the originating agent is a line, then TRAVER will identify the fabric or bearer network and apply that knowledge to any FABRIC or BEARNET conditional route selectors that it finds.

If the originating agent is a trunk group, then TRAVER cannot automatically identify the fabric or the bearer network information. This is because this designation is not made at the trunk group level but is made at trunk member level. Therefore, changes are made to TRAVER to allow either a trunk member to be specified explicitly or to specify the bearer network to use for the originating trunk group. The existing TRAVER option TRKMEM is modified to include the determination of the associated bearer network. A new option, BEARNET, is added to support the bearer network designation for a trunk group⁶.

Refer to the Configuration section of the document for additional information.

6. TRAVER determines the fabric based upon the associated bearer network.

USP messaging

In SN07, the USP is an optional component. When it is present, it provides the connection from the CS2000 Call Server to the SS7 network. ISUP signaling messages and TCAP transaction messages traverse through the USP interface.

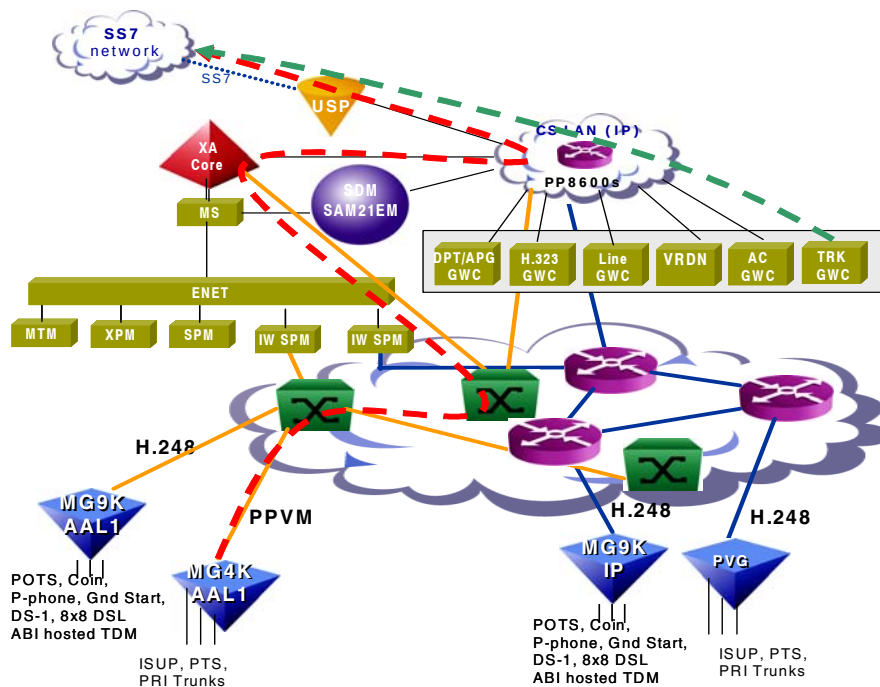
TCAP transaction messages are always generated by the CS2000 Call Server. However, ISUP signaling messages are generated from the ISUP trunk peripherals. The path that the ISUP message takes to get to the USP varies based upon the type of trunk peripheral.

USP messaging path for ISUP signaling messages

ISUP trunk peripheral	USP messaging path
GWC	GWC -> CS LAN -> USP
MG4K (AAL1)	MG4K -> AAL1 bearer network -> CS2000 -> CS LAN -> USP
DPT SPM (AAL1)	DPT SPM -> CS2000 -> CS LAN -> USP
legacy peripheral	Legacy peripheral -> CS2000 -> CS LAN -> USP

The USP supports multiple messaging paths and defines them on a per node basis.

USP messaging paths



ECAN across multiple bearer networks

Echo cancellation (ECAN) can be applied differently in each bearer network. In an IP bearer network, the packet latency is generally large enough to require 100% ECAN. ECAN is only turned off if an individual call requires that it be turned off (i.e., FAX call).

In an AAL1 bearer network, the packet latency may not be large enough to require ECAN. ECAN in the AAL1 network is generally expensive hardware to purchase and would like to be avoided, if possible. The existing office parameter, ECAN_EDGE_STRATEGY, determines the ECAN strategy used for the AAL1 networks.

Refer to feature A00004046: Echo Cancellation Support for TriModal Call Server 2000 for more information on ECAN.

Voice quality

In supporting the connections between packet bearer networks using multiple IW bridges, the voice quality may experience some degradation. The area of concern is in packet latency and delay.

Latency and delay are concerned with how long it takes for a packet of voice to transit the bearer network(s) from end to end. Generally, there is a budget of 150 ms given to a packet. If the delay increases past 150 ms, then the possibility of the end subscribers talking over top of each other increases. The following factors effect the latency and delay that a packet experiences:

- packetization rate and jitter buffer
- transcoding delay
- ECAN
- IP routers
- overall distance travelled

The following tables provides a few examples of latency.

MG9K IP to MG9K AAL1 call analysis

MG9K IP to MG9K AAL1 call analysis	10 ms packetization	20 ms packetization
MG9K IP packetization	10	20
Leg 3 router hops, assume 3 routers	3	3
IP IW SPM jitter buffer	30	60
ENET	1	1
AAL1 IW packetization	6	6

MG9K IP to MG9K AAL1 call analysis

MG9K IP to MG9K AAL1 call analysis	10 ms packetization	20 ms packetization
MG9K AAL1 jitter buffer	2	2
Total latency	52	92

H.323 to MG9K call analysis

H.323 to MG9K AAL1 call analysis	10 ms packetization	20 ms packetization
H.323 packetization	10	20
Leg 1 router hops (1 ms per router) assume worst case, 5 routers	5	5
Media Portal (1 ms assumed)	1	1
Leg 2 router hops, assume 1 router	1	1
PVG jitter buffer (3 x packetization rate)	30	60
PVG transcoding (G.729 to TDM)	5	5
PVG packetization	10	20
Leg 3 router hops, assume 3 routers	3	3
IP IW SPM jitter buffer	30	60
ENET	1	1
AAL1 IW packetization	6	6
MG9K AAL1 jitter buffer	2	2
Total latency	104	184

ONP

Due to the nature of the changes made to the connectivity function in the CS2000 Call Server, they are applicable to all Succession configurations in SN07, regardless of how many bearer networks are supported. In order to preserve call processing over the ONP, the provisioning of Tables BEARNETS, NETBRIDGE, NETPATH and NET2NET must be accomplished during the table transfer.

Refer to the Configuration section for more details on the ONP procedures.

Capacity

In general, there are no changes to the capacity parameters for a CS2000 Call Server that supports multiple bearer networks. The total number of endpoints (i.e., lines and trunks) supported remains unchanged. The BHCA capacity of the call server remains unchanged.

The only capacity change is the number of IW SPM bridge nodes supported in a single office. Prior to SN07, there was a limit of 14 IW SPM bridge nodes supported in an office. In SN07, this limit is removed. The limitation that the CS2000 Call Server can support only 78 SPM nodes of any type is the only remaining capacity limitation for IW SPM nodes. In other words, all the SPM nodes in the office must sum to less than (or equal to) 78 nodes. This includes all the legacy SPMs, MG4Ks, DPT SPMs and IW SPMs in the office.

Hardware Requirements or Dependencies

In SN07, the following gateways and packet agents are supported in the multi-bearer network configuration.

Gateways and packet agents supported in SN07

Bearer Network	Gateway	Agents
ENET	None ^a	supported SN07 legacy peripherals which includes both lines and trunk
ATM AAL1 (UA)	MG4000	ISUP trunks PTS trunks PRI trunks BICC DPT trunks
	GWC ^b	BICC DPT trunks
	MG9000	POTS lines Pphone lines Coin lines Ground Start lines
	MG9000 with ABI	supported SN07 ABI peripherals which includes both lines and trunk
	DPT SPM	BICC DPT trunks

Gateways and packet agents supported in SN07

Bearer Network	Gateway	Agents
IP (UA)	PVG (for loop-around trunk access only for support of H.323)	ISUP trunks PRI trunks
	MG9000	POTS lines Pphone lines Coin lines Ground Start lines
	MG9000 with ABI	supported SN07 ABI peripherals which includes both lines and trunk
IP (CHS)	PVG (for loop-around trunk access only for support of H.323)	ISUP trunks PRI trunks
	GWC ^c	SIP-T DPT trunks
	H.323 GWs (Cisco, Westel, BCM, M1)	PRI trunks

a. There are no 'gateways' support on the ENET. However, there is a list of supported legacy peripherals for Succession Call Servers. This list remains unchanged by this feature.

b. Not a true bearer gateway. This is included to illustrate the support for BICC DPT trunk support.

c. Not a true bearer gateway. This is included to illustrate the support for SIP-T DPT trunk support.

Software Requirements or Dependencies

This feature requires SN07 North America XA-CORE load or later.

Limitations and restrictions

In SN07, only one bearer network entry will be supported in table SERVINV and it will be restricted to the default network because SESM will only support a single bearer network per GWC.

In SN07, an IW bridge will be restricted to a single bridge pool.

In SN07, only one bearer network entry will be supported for DPT SPM and it will be required to be the default network.

In SN07, only one bearer network entry will be supported for MG4K and it will be required to be the default network.

In SN07, the DPT trunk groups datafilled in table TRKOPTS will be restricted to a single network protocol.

In SN07, networks must be configured with full inter-connectivity in table NET2NET.

Customer groups may contain agents from various bearer networks, but all agents within a customer group must be fully inter-connected via NET2NET.

The maximum size of the table BEARNETS will be 8 tuples.

The maximum size of the table NETBRDGE shall be 64 tuples.

The following list provides a view of the limitations associated with H.323 calls in this configuration:

- Multiple billing records generated - A call from an H.323 agent to an MG9000 AAL1 native line would be represented as two calls in the CS2000 call server, each generating its own billing record.
- H.323 agent access to announcements - Since there is no announcements accessible to the CHS IP network (i.e., no IP IW bridge supported), announcements cannot be played to the H.323 agent. Any CS2000 Call Server services will not be able to use announcements and any treatments will have to be configured to 'release with cause' and the announcement would be provided by the enterprise bearer network.
- H.323 agent access to conferencing - Since there is no conference circuits accessible to the CHS IP network (i.e., no IP IW bridge supported), conferencing services cannot be supported to the H.323 agent.
- H.323 agent access to test trunk facilities - Since there is no test trunk circuits accessible to the CHS IP network (i.e., no IP IW bridge supported), trunk tests cannot be supported to the H.323 gateway.

In a multiple packet bearer network configuration, it is expected that the service circuits (i.e., announcements, conference ports and test facilities) be accessed on the MTM (via the ENET).

E911 is a regulatory service that requires all lines to have access to a PSAP. This feature introduces a means to block connectivity between agents that are on different bearer networks. Care should be taken when engineering the office to ensure that all lines have connectivity access to an E911 PSAP. Line PSAPs are not supported.

Operator services is a regulatory service that requires all lines to have access to an operator. This feature introduces a means to block connectivity between agents that are on different bearer networks. Care should be taken when

engineering the office to ensure that all lines have connectivity access to operator services access points.

Hyper-PRI is not supported for packet-based agents. Multiple fabrics are not supported within a PRI group.

SIP-T is supported on a single IP network only, as the APG resource selection is not supported across multiple bearer fabrics.

This feature does not support in-service line/trunk migrations or cutovers from one bearer network to another bearer network.

This feature does not support in-service node migrations or cutovers from one bearer network to another bearer network.

Interactions

N/A

Applicable customer facing sections

Fault Management

Logs ☒ X ☐

Alarms ☐

Configuration

Data Schema ☒ X ☐

User Interface ☒ X ☐

Element Management ☒ X ☐

Security ☐

Service Order ☐ n/a ☐

Office Parameters ☒ X ☐

Accounting (includes AMA billing) ☐ n/a ☐

Performance (includes operational measurements) ☒ X ☐

Indicate with an X if you are completing the sections of the DDOC listed below. Indicate with "N/A" if these sections do not apply to this functionality.

Real-time ☒ X ☐

Engineering Information ☒ X ☐

Glossary

Term	Explanation
AAL1	ATM Adaptation Layer 1
AAL2	ATM Adaptation Layer 2
ABI	Access Bridging Interface
ATM	Asynchronous Transfer Mode
BICC	Bearer Independent Call Control
CODEC	Coder DECoder
CS2K	Call Server 2000
CS2K - MT	Communication Server 20000 Management Tool
DPT	Dynamic Packet Trunk
DPT-SPM	Interworking SPM (ENET interface on the c-side, packet network on the p-side)
ECAN	Echo Cancellation
ENET	Enhanced Network
GUI	Graphic User Interface
GW	GateWay
GWC	GateWay Controller
GWC-EM	Gateway Controller Element Manager
H.323	ITU-T "umbrella" standard for multimedia communications.
IDL	Interface Definition Language
IP	Internet Protocol
IW	Interworking
IW-SPM	Interworking SPM (ENET interface on c-side, packet network on p-side)
JNET	Junctored Network
LGRP	Logical Group
MG4K	Media Gateway 4000 - SPM capable of supporting TDM trunks and DPTs. External network only, no ENET.
MSH	Multi-Service Hub Layer
NA	North America

NV	Network View
OSSDI	Operations Support System DAta Interface
SESM	Succession Element Sub-element Manager
SHR	SHaRed Layer
SIP-T	Session Initiated Protocol - Trunking
SMG4	SPM Media Gateway 4000
SNMP	Simple Network Management Protocol
SPM	Spectrum Peripheral Module
TDM	Time Division Multiplexing
TL	Telecom Layer
TRKOPTS	TRunK OPTionS

Fault Management for A00003487

Fault management strategy

Fault management tools and utilities

Logs IWBm 800

Explanation

Log Title: IWBm 800

Name: Interworking Bridge Manager Pool Logs

Description: Log report IWBm800 indicates that the number of available IW bridges exceeds the first threshold (70%) when attempting to retrieve an IW-bridge ID from the IW bridge manager.

Event type: Unchanged

Format

Since it is possible to have multiple IW bridge pools in a single call server, a new line of information is included in the IWBm800 log. This new information is only visible when the Office Parameter

MULTINET_DISPLAY_ACTIVE is set to 'Y'. This thresholding log will be monitored and generated for each bridge pool defined in Table NETBRDGE.

Enhanced IWBm 800 Log

RTP7 ** IWBm800 SEP17 12:16:55 6600 1st Threshold Exceeded
The number of interworking bridges in use has exceeded 70 percent of all bridges in the pool.
Total number of IW bridges: 2016
Number of available IW bridges: <NN>
Bridge Pool: <bridge pool CLI from Table NETBRDGE>

Field descriptions

Field descriptions

Field	Value	Description
Number of available IW bridges	unchanged	unchanged
Bridge Pool	CLI	Bridge pool name as datafilled in Tale NETBRDGE

Action

This log report requires no action.

Associated Operational Measurements or Performance Measurements

New OM group IWBmNODE can be used to determine individual IW bridge node usage. To determine bridge pool usage, the per-node usage counts would have to be summed.

Additional information

This log report requires no additional information.

Logs IWBm 801

Explanation

Log Title: IWBm 801

Name: Interworking Bridge Manager Pool Logs

Description: Log report IWB801 indicates that the number of available IW bridges falls to less than 65% of bridges in the pool in use. This log always occurs after IWB800.

Event type: Unchanged

Format

Since it is possible to have multiple IW bridge pools in a single call server, a new line of information is included in the IWB801 log. This new information is only visible when the Office Parameter MULTINET_DISPLAY_ACTIVE is set to 'Y'. This thresholding log will be monitored and generated for each bridge pool defined in Table NETBRIDGE.

Enhanced IWB 801 Log

```
RTP7 ** IWB801 SEP17 12:16:55 6600 1st Threshold Cleared
The number of interworking bridges in use has
fallen below 65 percent of all bridges in the pool.
Total number of IW bridges: 2016
Number of available IW bridges: <NN>
Bridge Pool: <bridge pool CLI from Table NETBRIDGE>
```

Field descriptions

Field descriptions

Field	Value	Description
Number of available IW bridges	unchanged	unchanged
Bridge Pool	CLI	Bridge pool name as datafilled in Tale NETBRIDGE

Action

This log report requires no action.

Associated Operational Measurements or Performance Measurements

New OM group IWB801 can be used to determine individual IW bridge node usage. To determine bridge pool usage, the per-node usage counts would have to be summed.

Additional information

This log report requires no additional information.

Logs IWBm 802

Explanation

Log Title: IWBm 802

Name: Interworking Bridge Manager Pool Logs

Description: Log report IWBm802 indicates that the number of available IW bridges exceeds the second threshold (90%) when attempting to retrieve an IW-bridge ID from the IW bridge manager.

Event type: Unchanged

Format

Since it is possible to have multiple IW bridge pools in a single call server, a new line of information is included in the IWBm802 log. This new information is only visible when the Office Parameter MULTINET_DISPLAY_ACTIVE is set to 'Y'. This thresholding log will be monitored and generated for each bridge pool defined in Table NETBRDGE.

Enhanced IWBm 802 Log

```
RTP7 ** IWBm802 SEP17 12:16:55 6600 2nd Threshold Exceeded
The number of interworking bridges in use has
exceeded 90percent of all bridges in the pool.
Total number of IW bridges: 2016
Number of available IW bridges: <NN>
Bridge Pool: <bridge pool CLI from Table NETBRDGE>
```

Field descriptions

Field descriptions

Field	Value	Description
Number of available IW bridges	unchanged	unchanged
Bridge Pool	CLI	Bridge pool name as datafilled in Tale NETBRDGE

Action

This log report requires no action.

Associated Operational Measurements or Performance Measurements

New OM group IWBMMNODE can be used to determine individual IW bridge node usage. To determine bridge pool usage, the per-node usage counts would have to be summed.

Additional information

This log report requires no additional information.

Logs IWBMM 803

Explanation

Log Title: IWBMM 803

Name: Interworking Bridge Manager Pool Logs

Description: Log report IWBMM803 indicates that the number of available IW bridges falls to less than 85% of bridges in the pool in use. This log always occurs after IWBMM802.

Event type: Unchanged

Format

Since it is possible to have multiple IW bridge pools in a single call server, a new line of information is included in the IWBMM803 log. This new information is only visible when the Office Parameter MULTINET_DISPLAY_ACTIVE is set to 'Y'. This thresholding log will be monitored and generated for each bridge pool defined in Table NETBRIDGE.

Enhanced IWBMM 803 Log

```
RTP7 ** IWBMM803 SEP17 12:16:55 6600 2nd Threshold Cleared
The number of interworking bridges in use has
fallen below 85 percent of all bridges in the pool.
Total number of IW bridges: 2016
Number of available IW bridges: <NN>
Bridge Pool: <bridge pool CLI from Table NETBRIDGE>
```

Field descriptions

Field descriptions

Field	Value	Description
Number of available IW bridges	unchanged	unchanged
Bridge Pool	CLLI	Bridge pool name as datafilled in Tale NETBRDGE

Action

This log report requires no action.

Associated Operational Measurements or Performance Measurements

New OM group IWBMNODE can be used to determine individual IW bridge node usage. To determine bridge pool usage, the per-node usage counts would have to be summed.

Additional information

This log report requires no additional information.

XNET 600 Series logs (new)

The XNET 600 series logs provide information on external packet network bearer connection problems. Three new logs are created:

XNET605

Explanation

Bearer Networks Cannot connect

This log indicates that the bearer networks of the two parties in a connection attempt are not permitted to inter-connect, based on datafill in table NET2NET.

Format

XNET605 Log Example

```
RTP7  XNET605 MAY17 12:16:55 9600 INFO Bearer Networks Cannot Connect
From Agent          : VOIP 42 2 04 00   DN 6137204200
From Bearer Network: IP_PRIMARY
To   Bearer Network: AAL1_SECONDARY
Bearer Network Translations resulted in no interconnect
Check Table NET2NET, NETPATH and NETBRDGE
```

Field descriptions

The 'From Agent' line indicates the source party of the connection request. This can be in many forms:

- a LEN and DN,
- a Trunk Group name and member number
- a PM type and PM number,
- a Node number and TID (terminal id) when an appropriate device type and device id cannot be determined
- or an "Unavailable" indication when the connection source was an ENET hosted party, but that party can no longer be determined.

The 'From Bearer Network' line indicates the bearer network name, as datafilled in table BEARNETS, of the source party. The 'To Bearer Network' line indicates the bearer network name, as datafilled in table BEARNETS, of the connection destination party.

Action

The telco should determine whether the identified bearer networks are permitted to interconnect. If so, the appropriate datafill should be added to tables NET2NET, and if necessary NETPATH and NETBRDGE. If the bearer networks are not permitted to connect, the telco can:

- a. if possible, change DN translations so that the originator can no longer dial the terminator, but will receive a treatment of some type,
- b. use the EXTLOGCI command to disable the XNET605 log
- c. use LOGUTIL to SUPPRESS the XNET 605 log
- d. do nothing, the log will continue to print when two parties on the specified bearer networks attempt to dial one another.

Associated Operational Measurements or Performance Measurements

Additional Information

XNET606

Explanation

XNET606 - PKT Pathend Has NIL Bearer Net ID

This log indicates a software or provisioning problem in the switch, in that an appropriate bearer network could not be determined through provisioned data for a particular party in a connection attempt.

Format

XNET 606 Log Example

```
RTP7 XNET606 MAY17 12:16:55 9600 INFO PKT Pathend Has NIL Bearer Net ID
Path - Node: LGRP 07 Tid: 124
Agent - VOIP 42 2 04 00 DN 6137204200
Contact Product Support
```

Field descriptions

- The 'Path' line indicates the node at the network connection point, this can be in two forms:
 - a PM name and number, and a channel or TID id,
 - a node number, and a channel or TID id, when the PM name and number cannot be determined from the node number

The 'Agent' line identifies the suspect party, this can be in several forms:

- a LEN and DN,
- a Trunk Group name and member number
- or a Node number and TID (terminal id) when an appropriate device type and device id cannot be determined

Action

The telco should report this log to appropriate Nortel Product Support.

Associated Operational Measurements or Performance Measurements

Additional Information

The telco can:

- use the EXTLOGCI command to disable the XNET606 log
- use LOGUTIL to SUPPRESS the XNET 605 log
- do nothing, the log will continue to print when the suspect party attempts to place calls

XNET607

Explanation

XNET607 - IW Bridge Not Available

This log indicates that an IW SPM interworking bridge was not available for the connection request, either because

- of a bridge exhaust condition on one of the bridge pools involved in the connection request,
- bridges are not inservice, or provisioned for one of the bridge pools involved with the connection request

Format

XNET 607 Log Example

```
RTP7  XNET607 MAY17 12:16:55 9600 INFO IW Bridge Not Available
      Bridge Pool    : ENET_TO_IP
      From Agent     : VOIP 42 2 04 00    DN 6137204200
      From Bearer Network: IP_PRIMARY
      To    Bearer Network: AAL1_SECONDARY
```

Field descriptions

The 'Bridge Pool' line indicates the name of the bridge pool, as specified in table NETBRDGE, that has the 'trouble' condition. The 'From Agent' line indicates the source party of the connection request. This can be in many forms:

- a LEN and DN,
- a Trunk Group name and member number
- a PM type and PM number,

- a Node number and TID (terminal id) when an appropriate device type and device id cannot be determined
- or an “Unavailable” indication when the connection source was an ENET hosted party, but that party can no longer be determined.

The ‘From Bearer Network’ line indicates the bearer network name, as datafilled in table BEARNETS, of the source party. The ‘To Bearer Network’ line indicates the bearer network name, as datafilled in table BEARNETS, of the connection destination party.

Action

The telco can:

- check for IWB602 logs indicating a bridge exhaust condition,
- verify that the bridge pool identified in the log is provisioned on an SPM in table MNODE,
- verify that the bridges in the bridge pool identified in the log are in-service.
- use the EXTLOGCI command to disable the XNET607 log
- use LOGUTIL to SUPPRESS the XNET 607 log

Associated Operational Measurements or Performance Measurements

Additional Information

EXTLOGCI Tool

The EXTLOGCI tool is an existing CI command that controls the XNET series of logs. By using the ENABLE and DISABLE commands, the user can control the production of XNET logs. The XNET 605, 606 and 607 logs are automatically enabled on all restarts.

Related documentation

N/A

Configuration for A00003487

Hardware and Software Requirements

Hardware

No additional hardware is required in order to upgrade to a load capable of supporting multiple packet networks (support limited to IP interworking with AAL1 for SN07). All existing TDM/Packet configurations will continue to be supported, including:

- UA-AAL1

- PT-AAL1
- Ultralite AAL1
- UA-IP
- PT-IP
- PT-IP Compact (includes AAL2 via the PVG)
- AAL2 Wireless

In addition, the following new office configuration is supported:

- UA-AAL1/IP

New hardware will be required for the addition of the second packet network.

Software

The software reconfiguration to use the new networking tables (BEARNETS, NETBRIDGE, NETPATH, NET2NET) will occur automatically to include default datafill dictated by the value of a new office parameter. This parameter, PRE_SN07_DUMPSIDE_PACKET_FABRIC, must be set by the engineering team and applied to the office prior to the table transfer.

SESM will align with the standard SESM requirements.

In order to provision a second packet network, the customer will have to provision the new network, any bridging resources for that network, and the connectivity supported between the networks via the bridging resource paths.

Initial Configuration.

Office parameters

NETWORK_ACTIVE

The network_active office parameter will be set to EXTENET when upgraded to the SN07 Succession load, even if it had been previously set to ENET.

If it had been set to JNET, the value will remain as JNET. In these offices, there will be no default network datafill in the new network tables.

Note: If the value of the network_active office parameter is set to JNET, the packet connectivity function is not available.

PRE_SN07_DUMPSIDE_PACKET_FABRIC

Will be set to one of {UNDEF⁷, NONE, AAL1, AAL2, IP}. Once the ONP is complete, there is no need to change this office parameter.

7. Should be set to something other than UNDEF by the engineering team prior to table transfer. UNDEF will be an error condition if the network_active = EXTENET.

MULTINET_DISPLAY_ACTIVE = 'N'

The display control for the new OMs and Logs introduced by this activity is initially off.

New Network Tables - initial datafill

The examples that follow are the default tuples that will be in the new network tables after the ONP is complete. Note that the initial value of the NET 1 FABRIC field will be determined by the new office parameter PRE_SN07_DUMPSIDE_PACKET_FABRIC.

The following examples show the post TABXFER views of the new table data for the various “from” office network configurations.

JNET only on from side (JNET)

TABLE BEARNETS:				
NETIDX	NETNAME	DISPLAY	FABRIC	OPTIONS

TABLE CLLI:				
CLLI	ADNUM	TRKGRSIZ	ADMININF	

TABLE NETBRDGE				
BRDGCLLI	BRDGTYPE	DISPLAY	ADMININF	

TABLE NETPATH				
PATHIDX	NETPATH			

TABLE NET2NET				
BNETNAME	CONNNETS			

Note: If JNET, then the network_active = JNET, and packet networks are not supported at all.				

ENET only on from side (ENET)

TABLE BEARNETS:				
NETIDX	NETNAME	DISPLAY	FABRIC	OPTIONS

NET 0	TDM_ENET	ENET	ENET	\$
TABLE CLLI:				
CLLI	ADNUM	TRKGRSIZ	ADMININF	

TABLE NETBRDGE				
BRDGCLLI	BRDGTYPE	DISPLAY	ADMININF	

TABLE NETPATH				
PATHIDX	NETPATH			

0	\$			
TABLE NET2NET				
BNETNAME	CONNNETS			

TDM_ENET	\$			

ENET & AAL1 on from side (UA-AAL1 & PT-AAL1)

TABLE BEARNETS:				
NETIDX	NETNAME	DISPLAY	FABRIC	OPTIONS

NET 0	TDM_ENET	ENET	ENET	\$
NET 1	NET_AAL1	ATM	AAL1	(PACKET_NETWORK_DEFAULT) \$
TABLE CLLI:				
CLLI	ADNUM	TRKGRSIZ	ADMININF	

ENET_TO_AAL1	725	0	ENET_TO_AAL1_BRIDGE_POOL	
TABLE NETBRDGE				
BRDGCLLI	BRDGTYPE	DISPLAY	ADMININF	

ENET_TO_AAL1	CORE_BRDG	E-A1	(TDM_ENET NET_AAL1) \$	
TABLE NETPATH				
PATHIDX	NETPATH			

0	\$			
1	(ENET_TO_AAL1) \$			
TABLE NET2NET				
BNETNAME	CONNNETS			

TDM_ENET	(NET_AAL1 1) \$			
NET_AAL1	(TDM_ENET 1) \$			

AAL1 on from side (Ultralite-AAL1)

```

TABLE BEARNETS:
NETIDX  NETNAME          DISPLAY          FABRIC          OPTIONS
-----
NET 0    TDM_ENET        ENET            ENET            $
NET 1    NET_AAL1        ATM            AAL1            (PACKET_NETWORK_DEFAULT) $

TABLE CLLI:
CLLI          ADNUM          TRKGRSIZ          ADMININF
-----

TABLE NETBRDGE
BRDGCLLI      BRDGTYPE          DISPLAY          ADMININF
-----

TABLE NETPATH
PATHIDX          NETPATH
-----
0                $

TABLE NET2NET
BNETNAME          CONNNETS
-----
TDM_ENET          $
NET_AAL1          $

```

ENET & IP on from side (UA-IP and PT-IP)

TABLE BEARNETS				
NETIDX	NETNAME	DISPLAY	FABRIC	OPTIONS
NET 0	TDM_ENET	ENET	ENET	\$
NET 1	NET_IP	IP	IP	(PACKET_NETWORK_DEFAULT) \$

TABLE CLLI				
CLLI	ADNUM	TRKGRSIZ		ADMININF
ENET_TO_IP	725	0		ENET_TO_IP_BRIDGE_POOL

TABLE NETBRDGE				
BRDGCLLI	BRDGTYPE	DISPLAY		ADMININF
ENET_TO_IP	CORE_BRDG	E-IP		(TDM_ENET NET_IP) \$

TABLE NETPATH		NETPATH
PATHIDX		
0		\$
1		(ENET_TO_IP) \$

TABLE NET2NET		CONNNETS
BNETNAME		
TDM_ENET		(NET_IP 1) \$
NET_IP		(TDM_ENET 1) \$

IP on from side (PT-IP Compact)

TABLE BEARNETS				
NETIDX	NETNAME	DISPLAY	FABRIC	OPTIONS
NET 1	NET_IP	IP	IP	(PACKET_NETWORK_DEFAULT) \$

TABLE CLLI				
CLLI	ADNUM	TRKGRSIZ		ADMININF

TABLE NETBRDGE				
BRDGCLLI	BRDGTYPE	DISPLAY		ADMININF

TABLE NETPATH		NETPATH
PATHIDX		
0		\$

TABLE NET2NET		CONNNETS
BNETNAME		
NET_IP		\$

New fields in existing tables

MNNODE

- IW SPM: will include new field BRDGCLLI set to key of only entry in table NETBRDGE.
- IW DPT: will include a new field BEARNETS set to (<name of NET 1> Y) \$.
- MG4K: will include a new field BEARNETS set to (NET_AAL1 Y) \$

Note: NET 1 reflects the previously existing packet network as datafilled in table BEARNETS.

TRKOPTS

- DPT tuples will be pulled out of the DYNAMIC option as an application type and moved into its own option area.
- DPT tuples will contain a new BEARNETS field, that will contain (<name of NET 1> Y) \$
- SIPT DPT tuples contain a new selector named NGSS. This selector indicates if the trunk group uses the new Next Generation Session Server (NGSS) for SIP architecture implemented by activities A00003933. The values of this field is either 'Y' or 'N'.

Note: NET 1 reflects the previously existing packet network as datafilled in table BEARNETS.

SERVINV

- Will contain a new BEARNETS field, which will be set to:
 - (<name of NET 1> Y) \$ if GWC is not a DPT GWC
 - \$ if a DPT GWC

Note: NET 1 reflects the previously existing packet network as datafilled in table BEARNETS.

Routing tables: CND/NOT PKT selector

The existing CND/NOT PKT routing selector will be converted to CND FABRIC in all of the applicable routing tables.

SESM

Each non DPT GWC provisioned will have a network codec profile associated with it, using the existing network codec profile that is configured for the office.

DPT GWCs will not have a network codec profile associated with them.

Office/Subnet parameters (OP/SP) (CM & SESM)

New/modified office/subnet parameters

New or modified parameter

Parm table	Parameter name	NEW/CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management)
OFCOPT	network_active	Unchanged	CM
OFCVAR	multinet_display_active	New	CM
OFCSTD	pre_sn07_dumpside_packet_fabric	New	CM

Parameter information

OFCOPT::NETWORK_ACTIVE

- The parameter itself is not really changing in SN07. It will simply be used to aid in the detection of an upgrade to a Succession call server capable of supporting multiple packet networks.
- As of SN04, any ENET offices upgrading to a packet capable Succession load will have this office parameter converted to EXTENET automatically during the upgrade.
- The value EXTENET is now expanded to include the ability to support multiple packet networks.
- The use of the network tables (BEARNETS, NETBRIDGE, NETPATH, and NET2NET) is enforced in connectivity for interworking the various networks, even when only a single packet network exists.

Functional description

This parameter controls various aspects of call processing, most importantly the network connectivity capabilities that are supported by the system.

Provisioning rules

For JNET call processing, set the value of this parameter to JNET.

For Succession (single or multiple packet networks), the value should be set to EXTENET. "Succession" includes all cases where the load is packet capable, such that it includes the MSH DRU. This includes offices that currently only have an ENET provisioned.

Range information

Unchanged.

Activation

Unchanged.

Dependencies

No additional dependencies.

Consequences

Unchanged.

Verification

Not applicable.

Memory requirements

No memory impact.

Parameter release history update

Office parm value EXTENET now implies that the software can support multiple packet networks.

Note: The current SN06 NTP documentation does not reflect that this parameter will be changed on an ONP to EXTENET, if the from side is currently set at "ENET" and the to load contains the MSH DRU. The update that does this was submitted in TL16.

OFCVAR::MULTINET_DISPLAY_ACTIVE

Multiple Networks Display Active

Functional description

This is a new office parameter associated with Succession Call Server that activates the new and changed OMs and logs. This allows the customer the flexibility of enabling multiple packet networks (likely for testing purposes only) prior to having the back-office system (i.e., OSS systems) ready to support the new OMs and log fields. This is an Y/N type parameter. This parameter would be part of OFCVAR table. The default would be set to 'N'.

This parameter does not control the display of the IWBK per bridge pool OMs.

Provisioning rules

This office parameter cannot be turned on unless NETWORK_ACTIVE = EXTENET.

There are no restrictions for setting it to 'N'.

Behavior when the parameter is set to 'Y'

- Change from 'N' to 'Y' using table control.

- The tuples in the new OM groups TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP are created (if non-existent) displayed.
- Pegging of the OM group registers in TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP is started.
- The signaling type for the DPT node tuple in the DPTNODE OM group is displayed. The bearer network is also displayed for DPTNODE OMs if the DPT node is SPM based. The bearer network will not be displayed for GWC hosted DPT.
- The display of the bridge pool in IWBm 800 series of LOGS is enabled.

Behavior when the parameter is set to 'N'

- Change from 'Y' to 'N' using table control
 - A warning message would be displayed "All OM and LOGs data pertaining to multiple bearer networks on this call server will be lost."
 - The tuples in the new OM groups would not be displayed.
 - The signaling type and bearer network for the DPT node tuple in the DPTNODE OM group would not be displayed.
 - All the counters for the registers of the new OM groups would be set to zero.
 - The counters of the registers of the new OM groups would not be pegged.
 - The display of bridge pool in IWBm 800 series of LOGS would be disabled.
 - The OMSHOW command would display the OM groups TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2 and DPTOFCP and its fields. However the tuples of these OM groups is not be displayed.

Range information

Minimum	Maximum	Default
Y/N	Y/N	N

Activation

Immediate

Dependencies

This parameter cannot be set to Y unless NETWORK_ACTIVE = EXTENET.

Consequences

Setting this parameter to Y will result in new OM tuples and log fields to be displayed. This could adversely affect downstream OOS systems that have not yet been upgraded to handle this additional data.

Verification

To verify that the MULTINET Display is active and OM groups are created, use the CI command OMSHOW DPTOFCP. This command should display the OM group files and its tuples.

Memory requirements

The new OM groups will be created at IPL time, but the tuples will not be created/displayed until the office parameter is set to Y.

- For the OM groups DPTOFCP, OFZ2NET1 and OFZ2NET2 the tuples would be created but not displayed.
- For the OM TRK2NET1 and TRK2NET2, the tuples would not be created and would be created when the office parameter “MULTINET_DISPLAY_ACTIVE” is set to Y for the first time.

Parameter release history update

New in SN07.

OFCSTD::PRE_SN07_DUMPSIDE_PACKET_FABRIC

SN07 Dumpsides Packet Fabric prior to Succession MULTINET upgrade.

Functional description

This office parameter is set by the Nortel engineering team in an office parm changes flat file prior to the night of ONP. It is to be applied after the transfer of the office parameters and prior to the TABXFER.

The purpose of the parameter is to identify the FABRIC type of the single packet fabric supported on the from side prior to the upgrade, in order for the proper network tuples to be created in tables BEARNETS, CLLI, NETBRDGE, NETPATH, and NET2NET, as well as allow the new network related fields in tables MNNODE, TRKOPTS, and SERVINV to be assigned the proper default values.

It is very important that this parameter be set correctly.

Provisioning rules

This parameter has the following range: {UNDEF, NONE, AAL1, AAL2, IP}. It will be defaulted to UNDEF at IPL in a Succession load, and NONE if in a non-Succession load. It should be set to one of the other values (not UNDEF) on all upgrades to Succession loads. Although present in non Succession loads, it does not need to be set for these loads. Once an office is already on an SN07 or later load, it does not need to be set again.

A warning will be output on all changes except “UNDEF” to one of the other values that this parameter impacts the automatic creation of the network data on ONP, and should be changed with care.

Once a packet tuple is provisioned in table BEARNETS, changes will not be allowed.

In order to properly set the value, datafill will be required from the dump side from the following tables: MNNODE, MNCKTPAK, SERVINV, TRKOPTS, LGRPINV.

Explanation of parameter values:

- UNDEF: Default value at IPL. Indicates that the engineering team has not looked at the data.
- NONE: The engineering team has analyzed the from side data and detected that no packet nodes are provisioned. Indications that a packet node existed would include:
 - MNNODE: IW SPM, DPM SPM, or MG4K SPMs are provisioned.
 - SERVINV: any tuple provisioned.
 - Although one could argue that datafill in tables SERVSINV or LGRPINV also indicates a packet node, it cannot be added without a GWC first.
- AAL1: The from side packet datafill contained one of the following:
 - MNNODE contained an SMG4 (MG4K).
 - MNNODE IW or DPT SPM whose circuit card in table MNCKTPAK is ATM RM.
- AAL2:
 - Cannot be detected based on table datafill. Hopefully the engineering team knows if the PVG is using AAL2 or IP/AAL5.
- IP:
 - MNNODE IW or DPT SPM whose circuit card in table MNCKTPAK is GEM RM.
 - Table LGRPINV contains tuples whose GRPTYPE field is ‘M’ or ‘C’. indicating IAD devices or CICM.
 - The parm should also be set to IP if dumpsides was using IP/AAL5. This will not be distinguished as a separate bearer network.

Range information

Minimum	Maximum	Default
{UNDEF, NONE, AAL1, AAL2, IP}	{UNDEF, NONE, AAL1, AAL2, IP}	ENET - if load does not contain the MSH DRU UNDEF - if load contains MSH DRU.

Activation

Not applicable. This office parameter is only used during the TABXFER of data to a new load. It should be set to the correct fabric PRIOR to the night of ONP, and not changed thereafter. It is not used by call processing.

Dependencies

The following tables rely on the proper provisioning of this parameter:

- BEARNETS
- NETBRDGE
- NETPATH
- NET2NET
- MNNODE
- TRKOPTS
- SERVINV

Consequences

- There are no consequences of incorrect provisioning if there are no packet nodes currently supported at the site. If the parameter is set to a packet fabric in a site that does not have a packet network, then network tuples will automatically be created in tables BEARNETS, NETBRDGE, NETPATH, NET2NET.
- If a packet network was supported, and the parameter is provisioned incorrectly, tuple transfer errors could occur in the following tables:
 - TABXFER data errors in MNNODE, TRKOPTS, SERVINV.
- For an SN07 to SN07 lab upgrade, where the new tables suddenly appear in the load:
 - The ONP will not detect this scenario as a multinet upgrade. Instead, the network tables will appear in the load first, and the lab primes will be notified of the change. They will be required to go to a website and download/apply a DMOPRO file for the type of lab they are working in that contains the default data. In a following load, the dependent

fields will be added to the existing tables, and type reformats will pick up the default datafill.

Verification

Not applicable.

Memory requirements

Minimal. Just need to store the fabric type in a protected variable. Does not control the allocation of any additional memory.

Parameter release history update

New in SN07.

Upgrade Impact

Dump and Restore

Callp functionality should not be affected over an upgrade from pre-SN07 to post-SN07. In order to maintain this, the new/changed tables need to be datafilled over the ONP. It is required that this upgrade has minimum impact to the customer. Aside from the traditional issues with type specific reformats, we have the additional issue of determining what the FABRIC type was on the from side, in order to properly create default tuples in the new network tables. Since call processing will start depending on this data to make inter-network connections, it is vital that this data is correct after the transfer is ONP.

Once the data transfer is complete, the goal is to have the correct network representation for the currently configured networks, such that only new network information is required for when the customer wishes to add additional networks.

The ONP strategy must handle the following information:

Office Parameters

- OFCOPT::NETWORK_ACTIVE - If ENET, convert to EXTENET, and ensure that appropriate datafill is created to handle the existing networks.
- OFCVAR::MULTINET_DISPLAY_ACTIVE - Ensure the new office parameter is defaulted to 'N'.
- OFCSTD::PRE_SN07_DUMPSIDE_PACKET_FABRIC: the new office parameter *must be set by the upgrade engineering team* to indicate the default packet fabric on the from side network. This is set in a flat file that is applied after the office parameters have been transferred and before the tables are transferred. The engineering team is responsible for setting the correct values, and the application team is responsible for applying the changes at the proper point. Note that this is simply a new parameter included in the existing office parameter process. No changes are required to the process. This parameter applies only to alternative 1.

ONP Creation of Default Network Tuples

Tuples will be created automatically during the TABXFER via post data move procedures for the following tables. For more information see “New Network Tables - initial datafill” on page 765.

- BEARNETS
 - Create a NET 0 tuple representing the ENET if ENET is present.
 - Create an appropriate NET 1 tuple representing the existing packet network. The FABRIC should be set to either AAL1, AAL2, or IP as appropriate.
- CLLI
 - Create the appropriate CLLI used as the index to table NETBRDGE.
- NETBRDGE
 - If there is both an ENET and a packet network defined, a bridge pool will be automatically created in table NETBRDGE for it.
- NETPATH
 - Path 0 will be created as \$. This is the nilpath, indicating that 2 networks can be interconnected without a bridge.
 - If there are two networks defined, create a path using the bridge pool from NETBRDGE, assuming that bridges exist and that the bridgepool can connect them.
- NET2NET
 - For each network in table BEARNETS, create a tuple in NET2NET.
 - If there are multiple networks (both an ENET and a packet network), assume that both the ENET and the packet network can be connected to the other using the path index containing the bridge pool defined in table NETPATH.
 - Ensure that the NET 1 packet network detected is assigned the PACKET_NETWORK_DEFAULT option.

Note: It is possible that an upgrade can occur in offices that have both an ENET and a packet network, but no interworking bridge nodes defined. In this case, the default datafill will still be created, but there will be no IW SPM nodes assigned to the bridge pool, so the interconnections defined in table NET2NET will not work. It is assumed that since this is an upgrade from a working office, that translations would prevent such attempts from occurring.

Initialization of new fields in existing tables

- MNNODE:

- IW SPM: Initialize the new BRDGCLLI field to the single bridge group defined in table NETBRDGE.
- DPT SPM: Initialize the new BEARNETS field to the NET 1 BNETNAME, and mark is as the default network for the node.
- MG4K: Initialize the new BEARNETS field to the NET 1 BNETNAME, and mark is as the default network for the node.
- TRKOPTS:
 - Initialize the new BEARNETS field to the NET 1 BNETNAME, and mark is as the default network for the DPT trunk group.
 - Initialize the new NGSS field, on SIPT trunks, to 'N'.
- SERVINV:
 - If not a DPT GWC, initialize the new BEARNETS field to the NET 1 BNETNAME, and mark is as the default network for the GWC.
 - If this is a DPT GWC, initialize the new BEARNETS field to \$.

Type reformat on existing tables

- TRKOPTS: Remove DPT trunk groups as an application under the DYNAMIC trunk option, and create a DPT trunk option.
- OFRn, IBNRTn, HNPACONT::RTEREF, FNPACONT::RTEREF:
 - Convert the CND PKT conditional selector to CND FABRIC in all of the applicable routing tables.

Element Management Upgrade

Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

New or modified tables

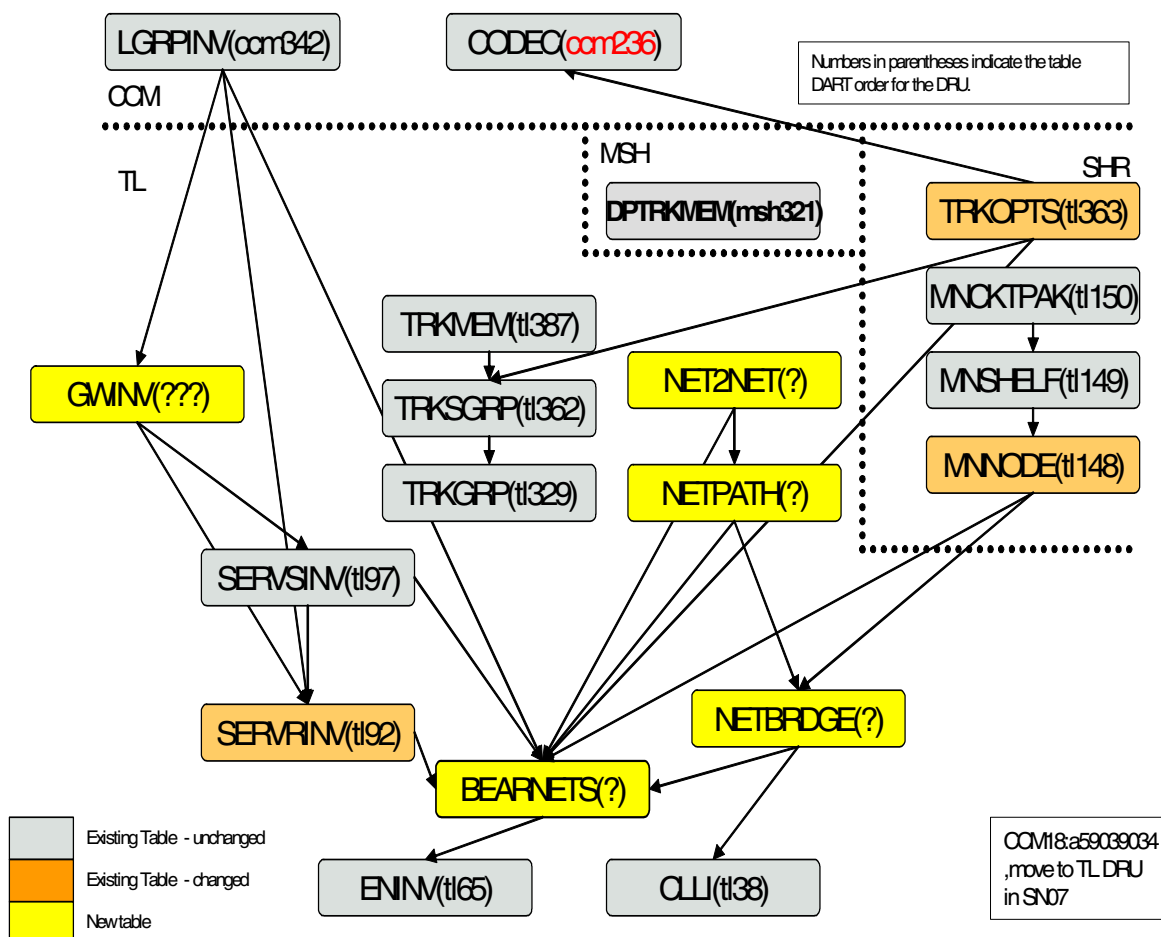
Table/MIB name	NEW/ CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
Core Tables:		
BEARNETS	NEW	NEW
NETBRDGE	NEW	NEW
NETPATH	NEW	NEW
NET2NET	NEW	NEW

New or modified tables

Table/MIB name	NEW/ CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
MNNODE	Changed	Unchanged
SERVRINV	Changed	Unchanged
SERVSINV	Changed	Unchanged.
TRKOPTS	Changed	Unchanged
MNCKTPAK	n/a	Unchanged
OFRn	Changed	Unchanged
IBNRTn	Changed	Unchanged
HNPACONT:RTEREF	Changed	Unchanged
FNPAACONT:RTEREF	Changed	Unchanged
SESM/GWCEM		
GWC_NETWORK_CODEEC_PROFILE	New	New
GWC_NETWORK_RECOMMENDED_CODEEC_SETTING	New	Old
GWCHandle	Changed	New
GATEWAYPROFILE	Changed	Old

Table/MIB/Remote Database Schema information

Core Table Dependencies



Core Table BEARNETS

Bearer networks

Functional description

On a Succession Call Server, this table identifies the bearer networks supported by the server and the network options that apply to the packet networks.

The overall default packet network for the office is determined by the assignment of the packet_network_default option to a single tuple in the table. If no packet network is detected in the provisioning hierarchy for a packet agent, this default packet network will be used.

Refer to the functional description section for table NET2NET for a full description of how the new network tables are used.

Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

ENINV

BEARNETS

NETBRDGE, NET2NET, MNNODE, SERVINV, TRKOPTS

Size

Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
BEARNETS	0	8	Memory not allocated unless tuples are provisioned. (Required if NETWORK_ACTIVE = EXTENET).

Fields/OIDs

The following table lists fields for BEARNETS.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NETIDX	New	No	0-7	Key to the table. Will be displayed as "NET 0" - "NET 7".
BNETNAME	New	No	Vector of up to 32 characters.	Identifies the name of the bearer network. This will be used in other tables to reference the associated bearer network and its characteristics. Making the name a field of the tuple rather than the index allows the customer to make name changes to the networks defined. The 32 character name of the network must be unique across the table.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DISPLAY	New	No	Vector of up to 4 characters.	Identifies the a 4 character string that will be used to display the bearer network on the MAP screens. It is recommended that this be a unique string across the bearer networks, but this will not be implemented in the table control. Use of non-unique names will diminish the usefulness of MAPCI displays which use this field.
FABRIC	New	No	ENET, AAL1, AAL2, IP	Identifies the bearer network fabric type.
OPTIONS	New	Refinements	Vector of {pkt_network_default}	Vector of options against the bearer network.
pkt_network_default	New	OPTIONS refinement (not a field)	n/a	Indicates that this tuple is the packet bearer network default for the office. Primarily used in initializing dependant tables during an ONP. Restrictions: Only one tuple in the table can have this option.

Datafill example

The following example shows sample datafill for table BEARNETS.

```

TABLE: BEARNETS
NETIDX  NETNAME      DISPLAY FABRIC  OPTIONS
-----
NET 0   TDM_ENET      ENET    ENET    $
NET 1   NET_AAL1     ATM     AAL1    (PKT_NETWORK_DEFAULT) $
NET 2   NET_IP          IP      IP      $
NET 3   NET_AAL2       AAL2    AAL2    $

```

Table release history update

New in SN07.

Supplementary information

Table BEARNETS, along with tables NETBRDGE, NETPATH, and NET2NET) is required to be provisioned in all Succession sites supporting bridged calls from a TDM network to a packet network.

When using the FINDREF tool on table BEARNETS, it is necessary to encapsulate the key field within single parentheses. For example:

FINDREF BEARNETS 'NET 1'

On an ONP, this table will be automatically provisioned with both TDM and packet networks tuples where they exist.

- If the from side datafill contained an ENET, the NET 0 tuple from the datafill example will be automatically provisioned.
- If the from side supported packet nodes (as indicated by the setting of the PRE_SN07_DUMPSIDE_NETWORK_FABRIC), the NET 1 tuple will be provisioned and marked as the PKT_NETWORK_DEFAULT.

BEARNETS Provisioning Restrictions

Field	Provisioning Restrictions
NETIDX	• Additions of packet networks to the table will not be allowed unless the NETWORK_ACTIVE = EXTENET. • Adding a tuple in table BEARNETS will automatically create a tuple in table NET2NET with \$. • Cannot delete a BEARNETS tuple unless the NET2NET entry contains a \$and that tuple is the only reference. It is a counted tuple type.
BNETNAME	• Must be unique in table. • Changes to the BNETNAME will be reflected immediately in logs, OMs, etc. • Should only contain alphanumeric and underscore characters.
DISPLAY	• No restrictions, but recommend that this field be unique in the table. Use of non-unique names will diminish the usefulness of MAPCI displays which use this field.
FABRIC	• Only 1 ENET tuple is allowed. • ENET tuple can only be added if ENET exists. • ENET tuple cannot be deleted if ENET exists. • Adds of UNDEF tuples are not allowed. • Changes are not allowed.

BEARNETS Provisioning Restrictions

Field	Provisioning Restrictions
OPTION pkt_network_default	• The first packet network added must be the default. • Only one tuple may have this option assigned. If the option is added to another tuple, it will be removed from the first. • Cannot be added if FABRIC = ENET. • Cannot be deleted from a tuple, except by adding to another tuple. • Can only delete the network default tuple if it is the only remaining packet network tuple.

Refer to the supplementary information for table NET2NET for additional information.

Translation verification other tools

BEARNETS does not use translation verification tools.

Core Table NETBRIDGE

Network bridging resources.

Functional description

This table defines the network bridging resources for interconnecting networks. Bridges provide the ability to connect one network to another without regard to the call type. Bridges typically have two connectivity endpoints, one for each of the networks that it interconnects.

Refer to the functional description section for table NET2NET for a full description of how the new network tables are used.

Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

CLLI, BEARNETS

NETBRIDGE

NETPATH, NET2NET, MNODE

Size

Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
NETBRDGE	0	64	Refer to the EI section after DSUM.

Fields/OIDs

The following table lists fields/OIDs for NETBRDGE.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
BRDGCLLI	New	No	CLLI common_language_name	Identifies the name of the bridge resource group.
BRDGTYPE	New	No	CORE_BRDG	The type of the bridging resource. For SN07, this is limited to core bridges, but could be expanded in the future.
DISPLAY	New	No	Vector of up to 4 characters	Identifies the a 4 character string that will be used to display the bearer network on the MAP screens. We recommend that this be a unique string across the bearer networks, but this will not be implemented in the table control.
BEARNETS	New	Structure	BNETNAME, BNETNAME	Identifies the two networks that can be bridged with this bridging resource group.

Datafill example

The following example shows sample datafill for table NETBRDGE.

```

TABLE: NETBRDGE
BRDGCLLI      TYPE      DISPLAY  BEARNETS
-----X-----
ENET_TO_AAL1  CORE_BRDG  E-A1     TDM_ENET NET_AAL1
ENET_TO_IP    CORE_BRDG  E-IP     TDM_ENET NET_IP

```

Table release history update

New in SN07.

Supplementary information

NETBRDGE Provisioning Restrictions

Field	Provisioning Restrictions
BRDGCLLI	- Common_language_name provisioned in table CLLI. - Counted tuple type. Deletions are not allowed if referenced by another table.
BRDGTYPE	- Only allowable value in SN07 is {CORE_BRDG}. - Cannot change.
DISPLAY	- Recommended, but not enforced, to be unique. - No change restrictions.
BEARNETS	- The two network names provided must be provisioned in table BEARNETS. - The two network names must be different. - Changes to the BEARNETS field is allowed only if the tuple is not referenced by another table.

Since the BRDGCLLI is the key to this table, it cannot be changed through the table control interfaces. BRDGCLLI names can be changed for this table using the CI command RENAMECLLI. The name change will then be reflected in all tables, OM, and logs that reference the particular bridge CLLI.

Translation verification other tools

NETBRDGE does not use translation verification tools.

Core Table NETPATH

Interconnecting network path.

Functional description

Tuples in this table identify the list of bridging resource groups (the bridge path) that can be used to interconnect two networks. In SN07, two bridges are required to connect an AAL1 agent and an IP agent, so the path consists of a bridge resource from each of those NETBRDGEs.

Refer to the functional description section for table NET2NET for a full description of how the new network tables are used.

Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

NETBRDGE

NETPATH

NET2NET

Size

Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
NETPATH	0	256	Refer to the EI section of this document following the DSUM.

Fields/OIDs

The following table lists fields/OIDs for NETPATH.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
PATHIDX	New	New	0 to 255	The key to the table.
NETBRDGE	New	New	Vector of BRDGCLLI	A list of the bridge pools that are required to go from one network to another. Bridge CLLIs must be listed in the order of the traversal required, without regard to the direction of the traversal (forward or backward).

Datafill example

The following example shows sample datafill for table NETPATH

```

TABLE: NETPATH
PATHIDX      NETBRDGE
-----
0             $
1             (ENET_TO_AAL1) $
2             (ENET_TO_IP) $
3  (ENET_TO_AAL1) (ENET_TO_IP) $

```

NOTE: PATHIDX 3 is not supported in SN07.

Table release history update

New table in SN07.

Supplementary information

The following tuple will be created automatically for all Succession offices:

0 \$

This will indicate the “nil path” that can be used in table NET2NET to indicate that two networks can be directed connected without the use of bridging resources.

NETPATH Provisioning Restrictions

Field	Provisioning Restrictions
PATHIDX	- Counted tuple. Deletions not allowed if referenced by another table. - PATHIDX = 0 is reserved for connections between packet networks of the same fabric which do not require an IW bridge for connectivity.
NETBRDGE	- The same bridge pool should not be in the list more than once. - Limit of 2 bridge pools in SN07. - Order of the bridge pools should be maintained. - Changes are allowed, and take effect immediately for all NET2NET tuples provisioned with this path. - The bridge pools must be listed in the order they will be traversed to go from one network to the other. The pools can be listed in either the forward or reverse direction.

Note: Allowing the NETBRDGE field to be changed allows this user to deload a particular IW SPM by creating another PATH with another NETBRDGE pool of the same type and assigning the desired SPMs to it. The CI tool IWBMCi:DBL can be used to validate when the deloaded SPM is no longer in use.

Translation verification other tools

NETPATH does not use translation verification tools.

Core Table NET2NET

Network interconnection.

Functional description

Tuples in this table define the allowable interconnections between networks, and the network path used to interconnect them.

Call processing will assume that any agents on the same network can be connected with one another.

Once the normal translations have occurred, a request will be made to connectivity to connect the agents.

- If the agents are on the same network, the connection request will proceed.
- If the agents are provisioned on separate networks, connectivity will check table NET2NET to see if the connection is allowed.
 - If the two networks are provisioned as connecting in the table, the NETPATH and associated bridge resources will be retrieved and the connection request will continue. If there are no idle members in the bridge groups, the connection request will then fail.
 - If the two networks are not provisioned as connecting in the table, the connection request will fail immediately.
- In SN07, no mechanism is provided for choosing an alternate bridging path if the bridging resources are unavailable in the provisioned path.

Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

BEARNETS, NETPATH

NET2NET

Size

Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
NET2NET	0	7	Allocated upon first tuple entry.

Fields/OIDs

The following table lists fields/OIDs for NET2NET.

Each CONNNETS vector entry consists of:

- NET2NET - the interconnecting network
- NETPATH - reference to tuple in table NETPATH defining the path by which the two networks interconnect.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
BNETNAME	New	No	BNETNAME defined in table BEARNETS	Identifies the name of the bearer network. Must be datafilled in Table BEARNETS first.
CONNNETS	New	No	Vector of connecting_network	Identifies a list of other bearer networks that are allowed to interconnect to this bearer network.
NET2NET	New	Field of connecting_network	BNETNAME provisioned in table BEARNETS	The interworking bearer network. Must be provisioned in Table BEARNETS first.
NETPATH	New	Field of connecting_network	Key to table NETPATH 0 - 255	Index into Table NETPATH.

Datafill example

The following example shows sample datafill for table NET2NET.

ENET/AAL1/IP NET2NET Datafill

```

TABLE BEARNETS
NETIDX  NETNAME      DISPLAY      FABRIC      OPTIONS
-----
NET 0    TDM_ENET    ENET        ENET        $
NET 1    NET_ATM      ATM        AAL1        $
NET 2    NET_IP       IP         IP          $

TABLE CLLI
-----
CLLI      ADNUM  TRKGRPSIZ  ADMININF
ENET_TO_IP  725    0          ENET_TO_IP_BRIDGE_POOL
ENET_TO_AAL1 724    0          ENET_TO_AAL1_BRIDGE_POOL

TABLE NETBRDGE
-----
BRDGCLLI  BRDGTYPE  DISPLAY      BEARNETS
ENET_TO_AAL1 CORE_BRDG  E-A1        (TDM_ENET NET_AAL1) $
ENET_TO_IP  CORE_BRDG  E-IP        (TDM_ENET NET_IP) $

TABLE NETPATH
-----
PATHIDX      NETPATH
0            (ENET_TO_AAL1) $
1            (ENET_TO_IP) $
2            (ENET_TO_AAL1) (ENET_TO_IP) $

TABLE NET2NET
-----
BNETNAME      CONNNETS
TDM_ENET      (NET_ATM 0) (NET_IP 1) $
NET_ATM       (TDM_ENET 0) (NET_IP 2) $
NET_IP        (TDM_ENET 1) (NET_ATM 2) $

```

Enterprise/Carrier Datafill

```

TABLE BEARNETS
NETIDX  NETNAME      DISPLAY      FABRIC      OPTIONS
-----
NET 0    TDM_ENET     ENET        ENET        $
NET 1    NET_ATM       ATM         AAL1        $
NET 2    NET_IP        IP          IP          $
NET 3    NET_IPE     IPE         IP          $

TABLE CLLI
-----
CLLI      ADNUM  TRKGRPSIZ  ADMININF
ENET_TO_IP  725    0          ENET_TO_IP_BRIDGE_POOL
ENET_TO_AAL1 724    0          ENET_TO_AAL1_BRIDGE_POOL

TABLE NETBRDGE
-----
BRDGCLLI  BRDGTYPE  DISPLAY      BEARNETS
ENET_TO_AAL1 CORE_BRDG  E-A1        (TDM_ENET NET_AAL1) $
ENET_TO_IP   CORE_BRDG  E-IP        (TDM_ENET NET_IP) $

TABLE NETPATH
-----
PATHIDX      NETPATH
0
1             (ENET_TO_AAL1) $
2             (ENET_TO_IP) $
3  (ENET_TO_AAL1) (ENET_TO_IP) $

TABLE NET2NET
-----
BNETNAME      CONNNETS
TDM_ENET      (NET_AAL1 1)  (NET_IP 2)  $
NET_AAL1      (TDM_ENET 1)  (NET_IP 3)  $
NET_IP        (NET_AAL1 3)  (TDM_ENET 2) $
NET_IPE      $

```

Note that NET_IPE does not connect to NET_IP, even though they have the same FABRIC.

This is the SN07 configuration example to support Carrier Hosted Services (i.e. H.323 and Media Call Server 5200) via PVG looparounds.

Different Networks, same Fabric

```

TABLE BEARNETS
NETIDX  NETNAME      DISPLAY      FABRIC      OPTIONS
-----
NET 0    TDM_ENET     ENET         ENET         $
NET 1    NET_ATM       ATM          AAL1         $
NET 2    NET_IP       IP           IP           $
NET 3    NET_IPE      IPE         IP           $

TABLE CLLI
-----
CLLI      ADNUM      TRKGRPSIZ      ADMININF
ENET_TO_IP 725        0              ENET_TO_IP_BRIDGE_POOL
ENET_TO_AAL1 724      0              ENET_TO_AAL1_BRIDGE_POOL

TABLE NETBRDGE
-----
BRDGCLLI  BRDGTYPE      DISPLAY      BEARNETS
ENET_TO_AAL1 CORE_BRDG    E-A1        (TDM_ENET NET_AAL1) $
ENET_TO_IP   CORE_BRDG    E-IP        (TDM_ENET NET_IP) $

TABLE NETPATH
-----
PATHIDX      NETPATH
0
1            (ENET_TO_AAL1) $
2            (ENET_TO_IP) $
3            (ENET_TO_AAL1) (ENET_TO_IP) $

TABLE NET2NET
-----
BNETNAME      CONNNETS
TDM_ENET      (NET_AAL1 1) (NET_IP 2) $
NET_AAL1      (TDM_ENET 1) (NET_IP 3) $
NET_IP        (NET_AAL1 3) (TDM_ENET 2) (NET_IPE 0) $
NET_IPE      (NET_IP 0) $

```

To interconnect two different networks on the same fabric, define a NETPATH that requires no bridges, and put entries in NET2NET using that path.

Table release history update

New in SN07.

Supplementary information

- NET2NET tuples will automatically be created with CONNNETS = \$ whenever new networks are added to table BEARNETS.
- On an ONP, the interconnecting networks should be provisioned with the appropriate bridges automatically.

NET2NET Provisioning Restrictions

Field	Provisioning Restrictions
BNETNAME	• Deletions are not allowed from this table. • User may change the tuple to the point that CONNNETS = \$. Tuple deletions will be handled via table BEARNETS, and allowed only if CONNNETS = \$.
CONNNETS	• Networks that connect only with themselves will have CONNNETS = \$. All provisioned networks in table BEARNETS will be represented in this table. • The order of the entries is used during trunk member selection as the network preference order for trunk members when a member that is on the originating agent's network is not available. The most efficient path is recommended to be provisioned first. • Adding a connecting network to a tuple should also add the connection to the tuple for the other network. This addition will be added to the end of the CONNNETS list of that tuple. • Deleting a connecting network from a tuple will also delete the interconnection from the connecting network's tuple. • Changes to NET2NET tuples will take effect immediately upon the change for all new connection requests. Used should be warned when removing an existing interconnection ability.
CONNNETS: NET2NET	• Valid BNETNAME from table BEARNETS. • Should not be the same as the key for the tuple. It is understood that a network can connect to itself. • A given network should appear in the connecting network list only once. • Changing the order will change the order of trunk member selection based on the network of the originating agent.
CONNNETS: NETPATH	• A valid PATHIDX from table NETPATH. • Path changes take effect immediately for new connection requests. Existing connections will continue with the old path until the connection has been released. • If NETPATH = 0 is specified, verify that the network FABRIC for both the BNETNAME network and the NET2NET network are on the same fabric. • Verify that once the starting end of the path is chosen based on the BNETNAME network, the path can then be traced in the appropriate direction to reach the CONNNETS network.

Translation verification other tools

NET2NET does not use translation verification tools.

Core Table MNNODE

Maintenance node table used to provision Spectrum nodes.

Functional description

Unchanged.

Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

All existing dependencies, plus BEARNETS, NETBRDGE

MNNODE

All existing dependant tables.

Size**Table size**

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MNNODE	Unchanged	Unchanged	Refer to the EI section of this document after DSUM complete.

Fields/OIDs

The following table lists fields/OIDs for MNNODE.

The following nodes provisioned in table MNNODE are impacted by these changes:

- Interworking bridges (NODEKEY=IW, DPT_INFO = BRDG_ONLY)
- DPT SPM (NODEKEY = IW, DPT_INFO = DPT_ONLY)
- MG4K (NODEKEY = SMG4)

Each of the applicable node type change is broken into its own table below.

Table field descriptions for IW Bridges

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NODEKEY	Unchanged	Unchanged	Unchanged	Unchanged
ALIAS	Unchanged	Unchanged	Unchanged	Unchanged

Table field descriptions for IW Bridges

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NODEINFO	Changed	IW refinement	IW	Changes below impact the IW refinement of CLASS.
FLOOR	Unchanged	Unchanged	Unchanged	Unchanged
CLKMODE	Unchanged	Unchanged	Unchanged	Unchanged
CLKREF	Unchanged	Unchanged	Unchanged	Unchanged
LEDTIMER	Unchanged	Unchanged	Unchanged	Unchanged
RSRUTLIM	Unchanged	Unchanged	Unchanged	Unchanged
ALRMCTRL	Unchanged	Unchanged	Unchanged	Unchanged
DPT_INFO	Changed	Unchanged	BRDG_ON LY	Refinements created based on this field.
BRDGCLLI	New	New subfield when DPT_INFO = BRDG_ON LY	List of BRDGCLLI (common_language_id entifier) provisioned in table NETBRDGE	List of the supported bridge groups the bridges belong to.
OPTIONS	Unchanged	Unchanged	Unchanged	Unchanged

Table field descriptions for DPT SPM

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NODEKEY	Unchanged	Unchanged	Unchanged	Unchanged
ALIAS	Unchanged	Unchanged	Unchanged	Unchanged
NODEINFO	Changed	IW refinement	IW	Changes below impact the IW refinement of CLASS.
FLOOR	Unchanged	Unchanged	Unchanged	Unchanged
CLKMODE	Unchanged	Unchanged	Unchanged	Unchanged
CLKREF	Unchanged	Unchanged	Unchanged	Unchanged
LEDTIMER	Unchanged	Unchanged	Unchanged	Unchanged

Table field descriptions for DPT SPM

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RSRUTLIM	Unchanged	Unchanged	Unchanged	Unchanged
ALRMCTRL	Unchanged	Unchanged	Unchanged	Unchanged
DPT_INFO	Changed	Unchanged	DPT_ONLY	Refinements created based on this field.
BEARNETS	New	New subfield when DPT_INFO = DPT_ONLY	Vector of (BNETNAME and DEFAULT)	List of the networks to which the DPT TIDs belong and whether or not the network should be considered the default network for the node. In SN07, only 1 network can be added, and it will be the default.
BNETNAME	New	Subfield of BEARNETS.	BNETNAME provisioned in table BEARNETS.	Name of the bearer network from table BEARNETS.
DEFAULT	New	Subfield of BEARNETS	{Y, N}	Indicates whether the particular bearer network is the default network
OPTIONS	Unchanged	Unchanged	Unchanged	Unchanged

Table 1 Table field descriptions for MG4K

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NODEKEY	Unchanged	Unchanged	Unchanged	Unchanged
ALIAS	Unchanged	Unchanged	Unchanged	Unchanged
NODEINFO	Changed	IW refinement	SMG4	Changes below impact the IW refinement of CLASS.
FLOOR	Unchanged	Unchanged	Unchanged	Unchanged
CLKMODE	Unchanged	Unchanged	Unchanged	Unchanged

Table 1 Table field descriptions for MG4K

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CLKREF	Unchanged	Unchanged	Unchanged	Unchanged
LEDTIMER	Unchanged	Unchanged	Unchanged	Unchanged
RSRUTLIM	Unchanged	Unchanged	Unchanged	Unchanged
ALRMCTRL	Unchanged	Unchanged	Unchanged	Unchanged
EXECTAB	Unchanged	Unchanged	Unchanged	Unchanged
DPT	Unchanged	Unchanged	Unchanged	Unchanged
DPT_NUM_REQ	Unchanged	Unchanged	Unchanged	Unchanged
SLINK_THRESHOLD_DATA	Unchanged	Unchanged	Unchanged	Unchanged
BOOTP_SUPPRESS	Unchanged	Unchanged	Unchanged	Unchanged
REMOTE	Unchanged	Unchanged	Unchanged	Unchanged
BEARNETS	New	New subfield when DPT_INFO = DPT_ONLY	Vector of (BNETNAME and DEFAULT)	List of the networks to which the DPT TIDs belong and whether or not the network should be considered the default network for the node. In SN07, only 1 network can be added, and it will be the default.
BNETNAME	New	Subfield of BEARNETS.	BNETNAME provisioned in table BEARNETS.	Name of the bearer network from table BEARNETS.
DEFAULT	New	Subfield of BEARNETS	{Y, N}	Indicates whether the particular bearer network is the default network

Datafill example

The following examples show sample datafill for the affected nodetypes in table MNNODE.

Example Datafill - IW SPM

```
TABLE: MNNODE
NODEKEY ALIAS NODEINFO
-----
SPM 1 SPM_1 IW 1 SYNCH INTERNAL 15 (DTMF 60) (ECAN
60) (TONESYN 60) $ (SYSB CR RPT) (MANB MJ RPT) (DTMFLOW MN RPT)
(ECANLOW MN RPT) (TONESLOW MN RPT) (PATCHFAIL MJ RPT) (ATMBCN
CR RPT) (SMCHLD MF RPT) (SMCHLD24 CR RPT) $ BRDG_ONLY
(ENET_TO_AAL1) $ (SPMECIDX 0)$
```

Example Datafill - DPT SPM

```
TABLE: MNNODE
NODEKEY ALIAS NODEINFO
-----
SPM 1 SPM_1 IW 1 SYNCH INTERNAL 15 (DTMF 60) (ECAN
60) (TONESYN 60) $ (SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT)
(SYSBNA CR RPT) (MANBNA MJ RPT) (DTMFLOW MN RPT) (ECANLOW MN RPT)
(TONESLOW MN RPT) (PATCHFAIL MJ RPT) (ATMBCN CR RPT) (SMCHLD MF
RPT) (SMCHLD24 CR RPT) $ DPT_ONLY (NET_AAL1 Y) $
(SPMECIDX 0)$
```

Example Datafill - MG4K

```
TABLE: MNNODE
NODEKEY ALIAS NODEINFO
-----
SPM 1 SPM_1 SMG4 0 SYNC LINE 50
(COT 60) (DTMF 60) (ECAN 60) (TONESYN 60) (MF 60) $ (SYSB CR
RPT) (MANB MJ RPT) (ISTB MN RPT) (SYSBNA CR RPT) (MANBNA MJ
RPT) (COTLOW MN RPT) (DTMFLOW MN RPT) (ECANLOW MN RPT) (MFLOW
MN RPT) (CMRLOW MN RPT) (TONESLOW MN RPT) (SMG4CN MJ RPT)
(PATCHFAIL MJ RPT) (ATMBCN CR RPT) (STE3HLD MJ RPT) (STE3HLD24
CR RPT) (SMCHLD MF RPT) (SMCHLD24 CR RPT) (SPMSRMNTD MN RPT)
(LOCUR MJ RPT) (TMCFAIL CR RPT) $ $ N 0 $ N N (NET_AAL1 Y) $
```

Table release history update

In SN07, The following mandatory fields were added:

- BEARNETS field added to IW DPT_ONLY and SMG4 nodes to indicate the bearer network associated with the node.
- BRDGCLLI field added to IW BRDG_ONLY nodes to indicate the list of bridge groups the particular SPM node contributes to.

Supplementary information

- As of SN07, in order for interworking bridges to be utilized, the BRDGCLLI for the IW must be included in a NETPATH used to interconnect two networks in table BEARNETS.

- Terminations to DPT will dynamically match the network of the DPT SPM to the network provisioned against the terminating trunk group in table TRKOPTS to properly select a DPT “terminal” on the correct network.

MNNODE IW bridg_only Provisioning Restrictions

Field	Provisioning Restrictions
BRDGCLLI	• Must be provisioned as a single entry in SN07. Cannot have either a nil vector or more than one provisioned. • Ensure the CLLI entered is a bridge clii. • Do not allow BRDGCLLI where the NETBRDGE packet network fabric is not IP or AAL1. AAL2 is currently not supported by SPM nodes. • Changes are allowed only if the IW is OOS (MANB or OFFL). • On changes, compare the packet fabrics for the networks bridged by the BRDGCLLI. If the fabrics are different, then this means the network cards must be changed as well. Network cards should be removed prior to changing the BRDGCLLI, so a check is made that no network cards are provisioned if the packet fabrics that are bridged are different.

MNNODE IW dpt_only Provisioning Restrictions

Field	Provisioning Restrictions
BEARNETS - vector of {BNETNAME, DEFAULT}	• Must have a single entry and it must be marked as the default. • The network entered must be provisioned in table BEARNETS. • The network entered must be a packet network with an IP or AAL1 fabric. • For changes, the SPM must be OFFL and all DPT carriers must be INB. (from DPTTRM, pos spm no, bsy, bsy inb). • If the network fabric is changing, then the network cards must be removed before the change is allowed.

MNNODE SMG4 Provisioning Restrictions

Field	Provisioning Restrictions
BEARNETS	• Must have a single entry and it must be marked as the default. • The network entered must be provisioned in table BEARNETS. • The network entered must be a packet network. • For changes, the SPM must be OFFL and all carriers must be INB. If DPT, then from DPTTRM, post <spm no>, bsy, bsy inb. If not DPT, then from TTP, post d <pm no>, bsy all, bsy inb all. • If the network fabric is changing, then the network cards must be removed before the change is allowed.

Generally, if the packet fabric for the IW is changing (whether a bridge or trunk members), then the following process must be followed to change the BEARNETS or BRDGCLLI provisioned:

- OFFL the SPM and bsy INB all carriers.
- Remove the network cards via table MNCKTPAK.
- Change the MNNODE BEARNETS or BRDGCLLI information.
- Add the correct circuit packs to MNCKTPAK (will be verified against the MNNODE datafill).
- RTS the SPM node.

Translation verification other tools

MNNODE does not use translation verification tools.

Core Table MNCKTPAK

Management Network Node Table

No semantic changes have been made to this table.

Additional validation checking has been added for when the GWM RM and ATM RM card provisioning, to ensure that the network implies by the card agrees with the bearer network provisioned against the node.

Supplementary information

MNCKTPAK Provisioning Restrictions

Field	Provisioning Restrictions
CPKINFO - GEM card	- If SPM is IW brdg_only, ensure that at least one IP network is supported by the BRDGCLLI assigned. - If the SPM is either IW dpt_only or SMG4 (MG4K), ensure that the BEARNETS fabric provisioned in table MNNODE is IP.
CPKINFO - ATM card	- If SPM is IW brdg_only, ensure that at least one AAL1 network is supported by the BRDGCLLI assigned. - If the SPM is either IW dpt_only or SMG4 (MG4K), ensure that the BEARNETS fabric provisioned in table MNNODE is AAL1.

Core Table SERVRINV

Server Inventory

Functional description

A new field, BEARNETS is added to the SERVRINV table to indicate the bearer networks of the packet nodes it controls. For SN07, there will be a limit of one bearer network per gateway controller, and it will be the default.

In addition, DPT GWCs should not be provisioned with a bearer network, as it is a signalling only network element.

Usage sequence and implications (CM Only)

The following provisioning dependencies is added:

BEARNETS

SERVRINV

Size

Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SERVRINV	Unchanged	Unchanged	tbd

Fields/OIDs

The following table lists fields/OIDs for SERVRINV.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SERVNAME	Unchanged	Unchanged	Unchanged	Unchanged
SERVADDR	Unchanged	Unchanged	Unchanged	Unchanged
SERVEXEC	Unchanged	Unchanged	Unchanged	Unchanged
SERVRTONE	Unchanged	Unchanged	Unchanged	Unchanged
BEARNETS	New	New	Vector of (BNETNAME and DEFAULT)	List of the networks to which the DPT TIDs belong and whether or not the network should be considered the default network for the node. In SN07, only 1 network can be added, and it will be the default. DPT GWC's should not be provisioned with a bearer network. Enter \$.
BNETNAME	New	Subfield of BEARNETS	BNETNAME provisioned in table BEARNETS	Name of the bearer network from table BEARNETS.
DEFAULT	New	Subfield of BEARNETS	{Y, N}	Indicates whether the particular bearer network is the default network
SERVROPTS	Unchanged	Unchanged	Unchanged	Unchanged

Datafill example

The following example shows sample datafill for table SERVINV.

Example Datafill

```
TABLE: MNODE
SERVNAME SERVADDR SERVEXEC SERVRTONE BEARNETS SERVROPTS
-----
GWC 0      IP  47 192 48 24 (POTS POTSEX)  (KEYSET KSETEX)  $
NORTHAA (NET_IP Y) $ $
```

Table release history update

Added BEARNETS field in SN07.

Supplementary information

- SERVRINV is the bearer network provisioning point for the following nodes, if the BEARNETS field contains a default network. If the GWC does not have a BEARNETS entry, the office default (the tuple in table BEARNETS with the default_packet_network option assigned) will be taken as the bearer network for the following agents.
 - IP trunking gateways (PVG, Audiocodes)
 - Logical groups
 - ABI lines and trunks
 - H.323 & Media Call Server 5200
 - UAS (for CALEA)
- DPT GWCs do not have a bearer network provisioning against them, as the DPT TIDs against the GWC do not have associated hardware. If a network is provisioned against DPT GWC, it will have no effect on call processing. DPT trunk groups get their bearer network from table TRKOPTS.
- It is assumed that SERVRINV will be provisioned via SESM, which will ensure that a default bearer network is added for non-DPT GWCs, and that no bearer network will be added to DPT GWCs. A warning message is output to the user when provisioning changes are made to SERVRINV warning of potential data corruption. This warning message already exists.

SERVRINV Provisioning Restrictions

Field	Provisioning Restrictions
BEARNETS - vector of {BNETNAME, DEFAULT{	• BEARNETS does not apply if the GWC is a DPT GWC. • If a nil entry is added for a non-DPT GWC, the bearer network will be taken from the office default provisioned in table BEARNETS as the pkt_default_network. • Entry must either be assigned a "\$" or a single BNETNAME marked as the default. • Changes require that the GWC be OOS (MANB or OFFL). • Non-DPT trunks must be BSY INB prior to change. • Allow changes to a non-nil BEARNETS field only if not DPT in SERVSINV. Allow deletion of BEARNETS entry only if DPT.

Translation verification other tools

SERVRINV does not use translation verification tools.

Core Table SERVSINV

Server Subtending Inventory

Table unchanged by this activity. Only additional provisioning consistency checks are added for use during an ONP.

Supplementary information

DPT terminal groups are signalling only, and do not have any physical hardware associated. The DPT trunk group, via provisioning in table TRKOPTS, contains the bearer network information, and DPT “terminals” can be associated with any bearer network provisioned against the trunk group, as long as the signalling type matches.

When transferring table data during an ONP for table SERVINV, it is not known if the GWC is a DPT GWC, so the BEARNETS will be automatically set to the bearer network default. Therefore, the write procedure for table SERVSINV will be hooked to check whether or not a multinet upgrade is in progress for DPT GWCs (SIPT or BICC) and if it is, it will delete the BEARNETS entry for its host GWC.

Core Table TRKOPTS

Trunk Options.

Functional description

Unchanged.

Usage sequence and implications (CM Only)

The following dependency is added to the existing provisioning order:

BEARNETS

TRKOPTS

Size**Table size**

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TRKOPTS	Unchanged	Unchanged	Refer to EI section after DSUM.

Fields/OIDs

The following table lists fields/OIDs for TRKOPTS.

```

>range
 1 OPTKEY          TRKOPTS_KEY
 2 OPTINFO         TRKOPTS_OPTINFO_VAR_AREA
LOGICAL TUPLE TYPE: TRKOPTS_LOGICAL_TUPLE
>range 2
 2 OPTINFO         TRKOPTS_OPTINFO_VAR_AREA
TYPE IS TRKOPTS_OPTINFO_VAR_AREA    MULTIPLE WITH
OPTION                                TRKOPTS_OPTION REFINEMENTS:
{DYNAMIC}                          MULTIPLE WITH
    SIGNALING                      {ISUP,BICC,SIPT}
    SIGNALING_NETWORK              {IP,SS7,STRK}
    BEARER_NETWORK                {IP,ATM,STRK}
    APPLICATION                   {OC,POS,DPT,RAS,SIPBCPT,STRK}
{DPT}                               MULTIPLE WITH
    PROTOCOL                      {BICC,SIPT}
    BEARNETS                      {NETNAMES}
    PROTOCOL                     REFINEMENTS:
    {SIPT}                       MULTIPLE WITH
        NGSS                     MULTIPLE WITH
            NGSS_SELECTOR        {N,Y} REFINEMENTS:
            {Y}                 MULTIPLE WITH
                INTER_DOMAIN    {N,Y}
                {N}             MULTIPLE WITH
                    DEST_MGCNAME MGCINV_KEY
                    TPROFILE     TPROFILE_KEY
                    ALT_HOST_MGCNAME VECTOR OF UP TO 32 CHAR'S
                    INTER_DOMAIN {N,Y}
{BICC}                               MULTIPLE WITH
    CAPABILITY_SET              {1 TO 2}

```

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTKEY	Unchanged	No	Unchanged	Unchanged
OPTINFO	Changed	No	Add DPT to list of valid OPTIONS	Add DPT to list of valid OPTIONS
OPTION	Changed	Selector subfield of OPTINFO	DYNAMIC	Added new DPT option and refinement.
SIGNALING	Changed	Subfield of DYNAMIC option	Changed	ISUPPLUS renamed to BICC
SIGNALING_NETWORK	Unchanged	Subfield of DYNAMIC option	Unchanged	Unchanged

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
BEARER_NETWORK	Unchanged	Subfield of DYNAMIC option	Unchanged	Unchanged
APPLICATION	Changed	Subfield of DYNAMIC option	{OC, POS, RAS, SPBCPT, STRK}	DPT Removed from valid entry range. Should now be provisioned as a DPT option.
OPTION	Changed	Selector subfield of OPTINFO	DPT	Remove DPT from list of valid APPLICATIONs
PROTOCOL	New	Subfield of DPT option	{BICC, SIPT}	The DPT signalling protocol.
BEARER_NETWORK	New	Subfield of DPT option	BNETNAME from table BEARNETS	The BNETNAME of a bearer network provisioned in table BEARNETS.
PROTOCOL	New	Subfield of DPT option	SIPT	Subfields when protocol = SIPT.
NGSS	NEW	Subfield of SIPT protocol	{N,Y}	Identifies if the new NGSS SIP architecture is being used
DEST_MGCNAME	New	Subfield of NGSS 'N' selector	MGCINV_KEY	Enter the Media Gateway Controller (MGC) name from table MGCINV.
TPROFILE	New	Subfield of NGSS 'N' selector	TPROFILE_NAME	Enter the telephony profile name from table TELEPROF.
ALT_HOST_MGCNAME	New	Subfield of NGSS 'N' selector	Vector of up to 32 chars.	Enter an alternative Media Gateway Controller (MGC) name.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
INTER_DOMAIN	New	Subfield of NGSS 'N' and NGSS 'Y' selector	N, Y	Indicates if the SIP-T trunks are inter-domain or intra-domain (between Nortel Networks equipment in the same addressable range).
PROTOCOL	New	Subfield of DPT option	BICC	Subfields when protocol = BICC (old ISUPPLUS)
CAPABILITY_SET	New	Subfield of BICC protocol	{1 to 2}	This represents the BICC capability set (CS). If the remote switch (other side of the DPT trunk) is unable to support CS2 then datafill the CAPABILITY_SET as 1. If the remote switch can support CS2 then datafill CAPABILITY_SET as 2.

Datafill example

The following example shows sample datafill for table TRKOPTS.

Example Datafill

```

TABLE: TRKOPTS
OPTKEY          OPTINFO
-----
DPTTRK DPT      DPT BICC NET_AAL1 1
SIPTRK DPT      DPT SIPT NET_IP N MGC2 PROF MGCTWO Y
OCTRK  DYNAMIC  DYNAMIC ISUP IP IP OC $

```

Table release history update

- DPT is removed from APPLICATION field under the DYNAMIC option.
- DPT is added as a new OPTION.
- NGSS is added as a new selector field under the SIPT protocol

Supplementary information

The signaling network field is not required for DPT. The signaling protocol implies the signaling network: BICC implies SS7, and SIPT implies IP.

The bearer_fabric provisioned for DPT in table TRKOPTS indicates the bearer fabric for a specific DPT trunk group, and a given DPT trunk group can only have one bearer fabric.

GWC DPT trunk “agents” (provisioned in table SERVSINV) will be associated with the DPT trunk group during call processing based on the signaling protocol only. Bearer fabric is not provisioned against DPT GWCs in table SERVINV.

SPM DPT trunk “agents” (provisioned in table MNNODE) will be associated with the DPT trunk group during call processing based on both the signaling protocol and the bearer network provisioned in table MNNODE.

The new NGSS (New Generation Session Server) selector identifies the SIP architecture used by the trunk group. When the new NGSS architecture is selected only INTER_DOMAIN data is necessary. However, when NGSS is not selected, the fields previously under the Dynamic tuple are required.

TRKOPTS Provisioning Restrictions

Field	Provisioning Restrictions
BEARNETS	• BNETNAME must be provisioned in table BEARNETS. • Ensure compatibility of the signalling type with the fabric type of the bearer network. • Changes are allowed without restriction and will take effect immediately. Trunk members that are currently call processing will retain their existing network until the call is terminated.
PROTOCOL	• Changes to the protocol field are not allowed for DPT.

Translation verification other tools

N/A

Core Tables OFRT, OFR2, OFR3, OFR4

Office Routing Tables

Same change applies to each

Functional description

Unchanged.

New CND/NOT selector condition of BEARNET, to allow conditional routing based on the originator’s bearer network.

Changed the name of the PKT conditional selector to FABRIC, and increased the allowable FABRIC range from {ENET} to {ENET, AAL1, AAL2, IP}.

Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

BEARNETS

OFRT

Size

Not Changed

Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
OFRT	unchanged	unchanged	unchanged
OFR2	unchanged	unchanged	unchanged
OFR3	unchanged	unchanged	unchanged
OFR4	unchanged	unchanged	unchanged

Fields/OIDs

The following table lists fields/OIDs for OFRT, OFR2, OFR3, OFR4.

If CND/NOT condition is FABRIC, will be prompted for FABSEL.

If CND/NOT condition is BEARNET, will be prompted for BEARNETSEL.

OFRn Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RTE	Unchanged			
RTESEL	Unchanged			
CNDSEL	Changed	Yes	ALWAYS,RND,SNPA,EA,TO D,MIGRATE,NARS,COSMA P,NRR,SITE,CALLCHR,INT ERLATA, PKT ,TOPEAALT,T OPEAXFR,TOPEACLS,STS , FABRIC,BEARNET	Conditional Selector based on Bearer FABRIC and Network.
NOTSEL	Changed	Yes	ALWAYS,RND,SNPA,EA,TO D,MIGRATE,NARS,COSMA P,NRR,SITE,CALLCHR,INT ERLATA, PKT ,TOPEAALT,T OPEAXFR,TOPEACLS,STS, FABRIC,BEARNET	NOT Selector based on Bearer FABRIC and Network

OFRn Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
FABSEL	Changed.	No	ENET, AAL1, AAL2, IP	Fabrics defined in table BEARNETS
BEARNETS EL	NEW	No	Network Name	NTWKNAME values provisioned in Table BEARNETS

Datafill example

The following examples shows sample datafill for table OFRT.

CND BEARNET

```
TABLE OFRT
POS 99
100 (CND BEARNET DFLTTDM ST 901)
(CND BEARNET DFLTIP ST 902)
(CND BEARNET DFLTATM ST 903) $ $
```

Figure 1 CND FABRIC Selector Criteria ENET, IP and ATM

```
TABLE OFRT
POS 100
100 (CND FABRIC ENET ST 901)
(CND FABRIC IP ST 902)
(CND FABRIC AAL1 ST 903)
(CND FABRIC AAL2 ST 904) $ $
```

Table release history update

- CND/NOT PKT selector renamed to “FABRIC” and enhanced to support AAL1, AAL2 and IP fabrics.
- New BEARNET CND/NOT selector to support criteria checking based on network name of the originating agent.

Supplementary information

The above mentioned changes are applicable to all the routing tables OFR2, OFR3, OFR4, IBNRTE, IBNRT2, IBNRT3, IBNRT4 and HNPACONT\$RTEREF that have CND and NOT bound in as the route selector.

The bearer network of the originator can be provisioned in one of the following tables: MNNODE, SERVINV, or TRKOPTS (for DPT).

Translation verification other tools

The following example shows the output from Traver when it is used to verify OFRT.

Traver example: with BEARNET Option

```
traver tr isupicitt BEARNET MyAAL1NW 7211001 b
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING. CALL TYPE DEFAULT IS NP. PLEASE REFER TO
DOCUMENTATION.
TABLE TRKGRP
ISUPICITT ATC 0 NPDGP NCRT IC NIL MIDL EAP4 NSCR 613 613 ITT Y EAPLAN N COMB N $
TABLE STDPRTCT
EAP4 ( 0) ( 0) 0
. SUBTABLE STDPRT
. KEY NOT FOUND
. DEFAULT VALUE IS: N NP 0 NA
. SUBTABLE AMAPRT
. KEY NOT FOUND
. DEFAULT VALUE IS: NONE OVRNONE N
TABLE HNPACONT
613 Y 1002 2 ( 7) ( 1) ( 84) ( 0) 2 $
. SUBTABLE HNPACODE
. 721 721 LRTE 1001
. SUBTABLE RTEREF
. 1001 T OFRT 1001
. . TABLE OFRT
. . 1001 CND BEARNET TDM_ENET ST 1002
. . . CND BEARNET MYAAL1NW ST 1003
. . . SAME TABLE
. . . 1002 S D ISUPITOG
. . . EXIT SAME TABLE
. . . CND BEARNET MYIP4NW ST 1004
. . EXIT TABLE OFRT
. EXIT TABLE RTEREF
EXIT TABLE HNPACONT
...
...

AIN Info Analyzed TDP: trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 ISUPITOG 7211001 ST

TREATMENT ROUTES. TREATMENT IS: GNCT
1 *OFLO

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

Core Tables IBNRTn (IBNRTE, IBNRT2, IBNRT3, IBNRT4)

IBN Routing Table

Functional description

Unchanged

Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

BEARNETS

IBNRTE, IBNRT2, IBNRT3, IBNRT4

Size**Table size**

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
IBNRTE	Unchanged	Unchanged	Unchanged
IBNRT2	Unchanged	Unchanged	Unchanged
IBNRT3	Unchanged	Unchanged	Unchanged
IBNRT4	Unchanged	Unchanged	Unchanged

Fields/OIDs

The following table lists fields/OIDs for OFRT, OFR2, OFR3, OFR4.

If CND/NOT condition is FABRIC, will be prompted for PKTSEL.

If CND/NOT condition is BEARNET, will be prompted for BEARNETSEL.

IBNRTn Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RTE	Unchanged			
RTESEL	Unchanged			
CNDSEL	Changed	Yes	ALWAYS,RND,SNPA,EA,TO D,MIGRATE,NARS,COSMA P,NRR,SITE,CALLCHR,INT ERLATA, ~~PKT~~ ,TOPEAALT,T OPEAXFR,TOPEACLS,ST S, FABRIC,BEARNET	Conditional Selector based on Bearer FABRIC and Network.

IBNRTn Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NOTSEL	Changed	Yes	ALWAYS,RND,SNPA,EA,TO D,MIGRATE,NARS,COSMA P,NRR,SITE,CALLCHR,INT ERLATA, ~~PKT~~ ,TOPEAALT,T OPEAXFR,TOPEACLS,ST S, FABRIC,BEARNET	NOT Selector based on Bearer FABRIC and Network
PKTSEL	Changed.	No	ENET, AAL1, AAL2, IP	Fabrics defined in table BEARNETS
BEARNETSEL	NEW	No	Network Name	NTWKNAME values provisioned in Table BEARNETS

Datafill example

Similar to the above examples.

Table release history update

- CND/NOT PKT selector renamed to “FABRIC” and enhanced to support AAL1, AAL2 and IP fabrics.
- New BEARNET CND/NOT selector to support criteria checking based on network name of the originating agent.

Supplementary information

The bearer network of the originator can be provisioned in one of the following tables: MNNODE, SERVRINV, or TRKOPTS (for DPT).

Translation verification other tools

Refer to TRAVER information under table OFRT.

Core Tables HNPACONT::RTEREF and FNPACONT::RTEREF

Subtable Route Reference from the Home Numbering Plan Area

Subtable Route Reference from the Foreign Numbering Plan Area

Changes are the same as for OFRn and IBNRTn.

Functional description

Refer to OFRn.

Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

BEARNETS

HNPACONT::RTEREF & FNPACONT::RTEREF (order between these is unchanged)

Size

Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
HNPACONT::RTEREF	Unchanged	Unchanged	Unchanged
FNPACONT::RTEREF	Unchanged	Unchanged	Unchanged

Fields/OIDs

Same changes as table OFRn.

Datafill example

Refer to table OFRn.

Table release history update

- CND/NOT PKT selector renamed to “FABRIC” and enhanced to support AAL1, AAL2 and IP fabrics.
- New BEARNET CND/NOT selector to support criteria checking based on network name of the originating agent.

Supplementary information

The bearer network of the originator can be provisioned in one of the following tables: MNNODE, SERVINV, or TRKOPTS (for DPT).

Translation verification other tools

Refer to OFRn.

GWC_NETWORK_CODEC_PROFILE

Functional description

This new table is used to store network codec profiles that are created by the customer. The profiles will be used when the customer adds a GWC node.

Fields

The following table lists fields of this table.

Table field descriptions

Field	New/ Changed	Entry	Explanation and action
profilename	New	VARCHAR 2(32)	The name of the profile. It is not allow to be NULL. This field is the primary key of this table.

Field	New/ Changed	Entry	Explanation and action
bearerpath	New	NUMBER	Indicates the bearer network fabric type. Refer to table "BEARERPATH_MAP". The default value is "0".
defaultcodec	New	NUMBER	Indicate the default codec. Refer to table "CODEC_MAP". The default value is "0".
preferredcodec	New	NUMBER	Indicate the preferred codec. Refer to table "CODEC_MAP". The default value is "0".
alternativecodec	New	NUMBER	Indicate the alternative codec. Refer to table "CODEC_MAP". The default value is "0".
packetizationinteger	New	NUMBER	Indicate the packetization rate. Refer to table "PACKETIZATION_MAP". The default value is "0".
t38	New	NUMBER(1)	Indicate whether the T38 setting is enabled. Available values are "0" and "1". Number "0" indicates disabled, number "1" indicates enabled. The default value is "0".
rfc2833	New	NUMBER(1)	Indicate whether the RFC2833 setting is enabled. Available values are "0" and "1". Number "0" indicates disabled, number "1" indicates enabled. The default value is "0".
comfortnoise	New	NUMBER(1)	Indicate whether the comfort noise setting is enabled. Available values are "0" and "1". Number "0" indicates disabled, number "1" indicates enabled. The default value is "0".
bearertypedefault	New	CHAR(1)	Indicate whether this profile is a default profile. Available values are "Y" and "N". Char "Y" indicates this profile is default profile for this bearer network type, char "N" indicates this profile is not the default one. This field can not be NULL. The default value is "N". Please note that there will be up to 1 default profile every bearer network fabric type.
networkdefault	New	CHAR(1)	Indicate whether this profile is network default profile. Available values are "Y" and "N". Char "Y" indicates this profile is the default profile in network, char "N" indicates this profile is not the default one. This field can not be NULL. The default value is "N". Please note that there will be up to 1 network default profile totally.

GWCPROFILE

Functional description

This table is used to store attributes of Gateway Controller profile. One new field will be added into this table, which is used to indicate whether network instance is needed to be associated to this GWC or not.

Fields

The following table lists the new field of this table.

Table field descriptions

Field	New/ Changed	Entry	Explanation and action
BEARER_INSTANCE_REQUIRE	New	CHAR(1)	Indicate whether network instance is needed to be associated to this GWC or not. Available values are "Y" and "N". Char "Y" indicates need, char "N" indicates not need. The default value is "Y". This field can not be NULL.

GATEWAYPROFILE

Functional description

This table is used to store attributes of Gateway profile. One new field will be added into this table, which is used to enhance the fabric type check when customer associate gateway to GWC node. Please refer to DID document for details.

Fields

The following table lists fields of this table.

Table field descriptions

Field	New/ Changed	Entry	Explanation and action
BEARER_FABRIC_RESTRICTION_LIST	New	Embedded table of "RestrictList_NT" type	The Name of this field is: Bearer fabric restriction list. This field can be NULL. This field would list the bearer fabrics to which the gateway is restricted. In most cases, this list will be empty and there will be no restriction. But for some special gateway (e.g. MG9000IP and ATM versions), the values would be provided.

Service Orders (SO) (CM & SESM)

Not applicable.

Software optionality control (SOC)

Not applicable.

Element Management

Prior to SN07, the SESM server could support only one bearer network fabric type (IP/AAL1/AAL2) at one time. As of SN07, each GWC will be associated with a bearer network instance, which defines the associated bearer network fabric type. This information will be provided by the customer as they add the GWC through the GWC-EM. In addition to the bearer fabric instance, GWC-EM will allow the customer to define multiple network codec “profiles” in the system and will allow the customer to select the desired profile as they add the GWC to the network.

New/modified GUIs

New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
GWC-EM	Changed

GUI information

GWC-EM GUI

Gateway Controller Element Manager Graphical User Interface

Functional description

The GWC-EM database will be changed to include a new MIB table: GET_NETWORK_CODEC_PROFILE.

The following functionality is added to the GWC-EM:

1. Support the provisioning of multiple network codec profiles.
 - Display network codec profile on GWC-EM GUI.
 - Add network codec profile from GWC-EM GUI.
 - Delete network codec profile from GWC-EM GUI.
 - Change network codec profile from GWC-EM GUI.
2. Support the specification of a bearer network fabric instance and a network codec profile for each GWC.
 - Display bearer network fabric instance and network codec profile of each GWC on GWC-EM GUI.
 - Associate bearer network fabric instance and network codec profile with one GWC when adding GWC node from GWC-EM GUI.

- Change the associated network codec profile of one GWC node from GWC-EM GUI.

GUI usage and implications

GUIs must be used in the following sequence:

Current datafill order unchanged.

GUI size

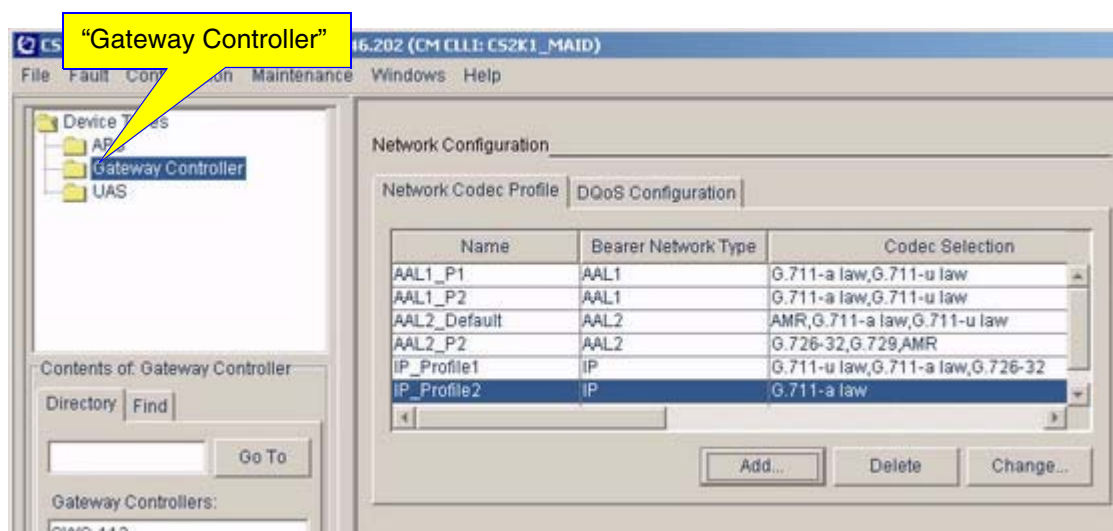
New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
GWC-EM	Unchanged	Unchanged	Unchanged

Usage Example: Display network codec profile

When customer click the “Gateway Controller” type from the device type tree at the left side, all network codec profiles will be displayed on the right side. (Please refer to “ Network codec profile display panel”.)

Network codec profile display panel



All existing codec profiles will be displayed in a table, each profile includes following parameters:

Parameters of network codec profile

Parameter name	Description	Notes
Name	The name of the profile.	

Parameter name	Description	Notes
Bearer Network Type	Indicates the bearer network fabric type.	
Codec Selection	Indicate the codecs used in this profile.	
Packetization rate	Indicate the packetization rate.	For IP bearer type only.
T-38	Indicate whether the T38 setting is enabled.	For IP bearer type only.
RFC2833	Indicate whether the RFC2833 setting is enabled.	For IP bearer type only.
Comfort noise	Indicate whether the comfort noise setting is enabled.	For IP bearer type only.
Default Profile	Indicate whether this profile is a default profile. Please note that there will be up to 1 default profile every bear network fabric type.	

Usage Example: Add network codec profile

Customer will be able to add one new network codec profile just by clicking the “Add” button, then a dialog “Add network codec profile” will be popped up. (Please refer to the following figure.)

Add network codec profile dialog

The screenshot shows the "Add network codec profile" dialog box. It features a "Profile Name" input field and a "Bearer Network Type" dropdown menu currently set to "IP". The "Codec Selection Options" section includes a list of "Available Codecs" (G.729, G.711-a law, G.711-u law) with "Add >>" and "<< Del" buttons. A central "Codec Selection Order" list box is empty, with "Up" and "Down" buttons below it. To the right, the "Packetization Rate" is set to "10 ms", and there are checkboxes for "T-38", "RFC2833", "Comfort Noise", "Set as bearer type default", and "Set as network default". "OK" and "Cancel" buttons are at the bottom right.

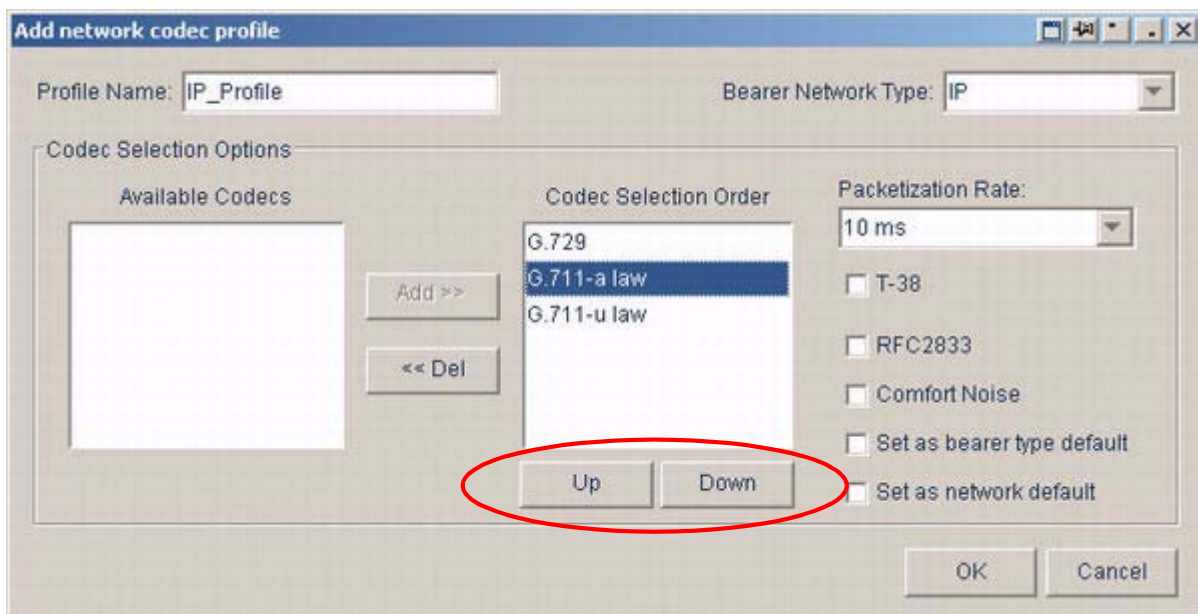
When customer select a bearer network type from the droplist box, the corresponding available codecs will be displayed below in the left list box. The available codec list may be different for different bearer network type.

Please note that the codec selecting is different from SN06 version. Customer won't select different codec for “Compression codec”, “Default codec” and “Alternative Codec” one by one. The available codecs will be listed at left side,

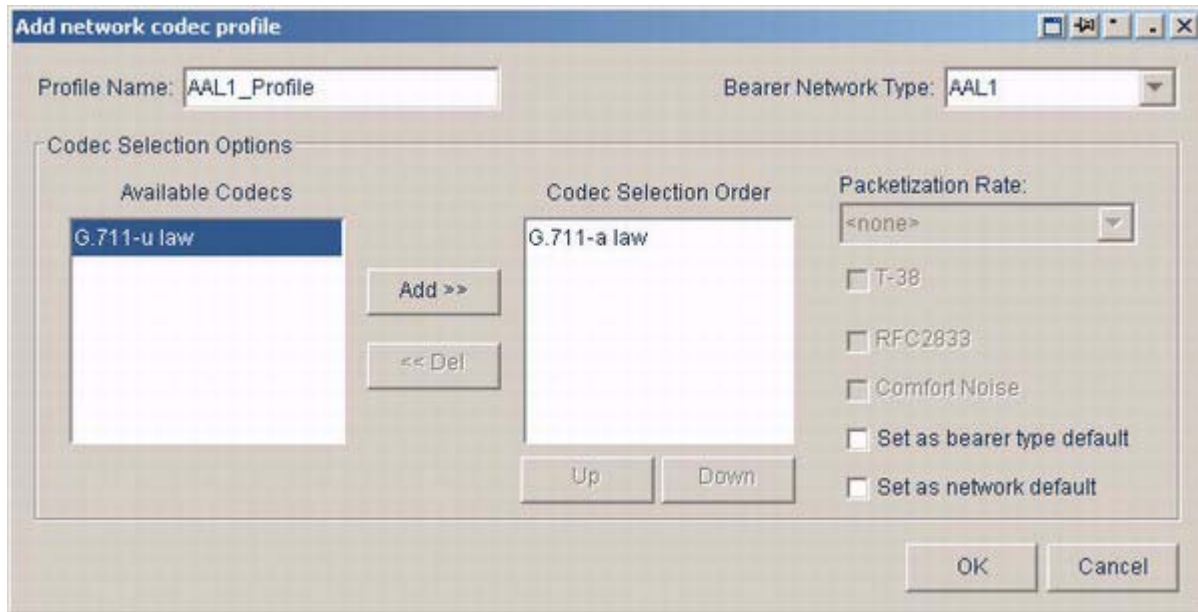
customer should be able to select them just by highlighting codec item and clicking the “Add >>” button. Then the selected codec will be added into codec selection. Contrarily, customer could delete some codec from the selection by highlighting the codec item and clicking the button “<< Del”.

In the codec selection, the order of the codec determines how the device will treat them. For example, the first one will be mapped to “Compression codec”, the second one will be mapped to “Default Codec”, and the last one will be mapped to “Alternative Codec”. Additional, customer could change the order of codecs by highlighting the codec item and clicking the “Up” and “Down” buttons.

Change the order of codecs in the selection

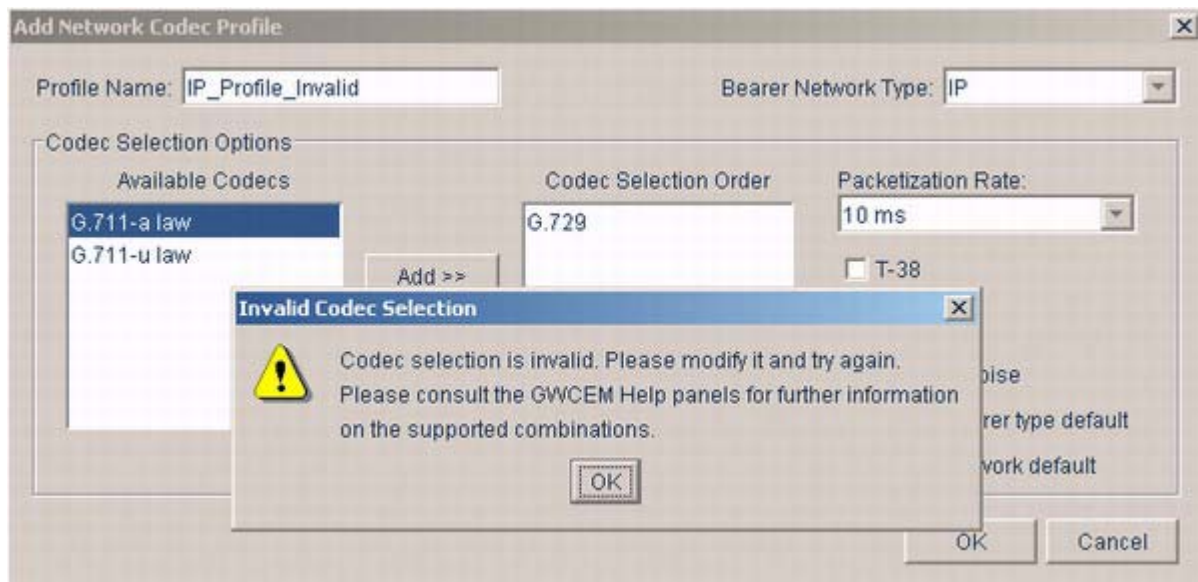


Please note that parameters “Packetization Rate” and LCO options (T38, RFC2833, and Comfort Noise) are settings for IP bearer type only. If customer select “AAL1” or “AAL2” as the bearer network fabric type, these settings will be disabled.

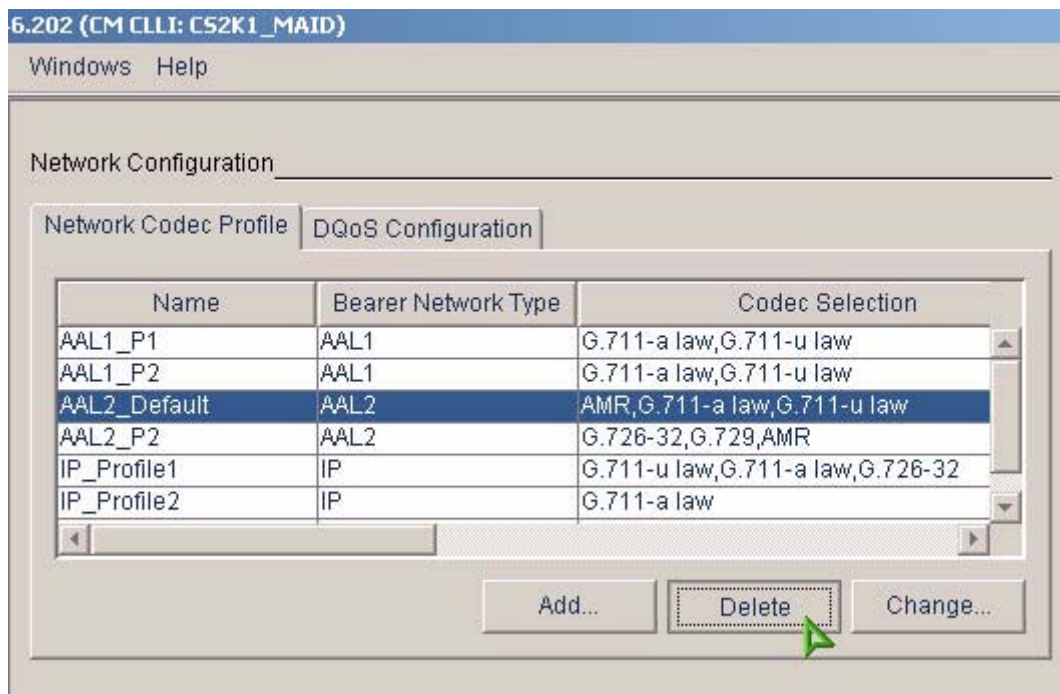
Select “AAL1” as the bearer network fabric type

Customers will be able to use the recommended codec setting by clicking the button “Recommended Codec Setting”, then the recommended setting will be restored into the dialog. Note that the recommended codec setting will be different for different bearer network type.

If customers select an invalid codec selection, alert dialog will be popped up. (Please refer to the following figure.)

Alert dialog for invalid codec selection**Usage Example: Delete network codec profile**

Customer will be able to delete one existing network codec profile just by highlighting the profile row from the table, and click the "Delete" button. (Please refer to the following figure.)

Delete existing network codec profile

Once customers click the “Delete” button, one confirmation dialog will be popped up.

Delete network codec profile confirmation dialog

The operation result will be displayed in a pop-up dialog, and the codec profile table will be updated according to the result. Please note that if any GWC is using this profile, the delete operation will be failed.

Usage Example: Change network codec profile

Customers will be able to change one existing network codec profile just by highlighting the profile row from the table, and clicking the “Change” button. Then the dialog “Change network codec profile” will be popped up. All parameters of the profile will be filled in the dialog. (Please refer to the following figure.)

Change existing network codec profile

Change network codec profile

Profile Name: IP_Profile1 Bearer Network Type: IP

Codec Selection Options

Available Codecs

G.729

Add >>

<< Del

Codec Selection Order

G.711-u law
G.711-a law
G.726-32

Up Down

Packetization Rate: 20 ms

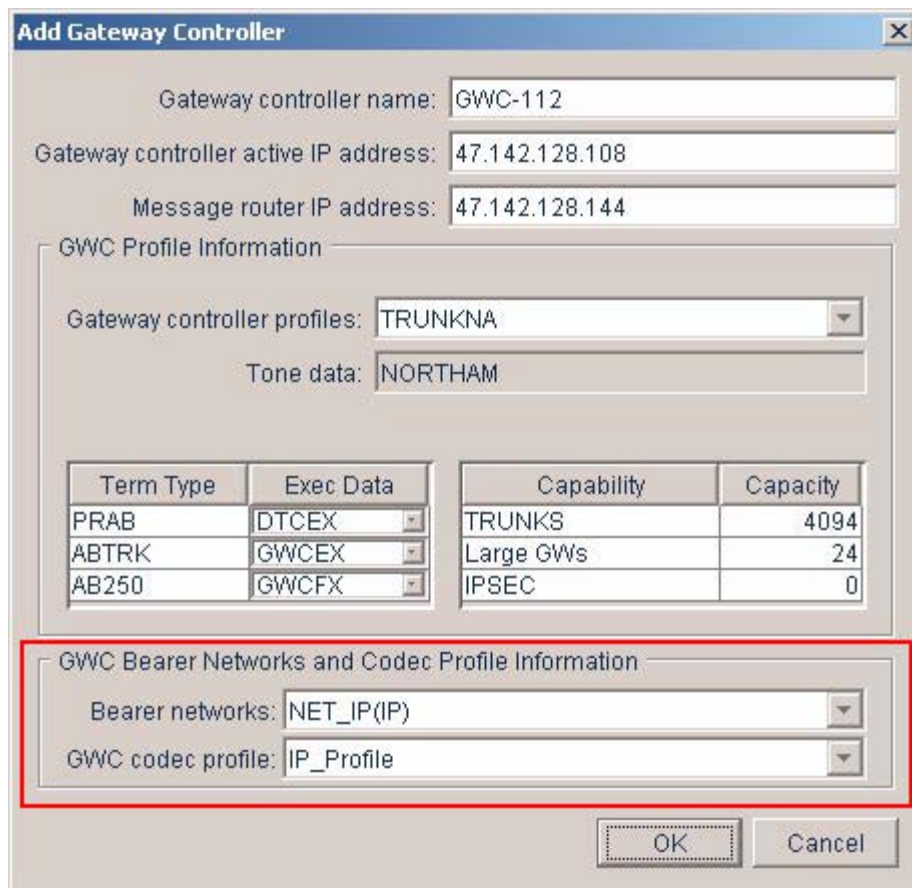
☐ T-38
☐ RFC2833
☐ Comfort Noise
☐ Set as bearer type default
☐ Set as network default

OK Cancel

Note that the bearer network type of the profile is not allowed to be changed. Please refer to section “Usage Example: Add network codec profile” on page 821 for how to change other parameters. Once the profile was updated successfully, these parameters will be updated into all GWCs using this profile.

Usage Example: Display GWC node

A new section will be added to the GWC provisioning panel to indicate the bearer network and codec profile configuration for the selected GWC.

Add GWC node

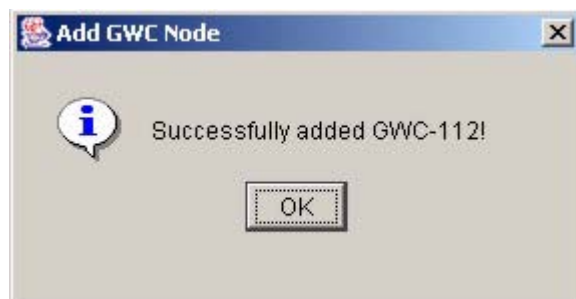
The dialog box titled "Add Gateway Controller" contains the following fields and sections:

- Gateway controller name: GWC-112
- Gateway controller active IP address: 47.142.128.108
- Message router IP address: 47.142.128.144
- GWC Profile Information**
 - Gateway controller profiles: TRUNKNA
 - Tone data: NORTHAM
- | Term Type | Exec Data | Capability | Capacity |
|-----------|-----------|------------|----------|
| PRAB | DTCEX | TRUNKS | 4094 |
| ABTRK | GWCEX | Large GWs | 24 |
| AB250 | GWCFX | IPSEC | 0 |
- GWC Bearer Networks and Codec Profile Information** (highlighted with a red border)
 - Bearer networks: NET_IP(IP)
 - GWC codec profile: IP_Profile
- OK and Cancel buttons

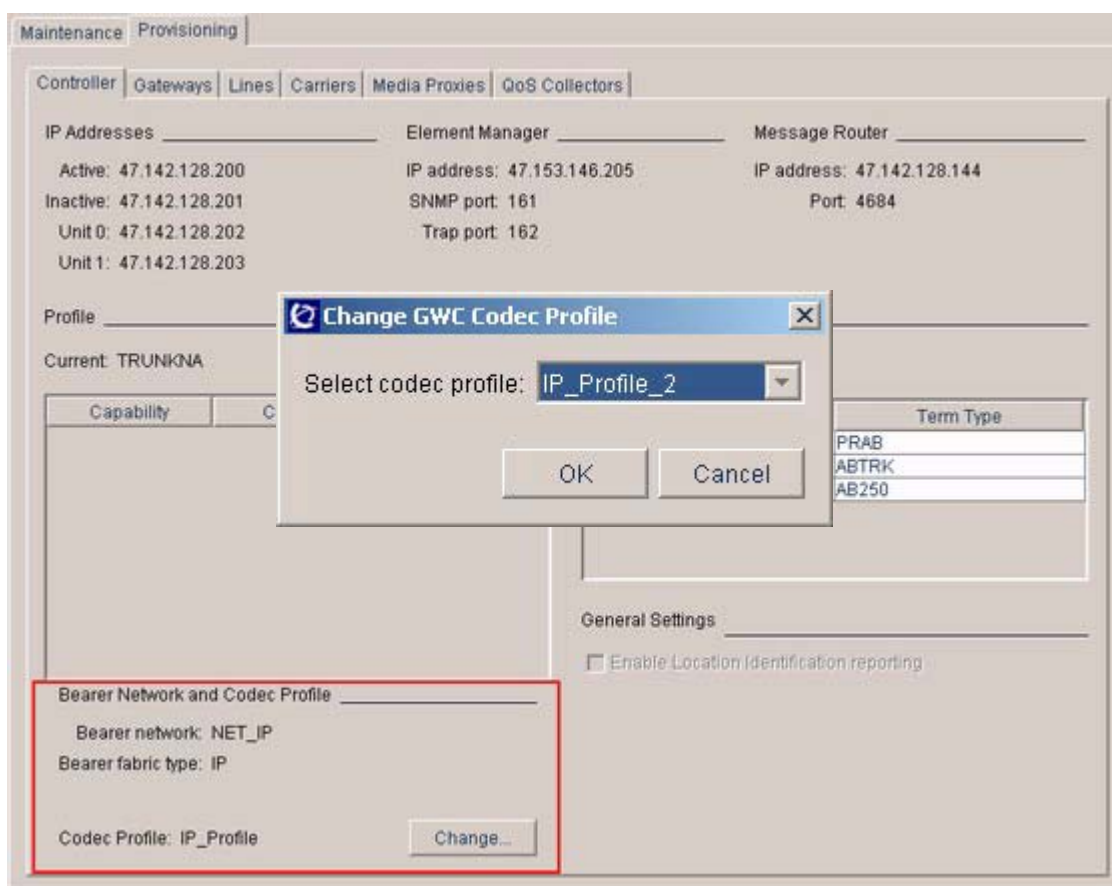
One of these two new boxes contains the bearer network list, another contains the codec profile list. The codec profile list must match the bearer network, that means, if customers select a bearer network instance belonging to "IP" bearer type, then the codec profile box will only contain the names of "IP" codec profiles; if customer select a "AAL1" bearer network instance, the codec profile box will be changed to only contain the "AAL1" codec profile names.

And if customers leave the codec profile box not selected, a default codec profile based on the bearer network type will be selected automatically.

Once the addition operation has been performed successfully, a dialog like the following will be pushed to the customer to indicate that the GWC was added to the system without errors.

Add GWC node result dialog**Usage Example: Change GWC network codec profile**

When customers click the "Change..." button on the right of the codec profile fields on the GWC provisioning panel, a "Change Codec Configuration" dialog will be created like the following figure.

Change GWC's network codec profile

From this dialog, customers can select a different codec profile for the specific GWC even after the GWC has been provisioned already and a dialog with

successful information will be displayed for customers if the operation has been performed without errors. Otherwise, a error message will be returned to the customers.

GUI release history update

1. Support the provisioning of multiple network codec profiles.
 - Display network codec profile on GWC-EM GUI.
 - Add network codec profile from GWC-EM GUI.
 - Delete network codec profile from GWC-EM GUI.
 - Change network codec profile from GWC-EM GUI.
2. Support the specification of a bearer network fabric instance and a network codec profile for each GWC.
 - Display bearer network fabric instance and network codec profile of each GWC on GWC-EM GUI.
 - Associate bearer network fabric instance and network codec profile with one GWC when adding GWC node from GWC-EM GUI.
 - Change the associated network codec profile of one GWC node from GWC-EM GUI.

Supplementary information

Command interface changes

Directory: TRAVER

Directory description

TRAnslations VERification.

Accessing directory: TRAVER

Access to directory or MAP level and return to CI

CI> TRAVER <traver options>

Traver is a single command interface rather than an environment that is entered. You are automatically returned to the CI level after execution of the command.

Command: TRAVER TR

Command type: unchanged

Command target: unchanged

Command availability: unchanged

Command description

Traver an originating trunk based with the digits provided. The originating trunk (TRAVER TR) command is changed as follows:

When encountering a CND FABRIC or CND BEARNET selector in the translations route, three options are created for determining the originator's bearer fabric or network in order to determine how to interpret the CND route selection.

- **TRKMEM** option: The fabric or network of the member specified will be used.
- **NEW BEARNET** option: Allows the user to specify the bearer network (32 char vector identifying a BNETNAME provisioned in table BEARNETS) of the specified trunk group.
- If none of the above options is specified, the TDM network will be assumed for the specified trunk group for non-DPT trunk groups.
- For DPT trunk groups, where none of the above options is specified, the bearer fabric or network will be obtained from table TRKOPTS.

Command syntax

<CommandName> command parameters and variables

Command	Parameters and variables
TRAVER TR	Next par is: <CLI> STRING Enter: <CLI> [<CLLOPT>] [<MBGOPTS>] [<TRIGOPT>] [<TRKMEM>] [<BEARNET>] <DIGITS OR N FOR NO DIGITS> [<CDNIE>] [<NSF>] [<TNSIE>] [<OSAIE>] [<BC>] [<SR>] [<PI>] [<TRI>] [<NETINFO>] [<FINFO>] [<RPOAP>] [<RPOAS>] [<NOA>] [<AIN_OPTIONS>] [<AIN_INFO>] [<SCAIIN>]
Parameters and variables	Description
[<TRKMEM>]	Existing option. Input is unchanged. Will now be used to obtain the bearer network and bearer fabric to be used when making conditional translations decisions CND FABRIC or CND BEARNET.

<CommandName> command parameters and variables

Command	Parameters and variables
[<BEARNET>]	New option. Allows user to specify the bearer network (up to 32 character BNETNAME provisioned in table BEARNETS) to use as the originating bearer network. This will also imply the FABRIC, since the FABRIC is a field in table BEARNETS. Both of these will be used when making conditional routing decisions based on FABRIC or BEARNET (CND selectors). The network specified will be used, even if the trunk group does not have members on that network.

Qualifications and warnings

- Non-DPT trunk groups can have members that are spread across the various networks. During call processing, an effort will be made to match the originator's network to a trunk member of a like network. Traver will not be enhanced to show this selection process.
- Line group originations (e.g.: HUNT, MDN, ACD) will use the network fabric of the originating member of the group to determine the network fabric.
- If the FABRIC or BEARNET option is used to specify the bearer network information of a trunk group, this information will be used in TRAVER to determine the routing, even if the trunk group does not have members in that network. This allows users to test the translations before adding members, but also allows for verification to pass when during call processing it could actually fail.

Responses**Undefined BEARNET specified**

Since the user will be prompted for a 32 character string rather than a list of tuples provisioned in table BEARNET, an invalid entry should be met with a response indicating where to look for the valid information.

MAP outputs with associated meanings and actions

Command TRAVER TR <trunk group CLLI> <digits> BEARNET <BNETNAME>
<RESPONSE>: <description> Meaning: The BEARNET name entered does not exist in table BEARNETS. System or user actions: Choose a BNETNAME of out table BEARNETS.
<RESPONSE>: <description> Meaning: System or user actions:

Example of TRKMEM option

Usage examples for TRAVER TR command with TRKMEM option

Description of task:	traver tr isupicitt TRKMEM 1001 7211001 b
Description of task	Verify the translations for originating trunk group ISUPICITT dialing '7211001' where the network and fabric used in the CND BEARNET and CND FABRIC conditional selectors will be obtained from the trunk member data.
Command: MAP response:	<pre> WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE BILLING. CALL TYPE DEFAULT IS NP. PLEASE REFER TO DOCUMENTATION. TABLE TRKGRP ISUPICITT ATC 0 NPDGP NCRT IC NIL MIDL EAP4 NSCR 613 613 ITT Y EAPLAN N COMB N \$ TABLE STDPRTCT EAP4 (0) (0) 0 . SUBTABLE STDPRT . KEY NOT FOUND . DEFAULT VALUE IS: N NP 0 NA . SUBTABLE AMAPRT . KEY NOT FOUND . DEFAULT VALUE IS: NONE OVRNONE N TABLE HNPACONT 613 Y 1002 2 (7) (1) (84) (0) 2 \$. SUBTABLE HNPACODE . 721 721 LRTE 1001 . SUBTABLE RTEREF . 1001 T OFRT 1001 . . TABLE OFRT . . 1001 CND BEARNET TDM_ENET ST 1002 . . . CND BEARNET MYAALINW ST 1003 . . . SAME TABLE . . . 1003 S D ATMTRK1 . . . EXIT SAME TABLE . . . CND BEARNET MYIP4NW ST 1004 . . EXIT TABLE OFRT . EXIT TABLE RTEREF EXIT TABLE HNPACONT AIN Info Analyzed TDP: trigger criteria not met. +++ TRAVER: SUCCESSFUL CALL TRACE +++ DIGIT TRANSLATION ROUTES 1 ISUPITOG 7211001 ST TREATMENT ROUTES. TREATMENT IS: GNCT 1 *OFLO +++ TRAVER: SUCCESSFUL CALL TRACE +++ </pre>

Usage examples for TRAVER TR command with BEARNET option

Description of task:	traver tr isupicitt BEARNET MyAAL1NW 7211001 b
Description of task	Verify the translations for originating trunk group ISUPICITT dialing '7211001' where the network and fabric used in the CND BEARNET and CND FABRIC conditional selectors will be obtained from the BEARNETS MyAAL1NW tuple entry.
Command: MAP response:	<pre> WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE BILLING. CALL TYPE DEFAULT IS NP. PLEASE REFER TO DOCUMENTATION. TABLE TRKGRP ISUPICITT ATC 0 NPDGP NCRT IC NIL MIDL EAP4 NSCR 613 613 ITT Y EAPLAN N COMB N \$ TABLE STDPRTCT EAP4 (0) (0) 0 . SUBTABLE STDPRT . KEY NOT FOUND . DEFAULT VALUE IS: N NP 0 NA . SUBTABLE AMAPRT . KEY NOT FOUND . DEFAULT VALUE IS: NONE OVRNONE N TABLE HNPACONT 613 Y 1002 2 (7) (1) (84) (0) 2 \$. SUBTABLE HNPACODE . 721 721 LRTE 1001 . SUBTABLE RTEREF . 1001 T OFRT 1001 . . TABLE OFRT . . 1001 CND BEARNET TDM_ENET ST 1002 . . CND BEARNET MYAAL1NW ST 1003 . . . SAME TABLE . . . 1002 S D ISUPITOG . . . EXIT SAME TABLE . . CND BEARNET MYIP4NW ST 1004 . . EXIT TABLE OFRT . EXIT TABLE RTEREF EXIT TABLE HNPACONT AIN Info Analyzed TDP: trigger criteria not met. +++ TRAVER: SUCCESSFUL CALL TRACE +++ DIGIT TRANSLATION ROUTES 1 ISUPITOG 7211001 ST TREATMENT ROUTES. TREATMENT IS: GNCT 1 *OFLO +++ TRAVER: SUCCESSFUL CALL TRACE +++ </pre>

Security

Not applicable.

Configuration Walkthrough

NA

Performance for A00003487

Performance management strategy

Trimodal Call Server provides support for multiple bearer networks in a single CS2K Call Server. In order to monitor the performance of the call server, additional OM's are needed. These new OM's provide per-bearer network performance metric collection that will enable the customer management system to monitor the performance of the call server as a whole as well as the individual bearer networks.

Performance management tools and utilities

No change

Performance Measurements (PM), Operational Measurements (OM), and stats

The following is a list of the new and changed OM groups for the Trimodal Call Server feature:

- DPTNODE (changed)
- DPTOFCP (new)
- IWBM (changed)
- OFZ2NET1 (new)
- OFZ2NET2 (new)
- TRK2NET1 (new)
- TRK2NET2 (new)

PM, OM, and stats format

DPTNODE OM Group

OM description

DPTNODE OM group measures the DPT performance for each DPT capable node. The group contains registers that maintain DPT terminal usage and failure counts.

Release history update

The DPTNODE OM group is being modified in SN07 to add additional information to the OM tuples. If the DPT Node is a GWC, then the associated DPT protocol (i.e., BICC or SIP-T) is added to the information. If the DPT Node is an SPM (i.e., either MG4K or DTP SPM), then the associated bearer network, DPT protocol and SPM node type is added to the information. The registers are unchanged and the pegging of the registers are unchanged.

The addition of this new information is controlled by the value of a new SN07 office parameter, MULTINET_DISPLAY_ACTIVE. If this parameter is set to 'Y', then the new information is displayed. If the parameter is set to 'N', then the DPTNODE OM group appears as it did prior to SN07.

Registers

DPTNODE OM group registers display on the MAP terminal as follows:

DPTNODE OM Group Display

```
>omshow dptnode active
```

```
DPTNODE
```

```
CLASS: ACTIVE
```

```
START:2003/09/23 09:05:00 TUE; STOP: 2003/09/23 09:09:52 Tue;
```

```
SLOWSAMPLES: 3 ; FASTSAMPLES: 29 ;
```

```
INFO (DPT_PM_INFO)
```

		DPTGTAT	DPTGTAT2	DPTGTFL	DPTGTFL0
		DPTUSAG	DPTUSAG2	DPTHWT	
0					
	GWC 3 93 BICC				
		0	0	0	0
		0	0	0	
1					
	GWC 4 94 SIPT				
		0	0	0	0
		0	0	0	
2					
	SPM 1 70 NET 2 NET_AAL1 BICC SMG4				
		0	0	0	0
		0	0	0	
3					
	SPM 2 71 NET 0 ENET_TO_AAL1_DPT BICC DPT				
		0	0	0	0
		0	0	0	

Group structure

DPTNODE OM group provides 1 tuple(s) for each GWC or SPM node that is capable of hosting a DPT call.

Key field: Unchanged

Info field: DPT_PM_INFO

If the DPT node is a GWC, then the info field will contain the DPT protocol that is associated with the GWC. The DPT protocol will either be BICC or SIP-T. This information is derived from datafill for the GWC subnodes found in Table SERVINV.

If the DPT node is an SPM, then the info field will contain the associated bearer network, the DPT protocol and the SPM node type. The bearer network is both the Network ID and the Network Name as datafilled in Table BEARNETS and linked to the associated SPM node in Table MNNODE. The DPT protocol will always be BICC because SPM nodes do not support SIP-T protocol in SN07. The SPM node type is either SMG4 (for MG4Ks) or DPT (for DPT SPMs). This information is derived from the node type found in Table MNNODE.

Associated OM groups

Unchanged.

Associated functional groups

The following functional groups are associated with DPTNODE OM group:
Unchanged

Associated functionality codes

Functionality codes associated with OM group

Functionality	Code
Dynamic Packet Trunks	

OM group registers logic flow chart

Unchanged.

Register DPTGTAT

Register description

Get Terminal Attempts (DPTGTAT) registers a peg for each attempt to get a DPT terminal on the associated node.

Register release history update

Register is unchanged in SN07.

Associated registers

DPTGTAT2 (an extension register for DPTGTAT)

Associated logs

Unchanged.

Register DPTGTFL**Register description**

Get Terminal Failures (DPTGTFL) registers a peg for each failed attempt to get an un-optimized DPT terminal on the associated node.

Register release history update

Register is unchanged in SN07.

Associated registers

None.

Associated logs

Unchanged.

Register DPTGTFLO**Register description**

Get Terminal Failures Optimized (DPTGTFLO) registers a peg for each failed attempt to get an optimized DPT terminal on the associated node.

Register release history update

Register is unchanged in SN07.

Associated registers

None.

Associated logs

Unchanged.

Register DPTUSAG**Register description**

DPT Terminal Usage (DPTUSAG) registers a count of the total usage within a transfer period. Usage is pegged by the number of terminals in Call Processing Busy (CPB) or Call Processing Deload (CPD) state at a sampling that occurs every 100 seconds.

Register release history update

Register is unchanged in SN07.

Associated registers

DPTUSAG2 (extension register for DPTUSAG)

Associated logs

Unchanged.

Register DPTHWT**Register description**

DPT Terminals usage High Water (DPTHWT) registers a count of the terminal usage high water mark within a transfer period. The high water mark is equivalent to the following:

- (inservice number) - (low water mark)

The low water mark updates for each attempt to get a terminal. The OM compares the current high water mark to the previous high water mark every 100 seconds. An update is made if the current value exceeds the previous value.

Register release history update

Register is unchanged in SN07.

Associated registers

None.

Associated logs

Unchanged.

DPTOFCP OM Group**OM description**

DPTOFCP OM Group measures the performance of the supported dynamic packet trunk protocols for the office. The two supported protocols are BICC and SIP-T.

Release history update

DPTOFCP OM group is new in SN07.

The addition of this new DPTOFCP OM group is controlled by the value of a new SN07 office parameter, MULTINET_DISPLAY_ACTIVE. If this parameter is set to 'Y', then the new DPTOFCP OM group is displayed. If the parameter is set to 'N', then the DPTOFCP OM group is not displayed.

Registers

DPTOFCP OM group registers display on the MAP terminal as follows:

DPTOFCP OM Group Display

```
>omshow dptofcp active
```

DPTOFCP

CLASS: ACTIVE

START:2003/09/23 09:05:00 TUE; STOP: 2003/09/23 09:09:52 Tue;

SLOWSAMPLES: 3 ; FASTSAMPLES: 29 ;

INFO (DPT_PROTOCOL_INFO)

	DPGTATT	DPGTATT2	DPGETFL	DPGETFL2
	DPUSAGE	DPUSAGE2	DPOTFLO	DPOTFLO2
	DPHWTR	DPHWTR2	DPRTDPL	DPRTDPL2
0				
BICC				
	0	0	0	0
	0	0	0	0
	0	0	0	0
1				
SIPT				
	0	0	0	0
	0	0	0	0
	0	0	0	0

Group structure

DPTOFCP OM group provides 1 tuple(s) for each DPT protocol that is active in the office.

Key field: DPT_PROTOCOL_TYPE {BICC, SIP-T}

Info field: DPT_PROTOCOL_INFO

Identifies the protocol being used in the office.

Associated OM groups

DPTOFC OM group gives an overall office-wide DPT performance measurement. DPTNODE OM group provides a per-DPT capable node performance view.

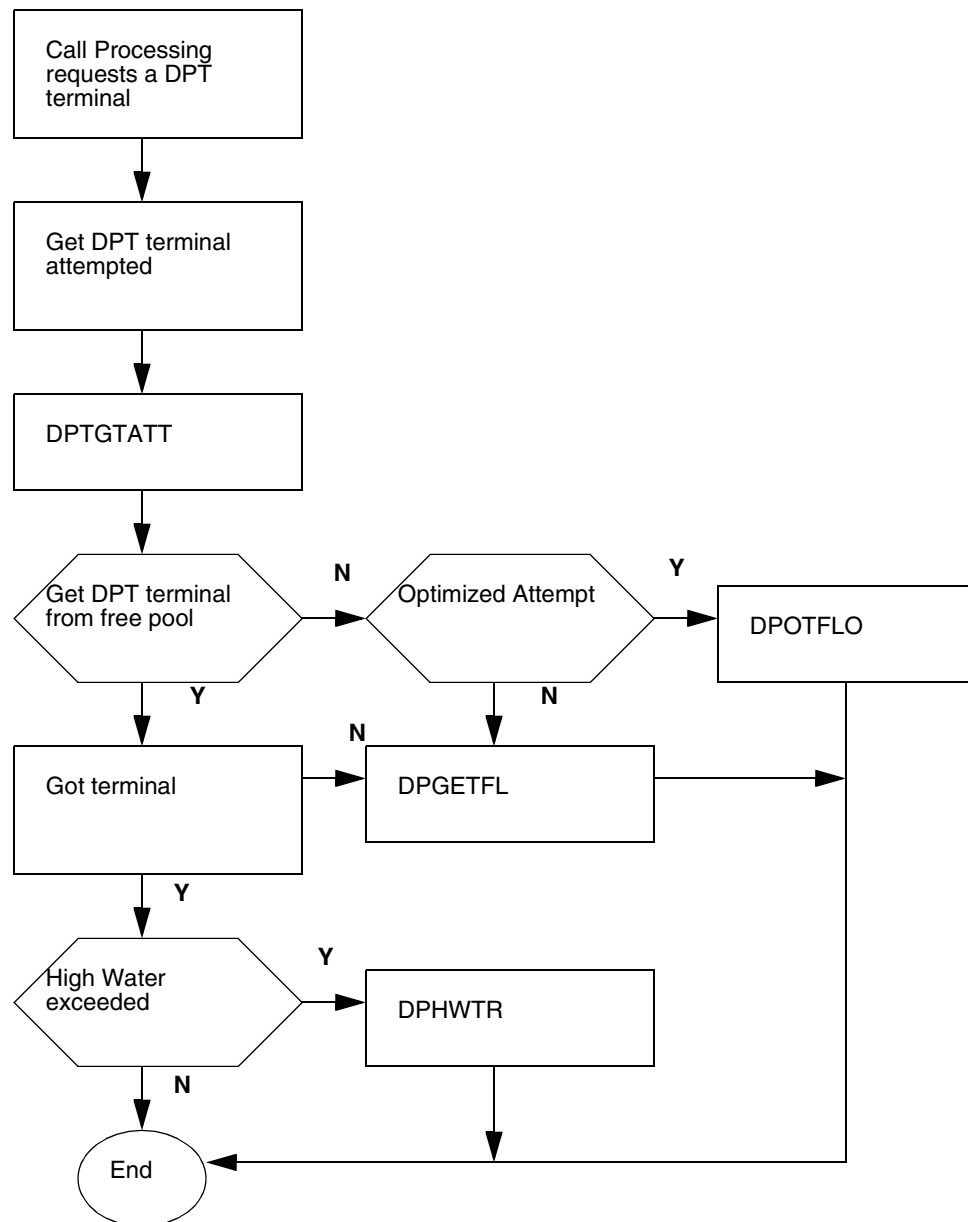
Associated functional groups

The following functional groups are associated with DPTNODE OM group:

- Dynamic Packet Trunks

Associated functionality codes**Functionality codes associated with OM group**

Functionality	Code
Dynamic Packet Trunks	

DPTOFCP OM group registers logic flow chart

Register DPGTATT

Register description

Get Terminal Attempts (DPGTATT) registers a peg for each attempt to get a DPT terminal on the associated protocol.

Register release history update

Register is new in SN07.

Associated registers

DPGTATT2 (an extension register for DPGTATT)

Associated logs

None.

Register DPGETFL

Register description

Get Terminal Failures (DPGETFL) registers a peg for each failed attempt to get an un-optimized DPT terminal on the associated protocol.

Register release history update

Register is new in SN07.

Associated registers

DPGETFL2 (an extension register for DPGETFL).

Associated logs

None.

Register DPOTFLO

Register description

Get Terminal Failures Optimized (DPOTFLO) registers a peg for each failed attempt to get an optimized DPT terminal on the associated protocol.

Register release history update

Register is new in SN07.

Associated registers

DPOTFLO2 (an extension register for DPOTFLO).

Associated logs

None.

Register DPUSAGE

Register description

DPT Terminal Usage (DPUSAGE) registers a count of the total usage within a transfer period. Usage is pegged by the number of terminals in Call Processing Busy (CPB) or Call Processing Deload (CPD) state at a sampling that occurs every 100 seconds.

Register release history update

Register is new in SN07.

Associated registers

DPUSAGE2 (extension register for DPUSAGE)

Associated logs

None.

Register DPHWTR

Register description

DPT Terminals usage High Water (DPHWTR) registers a count of the terminal usage high water mark within a transfer period. The high water mark is equivalent to the following:

- (inservice number) - (low water mark)

The low water mark updates for each attempt to get a terminal. The OM compares the current high water mark to the previous high water mark every 100 seconds. An update is made if the current value exceeds the previous value.

Register release history update

Register is new in SN07.

Associated registers

DPHWTR2 (an extension register for DPHWTR).

Associated logs

None.

Register DPRTDPL

Register description

DPT Port Depletion (DPRTDPL) registers the number of attempts to get a DPT terminal that failed due to port depletion (i.e., attempting to pass the DPT_MAX_PORT office parameter value).

Register release history update

Register is new in SN07.

Associated registers

DPRTDPL2 (an extension register for DPRTDPL).

Associated logs

None.

IWBM OM Group**OM description**

IWBM OM Group is modified to count different events on the specific bridge pools that are defined in the call server.

Release history update

IWBM OM group is changed in SN07.

Registers

IWBM OM group registers display on the MAP terminal as follows:

IWBM OM Group Display

```
>omshow iwbm active
```

IWBM

```
CLASS: ACTIVE
```

```
START:2003/09/23 09:05:00 TUE; STOP: 2003/09/23 09:09:52 Tue;
```

```
SLOWSAMPLES:      3 ; FASTSAMPLES:      29 ;
```

INFO (IWBM_POOL_INFO)

IWGBATT	IWGBATT2	IWGBFAIL	IWGBABRT
IWFBATT	IWFBATT2	IWFBFAIL	IWFBABRT
IWONSET1	IWONSET2	IWABATE1	IWABATE2
IWBTLTST	IWBCNFAN	IWBCALLN	IWBCLTRK

```
0
```

ENET_TO_ATM

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

```
1
```

ENET_TO_IP

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

Group structure

IWBM OM group provides 1 tuple(s) for each IW SPM bridge pool that is active in the office.

Key field: IW SPM bridge pools

Info field: IWBM_POOL_INFO

- Associated bridge pool name (i.e., 'ENET_TO_IP'). This bridge pool name is defined in Table CLLI and Table NETBRDGE. Each IW SPM bridge node is associated with a bridge pool in Table MNNODE.

Associated OM groups

None.

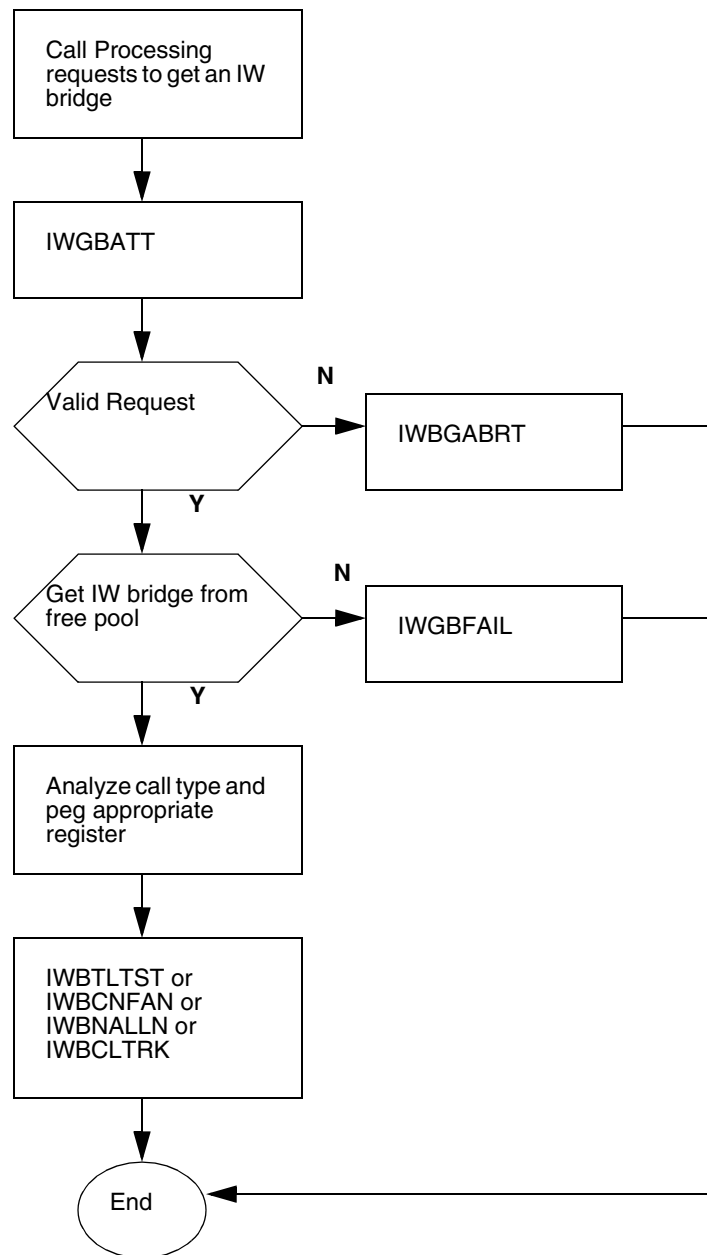
Associated functional groups

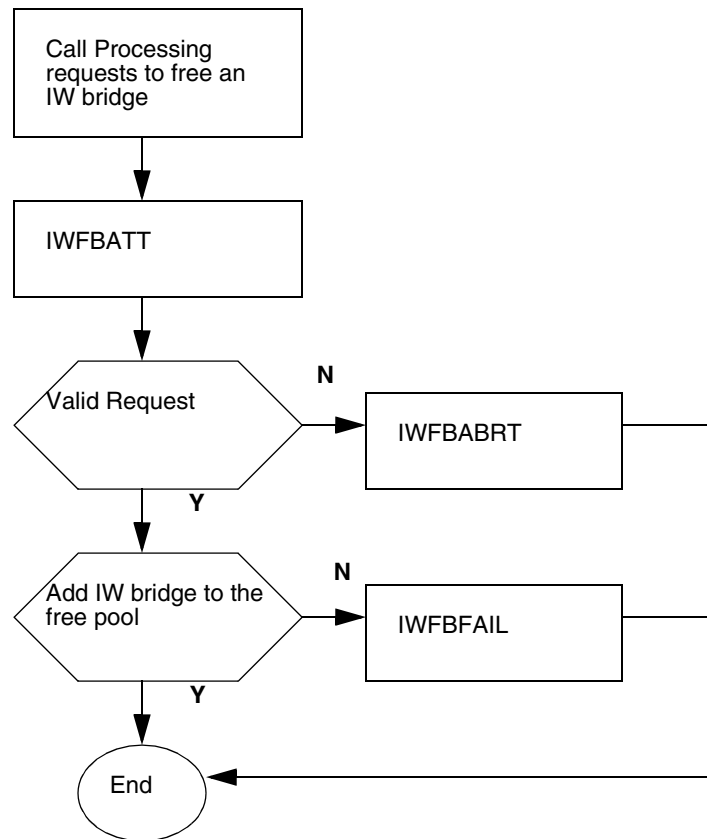
The following functional groups are associated with IWBM OM group:

- IW SPM Bridges

Associated functionality codes**Functionality codes associated with OM group**

Functionality	Code
IW SPM Bridges	

IWBM OM group registers logic flow chart



Register IWGBATT

Register description

IW Get Bridge Attempts (IWGBATT) registers a peg for each attempt to get an IW SPM bridge port on the associated IW SPM bridge node.

Register release history update

Register is changed in SN07.

Associated registers

IWGBATT2 (an extension register for IWGBATT)

Associated logs

None.

Register IWGBFAIL**Register description**

IW Get Bridge Failure (IWGBFAIL) registers a peg when a get bridge attempt fails as a result of queue failure. The normal cause of a queue failure is that all bridges are busy on the associated node.

Register release history update

Register is changed in SN07.

Associated registers

None.

Associated logs

None.

Register IWGBABRT**Register description**

IW Get Bridge Aborted (IWGBABRT) registers a peg when a get bridge attempt aborts the system as a result of incorrect data in the request.

Register release history update

Register is changed in SN07.

Associated registers

None.

Associated logs

None.

Register IWFBATT**Register description**

IW Free Bridge Attempts (IWFBATT) registers a peg when a attempt is made to free an IW SPM bridge from an associated call. When an interworked call ends, the system makes a free bridge attempt.

Register release history update

Register is changed in SN07.

Associated registers

IWFBATT2 (extension register for IWFBATT)

Associated logs

None.

Register IWFBFAIL**Register description**

IW Free Bridge Failure (IWFBFAIL) registers a peg when a free bridge attempt fails.

Register release history update

Register is changed in SN07.

Associated registers

None.

Associated logs

None.

Register IWFBABRT**Register description**

IW Free Bridge Aborted (IWGBABRT) registers a peg when a free bridge attempt aborts the system as a result of incorrect data in the request.

Register release history update

Register is changed in SN07.

Associated registers

None.

Associated logs

None.

Register IWBTLTST**Register description**

IW Bridge for Trunk and Line Testing (IWBTLTST) registers a peg every time an IW bridge is used for a packet agent's access to trunk and/or line test facilities present on the ENET (i.e., MTM test circuits).

Register release history update

Register is changed in SN07.

Associated registers

None.

Associated logs

None.

Register IWONSET1

Register description

IW Bridge Onset 1 (IWONSET1) indicates that the number of in use IW bridges exceeds 70% of the associated bridge pool. The system pegs this register when the number of in use bridges in the pool reaches 70%. The system must peg register IWABATE1 before pegging IWONSET1 again.

Register release history update

Register is changed in SN07.

Associated registers

IWABATE1. The system must peg register IWABATE1 before pegging IWONSET1 again.

Associated logs

None.

Register IWONSET2

Register description

IW Bridge Onset 2 (IWONSET2) indicates that the number of in use IW bridges exceeds 90% of the associated bridge pool. The system pegs this register when the number of in use bridges in the pool reaches 90%. The system must peg register IWABATE2 before pegging IWONSET2 again.

Register release history update

Register is changed in SN07.

Associated registers

IWABATE2. The system must peg register IWABATE2 before pegging IWONSET2 again.

Associated logs

None.

Register IWABATE1

Register description

IW Bridge Abate 1 (IWABATE1) indicates that the total number of IW bridges in use is less than 65% of the associated bridge pool. The system pegs this register after pegging register IWONSET1 and then crosses the 65% threshold. The system must peg register IWONSET1 again before it pegs this register a second time.

Register release history update

Register is changed in SN07.

Associated registers

IWONSET1. The system pegs this register after pegging register IWONSET1 and then crosses the 65% threshold. The system must peg register IWONSET1 again before it pegs this register a second time.

Associated logs

None.

Register IWABATE2**Register description**

IW Bridge Abate 2 (IWABATE2) indicates that the total number of IW bridges in use is less than 85% of the associated bridge pool. The system pegs this register after pegging register IWONSET2 and then crosses the 85% threshold. The system must peg register IWONSET2 again before it pegs this register a second time.

Register release history update

Register is changed in SN07.

Associated registers

IWONSET2. The system pegs this register after pegging register IWONSET2 and then crosses the 65% threshold. The system must peg register IWONSET2 again before it pegs this register a second time.

Associated logs

None.

Register IWBCNFAN**Register description**

IW Bridge for Conference and Announcement Usage (IWBCNFAN) registers a peg every time an IW bridge is used for a packet agent's access to conference or announcement facilities present on the ENET (i.e., MTM service circuits).

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

None.

Register IWBCALLN

Register description

IW Bridge for Call to Line Usage (IWBCALLN) registers a peg every time an IW bridge is used for a packet agent's access to a line agent present on the ENET or to a line agent that is present on another packet bearer network that connects via an IW SPM bridge.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

None.

Register IWBCLTRK

Register description

IW Bridge for Call to Trunk Usage (IWBCLTRK) registers a peg every time an IW bridge is used for a packet agent's access to a trunk agent present on the ENET or to a trunk agent that is present on another packet bearer network that connects via an IW SPM bridge.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

None.

OFZ2NET1 OM Group

OM description

OFZ2NET1 OM Group provides information for traffic analysis per bearer network. The OM group is modeled after group OFZ. The OFZ2NET1 OM group uses a primary route scoring philosophy. It pegs calls for the intended destination, not the destination where the call terminates.

The system routes a call to a tone or announcement if the tone or announcement is the *intended* destination of the call, or error condition occurs that includes a tone or announcement as a part of its treatment. If the treatment routes the call to another tone or announcement, note that OFZ2NET1 only counts the first tone or announcement.

OFZ2NET1 OM group records the structure of traffic that arrives at an office on a particular bearer network, the first routing, and the routing of outgoing traffic. The relationship between the type of call and the OFZ2NET1 registers is in the following tables.

The following table contains the registers that count incoming calls. The register TRKORIG counts each incoming call on the bearer network. One of the following registers counts each incoming call:

- ICANN
- ICLKT
- NICOG
- ICTRM
- ICTONE
- ICABNC
- ICABNM

The count depends on if the source of the call is a line or a trunk.

Incoming calls

Register	Intended destination	Routing
NICOG(2)	trunk	trunk
ICTRM(2)	line	line
ICANN	trunk, line, announcement	announcement
ICTONE	trunk, line, tone	tone
ICLKT	trunk, line	lockout
ICABNC	trunk, line	customer abandon
ICABNM	trunk, line	machine abandon
TRKORIG(2)	all	all

The following table contains a list of registers that count originating calls. Register LINEUSG counts each originating call. One register from registers LINEANN, LINELKT, LINEOG, LINETRM, LINETONE and LINEABDN counts each originating call. The system routes a call to an intended destination. The intended destination of the call is either a tone or an announcement. The system routes a call if an error condition is present. The error condition must include a tone or announcement as part of its treatment.

If a treatment routes the call to another tone or announcement, the OFZ2NET1 only counts the first tone or announcement.

Originating calls

Register	Intended designation	Routing
LINEOG(2)	trunk	trunk
LINETRM(2)	line	line
LINEANN	trunk, line, announcement	announcement
LINETONE	trunk, line, tone	tone
LINELKT	trunk, line	lockout
LINEABDN	trunk, line	abandon
LINEUSG(2)	trunk, line	all

The following table contains registers that count terminating calls on the associated bearer network. Register TRMLNAT counts each terminating call. Registers TRMMCHFL and TRMBLCK count calls on a blocked network. LNMBSYPC counts lines that are made manually busy.

Terminating calls

Register	Event
TRMMCHFL	Network Blockage Heavy Traffic (NBLH) or Network Blockage Normal Traffic (NBLN)
TRMBLCK	Network Blockage Normal Traffic (NBLN)
LNMBSYPC	line manual busy
TRMLNAT(2)	all outgoing traffic

Release history update

OFZ2NET1 OM group is new in SN07.

The addition of this new OFZ2NET1 OM group is controlled by the value of a new SN07 office parameter, MULTINET_DISPLAY_ACTIVE. If this parameter is set to 'Y', then the new OFZ2NET1 OM group is displayed. If the parameter is set to 'N', then the OFZ2NET1 OM group is not displayed.

Registers

OFZ2NET1 OM group registers display on the MAP terminal as follows:

OFZ2NET1 OM Group Display

>omshow ofz2net1 active

OFZ2NET1

CLASS: ACTIVE

START:2003/09/23 09:05:00 TUE; STOP: 2003/09/23 09:09:52 Tue;

SLOWSAMPLES: 3 ; FASTSAMPLES: 29 ;

INFO (BEARNETS_INFO)

ICANN	ICLKT	NICOG	NICOG2
ICTONE	TRKORIG	TRKORIG2	OGNWAT
OGNWAT2	OGTMFL	OGTRMFL	OGOSF
OGROSF	ICABNM	ICABNC	LINEANN
LINELKT	LINEOG	LINEOG2	LINETRM
LINETRM2	LINETONE	LINEUSG	LINEUSG2
ICTRM	ICTRM2	TRMLNAT	TRMLNAT2
TRMMCHFL	TRMBLCK	LNMBSYPC	LINEABDN

0

NET 0 TDM_ENET

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

1

NET 1 NET_AAL1

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

2

NET 2 NET_IP

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

The validity of a OFZ2NET2 register in an officetype is given in the following table

OFZ2NET1 OM registers

Register	Present In Officetype
ICANN	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
ICLKT	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
NICOG	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
NICOG2	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
ICTONE	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
TRKORIG	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
TRKORIG2	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
OGNWAT	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
OGNWAT2	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
OGMFL	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
OGTRMFL	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
OGOSF	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice

Register	Present In Officetype
OGROSF	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
ICABNM	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
ICABNC	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww, nooffice
LINEANN	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
LINELKT	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
LINEOG	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
LINEOG2	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
LINETRM	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
LINETRM2	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
LINETONE	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
LINEUSG	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
LINEUSG2	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
ICTRM	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
ICTRM2	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww

Register	Present In Officetype
TRMLNAT	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
TRMLNAT2	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
TRMMCHFL	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
TRMBLCK	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
LNMBSYPC	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww
LINEABDN	off100, offcomb, offcombtops, off100scp, off100oesd, offcomboesd, off250ibn, offeadas, offcombitops, offmtx100i, off500, offcomblww

Group structure

OFZ2NET1 OM group provides 1 tuple(s) for each bearer network datafilled in Table BEARNETS. The group structure is dependent upon the office type of the call server.

Key field: Bearer network ID

Info field: BEARNETS_INFO

- Bearer network ID (i.e., 'NET 0')
- Bearer network name (i.e., 'TDM_ENET')

Associated OM groups

OFZ OM group gives an overall office-wide traffic performance measurement.

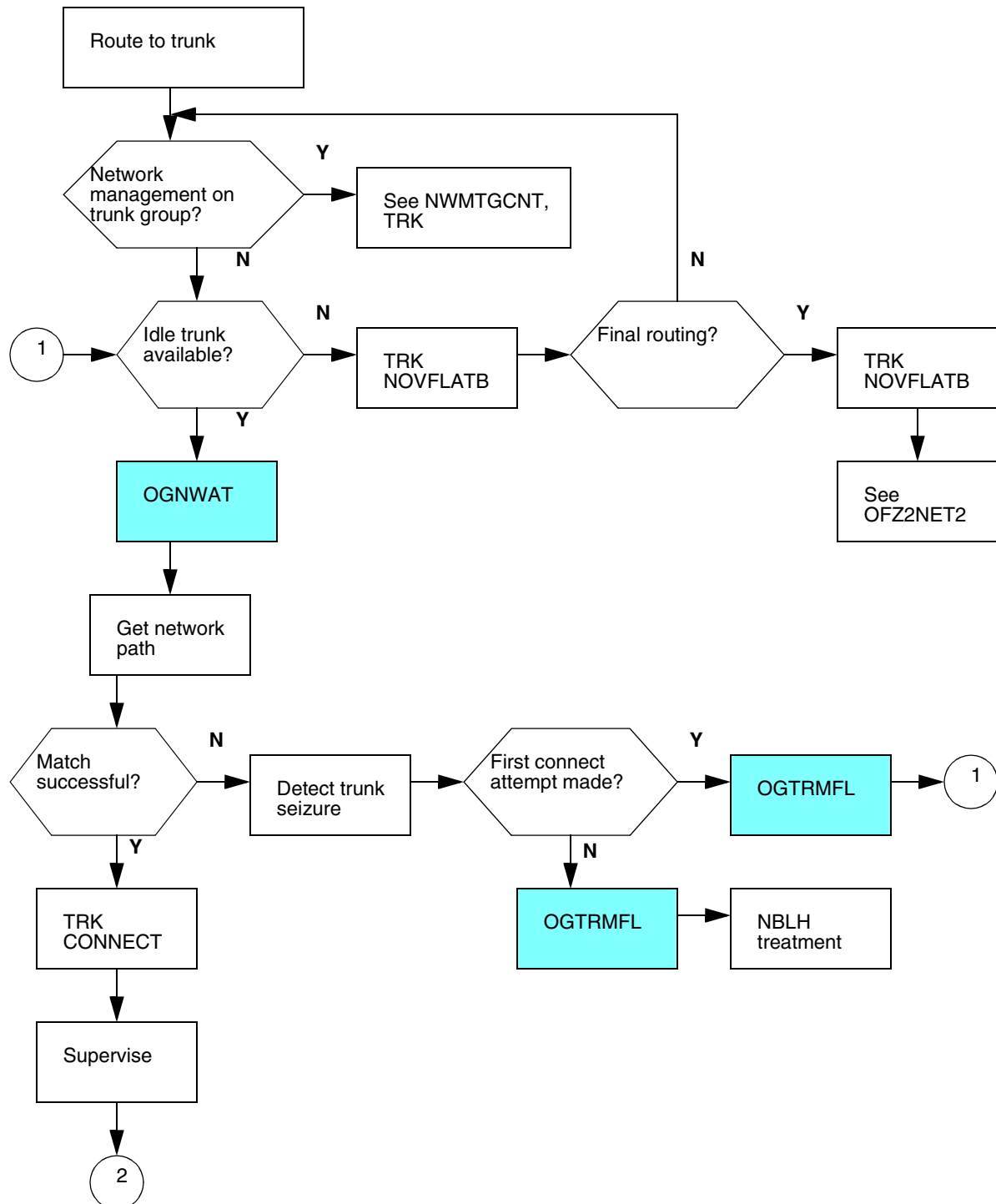
Associated functional groups

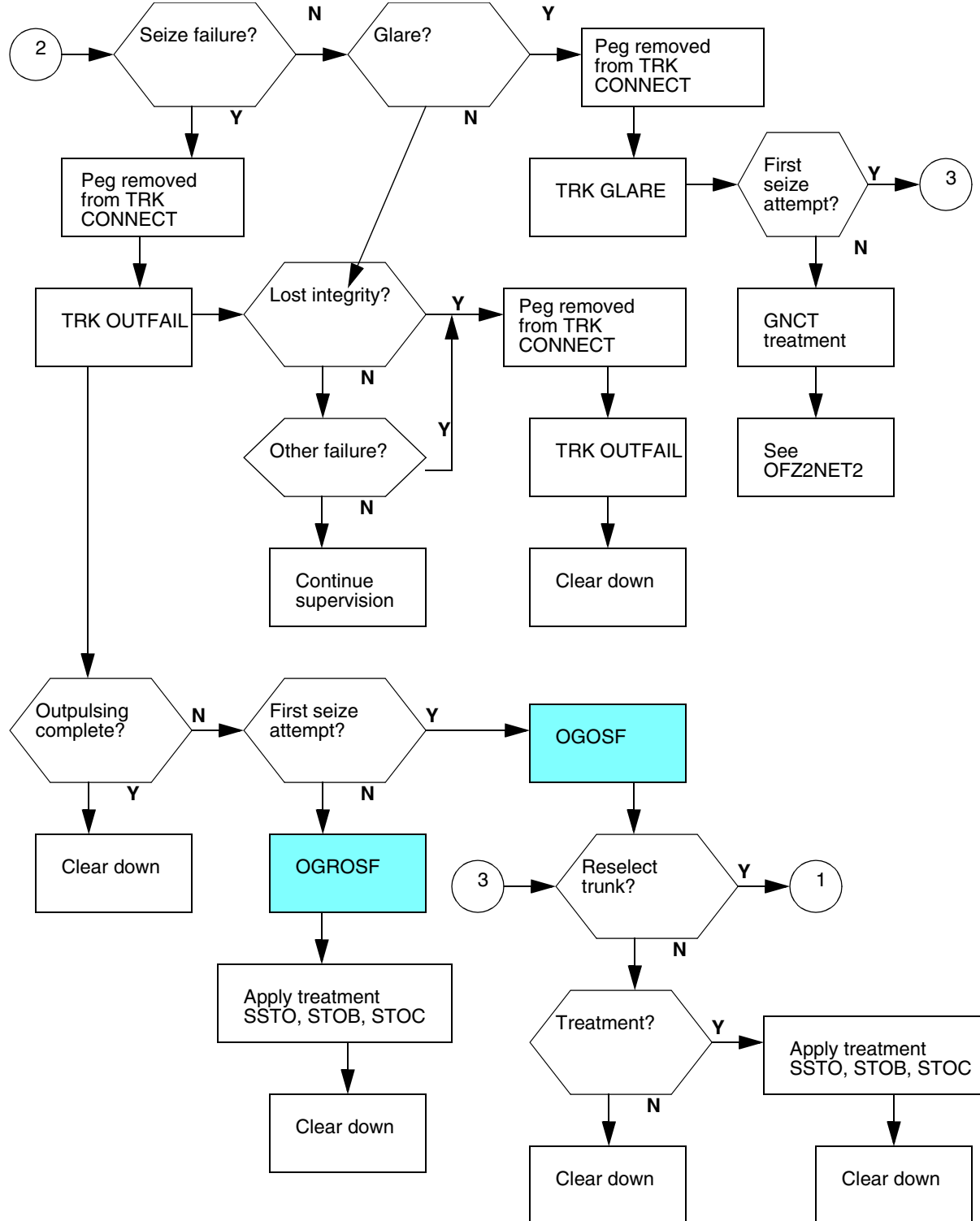
The following functional groups are associated with OFZ2NET1 OM group:

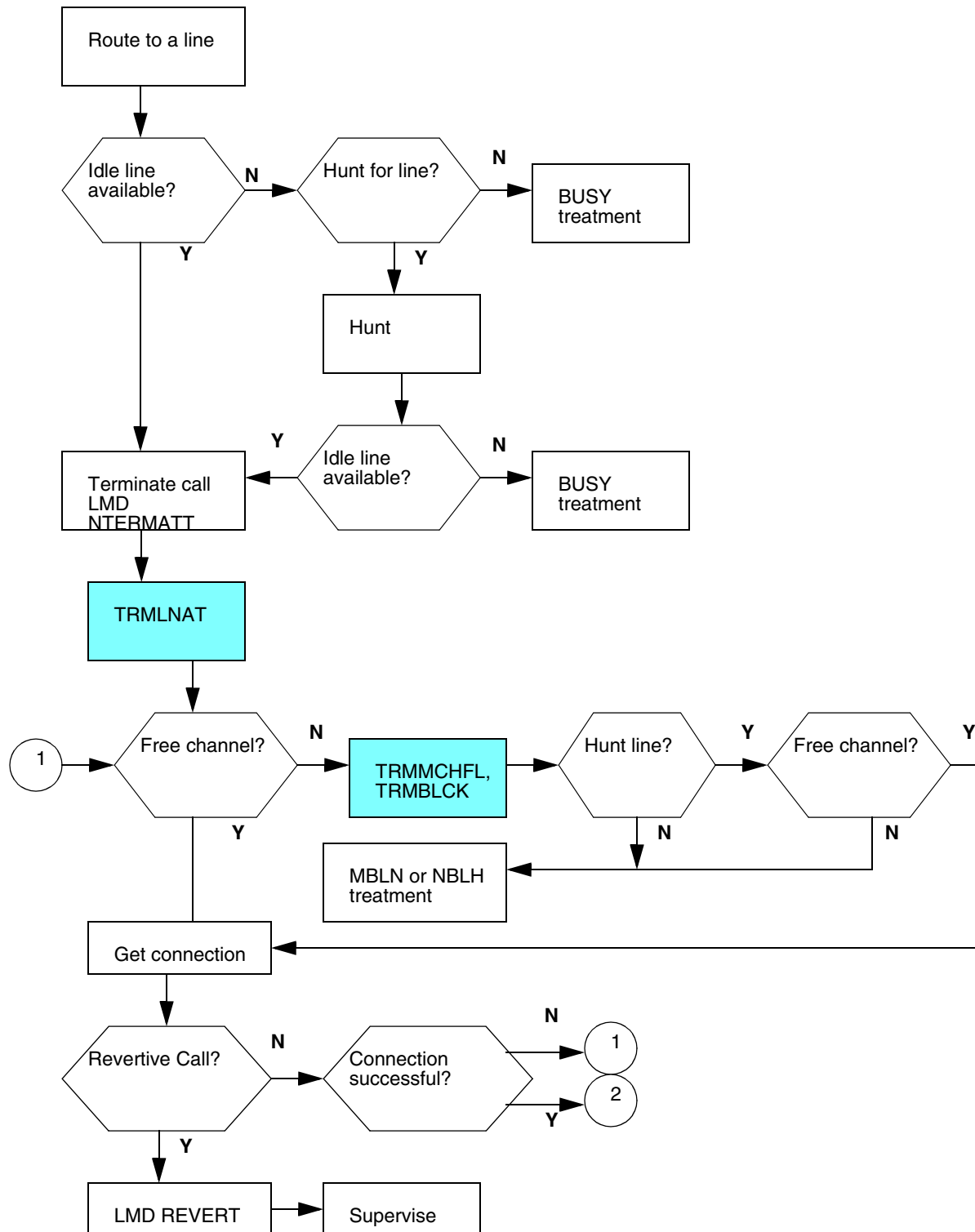
- Succession North America
- Succession International

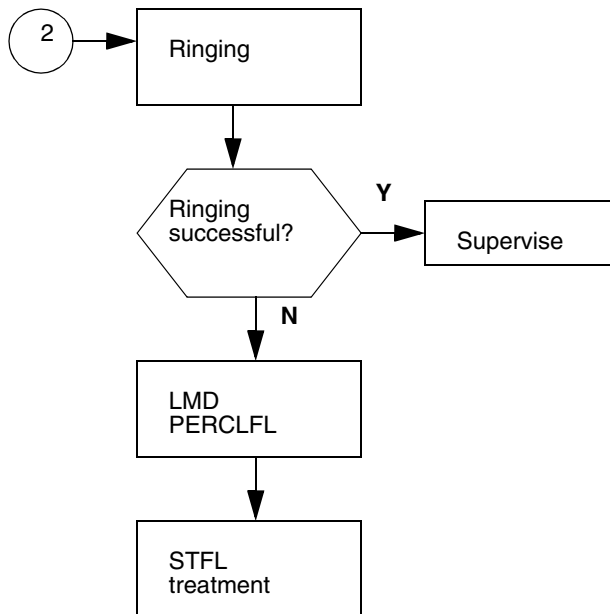
Associated functionality codes

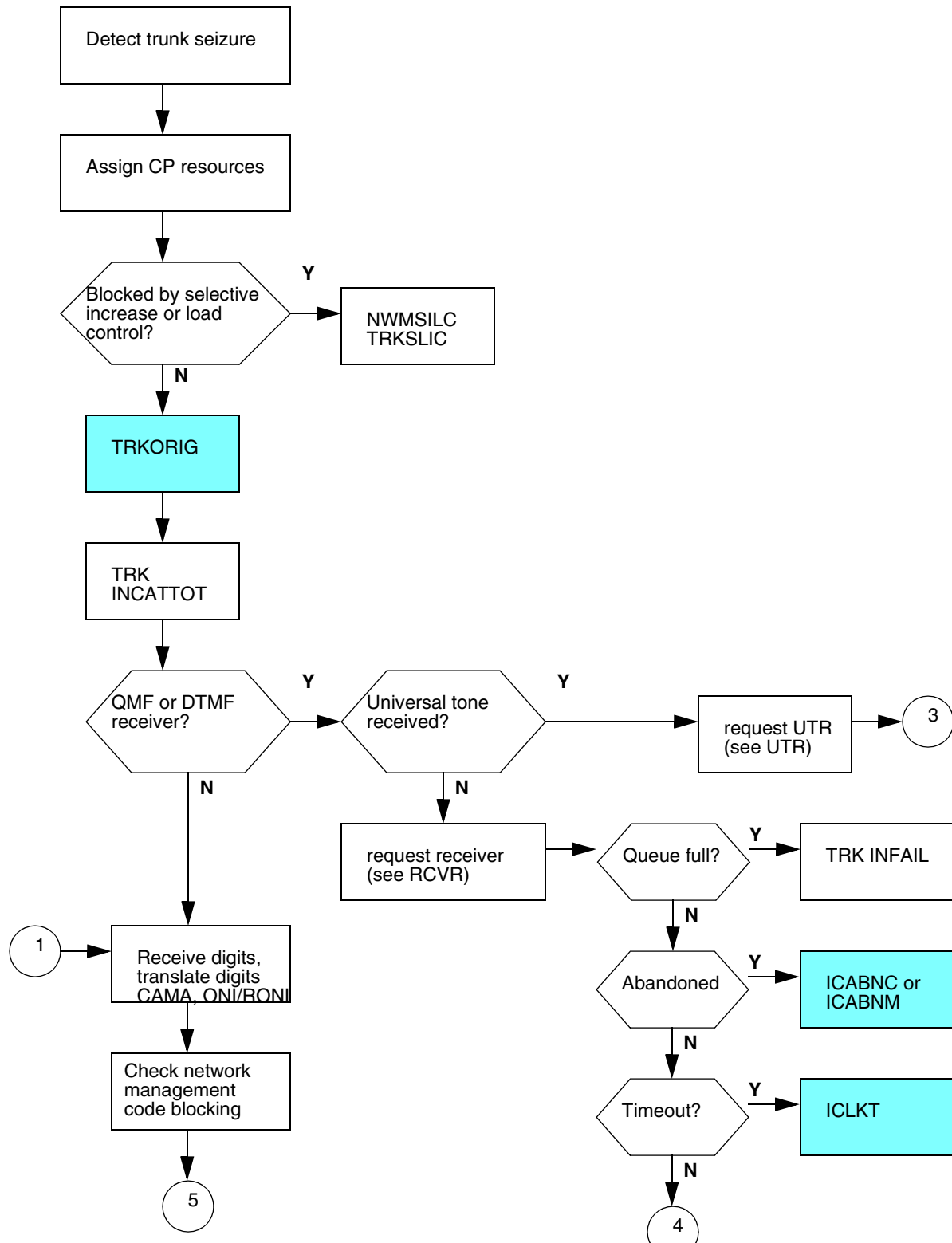
None

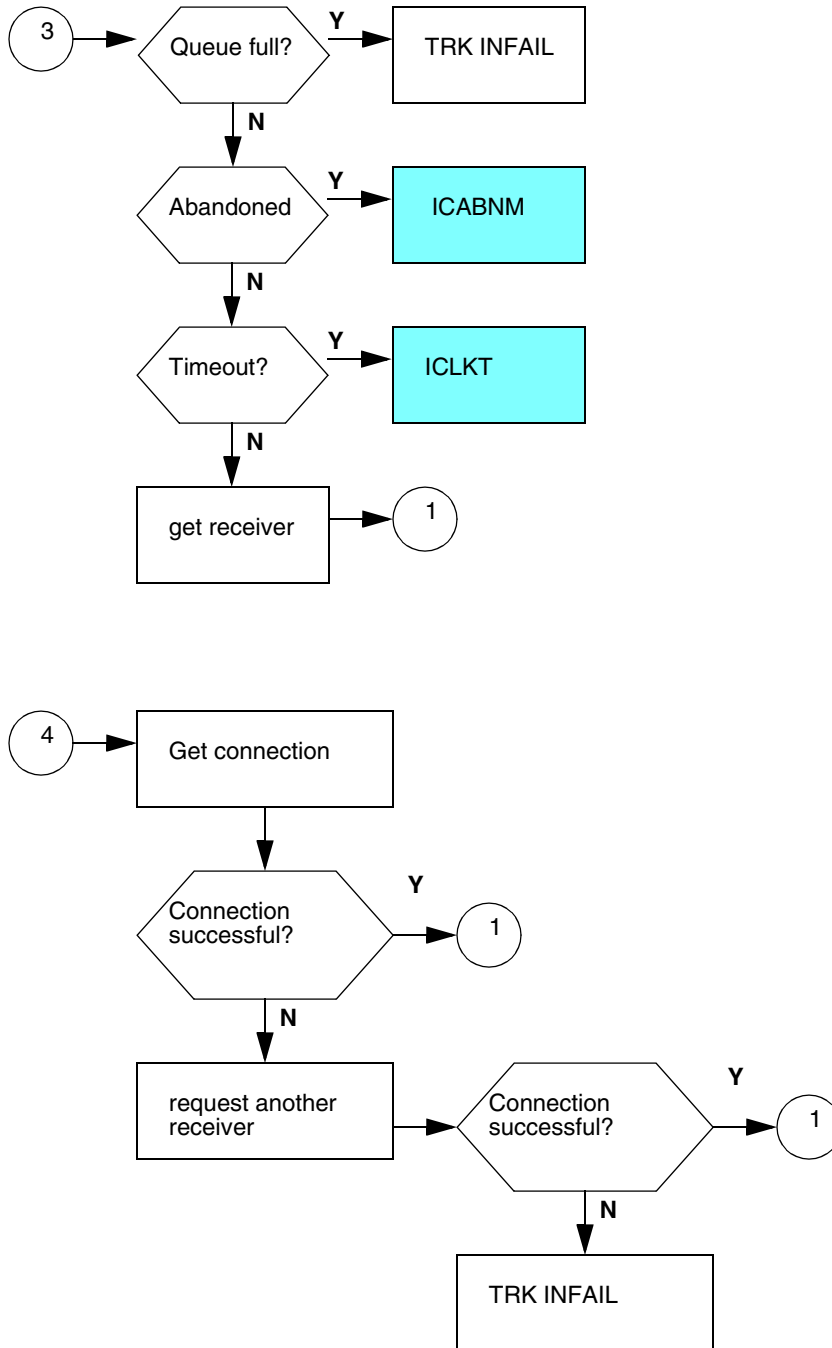
OFZ2NET1 OM group registers logic flow chart**Termination to an outgoing trunk**

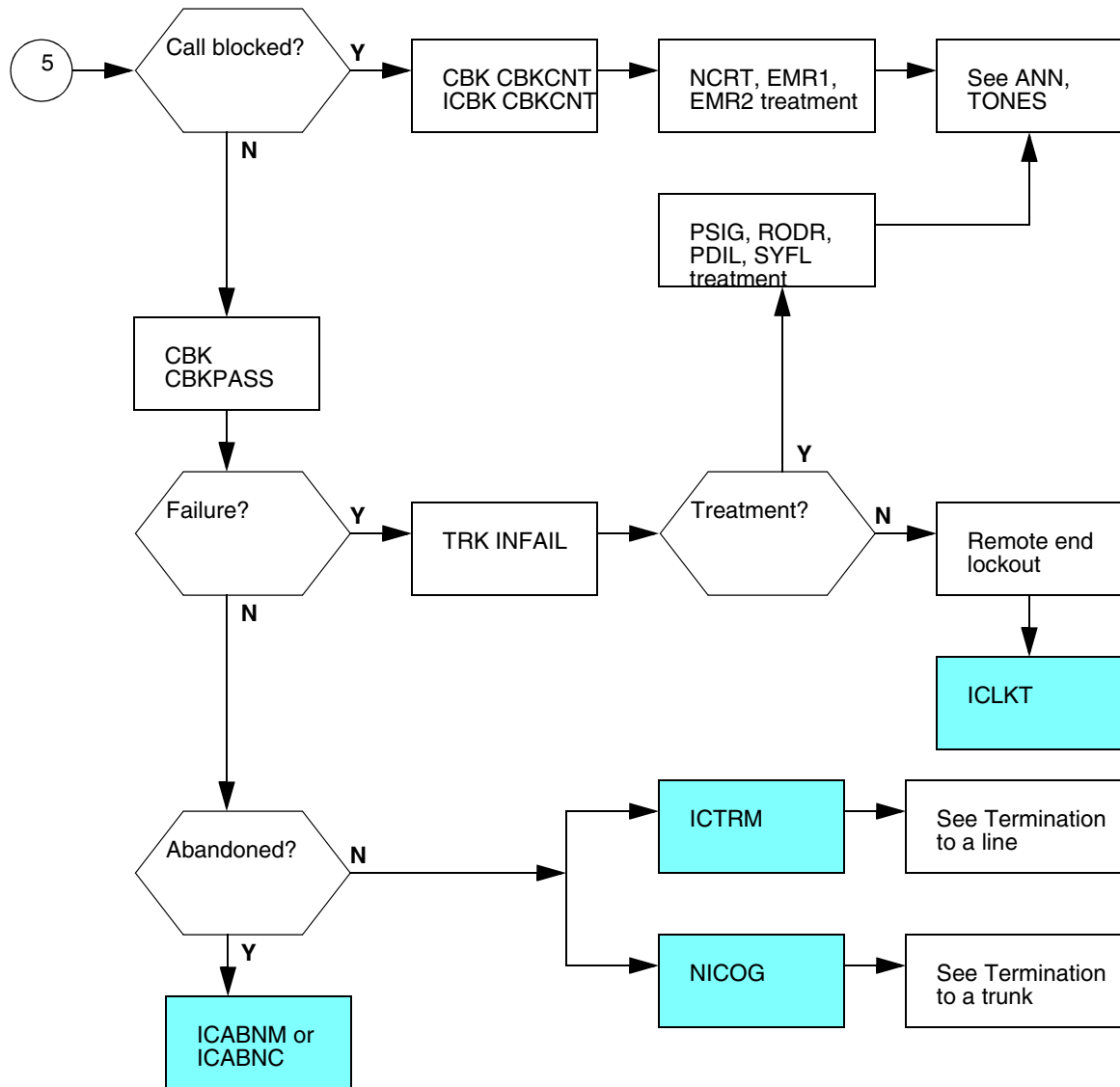
Termination to an outgoing trunk (continued)

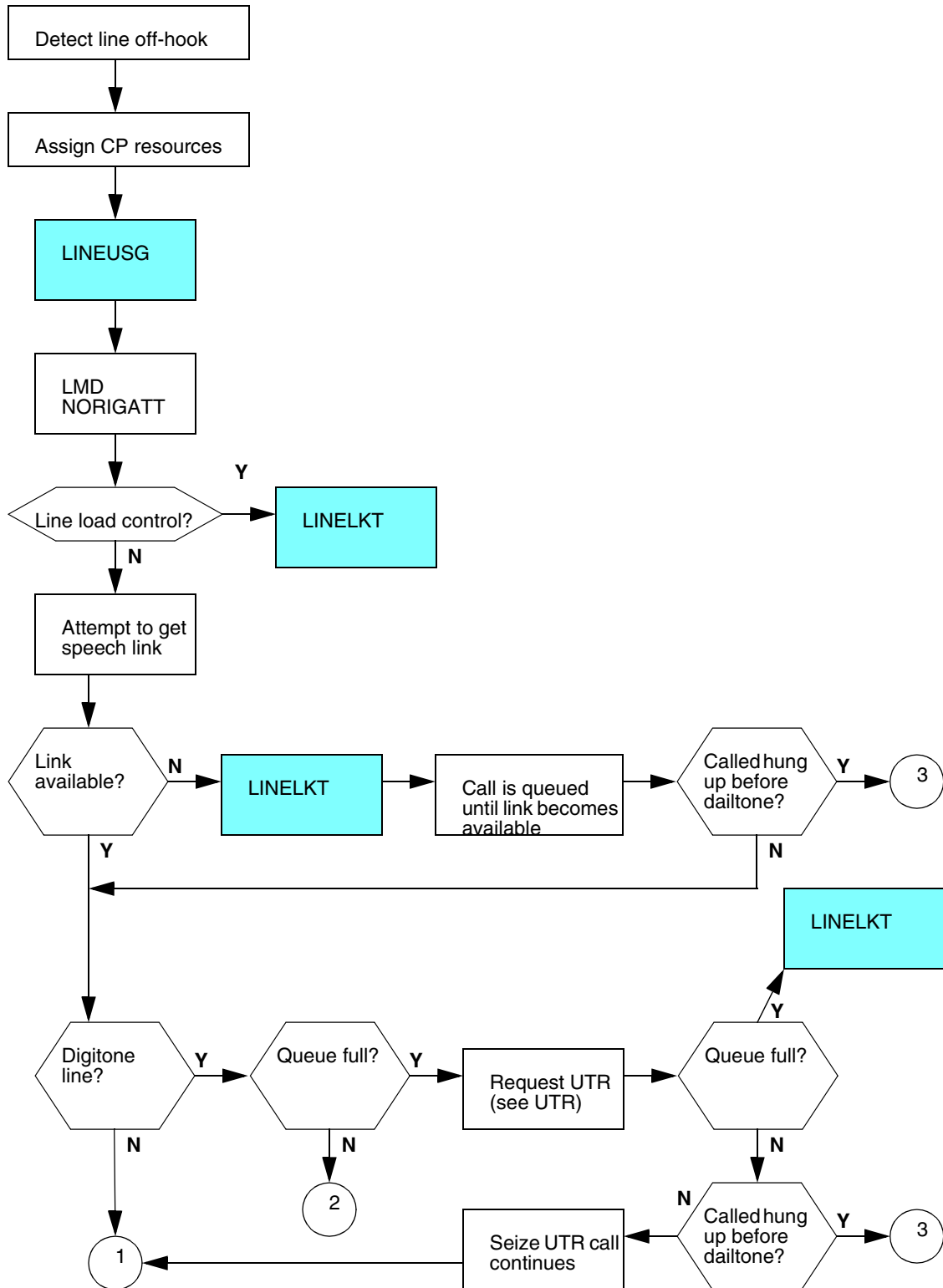
Termination to a line

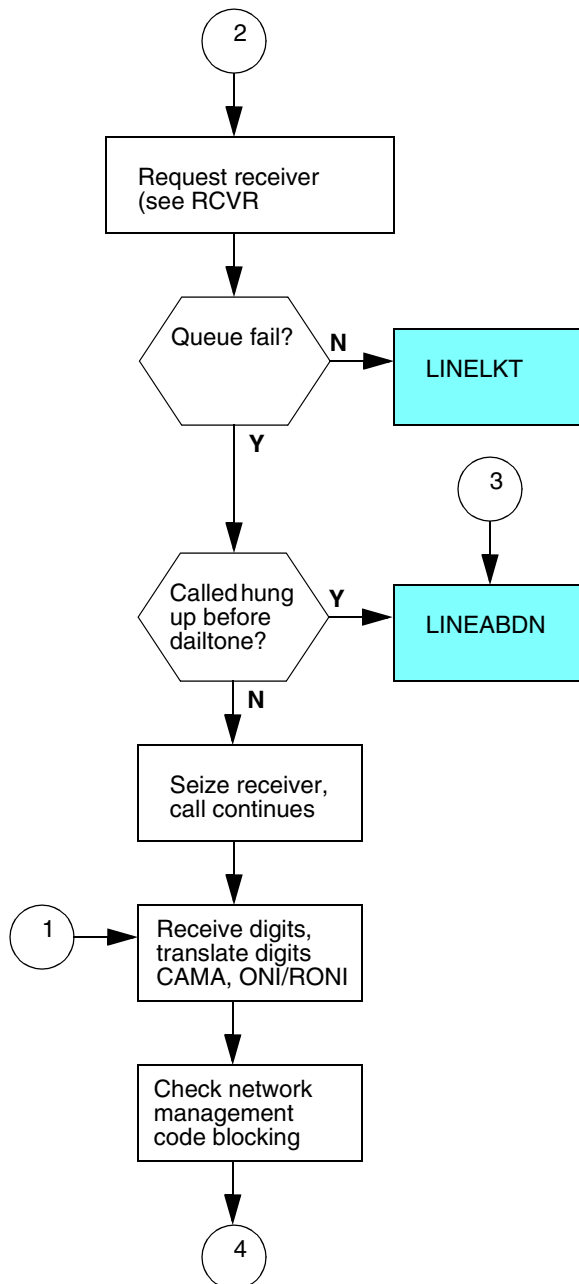
Termination to a line (continued)

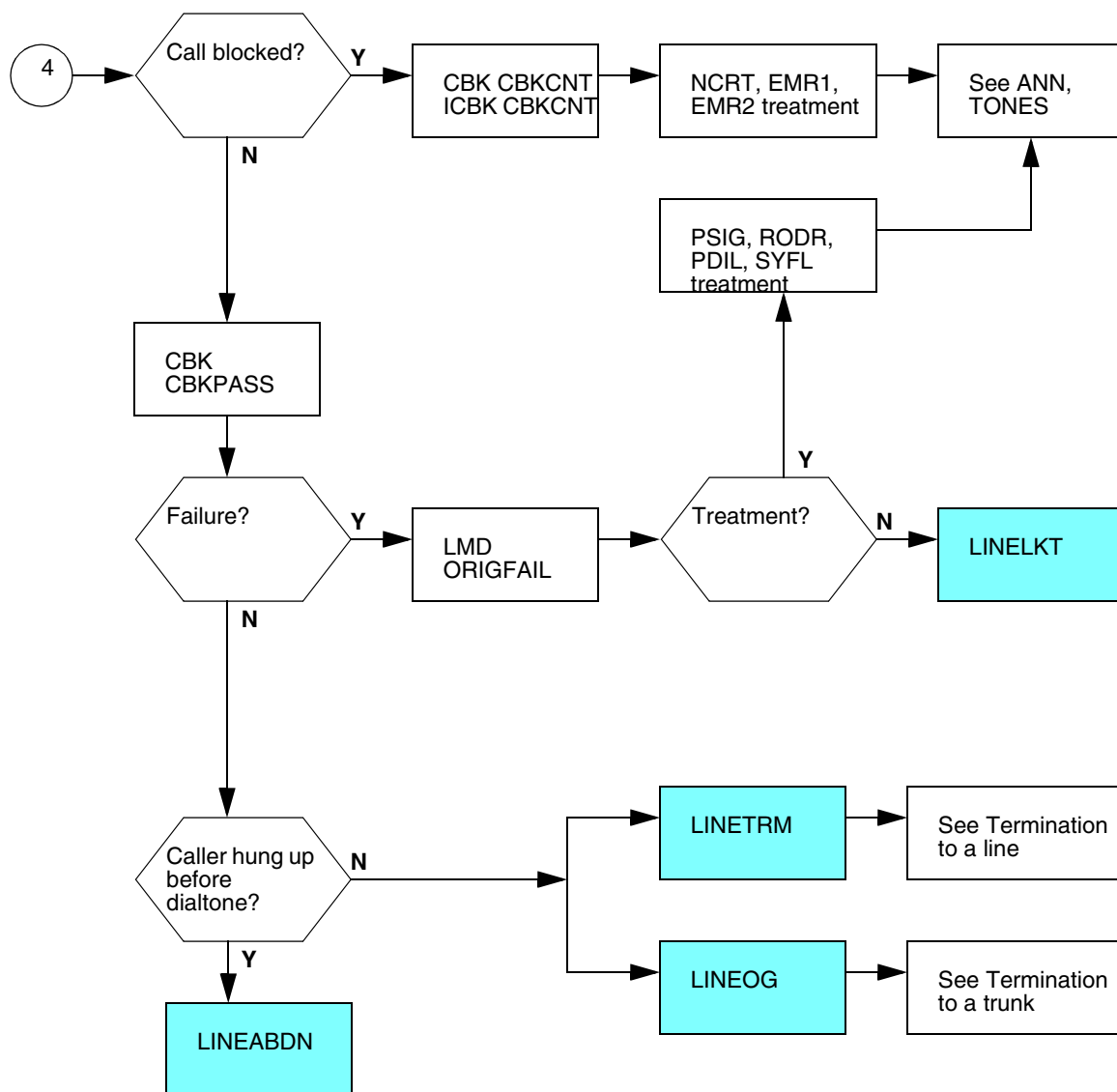
Origination from a trunk

Origination from a trunk (continued)

Origination from a trunk (continued)

Origination from a line

Origination from a line (continued)

Origination from a line (continued)**Register ICABNC****Register description**

Incoming Calls Abandoned (ICABNC) counts incoming calls on the associated bearer network that the subscriber abandons before processing. These calls do not require treatment.

Register release history update

Register is new in SN07.

Associated registers

Register ICABNM counts incoming calls on the associated bearer network that the machine abandons.

Associated logs

The system generates TRK114 when the system cannot determine the destination of an incoming call during DP reception.

The system generates TRK116 when the system cannot determine the destination of an incoming call during MF reception.

The system generates TRK162 is the outpulsing of either a trunk-to-trunk or line-to-trunk call encounters trouble. These calls use DTMF signaling.

Register ICABNM**Register description**

Incoming Calls Abandoned (ICABNM) counts incoming calls on the associated bearer network that the machine abandons before processing. The machine abandons a call when a call times out at the upstream office while waiting for a receiver. The machine also abandons a call when there is an equipment problem.

Register release history update

Register is new in SN07.

Associated registers

Register ICABNC counts incoming calls on the associated bearer network that the subscriber abandons.

Associated logs

The system generates TRK114 when the system cannot determine the destination of an incoming call during DP reception.

The system generates TRK116 when the system cannot determine the destination of an incoming call during MF reception.

The system generates TRK162 is the outpulsing of either a trunk-to-trunk or line-to-trunk call encounters trouble. These calls use DTMF signaling.

Register ICANN**Register description**

Incoming Call to an Announcement (ICANN) register counts incoming calls on the associated bearer network that the system routes to an announcement.

The announcement is the result of a treatment applied during origination, or the intended result of the call. Register ICANN counts the call before it

attempts to get a network connection. Register ICANN counts calls that the system routes to a treatment that routes the call to an announcement. The register only counts these calls one time.

Register release history update

Register is new in SN07.

Associated registers

Register LINEANN counts originating calls that the system routes to an announcement.

Associated logs

The system generates TRK138 when the system routes a call to a treatment after the call is call processing busy.

Register ICLKT**Register description**

Incoming Calls to Lockout (ICLKT) counts incoming calls that fail and that the system routes to lockout. The call fails for one of the following reasons:

- The incoming trunk loses its true identity
- The system cannot connect the call to a tone or announcement
- A forced release initiates manually
- A forced release initiates because call processing requests a delay (CP_WAITDENY count the call)

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates TRK111 if the system encounters a problem or assigns a treatment during a trunk-to-trunk call.

The system generates TRK113 when the call processing of a trunk-to-trunk call encounters a problem.

The system generates TRK123 when the node hosting the trunk member sends the wrong message to the core. The system generates TRK123 several times when a problem is present in one of the following elements:

- the originating trunk
- the terminating trunk

Register NICOG

Register description

Incoming to Outgoing (NICOG) counts incoming calls on the associated bearer network from the following agents:

- trunks
- preset conferences
- originating test lines

Register release history update

Register is new in SN07.

Associated registers

NICOG2 register (extension register for NICOG).

Associated logs

None.

Register ICTONE

Register description

Incoming Call to Tone (ICTONE) counts oncoming calls on the associated bearer network that the system routes to a tone.

The tone is the result of a treatment applies during origination, or the tone is the intended result of the call. Register ICTONE counts the call before it attempts to find a network connection. Register ICTONE count a call that the system routes to a tone one time.

Register release history update

Register is new in SN07.

Associated registers

Register LINETONE counts originating calls on the associated bearer network that the system routes to a tone.

Associated logs

The system generates TRK138 when the system routes a call to a treatment after the call is call processing busy.

Register ICTRM

Register description

Incoming to Terminating (ICTRM) counts incoming calls on the associated bearer network that the system routes to a line.

Register release history update

Register is new in SN07.

Associated registers

Register ICTRM2 (extension register for ICTRM).

Associated logs

None.

Register LNMBSYPC**Register description**

Line Manual Busy Peg Count (LNMBSYPC) counts lines on the associated bearer network that are manual busy.

Every POTS line is pegged by one when transitioning to a manual busy state. Pegging of each PPhone.PSET/DATA/ISDN line depends upon number of virtual identifiers (VIDs) associated with that line, and may be more than once, when made manual busy either by LTP/BSY or maintenance action.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

None.

Register TRKORIG**Register description**

Number of Incoming Calls (TRKORIG) counts incoming calls on the associated bearer network that the core recognizes. The intended destination of the call is a line, trunk, announcement or tone. Register TRKORIG counts calls after a call control block and a call process are obtained. The register may count the calls before all incoming digits are received.

Register release history update

Register is new in SN07.

Associated registers

Register TRKORIG counts each incoming call. A peg in this register should have a corresponding peg in one of the following registers as the destination is determined:

- Register ICABNC (counts the call if the subscriber abandons the call)
- Register ICABNM (counts the call if the core abandons the call)

- Register ICANN (counts the call if the destination is an announcement)
- Register ICLKT (counts the call if the call locks out)
- Register NICOOG (counts the call if the destination is a trunk)
- Register ICTRM (counts the call if the destination is a line)
- Register ICTONE (counts the call if the destination is a tone)

Register TRKORIG2 (extension register for TRKORIG).

Associated logs

None.

Register LINEUSG**Register description**

Number of Originating Calls (LINEUSG) counts originating call on the associated bearer network that the core recognizes.

After a call condense block and a call process are obtained, LINEUSG counts a call. Register LINEUSG counts the call before dialing is set up. LINEUSG can count a single call at least once. The call is only a single call from the point of view of the caller. The system counts a three-way call when the flashing switch hook recognizes a correct feature origination signal. The feature origination signal is for the flashing line.

Register release history update

Register is new in SN07.

Associated registers

Register LINEUSG counts each originating call. A peg in this register should have a corresponding peg in one of the following registers as the destination is determined:

- Register LINEABDN (counts the call if the call abandons)
- Register LINEANN (counts the call if the destination is an announcement)
- Register LINELKT (counts the call if the call locks out)
- Register LINEOG (counts the call if the destination is a trunk)
- Register LINETRM (counts the call if the destination is a line)
- Register LINETONE (counts the call if the destination is a tone)

Register LINEUSG2 (extension register for LINEUSG).

Associated logs

None.

Register LINEABDN**Register description**

Originating Calls Abandoned (LINEABDN) counts originating calls on the associated bearer network that the system abandons before the system routes the calls to a trunk, line or treatment.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates LINE106 if the system cannot determine a call destination during dial pulse reception on a line.

The system generates LINE108 if the digitone reception on a lines encounters a problem.

Register LINEANN**Register description**

Originating Calls to Announcement (LINEANN) counts originating calls on the associated bearer network that the system routes to an announcement.

The announcement can be the result of a treatment during origination, or the intended result of the call. The system counts the call in LINEANN before an attempt to find a network connection occurs.

Register release history update

Register is new in SN07.

Associated registers

The system counts ICANN incoming calls that the system routes to an announcement.

Associated logs

The system generates LINE138 if the system routes a call to a treatment after it is call processing busy.

Register LINELKT**Register description**

Originating Calls to Lockout (LINELKT) counts originating calls on the associated bearer network that fail on the intended destination that the system routes to lock out. The register counts these calls when the calls do not connect.

Register LINELKT also counts the calls when the system does not route the call to a treatment. The call fails for one of the following reasons:

- line load control (line is dead)
- a speech link is not available (call is queued until a speech link becomes available and if the caller remains off-hook that call can be successful, but LINELKT only pegs one time)
- A digitone receiver, or one of a network connection to a digitone receiver is not available (if caller remains off-hook, the call clears when the problem is successful, but LINELKT only pegs one time)

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates LINE104, LINE105, LINE109, or LINE204 if call processing encounters a problem.

The system generates NET130 if the system cannot find a network path.

The system generates OM2200 if a threshold condition exceeds the limit.

Register LINEOG**Register description**

Originating Calls to Outgoing (LINEOG) counts originating calls on the associated bearer network that the system routes to a trunk or a test facility.

Register release history update

Register is new in SN07.

Associated registers

Register LINEOG2 (extension register for LINEOG).

Associated logs

None.

Register LINETONE**Register description**

Originating Calls to Tone (LINETONE) counts originating calls on the associated bearer network that the system routes to a tone.

Register LINETONE counts the call before it attempts to find a network connection. The tone is either the result of a treatment, or the intended result of the call. Register LINETONE counts calls that the system routes to a treatment that routes the call to a tone. Register LINETONE only counts the call one time.

Register release history update

Register is new in SN07.

Associated registers

Register ICTONE counts incoming calls that the system routes to a tone.

Associated logs

The system generates LINE138 if the system routes a call to a treatment after it is call processing busy.

Register LINETRM**Register description**

Originating Calls to Terminating (LINETRM) counts originating calls on the associated bearer network that the system routes to a line. Register LINETRM counts the call if a line is available or is not available.

Register release history update

Register is new in SN07.

Associated registers

Register LINETRM2 (extension register for LINETRM).

Associated logs

None.

Register OGMFL**Register description**

Outgoing Match Failures (OGMFL) counts calls on the associated bearer network that fail to find a network path to a selected outgoing or test trunk on the first attempt. A second attempt occurs to find an idle trunk and a network path.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates NET130 if the system cannot find a network path.

Register OGNWAT

Register description

Outgoing Network Attempts (OGNWAT) counts incoming and outgoing calls on the associated bearer network that are intended for an exact outgoing or test trunk.

A single call can use two or more network paths to different ports for the service circuit. For example, connection by a conference circuit requires more than one network path.

Register release history update

Register is new in SN07.

Associated registers

Register OGNWAT2 (extension register for OGNWAT).

Associated logs

None.

Register OGOSF

Register description

Outgoing Original Seize Failures (OGOSF) counts calls on the associated bearer network that fail to seize an outgoing trunk on the first attempt after network paths are acquired. A second attempt occurs to find an idle trunk and a network path, and to seize the trunk. One of the following conditions causes a failure:

- a reversed trunk
- failure to receive a known start-dial
- not planned stop-dial
- time-out before expected stop-dial
- CCS7 errors

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates TRK113 is the call processing of a trunk-to-trunk call encounters a problem.

The system generates TRK121 if the system does not receive an acknowledgement wink from the far-end equipment. The wink indicates that it is ready to receive digits. The digits are received during outpulsing on an outgoing trunk.

The system generates TRK162 if the outpulsing of either a trunk-to-trunk or line-to-trunk call encounters a problem. The line-to-trunk calls use DTMF signaling.

The system generates C7UP111 when an outgoing ISUP call attempt fails.

Register OGTRMFL

Register description

Outgoing Retrial Match Failures (OGTRMFL) counts calls on the associated bearer network that fail on the second attempt to find a network path to a selected outgoing or test trunk.

Register release history update

Register is new in SN07.

Associated registers

Register OGMFL counts the first trial match failures.

Associated logs

The system generates NET130 if the system cannot find a network path.

Register OGROSF

Register description

Outgoing Retrial Seize Failures (OGROSF) counts calls on the associated bearer network that fail on the second attempt to seize an outgoing trunk. This attempt occurs after the network paths have been acquired. One of the following conditions causes a failure:

- a reversed trunk
- failure to receive a known start-dial
- not planned stop-dial
- time-out before expected stop-dial
- CCS7 errors

The system disconnects the call after the second failure and the call received start signal time-out (SSTO) treatment. An equal access call received signal timely BOC (STOB) or signal time-out IC.INC (STOC) treatment.

The system pegs OGROSF when a second attempt occurs to ruin a continuity test (COT) for an outgoing ISUP trunk. The second attempt occurs if the first COT attempt fails.

Register release history update

Register is new in SN07.

Associated registers

Register OGOSF counts the first seize failures.

Associated logs

The system generates TRK113 is the call processing of a trunk-to-trunk call encounters a problem.

The system generates TRK121 is the system does not receive an acknowledgement wink from the far-end equipment. The wink indicates that it is ready to receive digits. The digits are received during outpulsing on an outgoing trunk.

The system generates TRK162 if the outpulsing of either a trunk-to-trunk or line-to-trunk call encounters a problem. The line-to-trunk calls use DTMF signaling.

The system generates C7UP111 when an outgoing ISUP call attempt fails.

Register TRMBLCK**Register description**

Terminating Blocks (TRMBLCK) counts attempts to obtain a voice path to a terminating lines on the associated bearer network that fail. This failure occurs when no free channel is present between the host network and the terminating line.

The system counts more that one failed attempt if part of a hunt group directs the call.

The system also counts each attempt in OFZ2NET1 registers TRMMCHFL and TRMLNAT.

If no alternate line is available, the system routes the call to network blockage normal traffic (NBLN) treatment.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates NET130 if the system cannot find a network path.

The system generates LINE138 or TRK138 when the system routes a call to a treatment after the call is call processing busy.

Register TRMMCHFL**Register description**

Terminating Match Failures (TRMMCHFL) counts calls on the associated bearer network that fail to find a network path to terminating line.

The system counts more than one failed attempt if the call goes to a part of a hunt group.

Failure in the path search sequence can occur if the host switch network cannot obtain a path. If the network cannot find an alternate path, the system routes the call to a network blockage heavy traffic (NBLH) treatment.

Failure in the path search sequence can occur if the final cause of failure is failure to obtain a free channel on a link between the host switch network and the terminating line. Registers TRKBLK and TERMBLK count the failure to obtain a free channel.

If no alternate line is available, the system routes the call to network blockage normal traffic (MBLN) treatment.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates NET130 if the system cannot find a network path.

The system generates LINE138 or TRK138 when the system routes a call to a treatment after the call is call processing busy.

Register TRMLNAT**Register description**

Terminating Network Attempts (TRMLNAT) counts attempts to find a voice path on the associated bearer network to terminating line. The complete path includes the following elements:

- a segment through the network

- a channel on the link between the line module and the network
- a matching channel on the line shelf

Register TRMLNAT counts a call only for each attempt. The calls count each attempt, whether it succeeds or fails.

Register release history update

Register is new in SN07.

Associated registers

Register TRMLNAT2 (extension register for TRMLNAT).

Associated logs

None.

OFZ2NET2 OM Group**OM description**

OFZ2NET2 OM Group provides information for traffic analysis per bearer network. The OM group is modeled after group OFZ2. The OFZ2NET2 OM group counts calls that the system routes to generalized no circuit treatment (GNCT). The system routes a call to GNCT when a trunk group is the last route in the route list and all trunks are busy.

The OM group has 11 registers. These registers give the cause of the GNCT for outgoing trunks or for the outgoing side of two-way trunks. The name of each register corresponds to an entry in the no circuit class field, NCCLS in table TRKGRP.

Release history update

OFZ2NET2 OM group is new in SN07.

The addition of this new OFZ2NET2 OM group is controlled by the value of a new SN07 office parameter, MULTINET_DISPLAY_ACTIVE. If this parameter is set to 'Y', then the new OFZ2NET2 OM group is displayed. If the parameter is set to 'N', then the OFZ2NET2 OM group is not displayed.

Registers

OFZ2NET2 OM group registers display on the MAP terminal as follows:

OFZ2NET2 OM Group Display

>omshow ofz2net2 active

OFZ2NET2

CLASS: ACTIVE

START:2003/09/23 09:05:00 TUE; STOP: 2003/09/23 09:09:52 Tue;

SLOWSAMPLES: 3 ; FASTSAMPLES: 29 ;

INFO (BEARNETS_INFO)

	NCKTIT	NCKTTC	NCKTLT	NCKTBN
	NCKTID	NCKTOSC	NCKTOT	NCKTRT
	NCKTIM	NCKTON	NCKTOF	MDPSIG
	MDPD	DPTRC	DPTRC2	
0				
NET 0 TDM_ENET				
	0	0	0	0
	0	0	0	0
	0	0	0	0
	0	0	0	
1				
NET 1 NET_AAL1				
	0	0	0	0
	0	0	0	0
	0	0	0	0
	0	0	0	
2				
NET 2 NET_IP				
	0	0	0	0
	0	0	0	0
	0	0	0	0
	0	0	0	

Group structure

OFZ2NET2 OM group provides 1 tuple(s) for each bearer network datafilled in Table BEARNETS

Key field: Bearer network ID

Info field: BEARNETS_INFO

- Bearer network ID (i.e., 'NET 0')
- Bearer network name (i.e., 'TDM_ENET')

Associated OM groups

OFZ2 OM group gives an overall office-wide traffic performance measurement.

Associated functional groups

The following functional groups are associated with OFZ2NET2 OM group:

- Succession North America
- Succession International

OFZ2NET2 OM group registers logic flow chart**Register NCKTBN****Register description**

No circuit business network trunks (NCKTBN) counts calls on the associated bearer network that the system routes to generalized no circuit treatment (GNCT). The system routes the calls to GNCT because Meridian Digital Centrex (MDC) trunk is not available.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

Register NCKTID**Register description**

No circuit inward dial trunks (NCKTID) counts calls on the associated bearer network that the system routes to generalized no circuit treatment (GNCT). The system routes a call to GNCT when a direct inward dial or direct outward dial trunk is not available.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

Register NCKTIM**Register description**

No circuit intermachine trunks (NCKTIM) counts calls on the associated bearer network that the system routes to generalized no circuit treatment (GNCT). The system routes the calls to GNCT because a circuit intermachine trunk is not available.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

Register NCKTIT**Register description**

No circuit intertoll trunks (NCKTIT) counts calls on the associated bearer network that the system routes to generalized no circuit treatment (GNCT). The system routes the calls to GNCT because an intertoll trunk is not available.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

Register NCKTLT**Register description**

No circuit local tandem trunks (NCKTLT) counts calls on the associated bearer network that the system routes to generalized no circuit treatment (GNCT). The system routes the calls to GNCT because a local tandem trunk is not available.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

Register NCKTOF

Register description

No circuit offnet trunks (NCKTOF) counts calls on the associated bearer network that the system routes to generalized no circuit treatment (GNCT). The system routes the calls to GNCT because an offnet or direct dial trunk is not available.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

Register NCKTON

Register description

No circuit connect trunks (NCKTON) counts calls on the associated bearer network that the system routes to generalized no circuit treatment (GNCT). The system routes the calls to GNCT because a dedicated access or mobile telephone exchange trunk is not available.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

Register NCKTOT

Register description

No circuit other trunk (NCKTOT) counts calls on the associated bearer network that the system routes to generalized no circuit treatment (GNCT). The system routes the calls to GNCT because one of the following types of trunk is not available:

- test line
- test desk
- maintenance trunks
- AV101

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

Register NCKTRT

Register description

No circuit trunks (NCKTRT) counts calls on the associated bearer network that the system routes to generalized no circuit treatment (GNCT). The system routes the calls to GNCT because one of the following types of trunk is not available:

- 0+/0- tandem to TOPS
- outgoing to AMR2 or CAMA
- outgoing local
- recording completing outgoing

- TOPS outgoing

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

Register NCKTTC**Register description**

No circuit toll completing trunks (NCKTTC) counts calls on the associated bearer network that the system routes to generalized no circuit treatment (GNCT). The system routes the calls to GNCT because a toll completing trunk is not available.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

Register NCKTOSC

Register description

No service circuit trunks (NCKTOSC) counts calls on the associated bearer network that the system routes to generalized no circuit treatment (GNCT). The system routes the call because automatic number announcement or automatic intercept trunk is not available.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates ATB100 when the system routes again a call that the system blocks. The system blocks the call when the call attempts to seize a specified numbering plan area (NPA) The system can also block a call that attempts to seize a trunk to a specified central office (CO).

The system generates LINE138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

Register MDPD

Register description

Machine dialed partial dials (MDPD) counts machine-dialed calls on the associated bearer network that the system routes to partial dial treatment.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates TRK114 if the system cannot determine call destination during dial pulse (DP) reception for an incoming call.

The system generates TRK116 if the system cannot determine call destination during multi-frequency (MF) reception for an incoming call.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK182 when the system cannot determine call destination of an incoming call because the system had problems during Digitone reception.

Register MDPSIG

Register description

Machine dialed permanent signal (MDPSIG) counts machine-dialed calls on the associated bearer network that the system routes to permanent signal treatment.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates TRK115 when the system cannot determine call destination. The system was not able to determine call destination because the system had problems during dial pulse (DP) reception for an incoming call.

The system generates TRK117 when the system cannot determine call destination. The system was not able to determine call destination because system had problems during multi-frequency (MF) reception for an incoming call.

The system generates TRK138 if the system routes a call to treatment after the call was call processing busy.

The system generates TRK183 when a permanent signal problem occurs. The problem occurs because the system had problems during Digitone reception of an incoming call.

Register DPTRC

Register description

DPT Reservation Control (DPTRC) counts the number of DPT terminal requests that are blocked due to DPT bandwidth reservation.

Register release history update

Register is new in SN07.

Associated registers

Register DPTRC2 is an extension register for DPTRC.

Associated logs

None.

TRK2NET1 OM Group

OM description

TRK2NET1 OM Group provides information for per trunk group traffic analysis per bearer network. The OM group is modeled after group TRK. The TRK2NET1 OM group provides information on trunk traffic for each trunk group. The registers in TRK2NET1 count the following:

- routing attempts
- seizure attempts
- seize failures
- total trunk use
- busy state use

The OM groups OFZ and OTS provide office-wide traffic summaries for trunks. The OM groups OFZ2NET1 and OFZ2NET2 provide office-wide per bearer network traffic summaries for trunks.

Release history update

TRK2NET1 OM group is new in SN07.

The addition of this new TRK2NET1 OM group is controlled by the value of a new SN07 office parameter, MULTINET_DISPLAY_ACTIVE. If this parameter is set to 'Y', then the new TRK2NET1 OM group is displayed. If the parameter is set to 'N', then the TRK2NET1 OM group is not displayed.

Registers

TRK2NET1 OM group registers display on the MAP terminal as follows:

TRK2NET1 OM Group Display

>omshow trk2net1 active

TRK2NET1

CLASS: ACTIVE

START:2003/09/23 09:05:00 TUE; STOP: 2003/09/23 09:09:52 Tue;

SLOWSAMPLES: 3 ; FASTSAMPLES: 29 ;

KEY (COMMON_LANGUAGE_NAME_BEARNETS)

INFO (OM2TRKINFO)

INCAATT	PRERTEA1	NINFAIL	NATMPT
NVFLATB	GLARE1	OUTFL	CADEFLD
MBSYU	TRKNWBLK	TRFCU	SBSYU
ANIOFCFL	NANF	CNCTAT	TNDMATT
NACCCNG	NOANSWR	TOTBSYU	NANSWER
ANSUFIN		NINANSWR	OUTANSWR

100 TRK_TO_A NET 0 TDM_ENET

2W 0 0

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0			

100 TRK_TO_A NET 1 NET_AAL1

2W 0 0

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0			

100 TRK_TO_A NET 2 NET_IP

2W 0 0

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0			

Group structure

TRK2NET1 OM group provides 1 tuple(s) for each trunk group and each bearer network that the trunk group has members provisioned in.

Key field: None

Info field: OM2TRKINFO

- CLLI
- bearer network ID (i.e., 'NET 0')
- bearer network name (i.e., 'TDM_ENET')
- trunk group direction. (i.e., 'IC—incoming trunk, OG—outgoing trunk, 2W—two-way trunk')
- total number of trunk circuits in the group in the associated bearer network (i.e., '20')
- number of trunk circuits in the associated bearer network available for service at the end of the reporting period. (i.e., '19')

The office parameter OFFICETYPE in table OFCSTD specifies the type of office. The value of OFFICETYPE controls the generation of TRK2NET1 registers. Correct entries for OFFICETYPE appear below:

- OFF100 Local
- OFFCOMB Combined local/toll
- OFFCOMBTOPS Combined local/toll with traffic operator position system (TOPS)
- OFF200 Toll
- OFF200TOPS Toll with TOPS
- OFF250 DMS-250
- OFF500 DMS-500

The office type parameters appear in table OFCSTD. When the system reports an answer indication to CM from the outgoing trunk, the OM Answer register for the outgoing trunk increases.

The validity of a TRK2NET1 register in an officetype is given in the following table

TRK2NET1 OM Group Registers

Register	Present In Officetypes
INCAATT	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp, off100oesd, off200oesd, offcomboesd, offcomb300, nooffice
PRERTEA1	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp, off100oesd, off200oesd, offcomboesd, offcomb300, nooffice
NINFAIL	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp, off100oesd, off200oesd, offcomboesd, offcomb300, nooffice
NATMPT	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp, off100oesd, off200oesd, offcomboesd, offcomb300, nooffice
NVFLATB	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp, off100oesd, off200oesd, offcomboesd, offcomb300, nooffice
GLARE1	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp, off100oesd, off200oesd, offcomboesd, offcomb300, nooffice
OUTFL	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp, off100oesd, off200oesd, offcomboesd, offcomb300, nooffice
CADEFLD	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp, off100oesd, off200oesd, offcomboesd, offcomb300, nooffice
TRFCU	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp, off100oesd, off200oesd, offcomboesd, offcomb300, nooffice

Register	Present In Officetypes
SBSYU	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp, off100oesd, off200oesd, offcomboesd, offcomb300, nooffice
MBSYU	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp, off100oesd, off200oesd, offcomboesd, offcomb300, nooffice
TRKNWBLK	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp, off100oesd, off200oesd, offcomboesd, offcomb300, nooffice
CNCTAT	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, off200avon, offtollavon, off100scp, off100oesd, off200oesd, offcomboesd, offcomb300, nooffice
TNDMATT	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, off300, offtollavon, off100scp, off100oesd, off200oesd, offcomboesd, offcomb300, nooffice
ANIOFCFL	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off200tops, offcombtops, off500, offcomblww, offcomb300, offtollavon, nooffice
NANF	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off200tops, offcombtops, off500, offcomblww, offcomb300, offtollavon, nooffice
TOTBSYU	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, offcomb300, offtollavon, off100oesd, off200oesd, offcomboesd, nooffice
NANSWER	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off300, offcomb300, off100oesd, off200oesd, offcomboesd, nooffice
NACCCNG	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, nooffice
NOANSWR	off100, off200, offcomb, offcombitops, off200tops, offcombtops, off250, off250ibn, offmtx100i, off500, offcomblww, nooffice

Register	Present In Officetypes
NINANSWR	off100, off200, offcomb, offcombitops, off200tops, offcombtops, nooffice
OUTANSWR	off100, off200, offcomb, offcombitops, off200tops, offcombtops, nooffice
ANSUFIN	off100, off200, offcomb, offcombitops, off200tops, offcombtops, nooffice
INVATHCD	off250, off250ibn, offmtx100i, off500, offcomblww, offcomb300
MAXBSY	off250, off250ibn, offmtx100i, off500, offcomblww, offcomb300

Associated OM groups

The OFZ provides information about calls based on the source of the call. This OM group also provides information about calls based on the intended destination of the call. This information is on an office-wide basis.

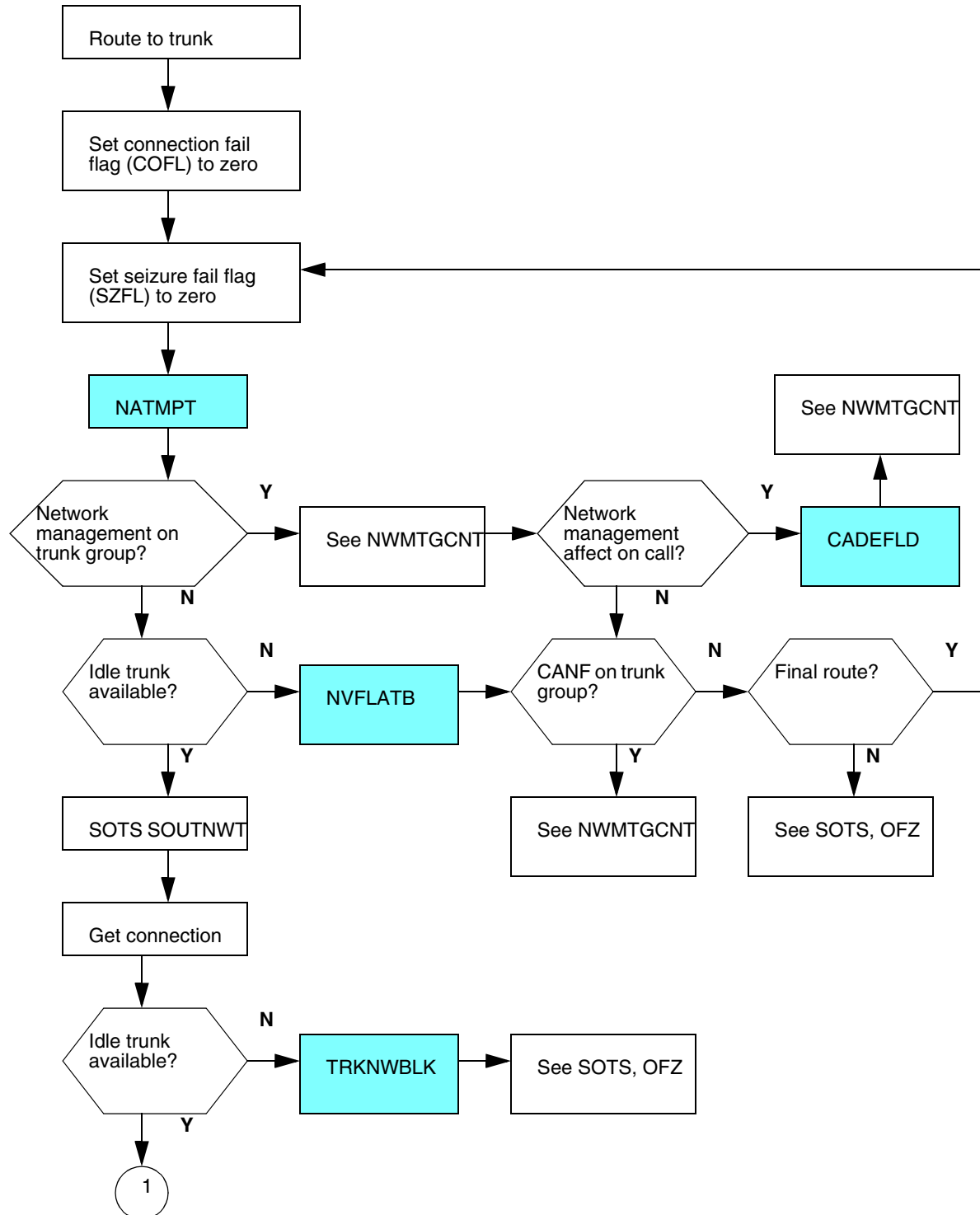
The OFZ2NET1 and OFZ2NET2 provide information about calls on a per bearer network based on the source of the call. This OM group also provides information about calls based on the intended destination of the call. This information is on an office-wide basis per bearer network.

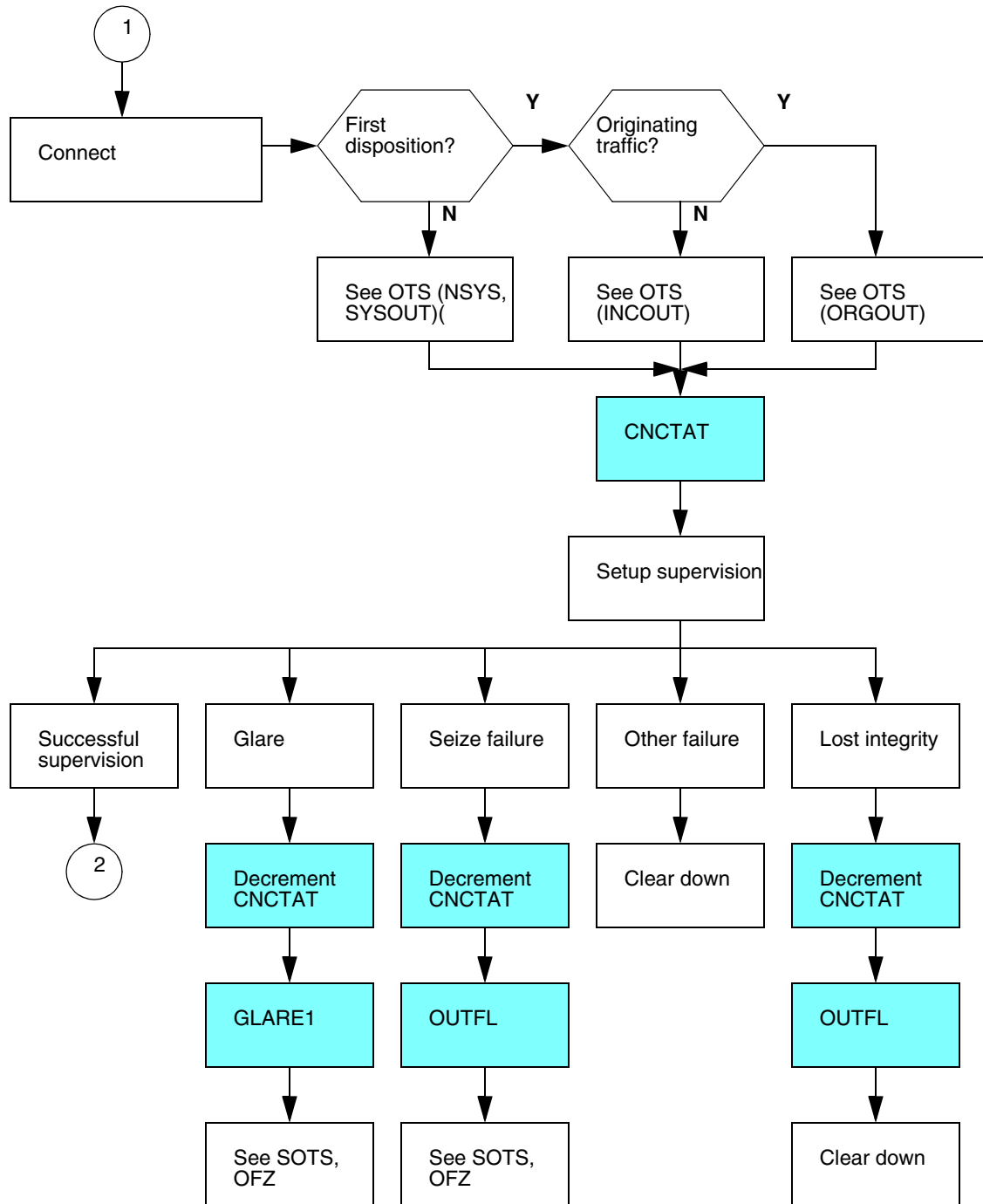
The OTS provides information about calls based on the source of the call. This OM group also provides information about calls based on the intended destination of the call. This information is on an office-wide basis.

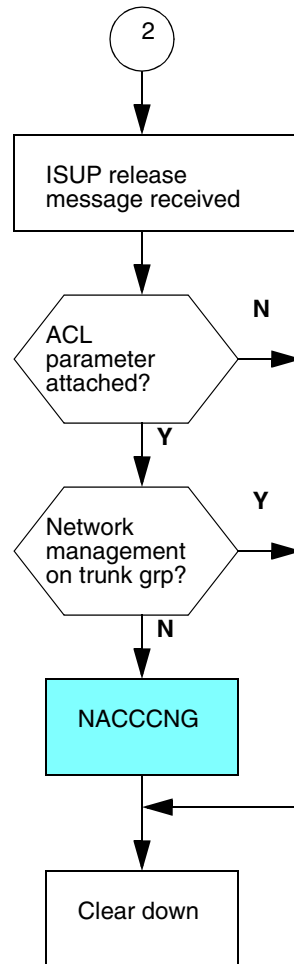
Associated functional groups

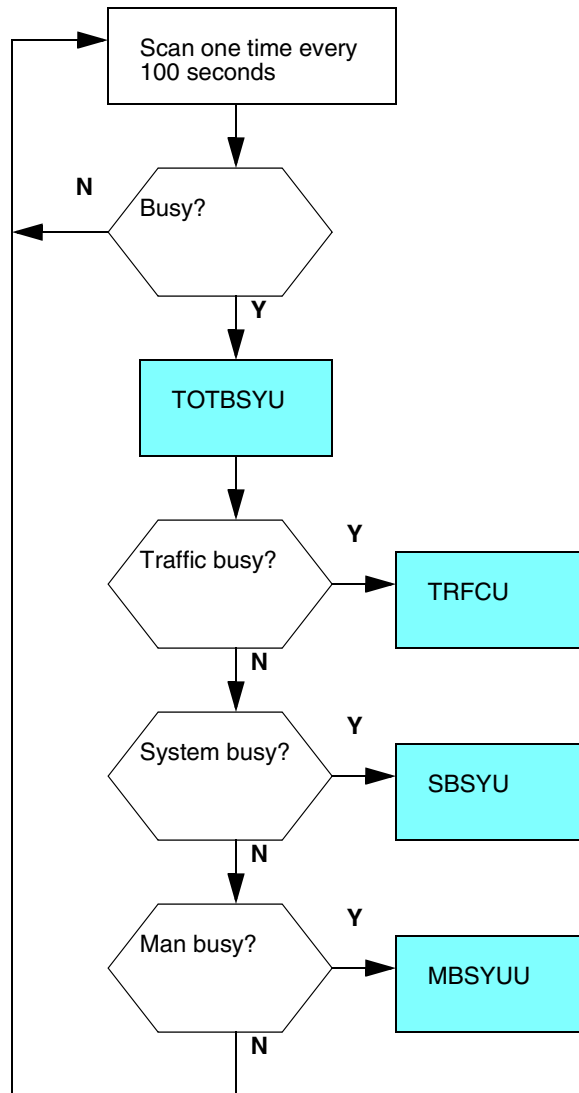
The following functional groups are associated with TRK2NET1 OM group:

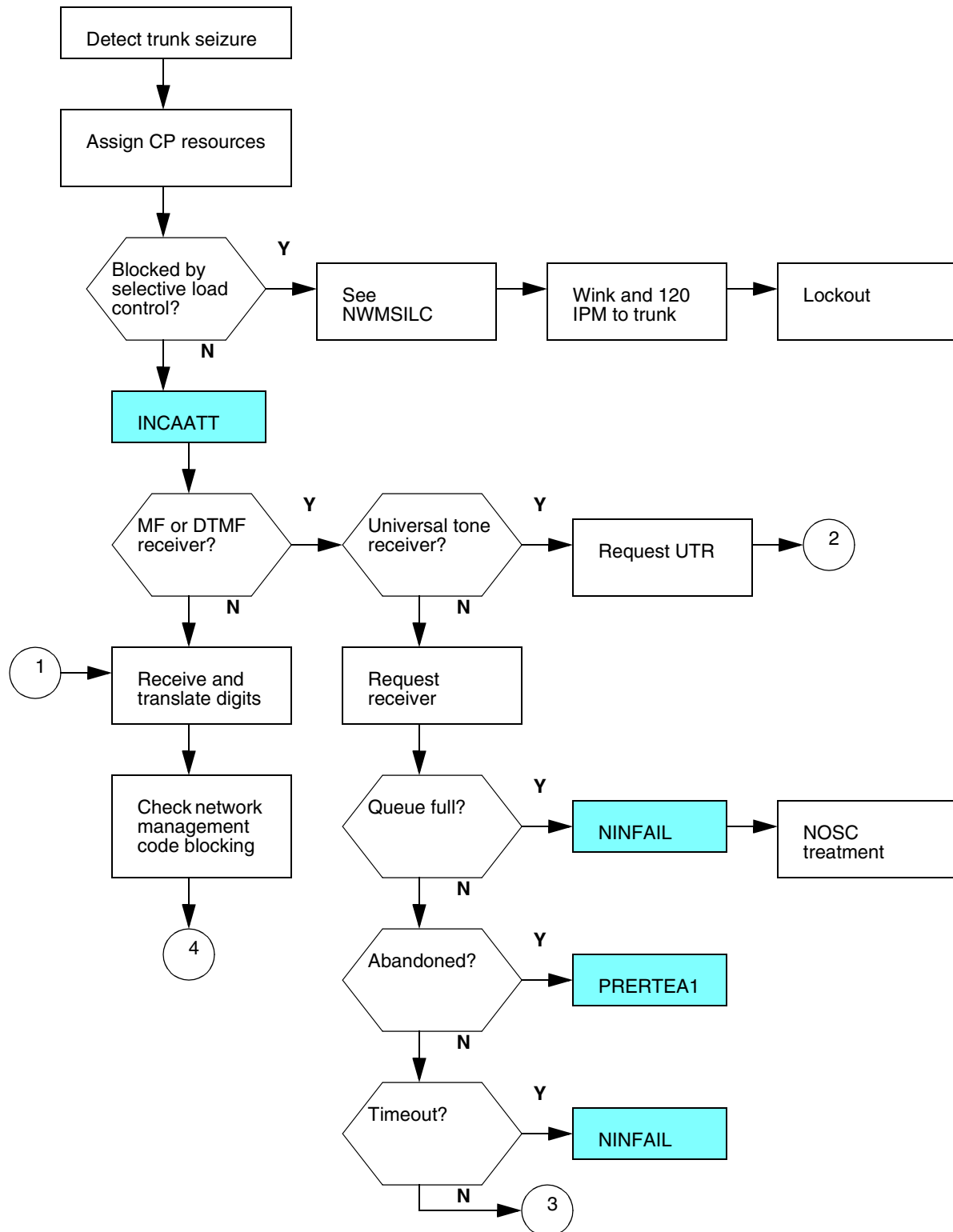
- Succession North America
- Succession International

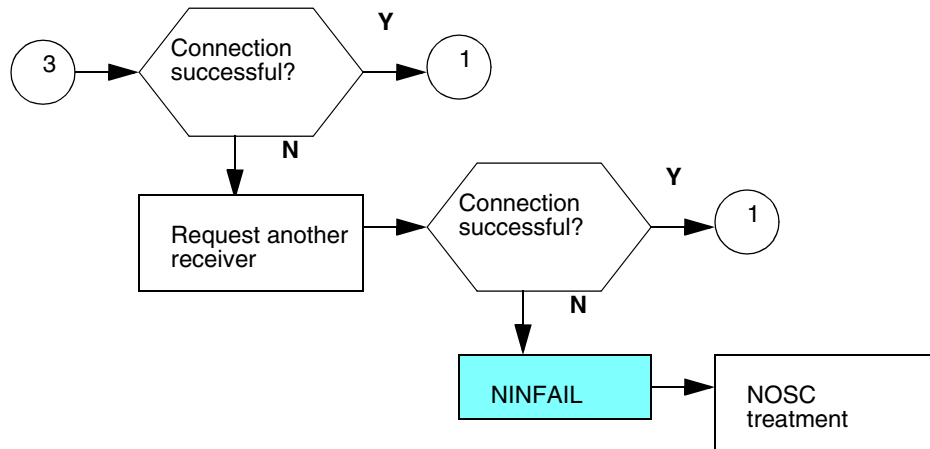
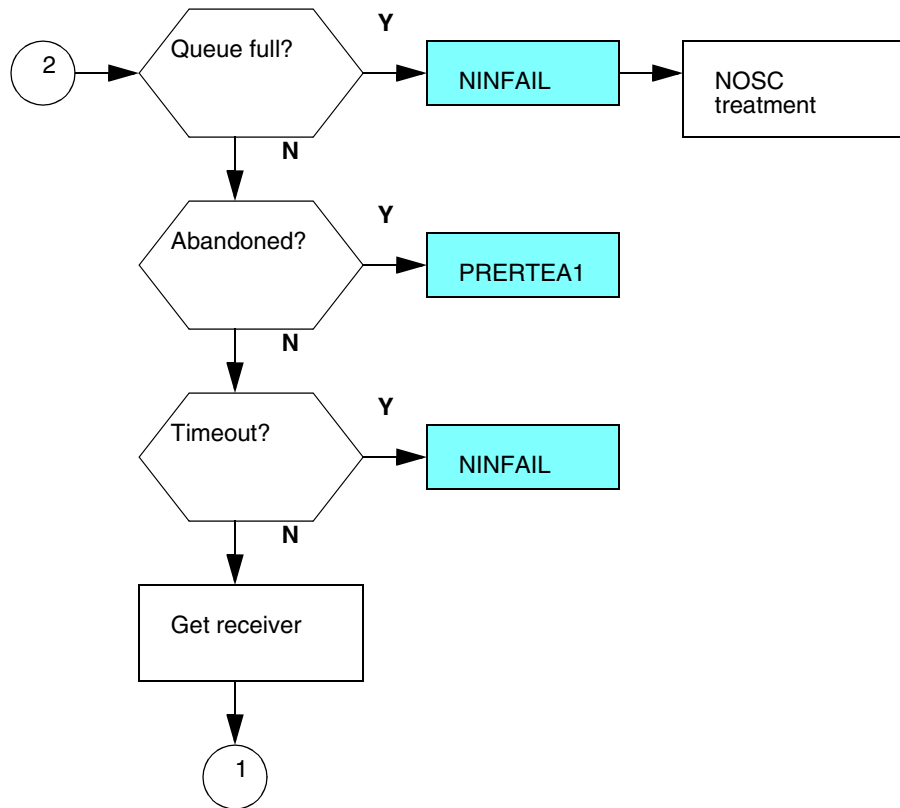
TRK2NET1 OM group registers logic flow chart**Termination to an outgoing trunk**

Termination to an outgoing trunk (continued)

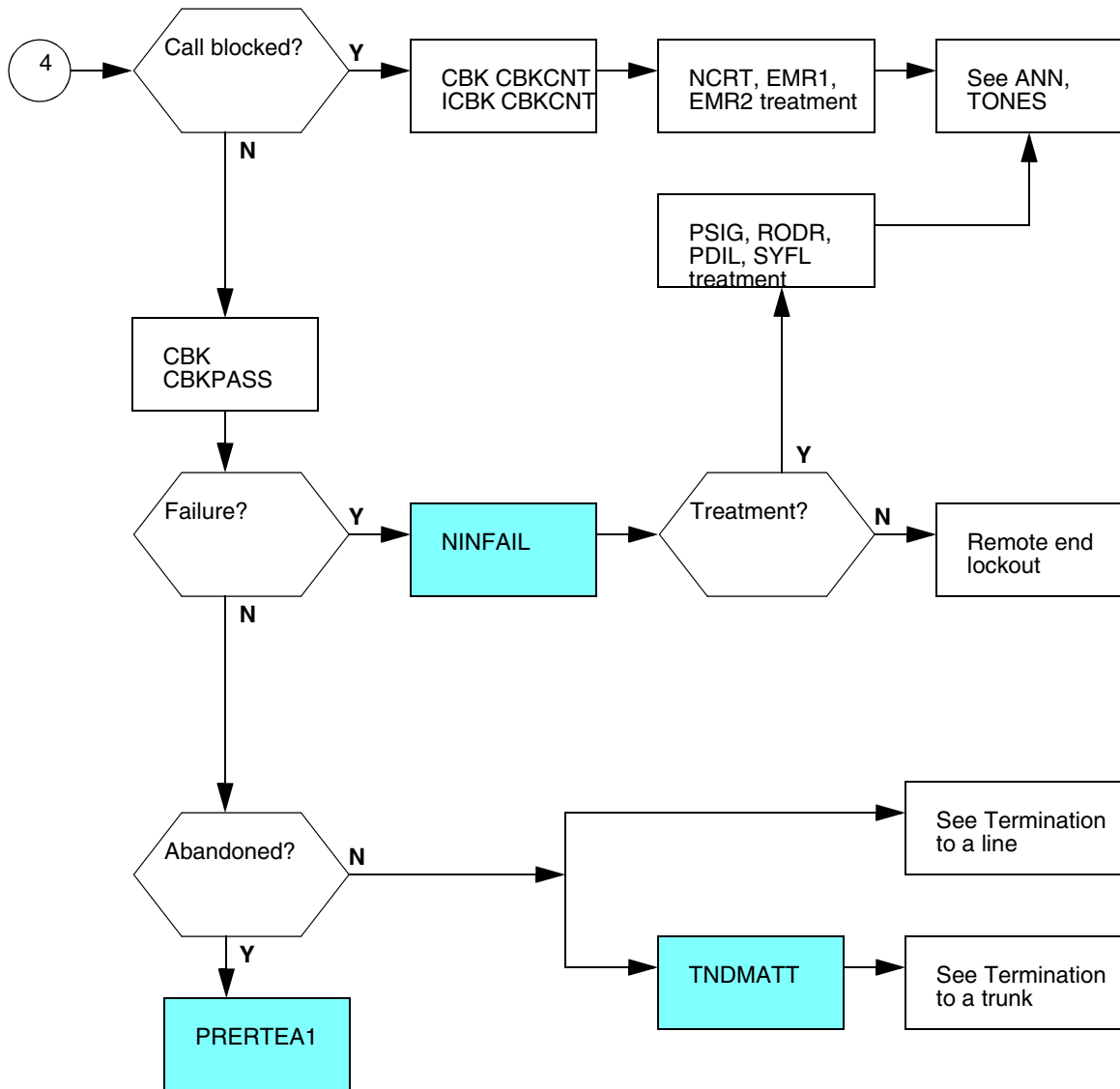
Termination to an outgoing trunk (continued)

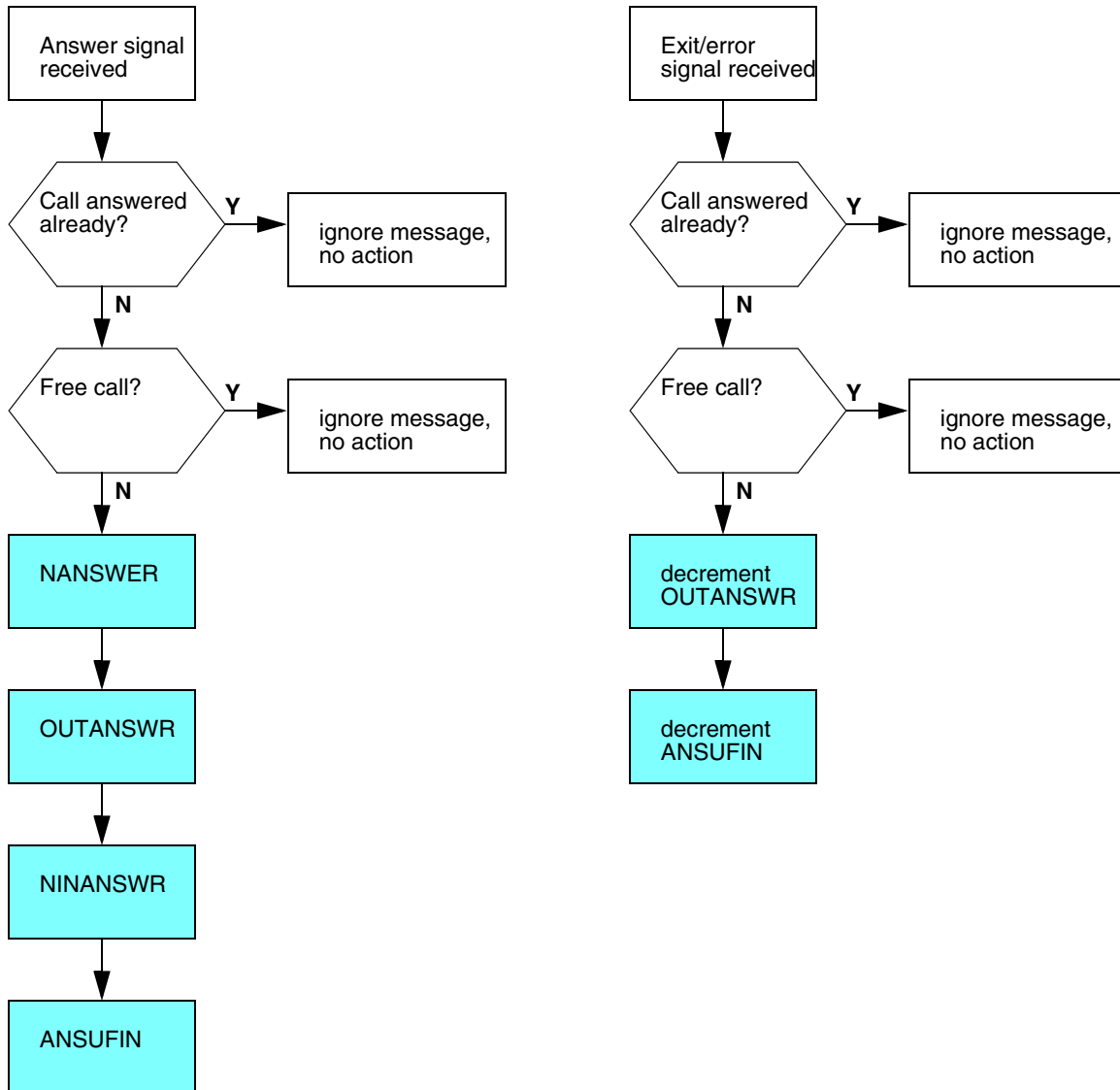
Trunk group busy usage registers

Origination from a trunk

Origination from a trunk (continued)

Origination from a trunk (continued)



Trunk group answered calls**Register NACCCNG****Register description**

Automatic congestion control (NACCCNG) counts the number of times that a trunk group enters Automatic Congestion Control (ACC) congestion.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

None.

Register NANF**Register description**

Invalid or no automatic number identification (ANI) signals (NANF) counts incoming centralized-automatic message accounting (CAMA) or TOPS calls for which:

- the system receives invalid ANI signaling
- the system did not receive ANI signaling
- the numbering plan area code (N0/1X) or the central office code (NNX) of the calling number for the incoming trunk group is not correct Register ANF increases when the system attaches the necessary receiver to the call.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates TRK120 when the call server or the intervening operator encounters problems. Problems can occur during operator number identification (ONI) spill for an incoming call over a CAMA trunk. The system cannot determine the call origination address.

Register NANSWER**Register description**

Answer supervisions (NANSWER) count all line/trunk to trunk answered calls. This register is the answer register for the outgoing trunk.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

None.

Register ANIOFCFL**Register description**

Automatic number identification (ANI) office failure (ANIOFCFL) counts incoming calls for which the originating office detects an ANI failure. Failure can be detected despite correct key pulse and signaling terminal control signals. The missing information digits, missing category code or the complete lack of digits indicates an ANI failure.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

Register TRK118 generates when the system encounters trouble during ANI spill for an incoming call. In this example, the system cannot determine call originating address.

Register TRK119 generates when an operator keys in the originating station number identification and releases the call. The operator releases the call because the system encounters trouble with DMS ANI.

Register CNCTAT**Register description**

Successful connections (CNCTAT) counts outgoing seizure attempts on the trunk group that appear to result in successful connection.

Register CNCTAT increases before the system knows if the seizure is successful. The count reduces by 1 (decreases) if an indication of glare or seizure failure is received. This register generates for all correct office types.

Register release history update

Register is new in SN07.

Associated registers

Register GLARE1 increases when the system drops an earlier selected trunk. The system drops the trunk because the peripheral module detects an origination before it can seize the trunk.

Associated logs

None.

Register CADEFD

Register description

Network management (NWM) reroute (CADEFD) counts calls that the system prevents from accessing the trunk group. The system routes the calls to this trunk group. The system denies access by the calls because of the action of network management controls.

Register CADEFD counts calls that the system denies for the activity of any of the following NWM controls:

- SKIP control is in effect
- the number of trunks qualified for incoming calls is at or below the directional reservation (DRE) level
- the number of idle trunks is at or below the protective reservation (PRE) level for calls that have been alternate-routed to the group
- time assignment speech interpolation (TASI) control is in effect
- selective trunk reservation (STR) control is in effect
- cancel to (CANT) control is in effect
- bidirectional trunk group reservation control (BRC) is in effect

If the control is SKIP, DRE, PRE, or TASI, the system routes the call. If cancel from (CANF) control is in effect, the system sends the call to treatment. If the control is STR or CANT the system sends the call to treatment.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates NWM100 when the system activates or deactivates DRE for a trunk group.

The system generates NWM101 when the system activates or deactivates PRE for a trunk group.

The system generates NWM102 when the system activates or deactivates CANT for a trunk group.

The system generates NWM103 when the system activates or deactivates CANF for a trunk group.

The system generates NWM104 when the system activates or deactivates SKIP for a trunk group.

The system generates NWM106 when the system activates or deactivates STR for a trunk group.

The system generates NWM108 when the system activates or deactivates TASI for a trunk group.

Register GLARE1

Register description

Glare (GLARE1) increases when the system drops a trunk that the system selects at an earlier time. The system drops this trunk because the PM detects an origination before the PM can seize the trunk. The operating company gives information that indicates that outgoing calls give way to simultaneous incoming calls (glare).

The system attempts a new selection. If the system encounters glare again, the system routes the call to generalized no-circuit (GNCT) treatment. Register GLARE1 increases again.

Register release history update

Register is new in SN07.

Associated registers

Register CNCTAT counts outgoing seizure attempts on the trunk group that result in connections.

Register OUTFL counts errors on an outgoing trunk after an attempt to seize the trunk.

Associated logs

The system generates log TRK113 if the system encounters problems during call processing of a trunk-to-trunk call. The system generates TRK121 if the call server does not receive an acknowledgement wink from the far-end equipment. An acknowledgement wink indicates that the far-end equipment is ready to receive digits.

Register NINANSWR

Register description

Answer messages sent and received on incoming trunk (NINANSWR) counts the answered calls for incoming traffic for each incoming or two-way trunk.

This register is not pegged in the current load.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

None.

Register ANSUFIN**Register description**

Answer messages received and sent usage on incoming trunk (ANSUFIN) is a usage register that shows the number of answered calls on incoming trunk calls. This register measures traffic in the answered state for each incoming or two-way trunk. The register measures the occupancy in Erlangs.

The value of register ANSUFIN increases every 100 seconds according to the number of trunks occupied with answered calls.

This register is not pegged in the current load.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

None.

Register INCAATT**Register description**

Incoming attempts total (INCAATT) counts incoming seizures on a trunk group, including seizures that fail or that the system abandons before routing.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

None.

Register NINFALL

Register description

Incoming failures (NINFALL) increases when any one of the following events occurs on a trunk that has originated a call or appears to have originated a call:

- permanent signal
- partial dial time-outs and false starts
- bad digits, including bad signaling terminal (ST) digit
- any originations on one-way outgoing trunks
- lost integrity on the network path while connected to a service circuit or to another trunk before answer
- failure to attach a receiver after two attempts
- receiver queue overflow
- receiver queue wait time-out
- failure to time-out after 30 s while waiting for a multi frequency receiver
- progress message of a type not expected in the current call environment
- force-release before connection

These events can indicate a need for maintenance action. These events can result in call failure if a call was in progress.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates TRK111 if a trunk-to-trunk call encounters problems or if the system routes the call to a treatment.

The system generates log TRK114 if the system cannot determine the call destination during dial pulse (DP) reception for an incoming call.

The system generates log TRK115 if the system cannot determine the call destination during DP reception for an incoming call.

The system generates log TRK116 if the system cannot determine call destination during multi frequency (MF) reception for an incoming call.

The system generates log TRK117 if the system cannot determine call destination during MF reception for an incoming call.

The system generates log TRK138 if the system routes a call to a treatment after being call processing busy.

The system generates log TRK182 if the system cannot determine call destination during Digitone (DT) reception for an incoming call.

The system generates log TRK183 if a permanent signal problem occurs when an incoming call encounters problems during DT reception.

The system generates log TRK213 when the system encounters problems on a trunk.

Register MBSYU

Register description

Maintenance busy usage (MBSYU) is a usage register. Every 100 s the system scans the trunk group. This register records if a trunk is in one of the following states:

- manual busy
- seized
- network management busy

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

None.

Register NATMPT

Register description

Number of attempts (NATMPT) increases when the system routes an outgoing call to a trunk group.

Register NATMPT increases before network management controls increase. This register increases before an idle trunk and a network connection to the trunk are available.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

None.

Register NOANSWR**Register description**

No Answer on trunk [Timed out] (NOANSWR) is a peg register which counts the number of times a call has been taken down after a specified time-out value has been reached, as part of Black Box Fraud prevention (BBFP). The time-out value is implemented on a trunk-group basis and can be set to either one, two, three, four, or five minute intervals. Upon expiration of the timer, the NOANSWR register is pegged.

NOANSWR functionality is activated and deactivated via the DLYFWDXMT option datafill of table TRKOPTS on a trunk-group basis. Register NOANSWR is pegged when the black box fraud timer or DLYFWDXMT timer expires before an answer supervision signal is received. The time-out value is datafilled in table TRKOPTS.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

Log TRK610 is generated each time the NOANSWR register is pegged.

Register NVFLATB**Register description**

Number of overflows, all trunks busy (NVFLATB) increases when a call with access to the trunk group overflows the group. The system routes the call because an idle trunk is not available. A call can access the same group more than one time. Overflow can occur only one time. Overflow occurs if the system cannot use the first trunk because of seize fail, glare or network blockage. Register NVFLATB increases when the system cannot find an idle trunk on the first or any of the following access attempts.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates ATB100 when the system blocks an attempt to seize a trunk to a specified numbering plan area or central office. The system advances the call to another route.

Register OUTANSWR**Register description**

Answer message received and sent usage on an outgoing trunk (OUTANSWR) is a usage register that shows the number of answered calls on outgoing trunk calls. This register measures traffic in the answered state for each outgoing or two-way trunk. The register measures the occupancy in Erlangs.

The value of register OUTANSWR increases every 100 seconds according to the number of trunks occupied with answered calls.

This register is not pegged in the current load.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

None.

Register OUTFL**Register description**

Outgoing failures (OUTFL) counts attempts to seize an outgoing trunk in the trunk group that fail because of following:

- signaling problems
- loss of accuracy
- outgoing failures
- seizure failures

The system releases the trunk. The system performs a maximum of two attempts to seize a trunk. The system counts each failed attempt in OUTFL. If a second attempt to seize a trunk fails, the system routes the call to treatment.

The system can generate a log message. Generation of a log message depends on the cause of the failure.

The system generates register OUTFL for office types that are correct.

Register release history update

Register is new in SN07.

Associated registers

Register CNCTAT counts outgoing seizure attempts on the trunk group that result in connections.

Register GLARE1 increases when the system drops a trunk that the system selects at an earlier time. The system drops the trunk because the PM detected an origination. The PM detects an origination before the PM seizes the trunk.

Associated logs

The system generates TRK113 if the system encounters problems during call processing of a trunk-to-trunk call.

The system generates TRK121 if the DMS does not receive an acknowledgement wink from the far-end equipment. The acknowledgement wink indicates that the equipment is ready to receive digits.

The system generates TRK122 if the central control detects a loss of accuracy on both planes of the trunk equipment.

The system generates TRK162 if the system encounters problems during outpulsing of a trunk-to-trunk or line-to-trunk call. The call uses dual-tone multi frequency (DTMF) signaling.

The system generates TRK213 if the system encounters problems on a trunk.

Register TRKNWBLK**Register description**

Outgoing matching failure (TRKNWBLK) counts attempts to find a path from an incoming trunk or originating line to a selected trunk that fail. Failure occurs as a result of network blockage.

If the system blocks an outgoing call, the call again attempts to select a trunk. If the system blocks this attempt, TRKNWBLK counts the call again. The system routes the call to NBLH treatment.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates NET130 if the system cannot find a network path.

Register PRERTEA1**Register description**

Preroute abandon (PRERTEA1) counts incoming attempts the system abandons before the system can complete routing.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates register TRK113 if the system encounters problems during call processing of a trunk-to-trunk call.

The system generates TRK116 if the system cannot determine the call destination during multi frequency reception for an incoming call.

Register SBSYU**Register description**

System busy usage (SBSYU) is a usage register. Every 100 seconds the system scans the trunk group. This register records if a trunk is in one of the following states:

- remote busy
- peripheral module busy
- system busy
- carrier fail
- deloaded

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

The system generates TRK106 if a self-test on trunk equipment fails.

The system generates TRK109 when a self-test on a DS-1 facility fails.

Register TNDMATT

Register description

Tandem (TNDMATT) counts incoming calls on a trunk group that first routes to an outgoing trunk group. Register TNDMATT increases before the system determines if the outgoing trunk group is busy, or if a junctor path is available.

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

None.

Register TOTBSYU

Register description

Total usage (TOTBSYU) is a usage register. Every 100 seconds the system scans the trunk group and register TOTU records if any trunk in the group is busy.

Register release history update

Register is new in SN07.

Associated registers

Register MBU counts manual busy trunks.

Register SBU counts system busy trunks.

Register TRU counts call processing busy trunks.

$TOTU = TRU + SBU + MBU$.

Associated logs

None.

Register TRFCU

Register description

Traffic busy usage (TRFCU) is a usage register. Every 100 s the system scans the trunk group. This register records if a trunk in the group is in one of the following states:

- call processing busy (TK_CP_BUSY)
- call processing busy deload (TK_CP_BUSY_DELOAD)
- lockout (TK_LOCKOUT)

Register release history update

Register is new in SN07.

Associated registers

None.

Associated logs

None.

TRK2NET2 OM Group**OM description**

TRK2NET2 OM Group provides information for per trunk group traffic analysis per bearer network. It contains extension registers for registers found in OM Group TRK2NET1.

Release history update

TRK2NET2 OM group is new in SN07.

The addition of this new TRK2NET2 OM group is controlled by the value of a new SN07 office parameter, MULTINET_DISPLAY_ACTIVE. If this parameter is set to 'Y', then the new TRK2NET2 OM group is displayed. If the parameter is set to 'N', then the TRK2NET2 OM group is not displayed.

Registers

TRK2NET2 OM group registers display on the MAP terminal as follows:

TRK2NET2 OM Group Display

```
>omshow trk2net2 active
```

```
TRK2NET2
```

```
CLASS: ACTIVE
```

```
START:2003/09/23 09:05:00 TUE; STOP: 2003/09/23 09:09:52 Tue;
```

```
SLOWSAMPLES: 3 ; FASTSAMPLES: 29 ;
```

```
KEY (TRK2NET_KEY)
```

```
INFO (OM2TRKINFO)
```

INCAATT2	NATMPT2	CADEFD2	TRFCU2
SBSYU2	CNCTAT2	TNDMATT2	TOTBSYU2
NANSWER2			

```
100 TRK_TO_A NET 0 TDM_ENET
```

2W	0	0		
	0	0	0	0
	0	0	0	0
	0			

```
100 TRK_TO_A NET 1 NET_AAL1
```

2W	0	0		
	0	0	0	0
	0	0	0	0
	0			

```
100 TRK_TO_A NET 2 NET_IP
```

2W	0	0		
	0	0	0	0
	0	0	0	0
	0			

Group structure

TRK2NET2 OM group provides 1 tuple(s) for each trunk group and each bearer network that the trunk group has members provisioned in.

Key field: None

Info field: OM2TRKINFO

- CLI
- bearer network ID (i.e., 'NET 0')
- bearer network name (i.e., 'TDM_ENET')

- trunk group direction. (i.e., 'IC—incoming trunk, OG—outgoing trunk, 2W—two-way trunk')
- total number of trunk circuits in the group in the associated bearer network (i.e., '20')
- number of trunk circuits in the associated bearer network available for service at the end of the reporting period. (i.e., '19')

The office parameter OFFICETYPE in table OFCSTD specifies the type of office. The value of OFFICETYPE controls the generation of TRK2NET2 registers. Correct entries for OFFICETYPE appear below:

- OFF100 Local
- OFFCOMB Combined local/toll
- OFFCOMBTOPS Combined local/toll with traffic operator position system (TOPS)
- OFF200 Toll
- OFF200TOPS Toll with TOPS
- OFF250 DMS-250
- OFF500 DMS-500

The office type parameters appear in table OFCSTD. When the system reports an answer indication to CM from the outgoing trunk, the OM Answer register for the outgoing trunk increases.

Associated OM groups

The TRK2NET1 OM group provides the primary registers. The registers found in TRK2NET2 are pegged only if the registers in TRK2NET1 overflow.

Associated functional groups

The following functional groups are associated with TRK2NET2 OM group:

- Succession North America
- Succession International

TRK2NET2 OM group registers logic flow chart

Refer to TRK2NET1 for register flow charts.

Register NANSWER2

Register description

Answer supervisions (NANSWER2) count all line/trunk to trunk answered calls. This register is the answer register for the outgoing trunk.

Register release history update

Register is new in SN07.

Associated registers

NANSWER in TRK2NET1 OM group.

Associated logs

None.

Register CNCTAT2**Register description**

Successful connections (CNCTAT2) counts outgoing seizure attempts on the trunk group that appear to result in successful connection.

Register CNCTAT2 increases before the system knows if the seizure is successful. The count reduces by 1 (decreases) if an indication of glare or seize failure is received. This register generates for all correct office types.

Register release history update

Register is new in SN07.

Associated registers

CNCTAT in TRK2NET1 OM group.

Associated logs

None.

Register CADEFD2**Register description**

Network management (NWM) reroute (CADEFD2) counts calls that the system prevents from accessing the trunk group. The system routes the calls to this trunk group. The system denies access by the calls because of the action of network management controls.

Register CADEFD2 counts calls that the system denies for the activity of any of the following NWM controls:

- SKIP control is in effect
- the number of trunks qualified for incoming calls is at or below the directional reservation (DRE) level
- the number of idle trunks is at or below the protective reservation (PRE) level for calls that have been alternate-routed to the group
- time assignment speech interpolation (TASI) control is in effect
- selective trunk reservation (STR) control is in effect

- cancel to (CANT) control is in effect
- bidirectional trunk group reservation control (BRC) is in effect

If the control is SKIP, DRE, PRE, or TASI, the system routes the call. If cancel from (CANF) control is in effect, the system sends the call to treatment. If the control is STR or CANT the system sends the call to treatment.

Register release history update

Register is new in SN07.

Associated registers

CADEFLD in TRK2NET1 OM group.

Associated logs

The system generates NWM100 when the system activates or deactivates DRE for a trunk group.

The system generates NWM101 when the system activates or deactivates PRE for a trunk group.

The system generates NWM102 when the system activates or deactivates CANT for a trunk group.

The system generates NWM103 when the system activates or deactivates CANF for a trunk group.

The system generates NWM104 when the system activates or deactivates SKIP for a trunk group.

The system generates NWM106 when the system activates or deactivates STR for a trunk group.

The system generates NWM108 when the system activates or deactivates TASI for a trunk group.

Register INCAATT2**Register description**

Incoming attempts total (INCAATT2) counts incoming seizures on a trunk group, including seizures that fail or that the system abandons before routing.

Register release history update

Register is new in SN07.

Associated registers

INCAATT in TRK2NET1 OM group.

Associated logs

None.

Register NATMPT2**Register description**

Number of attempts (NATMPT2) increases when the system routes an outgoing call to a trunk group.

Register NATMPT2 increases before network management controls increase. This register increases before an idle trunk and a network connection to the trunk are available.

Register release history update

Register is new in SN07.

Associated registers

INATMPT in TRK2NET1 OM group.

Associated logs

None.

Register SBSYU2**Register description**

System busy usage (SBSYU2) is a usage register. Every 100 seconds the system scans the trunk group. This register records if a trunk is in one of the following states:

- remote busy
- peripheral module busy
- system busy
- carrier fail
- deloaded

Register release history update

Register is new in SN07.

Associated registers

SBSYU in TRK2NET1 OM group.

Associated logs

The system generates TRK106 if a self-test on trunk equipment fails.

The system generates TRK109 when a self-test on a DS-1 facility fails.

Register TNDMATT2

Register description

Tandem (TNDMATT2) counts incoming calls on a trunk group that first routes to an outgoing trunk group. Register TNDMATT2 increases before the system determines if the outgoing trunk group is busy, or if a junctor path is available.

Register release history update

Register is new in SN07.

Associated registers

TNDMATT in TRK2NET1 OM group.

Associated logs

None.

Register TOTBSYU2

Register description

Total usage (TOTBSYU2) is a usage register. Every 100 seconds the system scans the trunk group and register TOTBSYU2 records if any trunk in the group is busy.

Register release history update

Register is new in SN07.

Associated registers

TOTBSYU in TRK2NET1 OM group.

Associated logs

None.

Register TRFCU2

Register description

Traffic busy usage (TRFCU2) is a usage register. Every 100 seconds the system scans the trunk group. This register records if a trunk in the group is in one of the following states:

- call processing busy (TK_CP_BUSY)
- call processing busy deload (TK_CP_BUSY_DELOAD)
- lockout (TK_LOCKOUT)

Register release history update

Register is new in SN07.

Associated registers

TRFCU in TRK2NET1 OM group.

Associated logs
None.



Product = CS 2000

A00003489 -- ABI SMS Support (UA-IP)

Functional Description

This activity adds support for the SMS and its subtending SLC-96s to the list of legacy PMs supported by the ABI program. The ABI program allows legacy host XPMs to be connected to the packet network without use of an ENET and an I/W Bridge. Instead the XPM is connected to an ABI card in the MG9K via its legacy DS-512 interface. The MG9K in turn provides connectivity to the packet network. This feature will support Mode 1 and Mode 2 SLC-96s. It will work with both the existing ATM MG9K and be integrated with the new IP version.

The main customer visible changes for this activity will be the ability to provision the EXTDS512 optional field as part of the tuple in table LTCINV for the SMS Peripheral Type. The optional field is used to identify the IP Address of the ABI Card and the Gateway Controller that the peripheral is 'hosted' off (the GWC must be datafilled in table SERVINV prior to entering this information). A full description of the table control changes is available in the Data Schema section of this document.

Hardware Requirements or Dependencies

There are no hardware requirements for this project. Integration with the IP project will require the new IP MG9K.

Software Requirements or Dependencies

The CM changes will go directly into SN07. The SMS load is currently frozen. The last load was built in the XPM14 time frame out of the XPM13BC context. The load will be brought on stream in XAX20 to add this new functionality.

Limitations and restrictions

- Only Mode 1 and Mode 2 SLCs will be supported. Mode 3 SLCs might also work, but, they will not be tested.
- RMM support will not be added to the SMS.
- Line Test will therefore only be supported using RMMs located in other XPMs at the site with the SMS or via DIal Up External test sets.

Interactions

This new code will need to interact with the existing ABI framework for link maintenance, packet connection setup, and MG9K ESA.

Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema _____X_____

User Interface _____X_____

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

Realtime _____X_____

Engineering Information _____X_____

Glossary

Term	Description
ABI	Access Bridging Interface
SLC	Subscriber Loop Carrier
SMS	Subscriber Module for SLC-96/RT
XAX	Current XPM design stream for MX77 loads

Configuration for A00003489

Hardware and Software Requirements

Not required.

Initial Configuration

Not required.

Office/Subnet parameters (OP/SP) (CM & SESM)

Not required.

Upgrade Impact

Not required.

Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
LTCINV	Changed	Unchanged

Table/MIB/Remote Database Schema information

Name: LTCINV

Table LTCINV lists all the line and trunk controlling peripherals in the office. Historically they all were connected to the ENET and this table was used (among other things) to datafill the details of this connection. With the ABI program some XPM types were now allowed to subtend the packet network. To support this architectural change the EXTDS512 optional field was added to this table in SN06. Only those XPM types that were allowed to subtend the packet network were allowed to use this new optional field. This feature adds SMS to the list of XPM types that can be datafilled as subtending the packet network using this optional field.

There is no change in the format of the table or in the format of the optional field, all that has been changed is the types of peripherals that are allowed to have the field provisioned. All other types of peripherals that can be added in table LTCINV will continue to receive an error message if the EXTDS512 field is provisioned.

Note: Please refer to the documentation for SN05 activity A59038361 for more detailed information of the initial EXTDS512 design.

Usage sequence and implications (CM Only)

Current datafill order unchanged (SERVRINV must be datafilled prior to adding EXTDS512 peripherals in LTCINV).

Size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
LTCINV	Unchanged by this activity.	Unchanged by this activity.	All existing tuples, regardless of whether the EXTDS512 attribute is provisioned or not, have the physical space allocated for the information contained in this field; therefore, there is no memory impact from this activity as the memory is already allocated for all tuples in this table.

Fields/OIDs

The following table lists fields for LTCINV.

CSLNKTAB = "\$"

OPT_ATTR = EXTDS512

When provisioning an external (non-ENET hosted) peripheral in LTCINV the EXTDS512 OPT_ATTR must be added. This optional attribute includes the IP Address of the DS512 (ABI) card in the MG9000 and Gateway Controller host name (as provisioned in table SERVINV).

It should be noted that the CSLNKTAB portion of the tuple is not datafilled when adding external XPMs. The content of the CSLNKTAB field is automatically generated by the LTCINV code and no longer refers to real C-side links to the ENET. A "\$" should be entered when prompted for the CSLNKTAB entry (this is unchanged from SN05 behavior).

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CSLNKTAB	Changed	Unchanged from SN05	None	For External XPMs this field no longer contains real C-side ENET links. Instead, "\$" should be entered when prompted for this field. With this activity you should now enter "\$" when provisioning External SMS tuples in LTCINV.
OPT_ATTR (EXTDS512)	Changed	Unchanged from SN05	Unchanged from SN05	When datafilling external SMS peripherals you should add this field and enter the IP address of the DS512 card in the MG9000 and the name of the host GWC (from table SERVINV).

Datafill example

The following example shows sample datafill for table LTCINV. The changes from standard ENET-based peripheral datafill is highlighted with **bold** characters.

```
TABLE: LTCINV
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
LTCNAME:
>sms 0
ADNUM:
>1007
FRTYPE:
>sme
FRNO:
>1
SHPOS:
>18
FLOOR:
>1
ROW:
>F
FRPOS:
>4
EQPEC:
>6X02AA
LOAD:
>ESS20BB
EXECTAB:
>POTS POTSEX
EXECTAB:
>$
CSLNKTAB:
>$
OPTCARD:
>UTR17
OPTCARD:
>MSG6X69
OPTCARD:
>CMR16
CMRLOAD:
>CMR10A
OPTCARD:
>$
TONESET:
>northaa
PROCPEC:
>MX77AA MX77AA $
EXTLINKS:
>0
E2LOAD:
>UPFWNQ03
OPT_ATTR:
>EXTDS512
IPADDR:
>192 2 7 69
```

```

GWC_HOST:
>GWC 3
OPT_ATTR:
>$
PEC6X40:
>6X40FA
EXTSHELF: N
>

```

The following shows the range values for the OPTATTR field of table LTCINV. Note that this has not changed from the SN05 version.

```

TABLE: LTCINV
>ran
 1 LTCNAME          XPM_KEY
 2 ADNUM            ADMIN_NUMBER
 3 FRTYPE           FRAME_NAME
 4 FRNO             FRAME_NO
 5 SHPOS            SHELF_POS
 6 FLOOR            FLOOR_POS
 7 ROW              ROW_POS
 8 FRPOS            FRAME_POS
 9 EQPEC            PEC
10 LOAD             NPMLoad_INFO
11 EXECTAB           TERM_EXEC_TC_TAB
12 CSLNKTAB          XPM_NET_CSLINK_TC_TAB
13 OPTCARD           EXT_OPT_CARD_TC_TAB
14 TONESET           TONE_SET_TYPE
15 PROCPEC           XPM_PEC_AREA_TAB
16 EXTLINKS          NUM_EXT_LNKS_RANGE
17 E2LOAD            NPMLoad_INFO
18 OPTATTR           LTCINV_OPT_ATTR_VECTOR
19 PEC6X40           NT_6X40_PEC
20 EXTINFO           EXTENSION_INFO
LOGICAL TUPLE TYPE: LTC_LOGTUPLE
>ran 18
18 OPTATTR           LTCINV_OPT_ATTR_VECTOR
TYPE IS LTCINV_OPT_ATTR_VECTOR VECTOR OF UP TO 12 MULTIPLES WITH
OPT_ATTR LTCINV_OPT_ATTR REFINEMENTS:
{EXTDS512} MULTIPLE WITH
IPADDR TABLE OF 4 {0 TO 255}'S
GWC_HOST MULTIPLE WITH
PMTYPE PM_TYPE
PMNO {0 TO 255}
OTHERWISE LTCINV_OPT_ATTR_NIL_DATA
>

```

Table release history update

The following changes were made:

1. EXTDS512 OPT_ATTR is now allowed for the SMS peripheral type.
2. "\$" should be entered in the CSLNKTAB field for external XPMs (the C-side link information will be generated automatically).

Supplementary information

- The CSLNKTAB and EXTDS512 optional attribute must align in each tuple in LTCINV. This means that if EXTDS512 exists then a “\$” must have been entered in the CSLNKTAB field. A tuple must be either ENET based on External but not a combination of both.
- Multiple tuples of each type (ENET and External) can exist in the table at the same time.
- The EXTDS512 optional attribute can be provisioned only against LTC, LGC, LTCI, LGCI, SMA2, and SMS peripheral types. Attempting to add the optional attribute to other peripheral types will result in the tuple failing verification and an error will be displayed.
- The derived CSLNKTAB entries for External XPMs cannot be changed by the user.
- The ability to change the Host Gateway Controller for External XPMs is not allowed.
- The EXTDS512 optional attribute cannot be added to an existing tuple using the change command in table control, nor can it be removed using change.

Translation verification other tools

Output from the check all table control command and tabaudit will be included at a later date, but no issues are expected with these commands as the changes to LTCINV are minor.

Table Changes

As part of feature A00003486 ‘Gateway location information’ the format of the LTCINV tuple will be changing. This will impact how an External SMS will be datafilled in the CM. There will be no changes to this table unique to SMS. For details on the changes consult the documentation for that feature.

Service Orders (SO) (CM & SESM)

Not Required.

Software optionality control (SOC)

Not Required.

Element Management

Not Required.

Command interface changes

Directory: MAPCI;MTC;PM

Directory description

No new commands or parameters have been introduced; however, due to the ABI supported host XPMs in this feature, certain maintenance functions and states will be supported for the ABI host XPMs. When an ABI peripheral (LTC, LTCI, LGC, LGCI, SMA2, or SMS) subtending a GWC is posted, the display looks just like it did for the same peripheral posted as a direct HOST peripheral (legacy).

Accessing directory: PM

Access to directory or MAP level and return to CI

The updated displays are accessed through the PM (peripherals) level of the maintenance (MTC) level of the DMS core command interface (MAPCI).

SN07 Enhancements

Features A00003486 'Gateway location information' and A00002137 'DS512 Link Mtc Robustness - CM' will be adding additional information and commands to the PM level for External XPMs. This will provide more information on the nodes on the C-Side of the XPM. The SMS will get full advantage of those changes and there is no SMS specific information being added. See the documentation for those two features for more details.

Command: TRNSL C

Command type: Listed MENU

Command target: All

But will only appear for Succession ABI peripherals.

Command availability: RES

Command description

TRNSL C (translate c-side links) is not a new command, however when an LTC, LTCI, LGC, LGCI, SMA2, or SMS subtends a GWC (gateway controller), the TRNSL C will display the c-side links of the peripheral as connecting to a GWC.

Each c-side link will simply reflect the name of the gateway controller to which it subtends. Link 0, 1, 4 and 5 (the message links) reflect the actual status of the c-side links. Currently, the speech links have the following string hardcoded as their status "***;Cap S;Status:OK".

It is important to note that TRNSL C indicates only which GWC supertends the ABI peripheral, it does not display the MG9K or ABI card that is in use for the messaging path.

Command syntax

TRNSL C command parameters and variables

Command	Parameters and variables
TRNSL C	unchanged
Parameters and variables	unchanged

Qualifications and warnings

The TRNSL C command will provide the user with the following additional information when a GWC is involved:

“Please refer to the DS512 Interface EM for all link maintenance commands.”

It should be noted that maintenance actions on the c-side links (e.g. bsy link 0, rts link 1, etc.) can only be performed on the c-side message links for ABI peripherals.

Usage example for “MAPCI;MTC;PM; POST <XPM>;TRNSL C “command

```

CM      MS      IOD      Net      PM      CCS      Lns      Trks      Ext      APPL
CM Flt  .      NO AMA  Istb    1LIU7  2    RS      .      52CC.  .      .
M      *C*
SMS
0 Quit      PM      SysB      ManB      OffL      CBSy      ISTb      InSv
2 Post_     SMS      14      1      11      3      35
3 ListSet   0      0      0      0      1
4
5 TrnsL_    SMS      0 ISTb  Links_OOS: CSide 0 , PSide 0
6 Tst_      Unit0:  Act  ISTb
7 Bsy_      Unit1:  Inact ISTb
8 RTS_      PM:
9 OffL      Link 0: GWC 3      20;Cap MS;Status:OK      ;MsgCond:OPN,
10 LoadPM_ Restrict
11 Disp_    Link 1: GWC 3      21;Cap MS;Status:OK      ;MsgCond:OPN,
12 Next     Restrict
13 SwAct    Link 2: GWC 3      **:Cap S;Status:OK
14 QueryPM  Link 3: GWC 3      **:Cap S;Status:OK
15          Link 4: GWC 3      22;Cap MS;Status:OK      ;MsgCond:OPN,
16          Unrestrict
17 Perform  Link 5: GWC 3      23;Cap MS;Status:OK      ;MsgCond:OPN,
18          Link 6: GWC 3      **:Cap S;Status:OK
          Link 7: GWC 3      **:Cap S;Status:OK
TEAM1
Time 13:56 >

```

Message link status is reflected accurately

Speech link state is hardcoded.

Shows which GWC is used to control packet c-side connections for this ABI peripheral.

PM can be SMA2, LTC, LTCL, LGC, LGCI, or SMS.

Security

Not Required.

Configuration Walkthrough

Not Required.

Product = CS 2000**A00003490 -- Network Change Upgrade Tools (UA-AAL1)*****Functional Description***

This feature provides the ability:

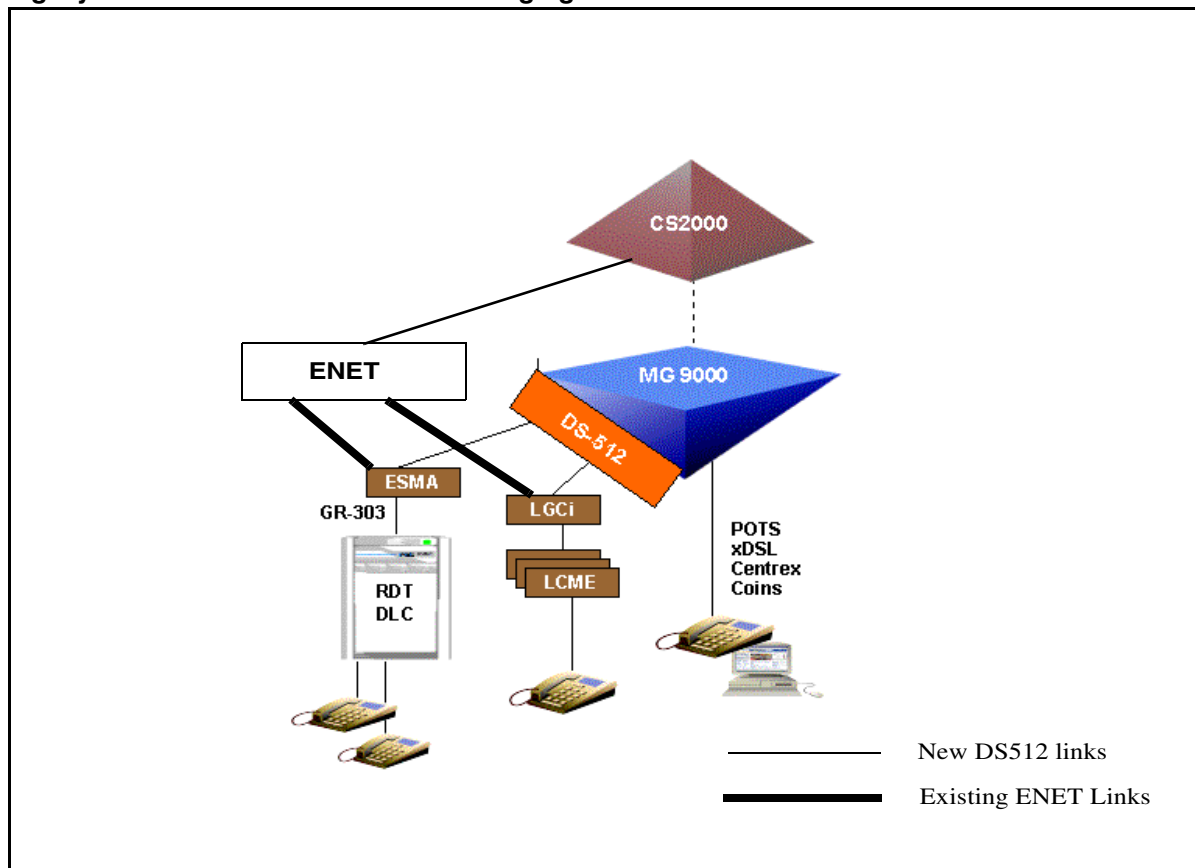
- to change the network fabric for a TDM based XPM from Enet/Jnet to DS512 interface
- restrict the use of this change only during the XPM rehome procedures

Currently, legacy XPMs are connected to either a ENET or JNET network. Rehome of the legacy XPMs to the ABI configuration is accomplished by connecting the XPM to the DS512 interface in a MG9000 gateway. The DS512 serves as the interface between the TDM links to the XPM and the OC3 interface coming out of the MG9000 and into the ATM network. Please refer to “ Legacy XPM Rehomed to an Access Bridging Interface” on page 937.

The ability to perform a network interface change has the following benefits:

- simplifies the ABI XPM rehome methods and procedures
- in some instances, this may be the only way to change to an ABI network interface. Offices with a fully configured network cannot datafill a “fake” XPM because there is no free network links

Legacy XPM Rehomed to an Access Bridging Interface



The ability to change the network interface via the table control change operation is only available during the XPM rehome activity. To control the

activation of the table control change operation, the installation personnel utilizes the TASTOOLCI and ABIREHOME CI tools. Please refer to “Command interface changes” on page 943 for detailed command information. This table control operation is merely one piece of the overall installation and rehome process. For the complete installation process, please refer to Installation Method 72-1682 XPM to MG9000 DS-512 Rehome. For a complete list of restrictions associated with the table control network change functionality, please refer to “Limitations and restrictions” on page 939.

Optionally, a secondary capability to rehome an ABI XPM to a different GWC, or to supply a different IP address, will also be provided. This provides the Central Office with the ability to manage GWC performance (load leveling) by re-distributing resources to other GWCs without having to perform a delete/add of associated configuration datafill. The ability to rehome an ABI XPM to a different GWC is accomplished by performing a tuple change operation in table LTCINV. For a complete list of restrictions and associated with the ABI XPM rehome operation, please refer to “Limitations and restrictions” on page 939.

In order to provide these new functionalities described above, the customer will see changes in the following areas:

- operation of table LTCINV
- operation of TASTOOLCI including new ABIREHOME CI tool

Table LTCINV Impacts

Table LTCINV changes consist of modifications to the original SN05 ABI XPM tuple change operation restrictions. No other changes have been made to the table. For a complete list of the current ABI XPM tuple operation restrictions, please refer to “Limitations and restrictions” on page 939.

TASTOOLCI Impacts and new ABIREHOME CI Tool

Two new commands have been added to the TASTOOLCI command, which is password protected. Both of these commands were added in the SN06 release.

- SET_ABI_REHOME_STATUS
- QUERY_ABI_REHOME_STATUS

In addition, a new CI directory has been created to contain commands specific to the rehoming process. This directory will contain only the following commands in SN06:

- DISP_LINK_CHANNEL_MAP/DLC
- DISP_LINK_INFO/DLI
- SET_LINK_CHANNELS_IDLE/SLC

In SN06.2/SN07 the below mentioned commands have been added to the ABIREHOME tool.

- Rehome query commands
 - QUERY_IMPACTED_NODES/QIN: This command is used to display all the nodes currently marked as impacted.
 - FIND_AFFECTED_NODES/FAN: This command is used to display all the nodes impacted by rehome of given XPM node.
 - SHOW_NODE_STATUS / SNS: This command displays the current status, through ABI rehome, of a specified node, or all rehoming nodes.
- INVASIVE rehome commands
 - SET_AFFECTED_NODES/SAN: This command is used to set the protected rehome bit for each node impacted by rehoming the given XPM.
 - CLEAR_AFFECTED_NODES/CAN: This command is used to clear the protected rehome bit for each node impacted by rehoming the given XPM.
 - MARK_DS512_LINK_VERIFIED/VER512: This command sets the DS512 Link Verified bit for the specified node.
 - ADJUST_FRAME_SYNC/AFS - This command is used to adjust the frame sync on the ABI cards to sync to the inactive XPM unit.
 - SEND_GWC_STATIC_DATA/GWCSD - This command is used to send a limited static data update request to GWCs with new or deleted ABI XPMs.
 - ABORT_GWC_STATIC_DATA/ABORT_GWCSD - This command is used to send a limited static data update request to UNDO the recent GWC static data updates.

Hardware Requirements or Dependencies

While this feature does allow for the change to the network interface for an existing XPM, it does not require that the hardware be present in order to perform this operation.

Software Requirements or Dependencies

This feature does require the Core load to be a Succession load. The Succession load contains the MSH DRU. The MSH DRU is where key software resides for this feature functionality.

Limitations and restrictions

It was thought to be beneficial to list the ABI XPM provisioning limitations and restrictions which existed before and after this feature.

Prior to SN06, the following limitations and restrictions existed for provisioning ABI XPMs:

- Each LTCINV tuple is restricted to only ENET-based CSLNKTAB datafill or the EXTDS512 optional attribute, but not both. There can be multiple tuples of the type, but each tuple is either ENET-based CSLNKTAB or has the EXTDS512 attribute.
- The DS512 interface provisioning only supports XPM types of LGC and SMA2. Attempting to datafill other XPM types will result in the tuple failing verification.
- The ability to change the derived CSLINKs are not allowed.
- The ability to change the Host GWC of the external XPM is not allowed.
- The ability to change the device from being ENET to External DS512-based or vise-versa is not allowed.
- Performing the TRNSL commands which use the C-side links: “TRNSL C”, “TRNSL MSG C”, and “TRNSL EMSG C” redirect the craftsperson to the MG9000 Element Manager. The MG9000 Element Manager is where the C-side links for these ABI XPMs are maintained. These C-side links of these ABI XPMs are not maintained in the Core.

With the SN07 release or the patch for this feature present in SN06, this feature and associated feature A00001847 now brings the following limitations and restrictions to provisioning of ABI XPMs:

- This feature does not provide in service rehome of the XPM to the ABI networks. This table control change capability is but a step in the overall rehome installation method.
- This feature is not supported over an ONP and therefore should not be performed while an ONP is in progress. Please check installation methods for details.
- Each LTCINV tuple is restricted to only ENET-based CSLNKTAB datafill or the EXTDS512 optional attribute, but not both. There can be multiple tuples of the type, but each tuple is either ENET-based CSLNKTAB or has the EXTDS512 attribute.
- The following peripherals will be allowed to have the EXTDS512 optional attribute assign to them:
 - LGC/LGCI
 - LTC/LTCI
 - SMS
 - SMA2
- The ability to change (add/delete/change) the derived CSLINKs are not allowed

- The ability to change the Host GWC of the ABI XPM is allowed to be changed under the following conditions:
 - the ABI XPM being rehomed must be ManBsy/Offline
- The ability to change the XPM from being ENET to External DS512-based or vise-versa is allowed under the following conditions:
 - the network change is performed on the Inactive side of the XA-Core
 - the network change can only be performed if the ABI XPM rehome is in progress
 - The Cside Links on the XPM under going the network change must be in a Offline, Unequipped or in a ManBsy state
 - The XPM under going the network change must be in a Offline or Node ManBsy state
- Performing the TRNSL commands which use the C-side links: “TRNSL C”, “TRNSL MSG C”, and “TRNSL EMSG C” will display the correct translate information as well as a message directing the craftsperson to the MG9000 Element Manager. The MG9000 Element Manager is where the C-side links for these ABI XPMs are maintained. These C-side links of these ABI XPMs are not maintained in the Core.

Interactions

This feature introduces the capability to change network interfaces for existing XPMs via a table control change operation during the rehome process. It is designed to have no impact on existing XPMs that will not be rehomed.

Applicable customer facing sections

Fault Management

Logs	<u> X </u>
Alarms	<u> n/a </u>

Configuration

Data Schema	<u> X </u>
User Interface	<u> X </u>
Element Management	<u> n/a </u>
Security	<u> n/a </u>
Service Order	<u> n/a </u>
Office Parameters	<u> n/a </u>

Accounting (includes AMA billing)	<u> n/a </u>

Performance (includes operational measurements)	<u> n/a </u>

Glossary

Term	Description
Rehome	Moving of XPMs from one network to another network. More specifically from the ENET to the ABI or vice-versa Also, Moving of subtending devices from one XPM to another XPM. In the case of an ABI configuration, the XPM is considered a subtending device to the GWC.
ABI XPM	An XPM which is provisioned in table LTCINV with the optional attribute EXTDS512
network change	When the network interface type of an XPM is changed via the Table Control Change operation in Table LTCINV.

Configuration for A00003490

Hardware and Software Requirements

The purpose of this feature is to rehome existing ENET/JNET XPMs to the ABI DS-512 interface off MG 9000.

Therefore the following hardware is required:

- An available LGCI, SMA2, LGC, LTC, LTCI, SMS
- GWCs that will be hosting XPMs need to be configured and datafilled in table SERVINV
- DS-512 Interface cards should be installed in the appropriate MG 9000 Gateways and their base IP address known.

Because this feature is a part of the larger installation method to rehome XPMs to the ABI configuration, please refer to the Installation Method 72-1682 “XPM to MG 9000 DS-512 Rehome” for a complete list of required hardware to perform the rehome.

Software requirements:

- SN06 Succession Core load with this feature patched back

-OR-

- SN07 or later Succession Core load

Initial Configuration

This feature, when enabled, provides the ability to rehome an existing ENET/JNET XPM by changing its data in table LTCINV. The ability to

rehome XPMs involves turning on the rehome capability via the TASTOOLCI tool and splitting the Core. This is but one step of an overall process to rehome the ENET/JNET based XPMs. For the complete process, please refer to Installation Method 72-1682 “XPM to MG 9000 DS-512 Rehome.”

Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable.

Upgrade Impact

No Impact.

Data schema (DS) (CM, MIBS, RDB)

This feature does not introduce any new tables, fields, or field values in any table. It permits, when enabled, the ability to rehome an existing ENET/JNET XPM by *changing* its data in table LTCINV (rather than having to delete and re-add the tuple).

In order to provide this *change* capability, some limitations and restrictions have been modified. Please refer to “Limitations and restrictions” on page 939 in the Functional description section for a complete list of limitations and restrictions.

Service Orders (SO) (CM & SESM)

Not Applicable.

Software optionality control (SOC)

Not Applicable.

Element Management

Not Applicable.

Command interface changes

Directory: TASTOOLCI (changed)

Two new commands added:

- SET_ABI_REHOME_STATUS
- QUERY_ABI_REHOME_STATUS

Directory description

This CI command directory is password protected and exists for use by TAS (Technical Assistance) personnel in various upgrade scenarios which involve splitting the switch and using the SWACT functionality to enable behavior.

Accessing directory: TASTOOLCI**Access to directory or MAP level and return to CI**

To access TASTOOLCI from the CI environment, enter “tastoolci” from the command interface.

To return to the CI environment, enter “quit”.

Directory: ABIREHOME (new)

Commands:

- DISP_LINK_CHANNEL_MAP/DLC
- DISP_LINK_INFO/DLI
- SET_LINK_CHANNELS_IDLE/SLC
- QUERY_ABI_REHOME_STATUS/QRS
- QUERY_IMPACTED_NODES/QIN
- FIND_AFFECTED_NODES/FAN
- DISP_IOUI_ROUTE_DATA/DRD
- SET_AFFECTED_NODES/SAN
- CLEAR_AFFECTED_NODES/CAN
- ADJUST_FRAME_SYNC/AFS
- SEND_GWC_STATIC_DATA/ GWCSO
- ABORT_GWC_STATIC_DATA/ ABORT_GWCSO

Directory description

This CI command directory is used for ABI rehome specific commands once the functionality has been enabled via the TASTOOLCI SET_ABI_REHOME_STATUS ON command has been issued.

Accessing directory: ABIREHOME**Access to directory or MAP level and return to CI**

To access ABIREHOME from the CI environment, enter “abirehome” from the command interface.

To return to the CI environment, enter “quit”.

Command: TASTOOLCI: SET_ABI_REHOME_STATUS**Command type: NON-MENU****Command target: All****Command availability: RES****Command description**

This command is used as a part of Installation Method 72-1682 “XPM to MG 9000 DS-512 Rehome” to enable the ability to rehome an XPM from ENET/JNET C-side links to an ABI DS-512 off of an MG 9000.

This command allows TAS personnel the ability to control the rehome status in an office. It affects both an overall control boolean and the initialization of per node rehome status data. In addition, this command enables the ability to position on the XPM's tuple in table LTCINV and execute a CHA, as opposed to deleting and re-adding the tuple.

Command syntax**<CommandName> command parameters and variables**

Command	Parameters and variables
SET_ABI_REHOME_STATUS	<STATUS> {ON, OFF, SUSPEND, RESUME}
Parameters and variables	Description
ON	Sets the control bool to TRUE and initializes all node rehome data to default values.
OFF	Sets the control bool to FALSE and initializes all node rehome data to default values.
SUSPEND	Sets the control bool to FALSE, leaving the per node rehome data as is.
RESUME	Sets the control bool to TRUE, leaving the per node rehome data as is.

Qualifications and warnings

In all cases, a warning message will be output to user that this command enables highly dangerous functionality and should be used by experienced personnel only, giving the user the option to quit.

In all cases, the current status of the rehome (ON, OFF, SUSPENDED) will be displayed prior to any parameter specific messages.

Responses

SET_ABI_REHOME_STATUS responses

MAP outputs with associated meanings and actions

SET_ABI_REHOME_STATUS
This command is intended for use during the rehomeing of XPMs to an ABI interface on an MG 9000. It enables highly dangerous functionality that should only be executed as directed by the installation method. This command should be used by qualified and experienced personnel ONLY in conjunction with IM. Do you wish to proceed? Meaning: Output regardless of status entered. This response warns the user that this command could result in an outage and that it should be executed by experienced personnel only. System or user actions: If the user is not qualified to proceed, he should enter NO and the command will exit at this point.
Current ABI Rehome State is: {ON, OFF, SUSPENDED} Meaning: Output regardless of status entered. If ON, the rehome process has been enabled. If OFF, the rehome process has been disabled, and all node rehome data is currently at default values. If SUSPENDED, a rehome was begun, and interrupted by the user. In this state, the control bool is FALSE, but there could be node rehome data that is not at default values. System or user actions: None. This is for informational purposes.
ABI Rehome state is already ON. Rehome data not impacted. Meaning: The user is attempting to turn ON the rehome status when it is already ON. System or user actions: None. This is for informational purposes.
Continuing with this command will cause all existing node rehome data to be lost. Consider using RESUME instead. Do you wish to continue? continue=no 'SET_REHOME_STATUS command aborted by user.' Meaning: The user is attempting to turn ON the rehome status when it is currently SUSPENDED. If there is an per node rehome data, it will be re initialized to default values. System or user actions: The user has an opportunity to abort the command, at which point they will receive the continue=no response.
Command Successful. ABI Rehome has been turned ON. Meaning: The ABI Rehome status has been turned ON and all per node rehome data has been initialized to default values. System or user actions: None.
Failed to enable ABI Rehome. Please check for swerrs. Meaning: The command to enable the ABI rehome has failed for some reason. System or user actions: Use the QUERY_ABI_REHOME_STATUS to determine current status and if any part is ON, use the SET_ABI_REHOME_STATUS to turn OFF.

MAP outputs with associated meanings and actions

SET_ABI_REHOME_STATUS
ABI Rehome state is already OFF. Rehome data not impacted. Meaning: The user is attempting to turn OFF the ABI rehome status when it is already OFF. System or user actions: None.
Continuing with this command will cause all existing node rehome data to be lost. Do you wish to continue? continue=no 'SET_REHOME_STATUS command aborted by user. Meaning: The user is attempting to turn OFF the ABI tool when it is currently ON or SUSPENDED. This could cause a loss of the per node rehome data. System or user actions: Opportunity to abort, in which case user gets the continue = no output.
ABI Rehome has been turned OFF. Meaning: The control bool has been turned OFF, and per node rehome data initialized to default values. System or user actions: None - informational only.
Failed to disable the ABI Rehome. Please check for swerrs. Meaning: The attempt to turn OFF the ABI rehome state has failed. System or user actions: Should not occur. Indicates a problem.
Cannot SUSPEND - ABI Rehome is not ON. Meaning: The user is attempting to SUSPEND the rehome status when it is not ON. System or user actions: None - informational only.
ABI Rehome has been SUSPENDED. Meaning: The control bool has been turned OFF, and per node rehome data was left intact. System or user actions: None - informational only.
Failed to suspend ABI Rehome. Please check for swerrs. Meaning: The attempt to suspend the ABI rehome state has failed. System or user actions: Should not occur. Indicates a problem.
Cannot RESUME - ABI Rehome is not SUSPENDED. Meaning: RESUME only makes sense when the rehome state was suspended. No data has been impacted. System or user actions: None - informational only.

MAP outputs with associated meanings and actions

SET_ABI_REHOME_STATUS
ABI Rehome has been RESUMED. Meaning: The control bool has been turned ON, and per node rehome data was left intact. System or user actions: None - informational only.
Failed to resume ABI Rehome. Please check for swerrs. Meaning: The attempt to resume the ABI rehome state has failed. System or user actions: Should not occur. Indicates a problem.

Example**Usage examples for SET_ABI_REHOME_STATUS command**

Description of task:	
SET_ABI_REHOME_STATUS ON	This command is intended for use during the rehomeing of XPMs to an ABI interface on an MG 9000. It enables highly dangerous functionality that should only be executed as directed by the installation method. This command should be used by qualified and experienced personnel ONLY in conjunction with IM. Do you wish to proceed? Current ABI Rehome State is: SUSPENDED Continuing with this command will cause all existing node rehome data to be lost. Consider using RESUME instead. Do you wish to continue? >N SET_REHOME_STATUS command aborted by user.
SET_ABI_REHOME_STATUS OFF	This command is intended for use during the rehomeing of XPMs to an ABI interface on an MG 9000. It enables highly dangerous functionality that should only be executed as directed by the installation method. This command should be used by qualified and experienced personnel ONLY in conjunction with IM. Do you wish to proceed? Current ABI Rehome State is: ON Continuing with this command will cause all existing node rehome data to be lost. Do you wish to continue? Y 'ABI Rehome has been turned OFF.

Usage examples for SET_ABI_REHOME_STATUS command

SET_ABI_REHOME_STATUS SUSPEND	This command is intended for use during the rehomeing of XPMs to an ABI interface on an MG 9000. It enables highly dangerous functionality that should only be executed as directed by the installation method. This command should be used by qualified and experienced personnel ONLY in conjunction with IM. Do you wish to proceed? Current ABI Rehome State is: ON ABI Rehome has been SUSPENDED.
SET_ABI_REHOME_STATUS RESUME	This command is intended for use during the rehomeing of XPMs to an ABI interface on an MG 9000. It enables highly dangerous functionality that should only be executed as directed by the installation method. This command should be used by qualified and experienced personnel ONLY in conjunction with IM. Do you wish to proceed? Current ABI Rehome State is: SUSPENDED ABI migration has been RESUMED.

Command: TASTOOLCI: QUERY_ABI_REHOME_STATUS**Command type: NON-MENU****Command target: All****Command availability: RES****Command description**

This command is used to display the current state of the ABI Rehome.

Command syntax

<CommandName> command parameters and variables

Command	Parameters and variables
QUERY_ABI_REHOME_STATUS	none

Qualifications and warnings

None.

Responses

QUERY_ABI_REHOME_STATUS responses

MAP outputs with associated meanings and actions

QUERY_ABI_REHOME_STATUS	
Current ABI Rehome State is: {ON, OFF, SUSPENDED}	Meaning: Output regardless of status entered. If ON, the rehome process has been enabled. If OFF, the rehome process has been disabled, and all node rehome data is currently at default values. If SUSPENDED, a rehome was begun, and interrupted by the user. In this state, the control bool is FALSE, but there could be node rehome data that is not at default values. System or user actions: None. This is for informational purposes.
ABI XPM Rehome Control Enabled: {TRUE, FALSE}	Meaning: Displays the state of the control bool that enables the table control and ABIREHOME CI tool functionality. System or user actions: None. This is for informational purposes.
There are nodes which have been marked as rehomed. Please use the ABIREHOME CI tool for additional information.	Meaning: There are nodes which have been marked as impacted, using SET_ABI_REHOME_STATE with ON or OFF will clear the per node rehome data. System or user actions: None. This is for informational purposes.
There are no nodes marked as impacted.	Meaning: There are no nodes which have rehome data associated with them. The rehome state can be turned ON or OFF without impacting any existing data. System or user actions: None. This is for informational purposes.

Example

Usage examples for QUERY_ABI_REHOME_STATUS command

Description of task:	
QUERY_ABI_REHOME_STATUS	ABI XPM Rehome Control Enabled: TRUE Current ABI Rehome State is: ON There are no nodes marked as impacted.

Command: ABIREHOME: DISP_LINK_CHANNEL_MAP**Command type: NON-MENU****Command target: All****Command availability: RES****Command description**

This command is used as a part of Installation Method 72-1682 “XPM to MG 9000 DS-512 Rehome” to enable the ability to rehome an XPM from ENET/JNET C-side links to an ABI DS-512 off of an MG 9000.

Command syntax**<CommandName> command parameters and variables**

Command	Parameters and variables
DISP_LINK_CHANNEL_MAP or DLC	node Node number of the XPM. Node number can be found by performing QueryPM while the XPM is POSTed at the map.
Parameters and variables	Description
node	<XPM_NODE> {0 to 4095}

Qualifications and warnings

None.

Responses

DISP_LINK_CHANNEL_MAP responses

MAP outputs with associated meanings and actions

DISP_LINK_CHANNEL_MAP			
ABIREHOME:			
>dlc 68			
Node Number: 68			
Number of cside links: 16			
Link Information:			
LN: Link Number LT: Link Type FC: Free Channel			
LN	LT	FC	Link Channel Map (0 to 31)
0=busy, 1=idle			

0	Duplex	Y	011111111111111011111111111111
1	Duplex	Y	011111111111111110111111111111
2	Duplex	Y	011111111111111110111111111111
3	Duplex	Y	011111111111111110111111111111
4	Duplex	Y	011111111111111110111111111111
5	Duplex	Y	011111111111111110111111111111
6	Duplex	Y	011111111111111110111111111111
7	Duplex	Y	011111111111111110111111111111
8	Duplex	Y	011111111111111110111111111111
9	Duplex	Y	011111111111111110111111111111
10	Duplex	Y	011111111111111110111111111111
11	Duplex	Y	011111111111111110111111111111
12	Duplex	Y	011111111111111110111111111111
13	Duplex	Y	011111111111111110111111111111
14	Duplex	Y	011111111111111110111111111111
15	Duplex	Y	000001111111111110111111111111
Meaning: Displays the link_chnl_map for the XPM. 0=busy, 1=idle. Messaging links show busy.			
System or user actions: None. Information purposes only.			

Example

Usage examples for DISP_LINK_CHANNEL_MAP command

Description of task:	
dlc 68	<pre> Node Number: 68 Number of cside links: 16 Link Information: LN: Link Number LT: Link Type FC: Free Channel LN LT FC Link Channel Map (0 to 31) 0=busy, 1=idle ----- 0 Duplex Y 0111111111111110111111111111111 1 Duplex Y 0111111111111110111111111111111 2 Duplex Y 0111111111111110111111111111111 3 Duplex Y 0111111111111110111111111111111 4 Duplex Y 0111111111111110111111111111111 5 Duplex Y 0111111111111110111111111111111 6 Duplex Y 0111111111111110111111111111111 7 Duplex Y 0111111111111110111111111111111 8 Duplex Y 0111111111111110111111111111111 9 Duplex Y 0111111111111110111111111111111 10 Duplex Y 0111111111111110111111111111111 11 Duplex Y 0111111111111110111111111111111 12 Duplex Y 0111111111111110111111111111111 13 Duplex Y 0111111111111110111111111111111 14 Duplex Y 0111111111111110111111111111111 15 Duplex Y 0000011111111110111111111111111 </pre>

Command: ABIREHOME: DISP_LINK_INFO

Command type: NON-MENU

Command target: All

Command availability: RES

Command description

This command is used as a part of Installation Method 72-1682 “XPM to MG 9000 DS-512 Rehome” to enable the ability to rehome an XPM from ENET/JNET C-side links to an ABI DS-512 off of an MG 9000.

Command syntax

DISP_LINK_INFO command parameters and variables

Command	Parameters and variables
DISP_LINK_INFO or DLI	node Node number of the XPM. Node number can be found by performing QueryPM while the XPM is POSTed at the map.
Parameters and variables	Description
node	<NODE_NUMBER> {0 to 4095}

Qualifications and warnings

None.

Responses

DISP_LINK_INFO responses

MAP outputs with associated meanings and actions

DISP_LINK_INFO

```
node 68: LTC_NODE SMA2 1, node status: status=sysb, cs=FALSE
cside links:
  0: node= 41, cap=MS-, port= 0; host=ok      port 0: ls=ok      cs=N ps=Y
  1: node= 41, cap=MS-, port= 1; host=ok      port 1: ls=ok      cs=N ps=Y
  2: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
  3: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
  4: node= 41, cap=MS-, port= 2; host=ok      port 2: ls=ok      cs=N ps=Y
  5: node= 41, cap=MS-, port= 3; host=ok      port 3: ls=ok      cs=N ps=Y
  6: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
  7: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
  8: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
  9: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 10: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 11: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 12: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 13: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 14: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 15: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 16: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 17: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 18: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 19: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 20: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 21: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 22: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 23: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 24: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 25: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 26: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 27: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 28: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 29: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 30: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
 31: node= 41, cap=-S-, port=4095; host=ok     port 4095: ls=ok   cs=N ps=N
pside links:
  0: node= 77, cap=MS-, port= 0, ls=offl,clos cs=Y ps=Y; psn: manb
  1: node= 77, cap=MS-, port= 1, ls=offl,clos cs=Y ps=Y; psn: manb
  2: node= 77, cap=-S-, port= 2, ls=offl,clos cs=Y ps=Y; psn: manb
  3: node= 77, cap=-S-, port= 3, ls=offl,clos cs=Y ps=Y; psn: manb
```

Meaning: Displays information about both the cside and pside links for an XPM.

System or user actions: None. Informational only.

Example

Usage examples for DISP_LINK_INFO

Description of task:	
DISP_LINK_INFO 68	<pre> node 68: LTC_NODE SMA2 1, node status: status=sysb, cs=FALSE cside links: 0: node= 41, cap=MS-, port= 0; host=ok port 0: ls=ok cs=N ps=Y 1: node= 41, cap=MS-, port= 1; host=ok port 1: ls=ok cs=N ps=Y 2: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 3: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 4: node= 41, cap=MS-, port= 2; host=ok port 2: ls=ok cs=N ps=Y 5: node= 41, cap=MS-, port= 3; host=ok port 3: ls=ok cs=N ps=Y 6: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 7: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 8: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 9: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 10: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 11: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 12: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 13: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 14: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 15: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 16: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 17: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 18: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 19: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 20: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 21: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 22: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 23: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 24: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 25: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 26: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 27: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 28: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 29: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 30: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N 31: node= 41, cap=-S-, port=4095; host=ok port 4095: ls=ok cs=N ps=N pside links: 0: node= 77, cap=MS-, port= 0, ls=offl,clos cs=Y ps=Y; psn: manb 1: node= 77, cap=MS-, port= 1, ls=offl,clos cs=Y ps=Y; psn: manb 2: node= 77, cap=-S-, port= 2, ls=offl,clos cs=Y ps=Y; psn: manb 3: node= 77, cap=-S-, port= 3, ls=offl,clos cs=Y ps=Y; psn: manb </pre>

Command: ABIREHOME:SET_LINK_CHANNEL_MAP

Command type: NON-MENU

Command target: All

Command availability: RES

Command description

This command is used as a part of Installation Method 72-1682 “XPM to MG 9000 DS-512 Rehome” to enable the ability to rehome an XPM from ENET/JNET C-side links to an ABI DS-512 off of an MG 9000.

This command allows the user to reset the link_chnl_map for an XPM. This command is invasive and dangerous, and should be used by qualified personnel only following the instructions in IM 72-1682.

Command syntax

SET_LINK_CHANNEL_MAP command parameters and variables

Command	Parameters and variables
SET_LINK_CHANNEL_MAP or SLC	node Node number of the XPM. Node number can be found by performing QueryPM while the XPM is POSTed at the map.
Parameters and variables	Description
node	<XPM_NODE> {0 to 4095}

Qualifications and warnings

None.

Responses

SET_LINK_CHANNEL_MAP responses

MAP outputs with associated meanings and actions

SET_LINK_CHANNEL_MAP
This command must be enabled by TAS. Please refer to IM 72-1682. Meaning: The control bool to enable the command has not been turned on. System or user actions: Go into TASTOOLCI and use command SET_REHOME_STATUS ON to turn on the tool. Password required.
Node number is not a supported XPM. Meaning: The command is ended because the node number entered is not a node number of a valid XPM that can exist off of an ABI interface. The node number can be either ABI connected or ENET/JNET connected, but must be ABLE to be ABI connected. System or user actions: Get the right node number and reenter the command. The PMIST NODENO command can be used to get the correct node number.
Current IO format is: External Meaning: The node is currently provisioned as a packet node off of an ABI interface. System or user actions: None. Informational purposes.
Current IO format is: Internal Meaning: The node is currently provisioned as a tdm node off of an ENET/JNET. System or user actions: None. Informational purposes.

MAP outputs with associated meanings and actions

SET_LINK_CHANNEL_MAP
This command can be service impacting. Do you wish to continue? If continue=no: SLC command aborted by user. Meaning: Resetting the link channel map is dangerous if used improperly. This is the last chance to change your mind. System or user actions: Enter desire to continue.
Links/Channels have been reset for node <node number>. Meaning: The command was successful. System or user actions: None, but user can choose to use DLC to verify results.
Trouble resetting links/channels on node <node number>. Meaning: Something was wrong and the link channel map could not be reset. System or user actions: Look for swerrs and report problem. Use DLC to display current values.

Example**Usage examples for SET_LINK_CHANNEL_MAP command**

Description of task:	
SET_LINK_CHANNEL_MAP 68	Current IO format is: External This command can be service impacting. Do you wish to continue? Yes Links/Channels have been reset for node 68.

Command: ABIREHOME: QUERY_ABI_REHOME_STATUS**Command type: NON-MENU****Command target: All****Command availability: RES****Command description**

This command is used to display the current state of the ABI Rehome. It is a clone of the TASTOOLCI command of the same name, and placed here for convenience.

Command syntax

<CommandName> command parameters and variables

Command	Parameters and variables
QUERY_ABI_REHOME_STATUS or QRS	n/a
Parameters and variables	Description
n/a	

Qualifications and warnings

None.

Responses

QUERY_ABI_REHOME_STATUS responses

MAP outputs with associated meanings and actions

QUERY_ABI_REHOME_STATUS
Displays the status of the ABI Migration control structures. Meaning: Help associated with command. System or user actions: Informational purposes only.
Current ABI Rehome State is: {ON, OFF, SUSPENDED} Meaning: Output regardless of status entered. If ON, the rehome process has been enabled. If OFF, the rehome process has been disabled, and all node rehome data is currently at default values. If SUSPENDED, a rehome was begun, and interrupted by the user. In this state, the control bool is FALSE, but there could be node rehome data that is not at default values. System or user actions: None. This is for informational purposes.
ABI XPM Rehome Control Enabled: {TRUE, FALSE} Meaning: Displays the state of the control bool that enables the table control and ABIREHOME CI tool functionality. System or user actions: None. This is for informational purposes.

MAP outputs with associated meanings and actions

QUERY_ABI_REHOME_STATUS
There are nodes which have been marked as rehomed. Please use the ABIREHOME CI tool for additional information. Meaning: There are nodes which have been marked as impacted, using SET_ABI_REHOME_STATE with ON or OFF will clear the per node rehome data. System or user actions: None. This is for informational purposes.
There are no nodes marked as impacted. Meaning: There are no nodes which have rehome data associated with them. The rehome state can be turned ON or OFF without impacting any existing data. System or user actions: None. This is for informational purposes.

Example**Usage examples for QUERY_ABI_REHOME_STATUS command**

Description of task:	
QUERY_ABI_REHOME_STATUS	ABI XPM Rehome Control Enabled: TRUE Current ABI Rehome State is: ON There are no nodes marked as impacted.

Command: ABIREHOME: QUERY_IMPACTED_NODES/QIN**Command type: NON-MENU****Command target: All****Command availability: RES****Command description**

This command is used as a part of Installation Method 72-1682 “XPM to MG 9000 DS-512 Rehome” to enable the ability to rehome an XPM from ENET/JNET C-side links to an ABI DS-512 off of an MG 9000.

Query impacted nodes will display all nodes that have been marked as impacted by the rehome.

Command syntax

QUERY_IMPACTED_NODES command parameters and variables

Command	Parameters and variables
QUERY_IMPACTED_NODES or QIN	n/a
Parameters and variables	Description
n/a	

Qualifications and warnings

None.

Responses

QUERY_IMPACTED_NODES responses

MAP outputs with associated meanings and actions

QUERY_IMPACTED_NODES
Displays all nodes currently marked as impacted in the rehome node data. Meaning: Help associated with command. System or user actions: Informational purposes only.
There are no nodes marked as impacted. Meaning: No nodes have been marked as impacted. System or user actions: Informational purposes only.
Impacted Nodes ----- 69: LTC_NODE SMA2 1 77: IDT_NODE IDT 5 Meaning: Node numbers 69 and 77 have been marked as impacted, and will be treated as rehomed during a NRS (norestartswact). System or user actions: Informational purposes.

Example

Usage examples for command **QUERY_IMPACTED_NODES**

Description of task:	
QIN	<pre> Impacted Nodes ----- 69: LTC_NODE SMA2 1 77: IDT_NODE IDT 5 </pre>

Command: **FIND_AFFECTED_NODES/FAN**

Command type: NON-MENU

Command target: All

Command availability: RES

Command description

This command is used as a part of Installation Method 72-1682 “XPM to MG 9000 DS-512 Rehome” to enable the ability to rehome an XPM from ENET/JNET C-side links to an ABI DS-512 off of an MG 9000.

Given a node number of an XPM, this command will show all nodes that would be impacted by a rehome of that XPM, by recursively searching its p-side links.

Command syntax

command parameters and variables

Command	Parameters and variables
FIND_AFFECTED_NODES or FAN	node Node number of the XPM. Node number can be found by performing QueryPM while the XPM is POSTed at the map.
Parameters and variables	Description
node	<XPM_NODE> {0 to 4095}

Qualifications and warnings

None.

Responses

FIND_AFFECTED_NODES/FAN responses

MAP outputs with associated meanings and actions

FIND_AFFECTED_NODES/FAN
FIND_AFFECTED_NODES: Displays the affected nodes for given XPM node ----- Syntax: FIND_AFFECTED_NODES node or FAN node Parameters: node Node number of the XPM Parms: <XPM_NODE> {0 TO 4095} Meaning: Help associated with command. System or user actions: Informational purposes only.
Node number is not a supported XPM. Meaning: The node number provided is not an XPM that can be supported from an ABI interface. The command will work whether the XPM is currently on an ENET/JNET interface or off of an ABI interface, but the XPM type must be able to be supported on either interface. System or user actions: Informational purposes.
Given node: ----- Node 69: LTC_NODE SMA2 1 Subtending nodes: ----- Node 77: IDT_NODE IDT 5 Meaning: For the given XPM number, display the node type and device information for each subtending nodes. Nodes which subtend a node are shown indented under that node. System or user actions: Informational purposes only.

Example

Usage examples for command FIND_AFFECTED_NODES/FAN

Description of task:	
FIND_AFFECTED_NODES or FAN	Given node: ----- Node 69: LTC_NODE SMA2 1 Subtending nodes: ----- Node 77: IDT_NODE IDT 5

Command: ABIREHOME: DISP_IOUI_ROUTE_DATA/DRD

Command type: NON-MENU

Command target: All

Command availability: RES

Command description

This command is used as a part of Installation Method 72-1682 “XPM to MG 9000 DS-512 Rehome” to enable the ability to rehome an XPM from ENET/JNET C-side links to an ABI DS-512 off of an MG 9000.

Displays the current IOUI routing data associated with the given node.

Command syntax

DISP_IOUI_ROUTE_DATA/DRD command parameters and variables

Command	Parameters and variables
DISP_IOUI_ROUTE_DATA or DRD	node Node number of the XPM. Node number can be found by performing QueryPM while the XPM is POSTed at the map.
Parameters and variables	Description
node	<NODE> {0 to 4095}

Qualifications and warnings

None.

Responses

DISP_IOUI_ROUTE_DATA/DRD responses

MAP outputs with associated meanings and actions

DISP_IOUI_ROUTE_DATA/DRD
DISP_IOUI_ROUTE_DATA: Displays the IOUI Route Data for given node ----- Syntax: DISP_IOUI_ROUTE_DATA node or DRD node Parameters: node Node number Parms: <NODE> {0 TO 4095} Meaning: Help associated with command. System or user actions: Informational purposes only.
Node undefined. Meaning: The given node is undefined. System or user actions: Try the command again with a valid node number.
<pre>Node 69: LTC_NODE SMA2 1 node_data3 info: msg_format: jts mts network: external is_ip_host: N IPaddress (of GWC): 47.142.106.64 dest_port: 4683 dms_msg_route: network: external is_ip_host: N IPaddress (of GWC): 47.142.106.64 dest_port: 4683</pre> Meaning: Shows the current values of the internal data structures relating to the IOUI routing data when the node provided is a packet node. This is the data that is impacted by the NRS procedures, and will be different on the active and inactive sides when a node has been rehomed. System or user actions: Informational and debug purposes only.

MAP outputs with associated meanings and actions**DISP_IOUI_ROUTE_DATA/DRD**

DISP_IOUI_ROUTE_DATA: Displays the IOUI Route Data for given node

Syntax: DISP_IOUI_ROUTE_DATA node

or

DRD node

Parameters: node Node number

Parms: <NODE> {0 TO 4095}

Meaning: Help associated with command.

System or user actions: Informational purposes only.

Node 47: LTC_NODE DTC 0

node_data3 info:

msg_format: jts mts

network: internal

dms_msg_route:

network: internal

Meaning: Shows the current values of the internal data structures relating to the IOUI routing data when the node provided is a TDM node. This is the data that is impacted by the NRS procedures, and will be different on the active and inactive sides when a node has been rehomed.

System or user actions: Informational and debug purposes only.

Example

Usage examples for command

Description of task:	
drd 69	<pre> Node 69: LTC_NODE SMA2 1 node_data3 info: msg_format: jts mts network: external is_ip_host: N IPaddress (of GWC): 47.142.106.64 dest_port: 4683 dms_msg_route: network: external is_ip_host: N IPaddress (of GWC): 47.142.106.64 dest_port: 4683 </pre>
drd 47	<pre> Node 47: LTC_NODE DTC 0 node_data3 info: msg_format: jts mts network: internal dms_msg_route: network: internal </pre>

Command: ABIREHOME: SET_AFFECTED_NODES/SAN

Command type: NON-MENU

Command target: All

Command availability: RES

Command description

This command is used as a part of Installation Method 72-1682 “XPM to MG 9000 DS-512 Rehome” to enable the ability to rehome an XPM from ENET/JNET C-side links to an ABI DS-512 off of an MG 9000.

Given the node number of the rehomed XPM, sets the impacted node table bits for the XPM and all of its subtending nodes, found by recursively searching its p-side links.

Command syntax

command parameters and variables

Command	Parameters and variables
SET_AFFECTED_NODES or SAN	node Node number of the XPM. Node number can be found by performing QueryPM while the XPM is POSTed at the map.
Parameters and variables	Description
node	<XPM_NODE> {0 to 4095}

Qualifications and warnings

None.

Responses

responses

MAP outputs with associated meanings and actions

SET_AFFECTED_NODES/SAN
SET_AFFECTED_NODES: Sets the rehome node bits for all nodes the are impacted by rehoming the given XPM, including its subtending nodes. Nodes must be marked as impacted on the INACTIVE processor element. Protected command for ABI Rehomes. ----- Syntax: SET_AFFECTED_NODES node Parameters: node Node number of XPM Parms: <XPM_NODE> {0 TO 4095} Meaning: Help info for command. System or user actions: Informational purposes only.
This command must be enabled by TAS via the TASTOOLCI SET_ABI_REHOME_STATUS command. Please refer to the installation method. Meaning: This is a protected command that must be enabled via TASTOOLCI. System or user actions: Use the TASTOOLCI SET_ABI_REHOME_STATUS ON (or RESUME) command to enable the ABI rehome functionality.
Node number is not a supported XPM. Meaning: The node number entered cannot be homed off of an ABI interface, and is therefore not a valid XPM for this command. System or user actions: Enter the correct node number of the rehomed XPM.
This command will SET the impacted node table bools for this XPM and all of its subtending nodes. Do you wish to continue? Meaning: Warning that using this command will set triggers that will impact the behavior of a NRS. System or user actions: Enter the correct response.
SAN command aborted by user. Meaning: Response indicating the command was aborted by the user and no action was taken. System or user actions: Informational purposes only.

MAP outputs with associated meanings and actions

SET_AFFECTED_NODES/SAN
SET_AFFECTED_NODES: Sets the rehome node bits for all nodes the are impacted by rehomeing the given XPM, including its subtending nodes. Nodes must be marked as impacted on the INACTIVE processor element. Protected command for ABI Rehomes. ----- Syntax: SET_AFFECTED_NODES node Parameters: node Node number of XPM Parms: <XPM_NODE> {0 TO 4095} Meaning: Help info for command. System or user actions: Informational purposes only.
Node 69: LTC_NODE SMA2 1 Set affected nodes PASSED. Use FIND_AFFECTED_NODES/FAN to see the nodes impacted. Meaning: Displays the XPM node provided, shows that the command passed, and suggests using the FAN command to see what nodes were impacted. System or user actions:
Set affected nodes FAILED. Check for swerrs and traps. Meaning: Indicates a problem with the software. Contact Nortel for support. System or user actions: Use the FAN command to see what nodes were likely impacted and compare to the QIN (impacted nodes) output. User should refer to the installation method to determine how to proceed.

Example

Usage examples for command SET_AFFECTED_NODES

Description of task:	
SAN 69	<pre>This command will SET the impacted node table bools for this XPM and all of its subtending nodes. Do you wish to continue? Please confirm ("YES", "Y", "NO", or "N"): >Y Node 69: LTC_NODE SMA2 1 Set affected nodes PASSED. Use FIND_AFFECTED_NODES/FAN to see the nodes impacted.</pre>

Command: ABIREHOME: CLEAR_AFFECTED_NODES/SAN

Command type: NON-MENU

Command target: All

Command availability: RES

Command description

This command is used as a part of Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome" to enable the ability to rehome an XPM from ENET/JNET C-side links to an ABI DS-512 off of an MG 9000.

Given the node number of the rehomed XPM, clears the impacted node table bits for the XPM and all of its subtending nodes, found by recursively searching its p-side links.

Command syntax

command parameters and variables

Command	Parameters and variables
CLEAR_AFFECTED_NODES or CAN	node Node number of the XPM. Node number can be found by performing QueryPM while the XPM is POSTed at the map.
Parameters and variables	Description
node	<XPM_NODE> {0 to 4095}

Qualifications and warnings

None.

Responses

CLEAR_AFFECTED_NODES responses

MAP outputs with associated meanings and actions

CLEAR_AFFECTED_NODES
CLEAR_AFFECTED_NODES: Sets the rehome node bits for all nodes the are impacted by rehomeing the given XPM, including its subtending nodes. Protected command for ABI Rehomes. ----- Syntax: CLEAR_AFFECTED_NODES node Parameters: node Node number of XPM Parms: <XPM_NODE> {0 TO 4095} Meaning: Help associated with command. System or user actions: Informational purposes only.
This command must be enabled by TAS via the TASTOOLCI SET_ABI_REHOME_STATUS command. Please refer to the installation method. Meaning: The ABI REHOME installation method has not been enabled. TAS must enable the process via the TASTOOLCI SET_ABI_REHOME_STATUS (ON or RESUME) commands before proceeding. System or user actions: If user wishes to proceed with the command, TAS will have to enable the tool.

MAP outputs with associated meanings and actions

CLEAR_AFFECTED_NODES
CLEAR_AFFECTED_NODES: Sets the rehome node bits for all nodes the are impacted by rehomeing the given XPM, including its subtending nodes. Protected command for ABI Rehomes. ----- Syntax: CLEAR_AFFECTED_NODES node Parameters: node Node number of XPM Parms: <XPM_NODE> {0 TO 4095} Meaning: Help associated with command. System or user actions: Informational purposes only.
This command will CLEAR the impacted node table bools for this XPM and all of its subtending nodes. Do you wish to continue? Meaning: Warning that using this command will set triggers that will impact the behavior of a NRS. System or user actions: Enter the correct response.
CAN command aborted by user. Meaning: Command was aborted by the user and no action has been taken. System or user actions: Informational purposes only.
Node 69: LTC_NODE SMA2 1 Clear affected nodes PASSED. Use FIND_AFFECTED_NODES to see the nodes impacted. Meaning: The impacted node bools have been cleared for this XPM and all of its subtending nodes. To see the nodes affected, use the FAN command. To see the current list of impacted nodes, use the QIN command. This command can be used to clear the impacted node table if it was inadvertently set via the SAN command. System or user actions: Informational purposes.
Clear affected nodes FAILED. Check for swerrs and traps. Meaning: Indicates a problem with the software. Contact Nortel for support. System or user actions: Use the FAN command to see what nodes were likely impacted and compare to the QIN (impacted nodes) output. User should refer to the installation method to determine how to proceed.

MAP outputs with associated meanings and actions

CLEAR_AFFECTED_NODES
CLEAR_AFFECTED_NODES: Sets the rehome node bits for all nodes the are impacted by rehomeing the given XPM, including its subtending nodes. Protected command for ABI Rehomes. ----- Syntax: CLEAR_AFFECTED_NODES node Parameters: node Node number of XPM Parms: <XPM_NODE> {0 TO 4095} Meaning: Help associated with command. System or user actions: Informational purposes only.
Meaning: . System or user actions:
Meaning: System or user actions:

Example

Usage examples for command

Description of task:	
CAN 69	<pre>>can 69 This command will CLEAR the impacted node table bools for this XPM and all of its subtending nodes. Do you wish to continue? Please confirm ("YES", "Y", "NO", or "N"): >y Node 69: LTC_NODE SMA2 1 Clear affected nodes PASSED. Use FIND_AFFECTED_NODES to see the nodes impacted.</pre>

Command: ABIREHOME: ADJUST_FRAME_SYNC/AFS

Command type: NON-MENU

Command target: All

Command availability: RES

Command description

This command is used as a part of Installation Method 72-1639 "XPM - ABI Link Verification" to enable the ability to rehome an XPM from ENET/JNET C-side links to an ABI DS-512 off of an MG 9000.

Given the node number of the XPM to be rehomed, this command will cause the ABI cards to adjust their frame sync to that of the inactive XPM unit. This is one step in the process of verifying the DS-512 fiber connection of the XPM before the actual rehome occurs.

Command syntax

command parameters and variables

Command	Parameters and variables
ADJUST_FRAME_SYNC or AFS	node Node number of the XPM. Node number can be found by performing QueryPM while the XPM is POSTed at the map.
Parameters and variables	Description
node	<XPM_NODE> {0 to 4095}

Qualifications and warnings

None.

Responses

ADJUST_FRAME_SYNC responses

MAP outputs with associated meanings and actions

ADJUST_FRAME_SYNC
ADJUST_FRAME_SYNC: Sets the rehome node bits for all nodes the are impacted by rehoming the given XPM, including its subtending nodes. Protected command for ABI Rehomes. ----- Syntax: ADJUST_FRAME_SYNC node Parameters: node Node number of XPM Parms: <XPM_NODE> {0 TO 4095} Meaning: Help associated with command. System or user actions: Informational purposes only.
This command must be enabled by TAS via the TASTOOLCI SET_ABI_REHOME_STATUS command. Please refer to the installation method. Meaning: The ABI REHOME installation method has not been enabled. TAS must enable the process via the TASTOOLCI SET_ABI_REHOME_STATUS (ON or RESUME) commands before proceeding. System or user actions: If user wishes to proceed with the command, TAS will have to enable the tool.

MAP outputs with associated meanings and actions

ADJUST_FRAME_SYNC
ADJUST_FRAME_SYNC: Sets the rehome node bits for all nodes the are impacted by rehomeing the given XPM, including its subtending nodes. Protected command for ABI Rehomes. ----- Syntax: ADJUST_FRAME_SYNC node Parameters: node Node number of XPM Parms: <XPM_NODE> {0 TO 4095} Meaning: Help associated with command. System or user actions: Informational purposes only.
This command will RESET the frame sync on the ABI cards.Both ABI cards must be locked and unlocked to recover from this condition. Do you wish to continue? Meaning: Adjust the frame sync on the ABI cards to sync to the inactive XPM unit. System or user actions: Enter the correct response.
AFS command aborted by user. Meaning: Command was aborted by the user and no action has been taken. System or user actions: Informational purposes only.
Meaning: . System or user actions:
Pass result Meaning: System or user actions: Informational purposes.
No reply received from ABI. Adjust Frame Sync FAILED. Check for swerrs and traps. Meaning: Indicates a problem with the software. Contact Nortel for support. System or user actions: Use the FAN command to see what nodes were likely impacted and compare to the QIN (impacted nodes) output. User should refer to the installation method to determine how to proceed.

Example

Table 1 Usage examples for command

Description of task:	
AFS 69	<pre>>afs 103 Node 103: LTC_NODE SMA2 7 (SMA2 7) This command will RESET the frame sync on the ABI cards. Both ABI cards must be locked and unlocked to recover from this condition. Do you wish to continue? Please confirm ("YES", "Y", "NO", or "N"): >y</pre>

Command: ABIREHOME: SEND_GWC_STATIC_DATA/GWCSD

Command type: NON-MENU

Command target: All

Command availability: RES

Command description

This command is used as a part of Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome" to enable the ability to rehome an XPM from ENET/JNET C-side links to an ABI DS-512 off of an MG 9000.

Given the node number of the rehomed XPM, clears the impacted node table bits for the XPM and all of its subtending nodes, found by recursively searching its p-side links.

Command syntax

command parameters and variables

Command	Parameters and variables
SEND_GWC_STATIC_DATA or GWCSD	n/a

Qualifications and warnings

None.

Responses**SEND_GWC_STATIC_DATA responses****MAP outputs with associated meanings and actions**

SEND_GWC_STATIC_DATA
SEND_GWC_STATIC_DATA: Sets the rehome node bits for all nodes the are impacted by rehomeing the given XPM, including its subtending nodes. Protected command for ABI Rehomes. ----- Syntax: SEND_GWC_STATIC_DATA Parms: none Meaning: Help associated with command. System or user actions: Informational purposes only.
This command must be enabled by TAS via the TASTOOLCI SET_ABI_REHOME_STATUS command. Please refer to the installation method. Meaning: The ABI REHOME installation method has not been enabled. TAS must enable the process via the TASTOOLCI SET_ABI_REHOME_STATUS (ON or RESUME) commands before proceeding. System or user actions: If user wishes to proceed with the command, TAS will have to enable the tool.
This command will send limited static data updates to the GWCs affected by the XPM Rehomes. Do you wish to continue? Meaning: Command to send the static data from the XACore to the GWC after a NoRestartSwact. System or user actions: Enter the correct response.
GWCSO command aborted by user. Meaning: Command was aborted by the user and no action has been taken. System or user actions: Informational purposes only.

Example

Usage examples for command

Description of task:	
GWCSO	<pre>>gwcsd This command will send limited static data updates to the GWCs affected by the XPM Rehomes. Do you wish to continue? Please confirm ("YES", "Y", "NO", or "N"): >y ></pre>

Command: ABIREHOME: ABORT_GWC_STATIC_DATA/ABORT_GWCSO

Command type: NON-MENU

Command target: All

Command availability: RES

Command description

This command is used as a part of Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome" to enable the ability to rehome an XPM from ENET/JNET C-side links to an ABI DS-512 off of an MG 9000.

Given the node number of the rehomed XPM, clears the impacted node table bits for the XPM and all of its subtending nodes, found by recursively searching its p-side links.

Command syntax

command parameters and variables

Command	Parameters and variables
ABORT_GWC_STATIC_DATA or ABORT_GWCSO	n/a

Qualifications and warnings

None.

Responses**ABORT_GWC_STATIC_DATA responses****MAP outputs with associated meanings and actions**

ABORT_GWC_STATIC_DATA
SEND_GWC_STATIC_DATA: Sets the rehome node bits for all nodes the are impacted by rehomeing the given XPM, including its subtending nodes. Protected command for ABI Rehomes. ----- Syntax: SEND_GWC_STATIC_DATA Parms: none Meaning: Help associated with command. System or user actions: Informational purposes only.
This command must be enabled by TAS via the TASTOOLCI SET_ABI_REHOME_STATUS command. Please refer to the installation method. Meaning: The ABI REHOME installation method has not been enabled. TAS must enable the process via the TASTOOLCI SET_ABI_REHOME_STATUS (ON or RESUME) commands before proceeding. System or user actions: If user wishes to proceed with the command, TAS will have to enable the tool.
This command will UNDO the limited static data updates which have been previously sent to the GWCs affected by the XPM Rehomes. This command should only be used in conjunction with XACore AbortSwact. Do you wish to continue? Meaning: This command will UNDO the limited static data updates which have been previously sent to the GWCs affected by the XPM Rehomes. System or user actions: Enter the correct response.
ABORT_GWCSD command aborted by user. Meaning: Command was aborted by the user and no action has been taken. System or user actions: Informational purposes only.

Example

Usage examples for command

Description of task:	
ABORT_GWCSD	This command will UNDO the limited static data updates which have been previously sent to the GWCs affected by the XPM Rehomes. This command should only be used in conjunction with XACore AbortSwact. Do you wish to continue? Please confirm ("YES", "Y", "NO", or "N"): >Y >

Security

Not Applicable.

Configuration Walkthrough

Walkthrough XPM Rehome to ABI Networks

This feature is a step in the overall Installation Method 72-1682 "XPM to MG 9000 DS-512 Rehome." This feature provides the functionality to change an XPM from ENET C-side links to DS-512 ABI links. The use of this feature is restricted and must be activated by appropriate Nortel personnel. A general sequence of events follow however, for full details please refer to the Installation method mentioned above.

1. Enter the TASTOOLCI tool and use command 'set_abi_rehome_status on' to enable the table control functionality.
2. Split the Core
3. On Inactive Core, Busy and Offline the XPM to be rehomed
4. On Inactive Core, position on the XPM to be rehomed via Table LTCINV
5. Change the tuple by removing the C-side links (\$) and adding the optional parameter EXTDS512. Please refer to "Before and After rehome view of the XPM in table LTCINV" on page 983.
6. Repeat steps 4 and 5 for each XPM to be rehomed

7. Provision/create the VMG on the ABI board via the MG9K-EM
8. Enable the VMG via the MG9K-EM
9. On Active Core, Busy and Offline the rehomed XPM

Note: Call-P Outage Starts
10. Move fibers and following the steps in the installation method, perform the NoRestartSwact to activate the table control changes.
11. On newly Active Core, Busy and RTS the XPM(s)

Before and After rehome view of the XPM in table LTCINV

Before view of the LGC tuple with ENET links and no EXTDS512 option.

TABLE: LTCINV

LTCNAME ADNUM FRTYPE FRNO SHPOS FLOOR ROW FRPOS EQPEC LOAD EXECTAB CSLNKTAB
OPTCARD TONESET PROCPEC EXTLINKS E2LOAD OPTATTR PEC6X40 EXTINFO

LGC 1 1001 LTEI 2 18 1 CC 2 6X02NA QLI19AZ (POTS POTSEX) (KEYSET KSETEX) \$ (0 12 1 0)
(0 12 1 1) (0 12 1 2) (0 12 1 3) (0 12 1 4) (0 12 1 5) (0 12 1 6) (0 12 1 7) (0 12 1 8) (0 12 1 9) (0 12 1 10)
(0 12 1 11) (0 12 1 12) (0 12 1 13) (0 12 1 14) (0 12 1 15) \$ (UTR15) (MSG6X69) (CMR13 CMR10A)
(ISP 16) \$ NORTHAM SX05AA \$ SX05AA \$ 0 SXFWAE08 \$ 6X40FB N

After view of the LGC tuple after the change operation has rehomed the XPM to the ABI DS-512 interface. The XPM now has ABI links (derived by the system, user entered a "\$") and the EXTDS512 options.

TABLE: LTCINV

LTCNAME ADNUM FRTYPE FRNO SHPOS FLOOR ROW FRPOS EQPEC LOAD EXECTAB CSLNKTAB
OPTCARD TONESET PROCPEC EXTLINKS E2LOAD OPTATTR PEC6X40 EXTINFO

LGC 20 1021 LTEI 2 19 1 CC 2 6X02NA QLI17AY1 (POTS POTSEX) \$ (4 0) (4 1) (4 2) (4 3) \$
(MSG6X69) \$ NORTHAM SX05AA \$ SX05AA \$ 0 SXFWAE08 (EXTDS512 47 142 23 24 GWC 9) \$ 6X40FA N

Walkthrough ABI XPM Rehost to another GWC

The ability to rehost (move) an ABI XPM from one hosting GWC to another GWC is independent from the XPM rehome operation. A general sequence of the steps to rehost ABI XPMs follows:

1. Busy and Offline the XPM to be rehosted
2. On the MG9K, Busy (lock) the VMG on the ABI via the MG9K-EM
3. In Table LTCINV, position on the XPM tuple to be rehosted
4. Change the hosting GWC in the EXTDS512 optional attribute, field 18 OPTATTR. Ensure static data sent, removing XPM from currently hosting GWC and adding XPM to the newly hosting GWC.

Note: XPM can only be moved to a GWC in the same SAM21 shelf.
5. On the MG9K, change the VMG provisioning on the ABI board pointing to the newly hosting GWC via MG9K-EM.
6. Unlock the VMG on the ABI board via the MG9K-EM

7. Busy and RTS the rehosted XPM

Before and After view of the Rehosted ABI XPM

Before view of the LGC tuple with XPM hosted on GWC 2.

TABLE: LTCINV

LTCNAME ADNUM FRTYPE FRNO SHPOS FLOOR ROW FRPOS EQPEC LOAD EXECTAB CSLNKTAB
OPTCARD TONESET PROCPEC EXTLINKS E2LOAD OPTATTR PEC6X40 EXTINFO

LGC 20 1021 LTEI 2 19 1 CC 2 6X02NA QLI17AY1 (POTS POTSEX) \$ (4 0) (4 1) (4 2) (4 3) \$
(MSG6X69) \$ NORTHAM SX05AA \$ SX05AA \$ 0 SXFWAE08 (EXTDS512 47 142 23 24 GWC 2) \$ 6X40FA N

After view of the LGC tuple now rehosted on GWC 7

TABLE: LTCINV

LTCNAME ADNUM FRTYPE FRNO SHPOS FLOOR ROW FRPOS EQPEC LOAD EXECTAB CSLNKTAB
OPTCARD TONESET PROCPEC EXTLINKS E2LOAD OPTATTR PEC6X40 EXTINFO

LGC 20 1021 LTEI 2 19 1 CC 2 6X02NA QLI17AY1 (POTS POTSEX) \$ (4 0) (4 1) (4 2) (4 3) \$
(MSG6X69) \$ NORTHAM SX05AA \$ SX05AA \$ 0 SXFWAE08 (EXTDS512 47 142 23 24 GWC 7) \$ 6X40FA N

Product = CS 2000

A00003506 -- H.248 Per Trunk Signaling Development (PT-IP)

Functional Description

This SN07 activity provides PTS trunking capabilities for the Succession Call Server 2000 (CS2K). Specifically, this activity provides incoming, outgoing, and two-way interconnections from a North American End Office (EO), Access Tandem (AT), or InterExchange Carrier (IEC) to the Public Switch Telephone Network (PSTN) as well as Private Branch eXchange (PBX) systems.

Figure “CS2K Network Configuration for PTS” on page 986 illustrates the CS2K network components that are applicable to this activity. The PSTN interconnection is provided using PTS trunk groups configured on a Gateway Controller (GWC) peripheral type where H.248 protocol is supported between the GWC and the Media Gateway (MG). The specific MG planned to provide this PTS functionality is Nortel’s Passport Voice Gateway (PVG). The PVG load that will support PTS trunks is planned to be available in the SN07.1 release time frame.

The PTS trunk group types providing interconnection to the PSTN and PBXs are listed in the following table.

Supported GWC PTS Trunk Group Types

Trunk Group Type	Direction
OP	IC,OG,2W
ES	IC,OG,2W
PX	IC,OG,2W
IBNTI	IC
IBNTO	OG
IBNT2	2W
ATC	IC,OG,2W
IT	IC,OG,2W
SC	IC,2W
CELL	IC,OG,2W
DAL	IC,OG,2W
EANT	IC,OG,2W
ONAT	IC,OG,2W

This activity supports the following pulse types:

- MF - Multi-Frequency
- DP - Dial Pulse (for PX, DAL, IBN2W, IBNTO, and IBNTI only)
- DT - DigiTone (for PX, DAL, IBN2W, IBNTO, and IBNTI only)
- NP - No Pulse (For Outgoing FXS signalling only)

This activity supports the following Start Signal types:

- WK - WinK
- IM - IMmediate
- DD - Delay Dial
- GS - Ground start fxS
- LS - Loop start fxS

This activity supports the following Card Codes:

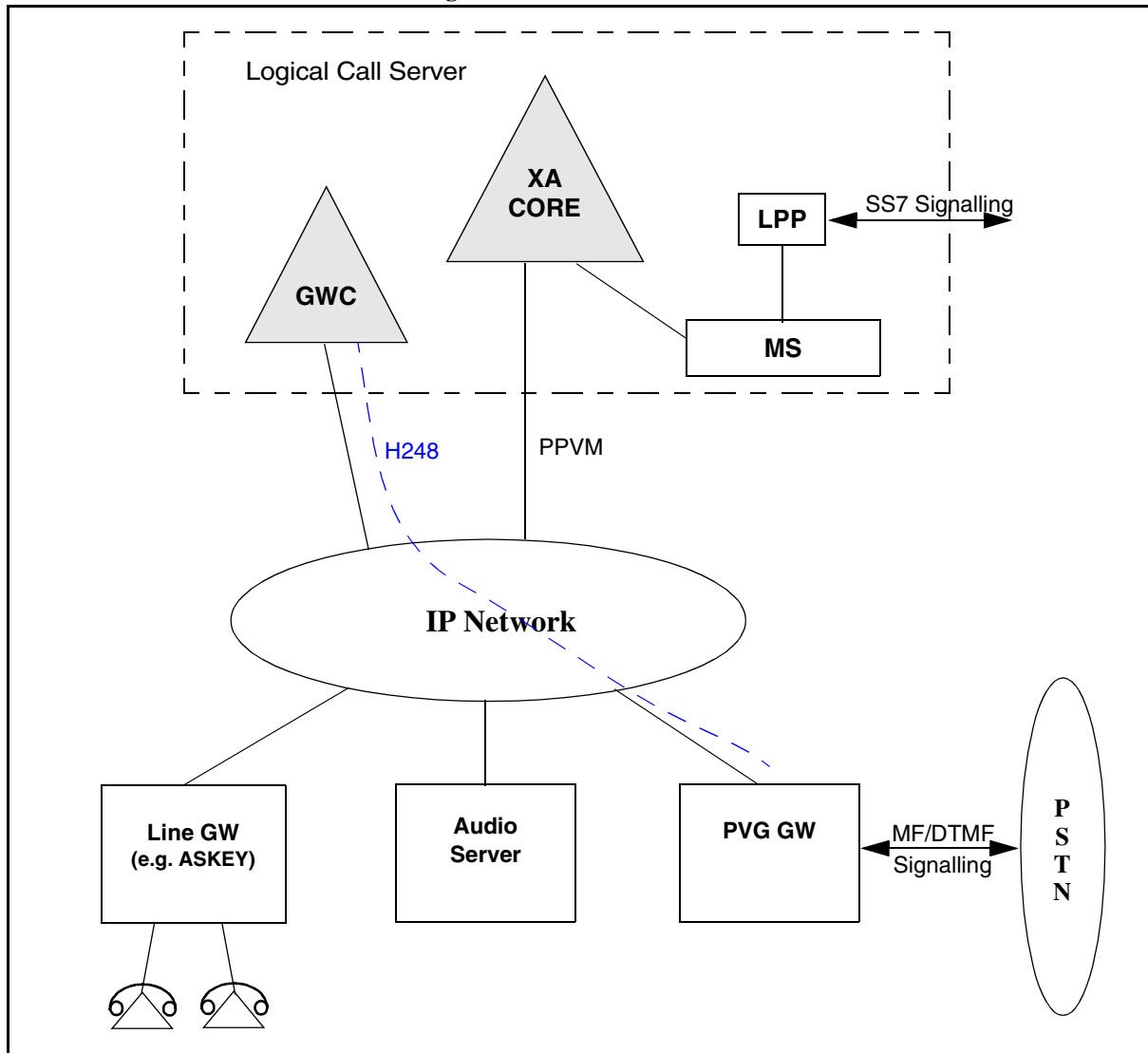
- DS1SIG
- FXSLS

- FXSGS

The supported combinations of trunk group type, pulse type and start signal type for this activity include the same combinations as supported in the legacy DM100 Switching System. Any restrictions or limitation from that support are included in section “Limitations and Restrictions” on page 996.

The base framework for H.248 PTS on GWC was established by prep features A89007187 and A89007652 in SN06. These prep features introduced limited PTS support for Outgoing Operator (OP), Emergency Services (ES), Direct Access Line (DAL), and Equal Access Network Trunk (EANT) trunk group types. This current activity in SN07 builds upon this base framework established in SN06.

CS2K Network Configuration for PTS



Functional Description

CS2K Provisioning Overview

As with the legacy DMS100 switching system, the GWC PTS trunk related data is provisioned on the CS2K core using the same data tables. These data tables include tables CLLI, TRKGRP, TRKSGRP, TRKOPTS, and TRKMEM. In addition, GWC node and endpoint provisioning is required and is accomplished using the Call Server 2000 Manager (CS2M).

When provisioning PTS trunks on a GWC, there are no restrictions regarding the distribution of the trunk members. Trunk members can be distributed over more than one GWC, over more than one MG, and can consist of any number of channels on a T1. However, if a T1 is to have its channels divided across trunks groups, those trunks groups must have the same card code provisioned in table TRKSGRP (e.g. DS1SIG, FXSLS, or FXSGS).

Also, a combination of trunk groups with different signalling types, on the same GWC, is supported. For example, ISUP and PTS trunks on the same GWC is a supported configuration.

Hybrid PTS trunk groups that consist of members distributed across a GWC and a different peripheral type, such as a DTC, are *not* supported.

CS2M GWC Node and Endpoint Provisioning

The CS2M provides the capability to configure a GWC by selecting the ADD GWC NODE command under the Configuration tab. The subsequent popup window allows the user to provision the GWC name, IP and router IP. In addition, the user provisions the Gateway controller profile and associated profile data information including Tone data, Exec data, and Type list for the GWC node being added. This activity provides the capability to select a specific GWC profile and profile data to configure GWCs to support PTS trunks.

The CS2M also provides the capability to configure an MG by selecting the Associate Media Gateway command under the configuration tab. The subsequent popup window allows the user to provision the GW name, IP, GWC name, and Gateway Profile name. For this activity the Gateway Profile name specified must be PVG. In addition, the user must also select the protocol type. For this activity, Megaco (4) must be selected to indicate H.248 protocol.

The CS2M also provides the capability to add carriers to a GWC. This is accomplished by first selecting a specific GWC, then selecting the provisioning tab. Once under the provisioning tab, the carrier tab can then be selected. Once under the carrier tab, the user can click the ADD button which triggers a POPUP where the user provisions the Carrier Name and Gateway

Name. This carrier provisioning task accomplishes the provisioning of 24 PTS endpoints at a time on the specified GWC and carrier. The endpoints and subsequent node and terminal numbers are mapped in the CS2K to a trunk group and member in table TRKMEM. See “Table TRKMEM” on page 990 for information regarding provisioning of table TRKMEM.

The capabilities to configure an MG and add carriers to a GWC are not introduced by this activity, but are included here to clarify the specific field values required to support PTS trunking.

Table SERVINV Provisioning

When a GWC node is added from the CS2M, a subsequent and corresponding tuple is added to table SERVINV. This tuple contains GWC name, network type, IP address, exec lineups and termtypes, tone set value, and options. This activity provides the capabilities to add a GWC node to table SERVINV, either manually or via the CS2M tool that will support new exec_lineups for GWCs configured as PTS GWCs. The following table includes the new exec_lineup and termtype combinations which are supported for the PTS GWC.

Supported PTS Exec Lineup/Term Type Combinations

PTS Exec Lineup with ABTRK TermType	PTS Exec Lineup with AB250 TermType	GWC PTS Trunks Supported
GWCEX	GWCEX	All GWC PTS trunk groups except for PX trunk groups using FXS signalling.
GWCEX	GWCFX	All GWC PTS trunk groups including PX with FXS signalling except for EANT, ONAT, and DAL trunk groups.
GWCEX	<none>	All GWC PTS trunk groups except for PX trunk groups using FXS signalling and EANT, ONAT, and DAL trunk groups.

Table TRKOPTS Provisioning

This activity enhances the functionality of table TRKOPTS by adding the capability to provision option GWCPTSTK to any PTS trunk group identified in Table , “Supported GWC PTS Trunk Group Types,” on page 985. “Table TRKOPTS GWCPTSTK Option” on page 989 shows an example tuple in table TRKOPTS with the GWCPTSTK option provisioned and highlighted.

In addition, the GWCPTSTK option contains a single sub-option, PRELOADANI. This sub-option is a boolean value which identifies GWC PTS trunk groups configured on a GWC which support a call model that allows the ANI digits to be sent from the Core to the GWC prior to receiving any ANI request from the peripheral. The SN07 Feature A00003630 TGCP for the

Cable Market introduced this PRELOADANI sub-option. This sub-option is currently only applicable to OP and ES trunk group types and will not be allowed to be set to Y for any other GWC PTS trunk group type. Please refer to the feature documentation for activity A00003630 for additional information.

Table TRKOPTS GWCPTSTK Option

TABLE: TRKOPTS	
OPTKEY	OPTINFO

GWCPSTCLLI	GWCPTSTK
	GWCPTSTK N

The GWCPTSTK option can only be added to a trunk group after the trunk group has been provisioned in table TRKGRP and before any trunk members of that group are provisioned in table TRKMEM.

In addition, the GWCPTSTK option is incompatible with some of the existing TRKOPTS options. Restrictions are added to prevent the incompatible options from being added together with the GWCPTSTK option on the same trunk group.

TRKOPTS Options Incompatible with GWCPTSTK

TRKOPTS Option	Incompatibility Reason
Q118OPT	This activity supports IBN basic call only. No option support
SUPVOPT	This activity supports IBN basic call only. No option support
DPT	ISUP Specific Option
DYNAMIC	ISUP Specific Option
CNAMINGN	ISUP Specific Option
RLT	ISUP Specific Option
OSNC	ISUP Specific Option
DLYFWDXMT	Not supported for GWC PTS trunks
BLOCKLNP	ISUP Specific Option
VOICELAW	ISUP Specific Option
CGETSRESP	ISUP or ISDN Specific Option

Table TRKOPTS is also used to restrict trunk group, subgroup, or member capabilities non-compatible with the GWCPTSTK option.

The trunk group restrictions enforced by the GWCPTSTK option are unique for each supported GWC PTS trunk group type. These trunk group restrictions are discussed in “Table TRKGRP” below, section “Limitations and Restrictions” on page 996, and in the Configuration section.

The trunk subgroup restrictions enforced by the GWCPTSTK option are discussed in section “Table TRKSGRP” section, “Limitations and Restrictions” on page 996, and in the Configuration section.

The trunk member restrictions enforced by the GWCPTSTK option are discussed in section “Table TRKMEM” on page 990, section “Limitations and Restrictions” on page 996, and in the Configuration section.

Table TRKGRP

The TRKGRP tuple for a GWC PTS trunk is unchanged from the legacy DMS100 switching system. However, restrictions are enforced on GWC PTS trunk groups in table TRKGRP when the GWCPTSTK option is added to the trunk group in table TRKOPTS. Refer to section “Limitations and Restrictions” on page 996 and the Configuration section for further information.

Table TRKSGRP

The TRKSGRP tuple for a GWC PTS trunk is unchanged from the legacy DMS100 switching system. However, restrictions are enforced on GWC PTS trunk groups in table TRKSGRP when the GWCPTSTK option is added to the trunk group in table TRKOPTS. Refer to section “Limitations and Restrictions” on page 996 and the Configuration section for further information.

Table TRKMEM

The provisioning of a GWC PTS tuple in table TRKMEM requires a node number and a terminal number on the GWC. The node and terminal numbers are mapped to the specific endpoints during endpoint provisioning from the CS2M. Provisioning of the endpoints on the CS2M is recommended prior to table TRKMEM provisioning in order to map trunk members to specific carriers. Refer to section “CS2M GWC Node and Endpoint Provisioning” on page 987 for additional information on GWC PTS endpoint provisioning.

Before a GWC PTS trunk member is allowed to be provisioned in table TRKMEM, the GWCPTSTK option must be present on the trunk group in table TRKOPTS. Table control enforces this restriction. In addition, if option GWCPTSTK exist on a trunk group, table control will disallow the addition of trunk members on non-GWC peripheral types, such as a DTC. Hybrid GWC PTS trunk groups that consist of members distributed across a GWC and a

different peripheral type, such as a DTC, are **not** supported. Please refer to section “Limitations and Restrictions” on page 996 and the Configuration section for further information.

Echo Cancellation

This activity restricts the ECSTAT field in table TRKSGRP to allow only values of EXTERNAL or INTERNAL for GWC PTS trunk groups. The ECSTAT value of INTERNAL signifies that echo cancellation is to be performed by the MGs where this trunk group is provisioned. The ECSTAT value of EXTERNAL signifies that echo cancellation is NOT to be performed by the MG where the trunk group is provisioned. The ECSTAT field value of UNEQ is not supported. Field ESUPR is also restricted to allow only a value of 'N' for GWC PTS trunk groups.

Padding

Padding data is provisioned on the CS2K core in table PADDDATA. For each GWC PTS trunk group in table TRKGRP, field PADGRP is provisioned. When a call is established, the padgrp for each agent involved in the call is retrieved and mapped in table PADDDATA to determine the gain or loss. This gain or loss is specified to the MG via H.248 signalling. The PADGROUP ETLL should be used for PTS packet trunks. Please refer to the SN06 PT-IP Engineering Guidelines for additional information on padgroup values.

H.248 Package Requirements

In order to support PTS trunks configured on a GWC using H.248 protocol between the GWC and MG the following H.248 packages are supported:

- Basic Channel Associated signalling (CAS) Package
ITU-T Recommendation H.248.25 (7/2003)
- Robbed Bit Signalling (RBS) Package -
ITU-T Recommendation H.248.25 (7/2003)
- Generic (G) Package -ITU-T Recommendation H.248.1 (03/2002)
- TDM Circuit (TDMC) Package - ITU-T Recommendation H.248.1 (03/2002)
- DTMF Detection (DD) Package - ITU-T Recommendation H.248.1 (03/2002)
- Extended DTMF (XDD) Package - ITU-T Recommendation H.248.16 (11/2002)
- Enhanced DTMF (EDD) Package - ITU-T Recommendation H.248.16 (11/2002)
- Basic Call Progress Tones Generator (BCG) Package - ITU-T Recommendation Q.1950 (12/2002)

- Call Progress Tones Generator (CG) Package - ITU-T Recommendation H.248.1 (03/2002)
- Extended Call Progress Tones (XCG) Package - ITU-T Recommendation Q.1950 (12/2002)
- Basic Service Tones (SRVTN) Package - ITU-T Recommendation Q.1950 (12/2002)
- Network (NT) Package - - ITU-T Recommendation H.248.1 (03/2002)
- H.248 Inactivity Timer (IT) Package - ITU-T Recommendation H.248.14 (03/2002)

Both the Basic CAS and RBS package include properties which the MG, to be compliant, must provide at least a default value for each of the properties. For interoperability with the CS2K, a set of these properties are provisioned on the MG.

PVG Profiles

For the PVG, a profile is provisioned on a DS1 carrier basis during installation of the PVG by Nortel Networks. Some office parameters are no longer applicable to PTS trunks provisioned on a GWC. Their values are now provisioned on the PVG through the use of PVG Profiles. The affected office parameters are listed in section [“Office Parameters” on page 996](#)

Trunk Maintenance

Trunk Maintenance Manager (TMM) Support

The following commands will be supported on the TMM for GWC PTS trunks. No changes were introduced to provide this functionality for GWC PTS trunks.

- POST
- BSY
- BSY ALL
- FRLS
- RTS
- RTS ALL

Trunk Test Position (TTP) Level Support

Support for the following TTP level commands for PTS trunks configured on GWCs is provided.

- QUIT
- Post_

- BSY [<STATE>] [<ALL or A>] where STATE is MB, SB, or INB. SB is not supported for GWC trunks
- BSY [<ALL or A>]
- RTS with opts RTS, ALL, RES, INI, IDL, RLS, C (M, CP, BOTH)
- Hold
- NEXT
- RLS
- CktInfo
- Level_
- FRLS
- SEIZE

The following TTP level commands are not supported for PTS trunks configured on GWCs:

- TST
- Ckt_

NOTE: The T108 test is supported for PTS incoming trunks. Note: special translations are required to support an incoming T108 test (e.g. call translated to CLLI TRKLPBK).

The following TTP level commands are not supported for all trunks configured on GWCs (PTS, ISUP, etc.):

- BSY SB
- CktLoc
- TrnsIVf_
- StkSdr_
- Pads

TTP MANUAL Level Support

The following MANUAL level commands are supported for PTS trunks configured on a GWC. The same restrictions on the BSY and RTS commands apply in the MANUAL level as exist in the TTP level for GWC PTS trunks.

- QUIT
- Post_
- BSY
- RTS

- Hold
- NEXT
- OP_
- FRLS
- SGNL
- RLS

The following MANUAL level commands are not supported for PTS trunks configured on a GWC:

- TST

The following MANUAL level commands are not supported for PTS trunks configured on a GWC because they require a hybrid office configuration:

- LOSS
- TGEN
- Noise
- TDet
- Hset

The following MANUAL level commands are not supported for all trunks configured on a GWC (PTS, ISUP, etc.):

- Jack_
- CallTrf

TTP MONITOR Level Support

The following MONITOR level commands are supported for PTS trunks configured on a GWC. The same restrictions on the BSY and RTS commands apply in the MONITOR level as exist in the TTP level for GWC PTS trunks.

- QUIT
- Post_
- BSY
- RTS
- Hold
- NEXT
- RLS
- FRLS

The following MONITOR level commands are not applicable to PTS trunks configured on a GWC:

- CPos_
- CktMon
- TST

The following MONITOR level commands are not supported for PTS trunks configured on a GWC because they require a hybrid office configuration:

- MonTalk
-

The following MONITOR level commands are not supported for all trunks configured on a GWC (PTS, ISUP, etc.):

- MONPOST
- MONLINK

TTP DATATTP Level Support

The following DATATTP level commands are supported for PTS trunks configured on a GWC. The same restrictions on the BSY and RTS commands apply in the DATATTP level as exist in the TTP level for GWC PTS trunks.

- Quit
- Post_
- Seize
- BSY
- RTS
- HOLD
- Next
- Rls

The following DATATTP level commands are not applicable to PTS trunks configured on a GWC and are restricted from use.

- BTerm

The following DATATTP level commands are not supported for PTS trunks configured on a GWC because they require a hybrid office configuration:

- BERT_

GWC Swact Support for PTS Trunks

This activity provides for the support of PTS trunks during GWC swact. Any stable call over a PTS trunk configured on a GWC, which performs a warm swact, will remain active over the warm swact. All stable calls are torn down over a GWC cold swact.

CS2K Restart Support for PTS Trunks

This activity provides for the support of PTS trunks configured on a GWC over all core restarts. Any stable call will remain active over a warm restart. For any other core restart type, all calls are torn down as expected.

CS2K SWACT Support for PTS Trunks

This activity provides support for PTS trunks configured on a GWC during all CS2K swact activities including norestartswact, restartswact, and abortswact.

Hardware Requirements or Dependencies

Succession Network Hardware

- CS2K
- CS2M
- GWC
- PVG with VSP3-0
- IP Router (i.e. Passport 8600)

Software Requirements or Dependencies

This activity makes changes to the CS2K core, GWC, and PVG software loads. In addition, changes are made to the CS2M software.

This activity has the following software dependencies:

- CS2K North American load - SNNCSH07
- GWC load - GC070
- SN07.1 PVG load - availability TBD
- SN07 CS2M load - CSM0007

Limitations and Restrictions**Office Parameters**

Office parameter PURE_FGD_INTL_TRANSYS in table OFCVAR must be set to "IP" in order to support International FGD calls.

Office parameter IMMED_PRE_DIAL_DELAY in table OFCSTD must be set to a value of 150 or higher in remote switches in order to support incoming PTS calls where Immediate dialing is used.

Some office parameters are no longer applicable to PTS trunks provisioned on a GWC. Their values are now provisioned on the PVG through the use of PVG Profiles. This chart will show which key PTS office parameters are not applicable to GWC PTS trunks.

Office Parameter	Still applicable to GWC PTS trunks?	Notes
PRE_SND_WK_DD_TIME (OFCSTD)	Yes	On originating wink start or delay dial trunks, this is the amount of time that the switch waits (minimum) before sending the leading edge of the start signal (either wink or DD) after origination has been detected. This parameter is in 10 millisecond granularity. This timing is not started until after the origination has been filtered (see ORIGFLTR in TRKGRP datafill).
REC_MAX_DD_TIME (OFCSTD)	No	Maximum duration Delay Dial recognized. On terminating DD trunks, any start signal with an offhook duration of greater than this value will be considered glare. This is in 160 millisecond granularity.
REC_MAX_WK_TIME (OFCSTD)	No	Same as above except for terminating wink start trunks.
REC_MIN_DD_TIME (OFCSTD)	No	Minimum duration Delay Dial recognized. On terminating DD trunks, any start signal with an offhook duration of less than this value will be ignored (probably resulting in a 'no start dial' condition with a route advance). This parameter is in 10 millisecond granularity.
REC_MIN_WK_TIME (OFCSTD)	No	Same as above except for terminating wink start trunks.
REC_PRE_DD_TIME (OFCSTD)	Yes	Timeout for receiving Delay Dial signal leading edge. On terminating DD trunks, the leading edge of the start signal must be received within this time or a "no start dial" condition will be experienced. This parameter is in 150 millisecond granularity. A value of 10 is recommended for GWC based and legacy trunks inter-connection.
REC_PRE_WK_TIME (OFCSTD)	No	Same as above except for terminating wink start trunks.
SND_DD_TIME (OFCSTD)	No	For DP trunks, this is the start signal duration (i.e. time between leading and trailing edges). This parameter is in 10 millisecond granularity.

SND_MF_WK_TIME (OFCSTD)	No	For non-DP trunks (MF trunks), this is the start signal wink duration (i.e. time between leading and trailing edges). This parameter is in 10 millisecond granularity.
SND_DP_WK_TIME (OFCSTD)	No	Same as above except for DP originators.
WK_DD_PRE_DIAL_DELAY (OFCSTD)	Yes	On terminating wink and delay dial trunks, this is the time delay after the trailing edge of the start signal before outpulsing begins.
EA_REC_MAX_WK_TIME (OFCSTD)	Yes	Equal Access Receive Maximum Wink Time - This parameter specifies the maximum time for recognition of wink for ATC type trunk groups, in 10-ms intervals.
EA_REC_SUB_PRE_WK_TIME (OFCSTD)	Yes	Equal Access Receive Subsequent Pre-wink - This parameter specifies the timeout for receiving the leading edge of next wink signals for ATC type trunk groups, in 160ms intervals.
EA_REC_1ST_PRE_WK_TIME (OFCSTD)	Yes	Equal Access Receive First Pre-wink Time - This parameter specifies the timeout for receiving the leading edge of the first wink signal for ATC type trunk groups, in 160-ms intervals.
EAE0_REC_1ST_PRE_WK_TIME (OFCSTD)	Yes	Equal Access End Office Receive First Pre-wink Time - This parameter specifies the time of the first pre-wink delay associated with outpulsing from an equal access end office (EAE0), in 160 ms intervals.
EAE0_REC_2ND_PRE_WK_TIME (OFCSTD)	Yes	Equal Access End Office Receive Second Pre-wink Time - This parameter specifies the time of the second pre-wink delay associated with outpulsing from an Equal Access End Office (EAE0), in 160-ms intervals.
IMMED_PRE_DIAL_DELAY (OFCSTD)	No, GWC PTS trunks will use a value of 1 second.	Two-way Immediate Start Trunks Pre-dial Delay - This parameter only applies to two-way immediate start and outgoing trunks. This parameter specifies the delay between seizure and outpulsing of digits, in 10-ms intervals.
MIN_REC_DP_PULSE_WD (OFCSTD)	No	Minimum Received Dial Pulse Width - This parameter allows variable settings for the minimum received dial pulse (DP) width.
PRE_ANI_SPILL_DELAY (OFCSTD)	Yes	Pre-automatic Number Identification Spill Delay - Switching units with outgoing trunks that perform wink and reversal signal calling number outpulsing require this parameter. This parameter specifies the delay between receiving the calling number request signal (wink), and outpulsing the calling number.
DPREC_INTER_DGT_TIMING (OFCSTD)	No	Interdigit timing in DP reception. This parameter specifies the end of digit timing value between two consecutive digits.

SHORT_TIMED_RELEASE_DISC_TIME (OFCSTD)	Yes	Disconnect timing performed on terminator disconnect. The Short TRD is typically used for unbilled calls.
LONG_TIMED_RELEASE_DISC_TIME (OFCENG)	Yes	Disconnect timing performed on terminator disconnect. The Long TRD is typically used for billed calls.
MF_LAST_DIGIT_DELAY (OFCENG)	No	This is a special interdigit delay between the second-to-last and last digit of an MF outpulsing stream. A value of 0 means the delay is no different than between other digits. This parameter is in 10 millisecond granularity.
ACK_WINK_DELAY_TIME (OFCVAR)	Yes	For FGD originations, this is the delay between the end of the address stream and the leading edge of the acknowledgment wink. This parameter is in 10 millisecond granularity.
ANS_DELAY_TIME (OFCVAR)	Yes	For FGD originations, this is the minimum delay between the trailing edge of the acknowledgment wink and offhook indicating answer. This parameter is in 10 millisecond granularity. 500 milliseconds seems large; however, in many cases the in-switch delay to route the call may be greater than 1/2 second.

Hybrid Office Restriction

A hybrid office configuration is not officially supported by this feature. Interworking Legacy agents with GWC PTS trunks require the use of an IW-SPM which is outside the scope of this development. This includes, but not limited to any test equipment that resides in an MTM shelf.

Universal Audio Server Restriction

The UAS does not support H.248 GWC PTS trunks since these trunks require support of the EG (Emergency) parameter. The UAS does not support use of the EG parameter and no further UAS development is planned. The AMS, Audio Media Gateway currently supports H.248 PTS GWC trunks and the EG parameter.

Dialtone Restriction

On some PTS trunk group types, EANT, DAL, ONAT, and possibly others, DIALTONE can be provisioned to values of S, C, or N, respectively Standard, Carrier, or None. The value of C is not restricted from provisioning, but when provisioned it will provide standard dialtone and not carrier dialtone. This restriction is based on the current limitations of the PVG.

Table DIGMAN Restriction

This feature does not support use of the DIGCOM field value of SIG in table DIGMAN with a pulse type of DT.

Table TRKGRP Restrictions

The following trunk group restrictions are enforced by the GWCPTSTK option in table TRKOPTS or the functionality has been determined to be unsupported for this feature.

OP Trunk Group Restrictions

- ANITYPE values of WK, REV, and NO are allowed but are restricted based on the value of the DIRECTION and MODE fields. The table below provides a support matrix for the combinations of DIRECTION, ANITYPE, MODE.

OP Trunk ANITYPE/Mode Support

DIR	ANITYPE	MODE	Supported
OG	REV	N/A	YES
OG	NO	N/A	NO
OG	WK	N/A	YES
2W	REV	AR/CR	YES
2W	REV	CV	YES
2W	REV	VF	NO
2W	NO	AR/CR	NO
2W	NO	CV	NO
2W	NO	VF	YES
2W	WK	AR/CR	YES
2W	WK	CV	YES
2W	WK	VF	NO

- HOLDTYPE value of JNTHOLD is disallowed for all OP groups.
- EAOSS value of N is allowed. Value of Y is disallowed.

ES Trunk Group Restrictions

- FDISCTIM is restricted to allow a value of 0 only.
- SWST is restricted to allow a value of DC only. AC and ADC are disallowed.
- ANI is restricted to allow a value of ANISPILL only. OUTPULSE and NOANI are disallowed.
- RMB has to be set to YES. A value of NO is disallowed.

PX Trunk Group Restrictions

No support for the TRKOPTS option DLYFWDXMT for PX trunks is provided by this feature.

IBNTI/IBNTO/IBNT2 Trunk Group Restrictions

This activity provides support for “basic call” only on IBN trunk groups. The following fields are restricted with table control, however, if any other field is outside the scope of “basic call”, then no support is implied.

Note: These 1st four fields conflict with requirements. Unsure how the support of these fields was agreed to as a requirement.

- DTI value is restricted to allow value of N. Value of Y is disallowed.
- TRKDSR value is restricted to allow value of N. Value of Y is disallowed.
- REORIG value is restricted to allow value of N. Value of Y is disallowed.
- FLASH value is restricted to allow value of N. Value of Y is disallowed.
- Disallowed IBN OPTIONS include PROPANS, ANISEND, ANIREC, ANIFAIL, DNIS, CLID, and OUTSCHM.

ATC Trunk Group Restrictions

None identified

IT Trunk Group Restrictions

None identified

SC Trunk Group Restrictions

- Option NOUTR is disallowed.

CELL Trunk Group Restrictions

None identified

DAL Trunk Group Restrictions

None identified

EANT Trunk Group Restrictions

None identified

ONAT Trunk Group Restrictions

None identified

Table TRKSGRP Restrictions

The Interdigital Timing Field (IDGTIME) needs to be set a value of 30 (300ms) or higher **if using DP signaling**. The following trunk subgroup

restrictions are enforced by the GWCPTSTK option in table TRKOPTS and are common to subgroups of all GWC PTS trunk group types.

- SGRP field is restricted to a value of 0 only.
- CARDCODE field is restricted to values of DS1SIG, FXSLS, or FXGLS.
- SGRPVAR is restricted to a value of STD only
- IPULSTYP/OPULSTYP are restricted to allow values of MF, DP, NP, or DT only. Each trunk group type may have additional restrictions.
- Pulse type NP is only supported for Outgoing FXS trunks.
- Pulse types DP and DT are only supported for DAL, PX, and IBN trunk group types.
- ISTARTSG/OSTARTSG are restricted to allow values of WK, IM, DD, GS, or LS. Each trunk group type may have additional restrictions.
- CCONT is restricted to allow values of MW or NO.
- RNGBCK is restricted to allow values of MW or NO.

— Note: For GWC PTS trunks the CCONT and RNGBCK functionality is a function of the GW.

— Note: Selecting the MW value for RNGBCK is equivalent to turning ON the ringback feature on a particular GWC PTS trunk group. But the physical characteristics of the ringback signal are dictated by the PVG CAS profile associated with a particular carrier (that belongs to the same trunk group via provisioning)

The PVG supports both types of physical ringback signalling - Expanded In-Band (EI) and Multi-Wink (MW). PVG CAS Profiles to Operator Ringback signalling types are mapped as:

ds1sigMfr1.prof -> sets the operator ringback signal to EI

ds1sigMwMfr1.prof -> sets the operator ringback signal to MW

For the GWC PTS trunks to interact properly with external operator signalling equipment, the proper profile has to be set on that particular carrier on the PVG. This is a per-carrier restriction.

— Note: Operator Ringback functionality is only supported while using MF signalling.

- ESUPR is restricted to allow a value of N only.
- ECSTAT is restricted to allow values of EXTERNAL or INTERNAL only.
- Option SPMECIDX is disallowed on GWC PTS trunks.

Table TRKMEM Restrictions

Hybrid GWC PTS trunk groups that consist of members distributed across a GWC and a different peripheral type, such as a DTC, are **not** supported.

GWC PTS Trunks Capacity/Engineering Restrictions

A maximum of 42 DS1s or 1008 DS0s worth of NA PTS trunks are supported on a per GWC basis.

For every PTS halfcall, H248/Megaco messages convey PTS trunk signalling and also the bearer path manipulation information to the PVG. This extensive messaging puts constraints on the GWC resources. Hence every GWC PTS trunk datafilled will use GWC resources equal to that of four (4) GWC ISUP trunks.

The following table is meant to illustrate this restriction, in the context of supporting multiple trunk types on the GWC.

GWC Trunks Capacity And PTS trunks

Number of PTS trunks Datafilled	Number of other (e.g. ISUP) trunks supported	Total GWC Trunks Capacity
1008	0	1008
504	2078	2582
350	2694	3044
200	3294	3494
0	4094	4094

Note: This feature does not restrict the support of different trunk types on the GWC, it only restricts the number of other trunk types 'members/end-points' that can be datafilled along with the PTS trunk 'members/end-points'.

Interactions

The goal of this activity is to provide transparency with the legacy DMS100 Switching System. The same service interactions and service restrictions that exist with legacy non-gwc PTS trunks will also apply to PTS trunks configured on a GWC.

This activity supports interworking with the following agent types during regular call processing as well as when a service interaction, such as three way calling or call transfer, results in a connection with a supported GWC PTS trunk.

- Line
- ISUP Trunk
- PRI Trunk

- SIPT Dynamic Packet Trunk (DPT)

Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema _____X_____

User Interface _____

Element Management _____X_____

Security _____

Service Order _____

Office Parameters _____X_____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____X_____

Indicate with an X if you are completing the sections of the DDOC listed below. Indicate with “N/A” if these sections do not apply to this functionality.

Realtime _____

Engineering Information _____

Glossary

Term	Description
AMA	Automatic Message Accounting
ANI	Automatic Number Identification
B911	Basic 911
CAS	Channel Associated Signalling
CFL	Carrier Failure
CLI	Calling Line Identification

Term	Description
CS2K	Call Server 2000
DAL	Direct Access Line
DMS	Digital Multiplex System
DN	Directory Number
DP	Dial Pulse
DPT	Dynamic Packet Trunk
DTC	Digital Trunk Controller
E911	Emergency 911
EANT	Equal Access Network Trunk
EAOSS	Exchange Access Operator Services Signalling
EO	End Office
ES	Emergency Service
FGC	Feature Group C
GWC	Gateway Controller
I	Information (I) digit
IEC	Inter-Exchange Carrier
IETF	Internet Engineering Task Force
II	Information (II) digits
IP	Internet Protocol
LEC	Local Exchange Carrier
MAP	Maintenance and Administration Position
MF	Multi-Frequency
MG	Media Gateway
MG2000	Media Gateway 2000
OM	Operational Measurement
OP	Operator
OSS	Operator Services Signalling
PBX	Private Branch Exchange
PPVM	Peripheral Processor Virtual Machine

Term	Description
PRI	Primary Rate Interface
PTS	Per Trunk Signalling
PSTN	Public Switched Telephone Network
RBS	Robbed Bit Signalling
SESM	Succession Element and Sub-Element Manager
SS7	Signalling System Number 7
TMM	Trunk Maintenance Manager
TTP	Trunk Test Position

Configuration for A00003506

Hardware and Software Requirements

It is assumed the hardware and software installation of the CS2K is complete. Additionally, the SESM GWC EM is initialized and available for provisioning data related to this activity.

This activity has the following software dependencies:

- CS2K North American load - SNNCSH07
- GWC load - GC070
- SN07.1 PVG load - availability TBD
- SN07 CS2M load - CSM0007

In summary, the SN07 release load lineup is required.

Initial Configuration

Refer to section “Configuration Walkthrough” on page 1028.

Office/Subnet parameters (OP/SP) (CM & SESM)

Some office parameters are no longer applicable to PTS trunks provisioned on a GWC. Their values are now provisioned on the PVG through the use of PVG Profiles. Please refer to section “Configuration Walkthrough” on page 1028. The chart below shows which key PTS office parameters are and are not applicable to GWC PTS trunks.

Office Parameter	Still applicable to GWC PTS trunks?	Notes
PRE_SND_WK_DD_TIME (OFCSTD)	Yes	On originating wink start or delay dial trunks, this is the amount of time that the switch waits (minimum) before sending the leading edge of the start signal (either wink or DD) after origination has been detected. This parameter is in 10 millisecond granularity. This timing is not started until after the origination has been filtered (see ORIGFLTR in TRKGRP datafill).
REC_MAX_DD_TIME (OFCSTD)	No	Maximum duration Delay Dial recognized. On terminating DD trunks, any start signal with an offhook duration of greater than this value will be considered glare. This is in 160 millisecond granularity.
REC_MAX_WK_TIME (OFCSTD)	No	Same as above except for terminating wink start trunks.
REC_MIN_DD_TIME (OFCSTD)	No	Minimum duration Delay Dial recognized. On terminating DD trunks, any start signal with an offhook duration of less than this value will be ignored (probably resulting in a 'no start dial' condition with a route advance). This parameter is in 10 millisecond granularity.
REC_MIN_WK_TIME (OFCSTD)	No	Same as above except for terminating wink start trunks.
REC_PRE_DD_TIME (OFCSTD)	YES	Timeout for receiving Delay Dial signal leading edge. On terminating DD trunks, the leading edge of the start signal must be received within this time or a "no start dial" condition will be experienced. This parameter is in 150 millisecond granularity. A value of 10 is recommended for legacy and GWC based trunks inter-connection.
REC_PRE_WK_TIME (OFCSTD)	No	Same as above except for terminating wink start trunks.
SND_DD_TIME (OFCSTD)	No	For DP trunks, this is the start signal duration (i.e. time between leading and trailing edges). This parameter is in 10 millisecond granularity.
SND_MF_WK_TIME (OFCSTD)	No	For non-DP trunks (MF trunks), this is the start signal wink duration (i.e. time between leading and trailing edges). This parameter is in 10 millisecond granularity.
SND_DP_WK_TIME (OFCSTD)	No	Same as above except for DP originators.

WK_DD_PRE_DIAL_DELAY (OFCSTD)	Yes	On terminating wink and delay dial trunks, this is the time delay after the trailing edge of the start signal before outpulsing begins.
EA_REC_MAX_WK_TIME (OFCSTD)	Yes	Equal Access Receive Maximum Wink Time - This parameter specifies the maximum time for recognition of wink for ATC type trunk groups, in 10-ms intervals.
EA_REC_SUB_PRE_WK_TIME (OFCSTD)	Yes	Equal Access Receive Subsequent Pre-wink - This parameter specifies the timeout for receiving the leading edge of next wink signals for ATC type trunk groups, in 160ms intervals.
EA_REC_1ST_PRE_WK_TIME (OFCSTD)	Yes	Equal Access Receive First Pre-wink Time - This parameter specifies the timeout for receiving the leading edge of the first wink signal for ATC type trunk groups, in 160-ms intervals.
EAE0_REC_1ST_PRE_WK_TIME (OFCSTD)	Yes	Equal Access End Office Receive First Pre-wink Time - This parameter specifies the time of the first pre-wink delay associated with outpulsing from an equal access end office (EAE0), in 160 ms intervals.
EAE0_REC_2ND_PRE_WK_TIME (OFCSTD)	Yes	Equal Access End Office Receive Second Pre-wink Time - This parameter specifies the time of the second pre-wink delay associated with outpulsing from an Equal Access End Office (EAE0), in 160-ms intervals.
IMMED_PRE_DIAL_DELAY (OFCSTD)	No, GWC PTS trunks will use a value of 1 second.	Two-way Immediate Start Trunks Pre-dial Delay - This parameter only applies to two-way immediate start and outgoing trunks. This parameter specifies the delay between seizure and outpulsing of digits, in 10-ms intervals.
MIN_REC_DP_PULSE_WIDTH (OFCSTD)	No	Minimum Received Dial Pulse Width - This parameter allows variable settings for the minimum received dial pulse (DP) width.
PRE_ANI_SPILL_DELAY (OFCSTD)	Yes	Pre-automatic Number Identification Spill Delay - Switching units with outgoing trunks that perform wink and reversal signal calling number outpulsing require this parameter. This parameter specifies the delay between receiving the calling number request signal (wink), and outpulsing the calling number.
DPREC_INTER_DGT_TIMING (OFCSTD)	No	Interdigit timing in DP reception. This parameter specifies the end of digit timing value between two consecutive digits.
SHORT_TIMED_RELEASE_DISC_TIME (OFCSTD)	Yes	Disconnect timing performed on terminator disconnect. The Short TRD is typically used for unbilled calls.

LONG_TIMED_RELEASE_DISC_TIME (OFCENG)	Yes	Disconnect timing performed on terminator disconnect. The Long TRD is typically used for billed calls.
MF_LAST_DIGIT_DELAY (OFCENG)	No	This is a special interdigit delay between the second-to-last and last digit of an MF outpulsing stream. A value of 0 means the delay is no different than between other digits. This parameter is in 10 millisecond granularity.
ACK_WINK_DELAY_TIME (OFCVAR)	Yes	For FGD originations, this is the delay between the end of the address stream and the leading edge of the acknowledgment wink. This parameter is in 10 millisecond granularity.
ANS_DELAY_TIME (OFCVAR)	Yes	For FGD originations, this is the minimum delay between the trailing edge of the acknowledgment wink and offhook indicating answer. This parameter is in 10 millisecond granularity. 500 milliseconds seems large; however, in many cases the in-switch delay to route the call may be greater than 1/2 second.

Upgrade Impact

Dump and Restore

None

Element Management Upgrade

None

Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
SERVINV	changed	unchanged
TRKGRP	changed	unchanged
TRKSGRP	changed	unchanged
TRKOPTS	changed	unchanged
TRKMEM	changed	unchanged

Table/MIB/Remote Database Schema information**Name: SERVRINV**

Server Inventory Table

Functional description

This activity adds three new exec line-ups, GWCEX, GWCFX, and GWC250 for GWC node types. The new exec line-ups are specific to Per Trunk Signaling (PTS) trunk types that are configured on a GWC node type.

The following table provides a mapping of which exec line-up and termtype combinations are required to support the various PTS trunk group types.

Supported PTS Exec Lineup/Term Type Combinations

PTS Exec Lineup with ABTRK TermType	PTS Exec Lineup with AB250 TermType	GWC PTS Trunks Supported
GWCEX	GWC250	All GWC PTS trunk groups except for PX trunk groups using FXS signalling.
GWCEX	GWCFX	All GWC PTS trunk groups including PX with FXS signalling except for EANT, ONAT, and DAL trunk groups.
GWCEX	<none>	All GWC PTS trunk groups except for PX trunk groups using FXS signalling and EANT, ONAT, and DAL trunk groups.

Usage sequence and implications (CM Only)

Current datafill order unchanged by this activity.

Size

The size of this table is unchanged.

Fields/OIDs

The following table lists fields for SERVRINV that are changed by this activity. The configuration information for all other fields in table SERVRINV are unchanged.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SRVREXEC	changed	TRMTYPE	ABTRK unchanged	The TRMTYPE subfield is unchanged. This activity adds 1 new EXEC entry for TRMTYPE ABTRK and 2 new EXEC entries for TRMTYPE AB250
		EXEC	GWCEX	ABTRK / GWCEX supports GWC PTS trunks OP, ES, PX, IBN, ATC, IT, SC & CELL, but does not support PX trunks using FXS signalling.
		TRMTYPE	AB250	ABTRK / GWCFX supports PX trunks using FXS signalling only. AB250 / GWC250 supports DMS250 GWC PTS trunks EANT, DAL, and ONAT. Also supports DAL with FXS signalling.
		EXEC	GWCFX	
		EXEC	GWC250	

Datafill example

The following example shows sample datafill for table SERVIRNV:

SRVRNAME	SRVRADDR	SRVREXEC	SRVRTONE	SRVROPTS

GWC 0	IP 47 174 66 4	(ABTRK GWCEX) (AB250 GWC250)		\$ NORTHAM \$
GWC 1	IP 47 174 66 8	(ABTRK GWCEX) (AB250 GWCFX)		\$ NORTHAM \$
GWC 2	IP 47 174 66 12	(ABTRK GWCEX) \$		NORTHAM \$

Table release history update

The following information was added to table SERVRINV:

exec line-up GWCEX is added to field SRVREXEC

exec line-up GWCFX is added to field SRVREXEC

exec line-up GWC250 is added to field SRVREXEC

Supplementary information

Tuples in table SERVRINV should not be added or changed via manual table control commands. Provisioning of this table should be performed using SESM node provisioning.

Translation verification other tools

Not Applicable

Name: TRKGRP

Trunk Group Table

Functional description

This activity introduces new provisioning restrictions in table TRKGRP for PTS trunks groups configured on a GWC. The restrictions apply when the trunk group is assigned the GWCPTSTK option in table TRKOPTS and when a PTS group tuple is changed in table TRKGRP.

Supported GWC PTS Trunk Group Types

Trunk Group Type
OP
ES
PX
IBNTO
IBNTI
IBNT2
ATC
IT
SC
CELL
DAL

Supported GWC PTS Trunk Group Types

Trunk Group Type
EANT
ONAT

Usage sequence and implications (CM Only)

When provisioning PTS trunk group members on a GWC, the following sequence of table provisioning is required. (NOTE: Table TRKSGRP is permitted to be provisioned before table TRKOPTS.)

1. table CLI
2. table TRKGRP
3. table TRKOPTS, option GWCPTSTK
4. table TRKSGRP
5. table TRKMEM

Size

The size of this table is unchanged by this activity.

Fields/OIDs

Not Applicable

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action

Datafill example

Not Applicable

Table release history update

The following information was added to table TRKGRP:

Restrictions are added for GWC PTS trunk groups

Supplementary information

When PTS trunk group data is changed in table TRKGRP, table control determines if option GWCPTSTK is provisioned in table TRKOPTS. GWCPTSTK identifies PTS trunk groups configured on a GWC that provide connectivity between the CS2K's packet network and the Public Switched Telephone Network (PSTN). If option GWCPTSTK is provisioned, table control performs error checking to ensure the TRKGRP data is provisioned

correctly. Table , “TRKGRP Restrictions.” lists the new error messages that may be generated by table control.

TRKGRP Restrictions

Trunk Type	Error Messages
ALL support GWC PTS groups	Trunk Members exist in table TRKMEM Non-GWC trunk members are disallowed CCONT in table TRKSGRP must be set to NO ESUPR in table TRKSGRP must be set to N Table Control Operation not allowed PRELOADANI must be set to N for this trunk type CCONT in table TRKSGRP must be set to NO or MW for this trunk type
Non-Supported trunk groups	It is not supported with this trunk group type
OP	ANITYPE in table TRKGRP must be set to WK or REV EAOSS in table TRKGRP must be set to N when EA is Y OPULSTYP in TRKSGRP must be set to MF for this trunk type OSTARTSG in TRKSGRP must be set to WK for this trunk type IPULSTYP in TRKSGRP must be set to MF for this trunk type ISTARTSG in TRKSGRP must be set to WK for this trunk type ANITYPE in table TRKGRP must be set to REV for this trunk type ANITYPE in table TRKGRP must be set to NO for this trunk type
ES	Only OG direction is supported with this trunk type FDISCTIM in table TRKGRP must be set to 0 SWST in table TRKGRP must be set to DC ANI in table TRKGRP must be set to ANISPILL OPULSTYP in TRKSGRP must be set to MF for this trunk type OSTARTSG in TRKSGRP must be set to WK for this trunk type RMB in table TRKSGRP must be set to YES
PX	PRELOADANI must be set to N for this trunk group type

TRKGRP Restrictions

Trunk Type	Error Messages
IBNTO	PRELOADANI must be set to N for this trunk group type ANITYPE in table TRKGRP must be set to WK or REV FLASH in table TRKGRP must be set to N for this trunk type. DNIS option disallowed for this trunk type. CLID option disallowed for this trunk type. OUTSCHM option disallowed for this trunk type. PROPANS option disallowed for this trunk type. ANISEND option disallowed for this trunk type.
IBNTI	PRELOADANI must be set to N for this trunk group type DTI in table TRKGRP must be set to N for this trunk type. TRKDSR in table TRKGRP must be set to N for this trunk type. REORIG in table TRKGRP must be set to N for this trunk type.
IBNT2	PRELOADANI must be set to N for this trunk group type ANITYPE in table TRKGRP must be set to WK or REV DTI in table TRKGRP must be set to N for this trunk type. TRKDSR in table TRKGRP must be set to N for this trunk type. REORIG in table TRKGRP must be set to N for this trunk type. FLASH in table TRKGRP must be set to N for this trunk type. DNIS option disallowed for this trunk type. CLID option disallowed for this trunk type. OUTSCHM option disallowed for this trunk type. PROPANS option disallowed for this trunk type. ANISEND option disallowed for this trunk type.
ATC	PRELOADANI must be set to N for this trunk group type
IT	PRELOADANI must be set to N for this trunk group type
SC	PRELOADANI must be set to N for this trunk group type. ANITYPE in table TRKGRP must be set to WK or REV NOUTR option is disallowed.

TRKGRP Restrictions

Trunk Type	Error Messages
CELL	PRELOADANI must be set to N for this trunk group type
DAL	PRELOADANI must be set to N for this trunk group type DETDIAL option is disallowed. ATDANS option is disallowed.
EANT	PRELOADANI must be set to N for this trunk group type
ONAT	PRELOADANI must be set to N for this trunk group type

Translation verification other tools

Not Applicable

Name: TRKSGRP

Trunk Subgroup Table

Functional description

This activity introduces new provisioning restrictions in table TRKSGRP for PTS trunks groups configured on a GWC. The restrictions apply when the trunk group is assigned the GWCPTSTK option in table TRKOPTS and when adding or changing the GWC PTS trunk subgroup tuples in table TRKSGRP.

Usage sequence and implications (CM Only)

When provisioning PTS trunk group members on a GWC, the following sequence of table provisioning is required.(NOTE: Table TRKSGRP is permitted to be provisioned before table TRKOPTS)

1. table CLLI
2. table TRKGRP
3. table TRKOPTS, option GWCPTSTK
4. table TRKSGRP
5. table TRKMEM

Size

The size of this table is unchanged by this activity.

Fields/OIDs

Not Applicable

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action

Datafill example

Not Applicable

Table release history update

The following information was added to table TRKSGRP:

Restrictions are added for GWC PTS trunk groups

Supplementary information

When PTS trunk groups are provisioned or tuples are changed in table TRKSGRP, table control determines if option GWCPTSTK is provisioned in table TRKOPTS. GWCPTSTK identifies PTS trunk groups configured on a GWC that provide connectivity between the CS2K's packet network and the Public Switched Telephone Network (PSTN). If option GWCPTSTK is provisioned, table control performs error checking to ensure the TRKSGRP data is provisioned correctly. Please refer to Table , "TRKSGRP Restrictions."

TRKSGRP Restrictions

TRKSGRP Field	Error Messages
SGRP	Only trunk subgroup 0 is allowed.
CARDCODE	CARDCODE is not supported with this trunk type
Signaling Data Selector	SGRPVAR in table TRKSGRP must be set to STD
DIR	n/a
IPULSTYP	Disallowed IPULSTYP in TRKSGRP. IPULSTYP in TRKSGRP must be set to MF for this trunk type
ISTARTSG	ISTARTSG in TRKSGRP must be set to WK for this trunk type Disallowed ISTARTSG in TRKSGRP.
OVLP	OVLP in table TRKSGRP must be set to N.
PSPDSEIZ	n/a
PARTDIAL	n/a

TRKSGRP Field	Error Messages
OPULSTYP	OPULSTYP in TRKSGRP must be set to MF for this trunk type Disallowed OPULSTYP in TRKSGRP.
OSTARTSG	OSTARTSG in TRKSGRP must be set to WK for this trunk type Disallowed OSTARTSG in TRKSGRP.
IDGTIME	n/a
NUMSTOPS	NUMSTOPS in table TRKSGRP must be set to 0.
GLAREYD	n/a
CCONT	CCONT in table TRKSGRP must be set to NO CCONT in table TRKSGRP must be set to NO or MW for this trunk type.
RNGBCK	RNGBCK in table TRKSGRP must be set to NO or MW for this trunk type.
ESUPR	ESUPR in table TRKSGRP must be set to N
SAT	n/a
REMB SY	n/a
DIALMODE	n/a
TRKGRDTM	n/a
ECSTAT	ECSTAT in table TRKSGRP must be set to INTERNAL or EXTERNAL
SPMECIDX	SPMECIDX option is disallowed.

Translation verification other tools

Not Applicable

Name: TRKOPTS

Trunk Options Table

Functional description

This activity adds the new trunk group option, GWCPTSTK, to table TRKOPTS. GWCPTSTK identifies PTS trunk groups configured on a GWC that provide connectivity between the CS2K's packet network and the Public Switched Telephone Network (PSTN). In the SN07 release, GWCPTSTK is supported with all GWC PTS supported trunk group types that are configured on a GWC. Please refer to "Supported GWC PTS Trunk Group Types" on page 1012.. This option must be provisioned prior to configuring trunk members in table TRKMEM.

Usage sequence and implications (CM Only)

When provisioning PTS trunk group members on a GWC, the following sequence of table provisioning is required. (NOTE: Table TRKSGRP is permitted to be provisioned before table TRKOPTS.)

1. table CLLI
2. table TRKGRP
3. table TRKOPTS, option GWCPTSTK
4. table TRKSGRP
5. table TRKMEM

Table TRKOPTS may be provisioned following table TRKSGRP. Table control restrictions will enforce table TRKOPTS be provisioned after table TRKGRP and before table TRKMEM.

Size

The size of this table is unchanged by this activity.

Fields/OIDs

The following table lists fields for TRKOPTS that are changed by this activity.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTKEY	changed	CLLI	unchanged	The CLLI subfield is unchanged. Provision the OP or ES trunk group CLLI.
		OPTION	GWCPTSTK	The new option GWCPTSTK is added. For PTS OP and ES trunks configured on a GWC, this option must be provisioned.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTION	changed	OPTION	GWCPTSTK	The new option GWCPTSTK is added. For PTS and trunks configured on a GWC, this option must be provisioned.
		PRELOAD ANI	Y or N	The new sub-option PRELOADANI is added. For GWC PTS trunks which support a call model that allows the ANI digits to be sent from the Core prior to receiving an ANI request, the field must be to Y.

Datafill example

The following example shows sample datafill for table TRKOPTS:

OPTKEY		OPTINFO

PTSCLLI	GWCPTSTK	GWCPTSTK N

Table release history update

The following information was added to table TRKOPTS:

Option GWCPTSTK is added for GWC PTS trunk groups

Supplementary information

Option GWCPTSTK is used to identify PTS trunk groups to be configured on a GWC that can provide connectivity between the CS2K's packet network and the PSTN. This option applies only to all GWC PTS supported trunk group types in the SN07 release. Table control in table TRKOPTS will block the addition of this option to a non-supported trunk type. Please refer to "Supported GWC PTS Trunk Group Types" on page 1012.. The following error message will result:

"GWCPTSTK cannot be assigned for the following reasons:"

"It is not supported with this trunk type."

This option can not be added if existing datafill in either table TRKGRP or table TRKSGRP that is incompatible with GWC PTS trunks. If an error message occurs when provisioning GWCPTSTK in table TRKOPTS, the tuple entry in table TRKGRP and/or table TRKSGRP must be changed. Please refer to Table , “TRKGRP Restrictions,” on page 1014 and Table , “TRKSGRP Restrictions,” on page 1017.

This option can not be added if the PTS trunk group already has members provisioned in table TRKMEM. This can occur if the members were provisioned on a peripheral type other than a GWC. Note that trunks members can not be assigned to a GWC in table TRKMEM if the GWCPTSTK option is not present in table TRKOPTS. Hybrid PTS trunk groups that consist of members distributed across a GWC and a different peripheral type, such as a DTC, are *not* supported. If trunk members exist while provisioning the GWCPTSTK option, the following error will result:

“GWCPTSTK cannot be assigned for the following reasons:”
“Trunk Members exist in table TRKMEM”

This option can not be deleted from table TRKOPTS until all members on the trunk group have been deleted from table TRKMEM. The following error will result:

“GWCPTSTK cannot be deleted for the following reasons:”
“Trunk Members exist in table TRKMEM”

Translation verification other tools

Not Applicable

Name: TRKMEM

Trunk Member Table

Functional description

This activity introduces new provisioning restrictions in table TRKMEM for PTS trunks groups configured on a GWC.

Usage sequence and implications (CM Only)

When provisioning PTS trunk group members on a GWC, the following sequence of table provisioning is required. (NOTE: Table TRKSGRP is permitted to be provisioned before table TRKOPTS.)

1. table CLI
2. table TRKGRP
3. table TRKOPTS, option GWCPTSTK
4. table TRKSGRP
5. table TRKMEM

Size

The size of this table is unchanged by this activity.

Fields/OIDs

Not Applicable

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action

Datafill example

Not Applicable

Table release history update

The following information was added to table TRKMEM:

Restrictions are added for GWC PTS trunk groups

Supplementary information

Table control for table TRKMEM determines if the option GWCPTSTK is provisioned in table TRKOPTS. If option GWCPTSTK is provisioned, table control performs error checking to ensure the TRKMEM data is provisioned correctly. Table , “TRKMEM Restrictions.”.

TRKMEM Restrictions

TRKMEM Action	Error Messages
Attempt to ADD member with GWC PMTYPE to PTS group without GWCPTSTK option.	To assign a trunk member with SGRPVAR = STD to a GWC, option GWCPTSTK must be present in table TRKOPTS
Attempt to ADD member with non-GWC PMTYPE to PTS group with GWCPTSTK option	With the GWCPTSTK option assigned for this trunk group: Non-GWC trunk members are disallowed TRKMEM data conflicts with data in table TRKOPTS
Attempt to Change PMTYPE from GWC to non-GWC.	With the GWCPTSTK option assigned for this trunk group: Non-GWC trunk members are disallowed TRKMEM data conflicts with data in table TRKOPTS
Attempt to CHANGE PMTYPE from Non-GWC to GWC	To assign a trunk member with SGRPVAR = STD to a GWC, option GWCPTSTK must be present in table TRKOPTS

Translation verification other tools

Not Applicable

Service Orders (SO) (CM & SESM)

Not Applicable

Software optionality control (SOC)

Not Applicable

SOC

SOC option name:	
SOC option title:	Yes/No
SOC option control type:	<state/usage/combined>
New SOC option?	<Yes/No>
SOC option order code	<order code>
Option defined in DRU:	<DRU>
Affected products:	<PCL(s)>

Element Management**New/modified GUIs**

The following levels of the MAP are changed by this activity.

New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
TTP	changed
MANUAL	changed
MONITOR	changed
DATATTP	changed

GUI information**GUI name: TTP**

Trunk Test Position

Functional description

New restrictions are added at this level for PTS trunk groups that are provisioned on a GWC.

GUI usage and implications

Not Applicable

GUI size

Unchanged

GUI fields

Not applicable

Usage example

Not applicable

GUI release history update

The following information was added:

TTP restrictions are added for GWC PTS trunks.

Supplementary information

New restrictions are added to the TTP level of the MAP for PTS trunks configured on a GWC.

The following commands are not supported for PTS trunks configured on a GWC:

- BSY SB
- Cktloc
- TrnsIVf
- Pads

The following error message is displayed if an attempt is made to execute any of these commands:

“Action not supported on GWC trunks.”

CLUI Interface

Not applicable

GUI name: MANUAL

Manual Trunk Test Position

Functional description

New restrictions are added at this level for PTS trunk groups that are provisioned on a GWC.

GUI usage and implications

Not Applicable

GUI size
Unchanged

GUI fields
Not applicable

Usage example
Not applicable

GUI release history update
The following information was added:

MANUAL restrictions are added for GWC PTS trunks.

Supplementary information
New restrictions are added to the MANUAL level of the MAP for PTS trunks configured on a GWC.

The following commands are not supported for PTS trunks configured on a GWC:

- Jack
- Calltrf

The following error message is displayed if an attempt is made to execute any of above commands:

“Action not supported on GWC trunks.”

The following commands are not supported for PTS trunks because a hybrid office configuration is not supported by this feature. An error message is generated indicating no test equipment is available.

- LOSS
- TGEN
- NOISE
- TDET
- Hset

The following error message is displayed if an attempt is made to execute any of these commands:

‘No IW SPM IP Bridges Available To Perform Action.’

CLUI Interface
Not applicable

GUI name: MONITOR

MONITOR Trunk Test Position

Functional description

New restrictions are added at this level for PTS trunk groups that are provisioned on a GWC.

GUI usage and implications

Not Applicable

GUI size

Unchanged

GUI fields

Not applicable

Usage example

Not applicable

GUI release history update

The following information was added:

MONITOR restrictions are added for GWC PTS trunks.

Supplementary information

New restrictions are added to the MONITOR level of the MAP for PTS trunks configured on a GWC.

The following commands are not supported for PTS trunks configured on a GWC:

- MONPOST
- MONLINK
- MonTalk
- CktMOn
- CPOS

The following error message is displayed if an attempt is made to execute any of these commands:

“Action not supported on GWC trunks.”

CLUI Interface

Not applicable

GUI name: DATATTP

Trunk Test Position

Functional description

New restrictions are added at this level for PTS trunk groups that are provisioned on a GWC.

GUI usage and implications

Not Applicable

GUI size

Unchanged

GUI fields

Not applicable

Usage example

Not applicable

GUI release history update

The following information was added:

DATATTP restrictions are added for GWC PTS trunks.

Supplementary information

New restrictions are added to the DATATTP level of the MAP for PTS trunks configured on a GWC.

The following commands are not supported for PTS trunks configured on a GWC:

- BTerm

The following error message is displayed if an attempt is made to execute any of these commands:

“Action not supported on GWC trunks.”

CLUI Interface

Not applicable

GUI name: CS2M - ADD GWC NODE

Call Server 2000 Management Tools Configuration- Add GWC Node

Functional description

The Add GWC Node command provides functionality to select a GWC profile that corresponds to the required termtype and exec_lineups that support the

specific type GWC PTS trunk group types that will be provisioned on the GWC node being added.

GUI usage and implications

Not Applicable

GUI size

Unchanged

GUI fields

Not applicable

Usage example

Not applicable

GUI release history update

The following information was added:

Add GWC node enhanced to select TERMTYPE and EXEC_LINEUP required for specific PTS group types supported on GWC being added.

Supplementary information

N/A

CLUI Interface

Not applicable

Command interface changes

Not Applicable - No new or changed CIs.

Security

Not Applicable

Configuration Walkthrough

Following is a high-level walkthrough of the steps required to provision supported PTS trunk groups on a GWC.

- Provision the GWC node using the CS2M. The CS2M will provision table SERVINV on the CS2K core. A new Gateway Controller Profile must be selected when provisioning the GWC node. Select "TRUNKNA" and choose exec lineups as specified in the following table.

Supported PTS Exec Lineup/Term Type Combinations

PTS Exec Lineup with ABTRK TermType	PTS Exec Lineup with AB250 TermType	GWC PTS Trunks Supported
GWCEX	GWC250	All GWC PTS trunk groups except for PX trunk groups using FXS signalling.
GWCEX	GWCFX	All GWC PTS trunk groups including PX with FXS signalling except for EANT, ONAT, and DAL trunk groups.
GWCEX	<none>	All GWC PTS trunk groups except for PX trunk groups using FXS signalling and EANT, ONAT, and DAL trunk groups.

- Provision the PTS MG(s) using the CS2M. The gateway profile number that should be provisioned for a PTS MG is 58. Additionally, Megaco protocol must be specified.
- When provisioning the PTS MGs, the GWC name must be entered. The GWC name must be entered to prevent the GWC EM from discovering an incorrect GWC.
- Provision the PTS MG endpoints on the GWC using the CS2M. The endpoint names and terminal numbers returned by the CS2M should be noted. The terminal numbers are required when provisioning table TRKMEM on the CS2K core.
- Provision table CLLI with the PTS group clii.
- Provision table TRKGRP with the PTS trunk group data. Please refer to “TRKGRP Restrictions” on page 1014..
- Provision the GWCPTSTK option for the PTS trunk group clii in table TRKOPTS.
- Provision table TRKSGRP with the PTS trunk subgroup data. Please refer to “TRKSGRP Restrictions” on page 1017..
- Provision table TRKMEM with the PTS trunk group members. The terminal number information provided by the CS2M is required when entering tuples in table TRKMEM.

PVG Profiles

For the PVG, a profile is provisioned on a DS1 carrier basis during installation of the PVG by Nortel Networks.

Product = CS2000

A00003562 -- SAM21 Element Manager support for CICM (UA-IP)

Description

The SAM21 Element Manager now allows the user to:

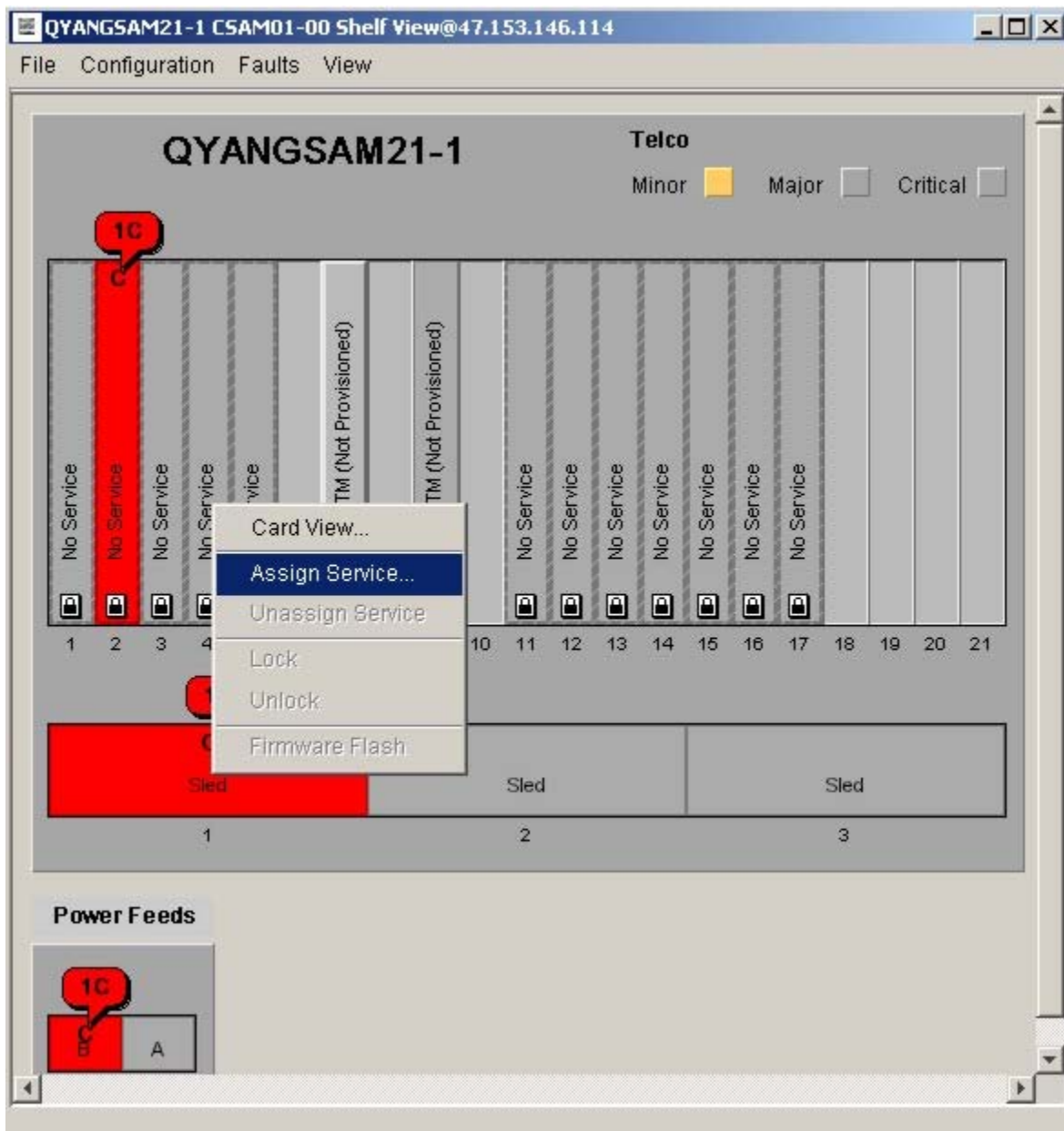
- Provision CentrexIP Client Manager application (also known as “CICM”) on a given MCPN5385 card
- Provision CICM Element Manager application (also known as “CICM-EM”) on a given MCPN5385 card

The SAM21 defines new provisioning panels for the new CICM and CICM-EM service respectively.

Provision CICM Service On a MCPN5385 card

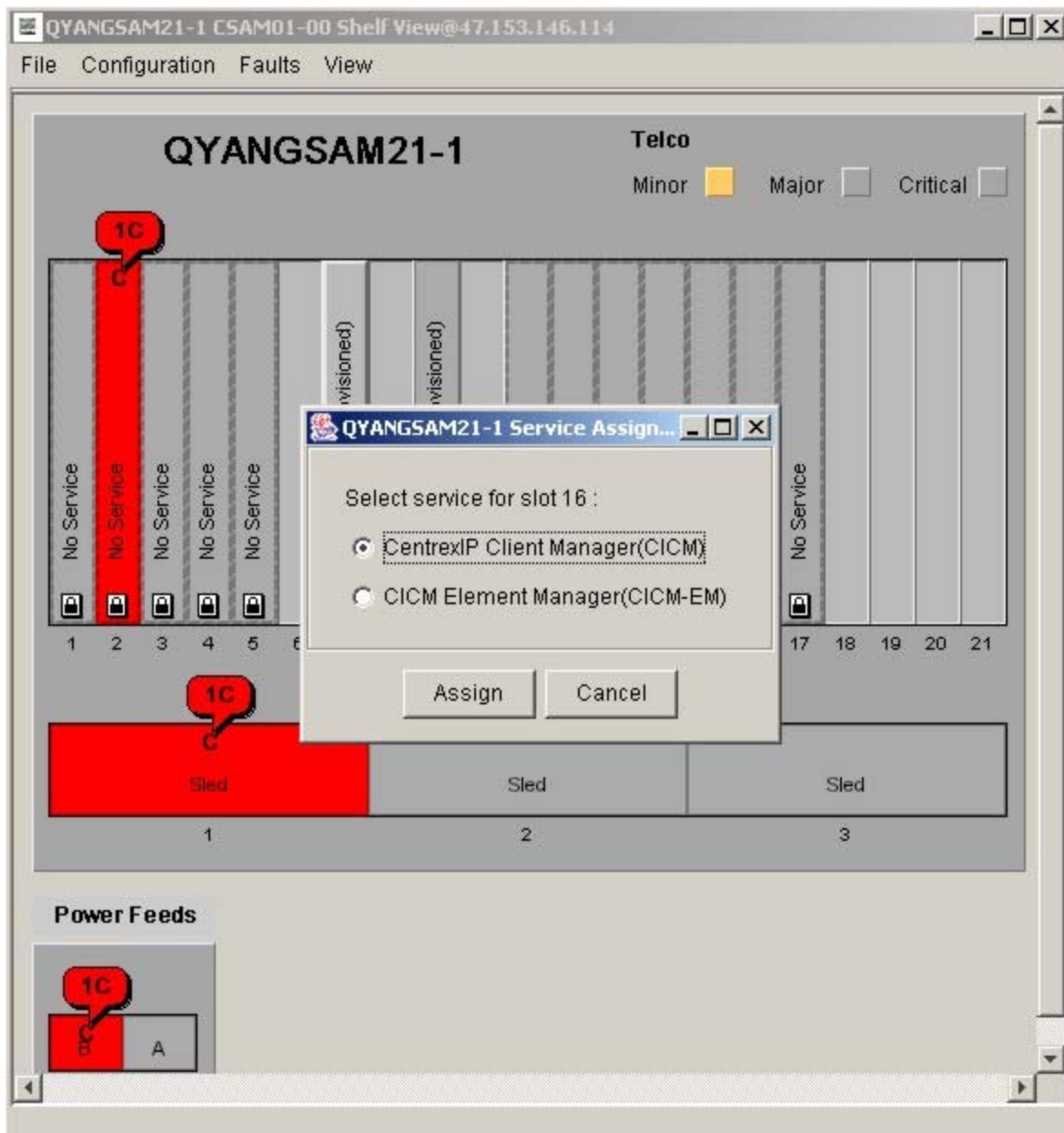
Assign Service

The SAM21 EM mechanism to provision service on a card has not changed. When displaying the shelf view, the user can right click on a card to view the Card Popup Menu. If the card currently is not assigned a service, the user can select “Assign Service...” from this menu.



When the user selects “Assign Service...”, the SAM21 EM displays the Service Assignment popup window. Based on the card’s hardware (model type and memory), the SAM21 EM determines the set of services that can be assigned to the card and allows the user to choose one of them.

The CICM service can be assigned to a MCPN5385 card.



When the user selects the listed “CICM” service and then clicks “Assign”, the SAM21 EM displays a CICM service provisioning panel.

CICM Provisioning Panel

The CICM Provisioning Panel displays the following fields. Fields in *italics* are automatically filled in for the user. A picture of the CICM Provisioning Panel follows.

- **IP:** The IP address of the MCPN5385 card.
- **Router IP:** The IP address of the card's router.
- **Subnet Mask:** The card's subnet mask.
- **FW Version:** The card's firmware version, will be set to "Not reported" by shelf controller.
- **MAC Address:** The MAC addresses of the MCPN5385 card, need manual input.
- **Instance ID:** The instance integer identifier of the CICM card, and applies to both CICM and CICM-EM.
- **UNIT ID:** 'A' or 'B', identifies the two units of a CICM/CICM-EM pair.
- **Primary NTP:** The primary NTP server IP address provisioned for NE.
- **Secondary NTP:** The secondary NTP server IP address provisioned for NE.
- (Load Info) **Server IP:** The IP address of the server (SDM) containing the CICM software load.
- (Load Info) **Path:** The server's directory that contains the CICM software load.
- (Load Info) **Load:** The file name of the CICM Linux bootstrap, distributed with the boot server.
- (Load Info) **Disk Image:** The file name of the CICM software load, distributed with the boot server.
- **FW Flash Enable:** Check this box to enable firmware flash on the card. Now Disabled.
- (CICM-EM) **Primary EM IP:** The IP address of the primary CICM-EM, for CICM only.
- (CICM-EM) **Backup EM IP:** The IP address of the backup CICM-EM, for CICM only.

QYANG-1 Slot 12 CardView@47.153.146.202 (CM CLLI: UNKNOWN)

File View

QYANG-1 : Slot 12

Alarms Equip States Provisioning

General

IP: 12.12.12.12 Router IP: 12.12.12.1

Subnet Mask: 255.255.255.0 FW Version: Not Reported

MAC Address: 123456789012 Instance ID: 003

Unit ID: A

NTP

Primary NTP: 47.140.160.113

Secondary NTP: 47.140.160.114

CICM-EM

Primary EM IP: 12.12.12.8

Backup EM IP: 12.12.12.9

Load Info

Server IP: 47.131.125.1

Path: /swd/storm

Load: pxelinux.1

Disk Image: CC699123

☐ FW Flash Enable

Modify Save Clear Cancel Details... Help

Provisioning Rules

Two CICM/CICM-EM cards (card A and B) form a pair to provide redundancy. When provisioning a mated pair of CICM cards, the user can provision the cards in either order. For example, “CICM-110-A” and “CICM-110-B” form a CICM pair.

There is no existing relationship between the IP addresses of the CICM/CICM-EM pair. And there are no active and inactive IP addresses (like the GWC) for CICM card.

Some provision information, including load info, subnet, router, and EM address, should be the same between the CICM/CICM-EM pair. But it is not

mandatory. If the craftsperson provides different datafill, the SAM21 EM will prompt a warning message for confirmation.

The CICM/CICM-EM Provisioning Panel verifies the following provisioning rules:

- At most two CICM/CICM-EM cards can be provisioned with the same instance ID, each CICM/CICM-EM pair has a unique instance ID.
- Each MAC address of a CICM/CICM-EM card must be unique among all the cards on SAM21 shelf.

When the user changes the datafill for an existing CICM card, the SAM21 EM performs the change and then displays the following message to the user: “The datafill for this CICM card has been changed. Please ensure that the card’s mate uses the same datafill.”

Maintenance Behavior

This section considers the behavior the user should see when the user attempts a maintenance action on a card provisioned with the CICM service.

- If the user attempts to lock the inactive CICM card, the SAM21 EM immediately attempts to lock the card.
- If the user attempts to lock the active CICM card, the SAM21 EM client displays the following message: “WARNING: This is the active CICM unit. Locking the active unit will cause a service outage. Contact next level NT support before continuing. Do you wish to proceed with the lock?” If the user clicks “Yes”, then the SAM21 EM immediately attempts to lock the card.
- If the user attempts to unassign service to an CICM card, the SAM21 EM client displays the following message: “WARNING: Unassigning service to the card in slot x decommissions one of the processor units of CICM node. Do you wish to proceed?”. If the user clicks “Yes”, then the SAM21 EM unassigns service.

Card Replacement

Firstly the user removes a CICM/CICM-EM card from SAM21 EM shelf. Then a card is inserted into the same slot, it will be auto-provisioned with the same provisioning data as the previous card in that slot, so the MAC address will be the old MAC.

Several scenarios are described here:

- If the craftsperson reseated the same card, he needn’t to take further action.
- If the craftsperson replaces the card with a different one, then he needs to reprovision its MAC address. If the craftsperson doesn’t reprovision the MAC address, the card will fail to boot.

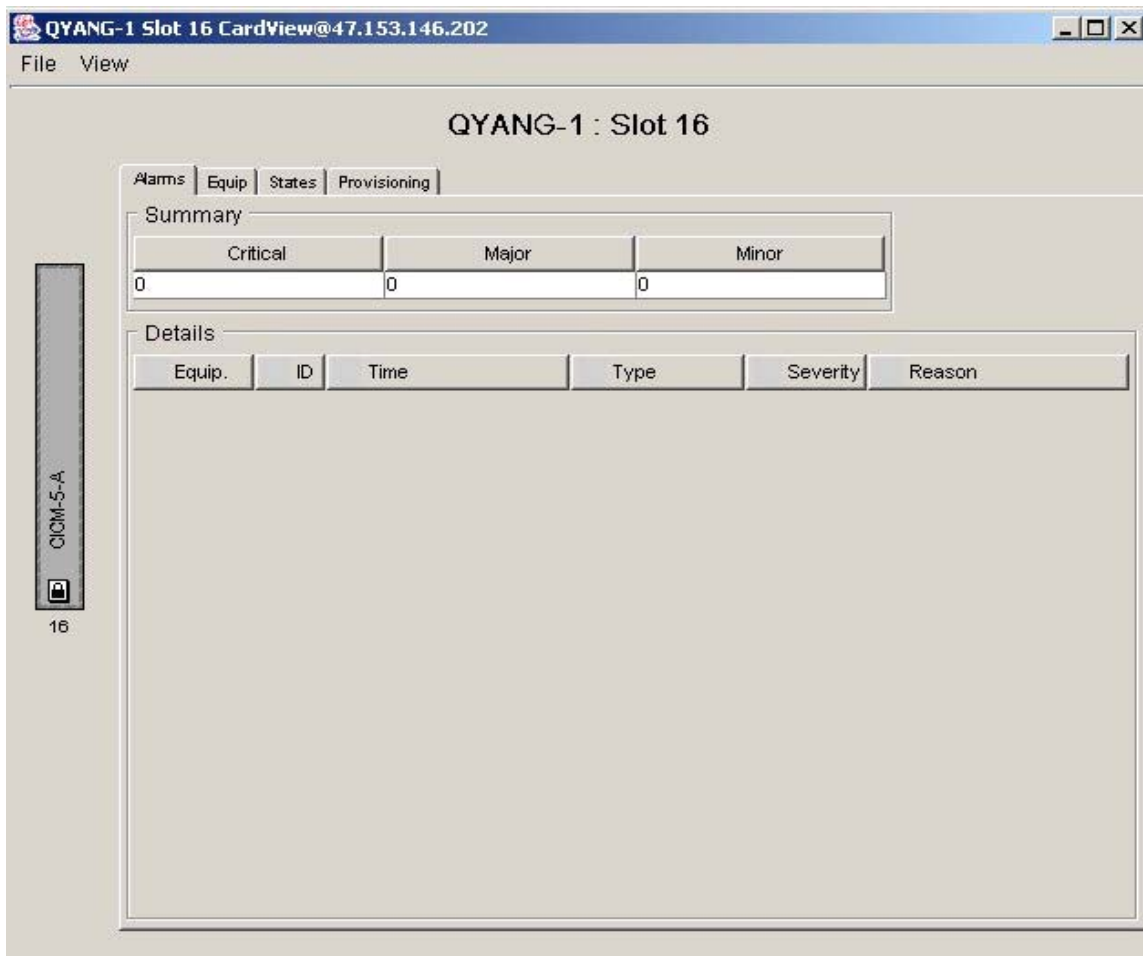
- If the craftsperson exchanges two cards in the same shelf or from different shelves, for example, card A in slot 1, card B in slot 2. After exchange, card A is in slot 2, card B is in slot 1. Card A will be auto-provisioned as card B, card B auto-provisioned as card A. If the user does not reprovision them accordingly, the two cards will not work properly after booted.

The craftsperson must reprovision the MAC address after card replacement. It is recommended that when replace the card with a different one the user unassigns service from CICM card before removal.

If the craftsperson wants to reinsert a CICM card into a different slot, he must reprovision its MAC address to a dummy one, such as “aaaaaaaaaaaa” before removal, then he can insert it into another slot. Otherwise, he will get an error message stating that the mac address has been reserved by the previous slot. It is recommended that when move the card to another slot the user unassigns service before removal.

Card View

Out-of-Service Diagnostics (OOS Diags) for the CICM hardware is not supported in SN07. So the diagnostics tab will not appear on CICM card view. A picture of the CICM Card View follows.



Popup Menu for CICM card

Firmware flash for the CICM hardware is not supported in SN07. When the user right-clicks on the CICM card item on the shelf view, a popup menu will appear, but the "firmware flash" menu item is disabled.

A picture of the CICM Card popup menu follows.



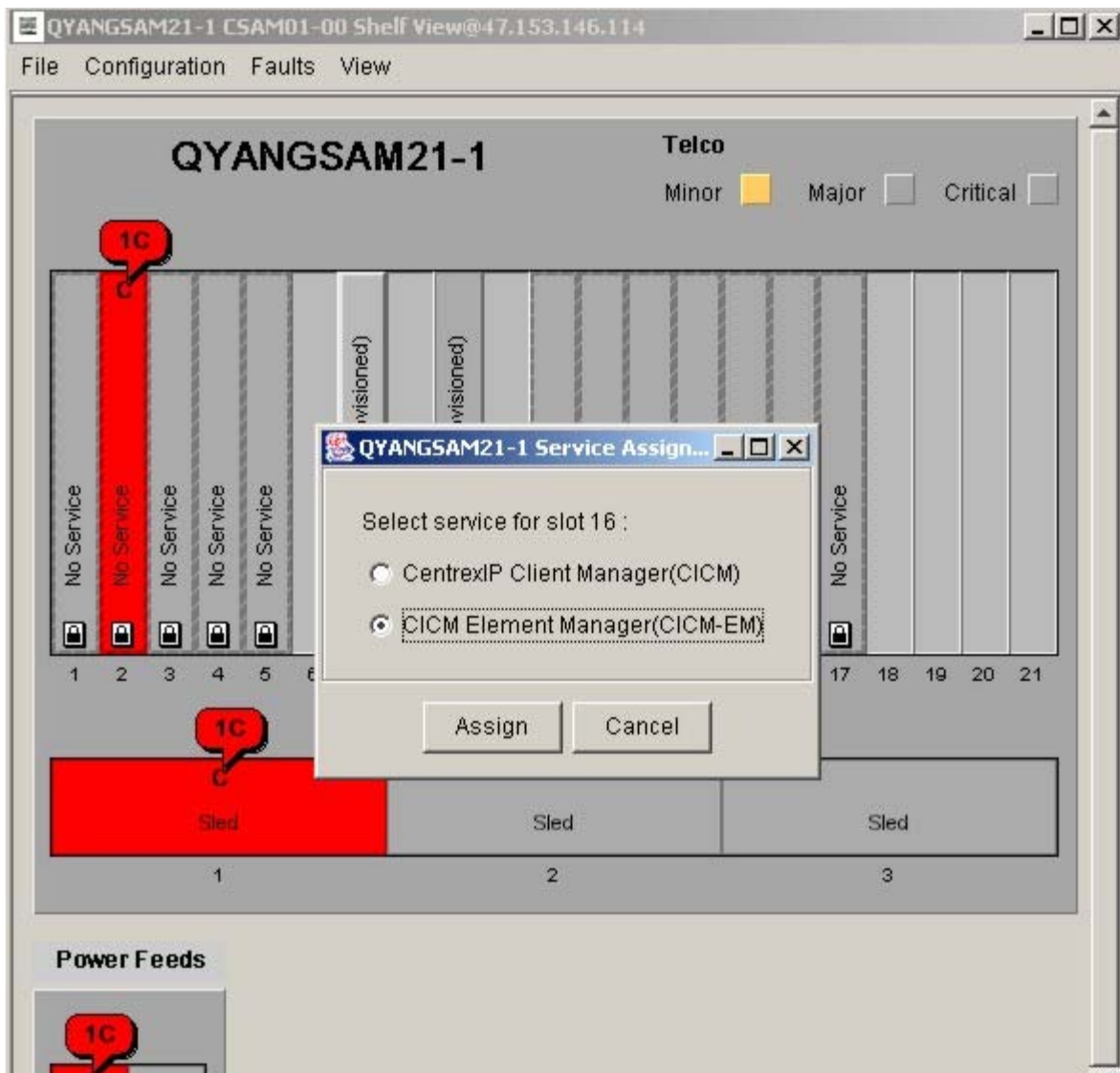
Provision C1CM-EM Service On a MCPN5385 card

The C1CM-EM is different from C1CM card on its provisioning panel. The other aspects, such as maintenance, provisioning rules, etc., is the same as C1CM card.

Assign Service

When the user selects “Assign Service...” on a MCPN5385 card, the SAM21 EM displays the Service Assignment popup window.

The C1CM-EM service can be assigned to a MCPN5385 card.



When the user selects the listed “CICM-EM” service and then clicks “Assign”, the SAM21 EM displays a CICM-EM service provisioning panel.

CICM-EM Provisioning Panel

The CICM-EM Provisioning Panel displays the following fields. Fields in *italics* are automatically filled in for the user. A picture of the CICM-EM Provisioning Panel follows.

- **IP:** The IP address of the MCPN5385 card.
- **Router IP:** The IP address of the card’s router.
- **Subnet Mask:** The card’s subnet mask.

- **FW Version:** The card's firmware version, will be set to "Not reported" by shelf controller.
- **MAC Address:** The MAC addresses of the MCPN5385 card, need manual input.
- **Instance ID:** The instance integer identifier of the CICM-EM card
- **UNIT ID:** 'A' or 'B', identifies the two units of a CICM/CICM-EM pair.
- **Primary NTP:** The primary NTP server IP address provisioned for NE.
- **Secondary NTP:** The secondary NTP server IP address provisioned for NE.
- (Load Info) **Server IP:** The IP address of the server (SDM) containing the CICM-EM software load.
- (Load Info) **Path:** The server's directory that contains the CICM-EM software load.
- (Load Info) **Load:** The file name of the CICM-EM Linux bootstrap, distributed with the boot server.
- (Load Info) **Disk Image:** The file name of the CICM-EM software load, distributed with the boot server.
- **FW Flash Enable:** Check this box to enable firmware flash on the card. Now not supported.

QYANG-1 Slot 13 CardView@47.153.146.202 (CM CLI: UNKNOWN)

File View

QYANG-1 : Slot 13

Alarms Equip States Provisioning

General

IP: 13.13.13.13 Router IP: 13.13.13.1

Subnet Mask: 255.255.255.0 FW Version: Not Reported

MAC Address: 123456789013 Instance ID: 003

Unit ID: A

NTP

Primary NTP: 47.140.160.113

Secondary NTP: 47.140.160.114

Load Info

Server IP: 47.131.125.1

Path: /swd/storm

Load: pxelinux.1

Disk Image: CE678901

☐ FW Flash Enable

Modify Save Clear Cancel Details... Help

CICMEM-003-A

13

Glossary

Acronym	Definition
EM	Element Manager
CICM	CentrexIP Client Manager
CICM-EM	CentrexIP Client Manager's Element Manager
SAM	Service Application Module
SC	Shelf Controller
SDM	Succession Data Manager

SSPFS

Succession Server Platform Foundation Software

GWC

Gateway Controller

Product = CS2000

A00003568 -- CICM ECS Location Identification (UA-IP, IAC, IAW)

Functional Description (FN)

Nortel Networks is expanding its Emergency Call Services (ECS) to handle mobility of Internet Protocol (IP) telephony clients in a Voice over IP (VoIP) Enterprise environment. To provide this capability, enhancements to existing network components are required.

Scope

This document covers the Centrex IP Client Manager (CICM) ECS Location Identification reporting solution. The Location Identification information may also be used for purposes other than ECS.

This functionality is not applicable to the Time Division Multiplexing (TDM) CICM product.

Description

For fixed lines, either in a traditional TDM network or a line connected to an analogue line gateway, the location of the line, for Emergency Call Services (ECS), can be determined using the Calling Line Identity (CLI). Information from region's telecommunications providers would be required to associate a CLI with a location. As the lines are of fixed location the ECS call routing is statically configured as well.

For CICM telephony clients the location of a user is not fixed. Unistim terminals, in an Enterprise, connecting to the Call Server 2000 (CS2K) via the CICM are not statically configured against a particular node in the network topology and their physical location may be anywhere in the Enterprise.

We have implemented a solution where the location information is configured in, and provided by, the Dynamic Host Configuration Protocol (DHCP) server. When the CICM telephony client registers with the DHCP server it can request the Location Identification information options. If available, the DHCP server will return the location information to the set. The CICM gateway may then request the location information from the CICM telephony client at any time and report the location information, via H.248, to the GWC. If configured, an

application running on the Gateway Controller (GWC) re-packages the information and reports it to a Location Recipient application.

The solution also supports the reporting of user defined location identification. This is required for CICM telephony soft clients on networks with DHCP servers that do not support the new location identification DHCP options.

The Location Recipient is outside the scope of this activity.

This solution reports the necessary information to support the Enterprise ECS solution. This solution uses a Location Information Server (LIS) to provide the physical location information. The ECS correlates the LIS information with the client information using IP addresses and MAC address. Please refer to reference [3] for more details.

The mechanism for reporting CICM telephony client location information can also be employed to report the client's location, unique network id (unid), within the network topology. This is required for location/network based policy services:

- Correctly inserting the media portal to traverse NAT devices
- Admissions control

Reference Network

“CICM Carrier ECS solution reference network” on page 1045 shows an example network configuration. It shows an enterprise with a large central campus and several locations.

The following table describes each of the locations shown, how they are connected to the carrier network and the DHCP capabilities provided on site.

Network Locations

Site	Description	Connectivity to carrier	DHCP capabilities
A1	Central campus	Direct connection to carrier network via NAT.	On site DHCP server supporting multiple scopes and vendor options.
A2	Secondary campus	Via limited bandwidth link to central campus.	On site DHCP server supporting multiple scopes and vendor options.
A3	Satellite office	Via limited bandwidth link to secondary campus.	DHCP is relayed to server on secondary campus
A4	Remote branch office	Hardware VPN device provides access to central campus over a limited bandwidth link into the internet.	VPN device provides DHCP for site – no support for vendor options.
A5	Home user	Dialup or software VPN over the internet to enterprise RAS/VPN.	None – RAS/VPN provides IP address.

The distinction between sites A4 and A5 is that site A4 is a “known” location, but A5 is a site that is being used for temporary access to the enterprise (e.g. home or hotel).

The DHCP servers in the enterprise are configured with the Location and UNID for each scope it supports. For example, consider a CICM telephony client on the ground floor in the Central Campus building. The DHCP server is configured with the location of CEN GF and UNID of 31 for this scope. The CICM telephony client may request the DHCP vendor option X to retrieve the configured location and unid.

Note: Option X refers to the IETF GEOPRIV working group civil and geographic location identification DHCP options. Please refer to references [1] and [2].

“[CICM Carrier ECS solution reference network](#)” on page 1045 also shows the ‘default’ location identification information configured on the CICM. This is configured against a network domain profile. If a user logs in from CICM telephony client that cannot provide the location identification information, e.g. from site A4 or A5, the default location identification information is used for the client.

Enterprise ECS solution

For completeness, a description of the Enterprise ECS solution will be outlined and how the CICM ECS Location Identification reporting functionality introduced by this activity meets its requirements.

Please refer to reference [3].

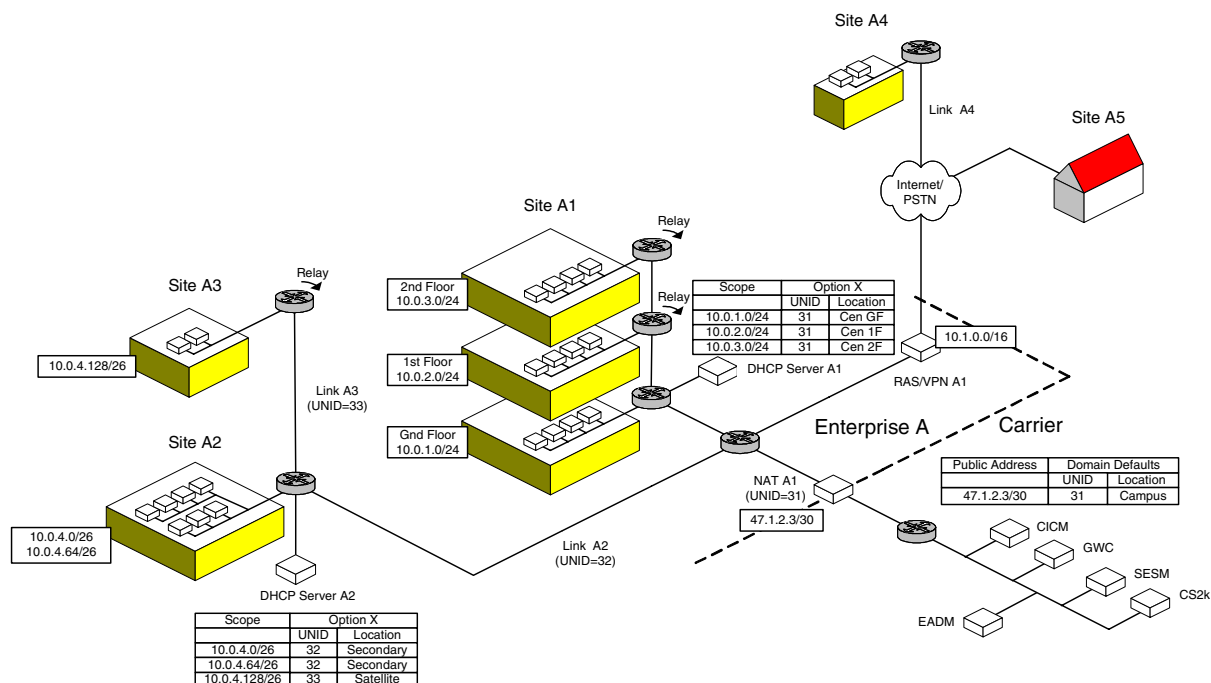
“[Enterprise ECS solution reference network](#)” on page 1046 gives an example of the network configuration for the Enterprise ECS solution.

In the Enterprise ECS solution the Location Identification information is not configured as options in the DHCP servers. Instead the Location Information Service (LIS) gathers etherswitch/port-to-IP/MAC address associations for all devices connected to the network. The LIS performs this function by gathering information from routers and etherswitches. The LIS forwards the information onto the Emergency Application/Data Manager (EADM).

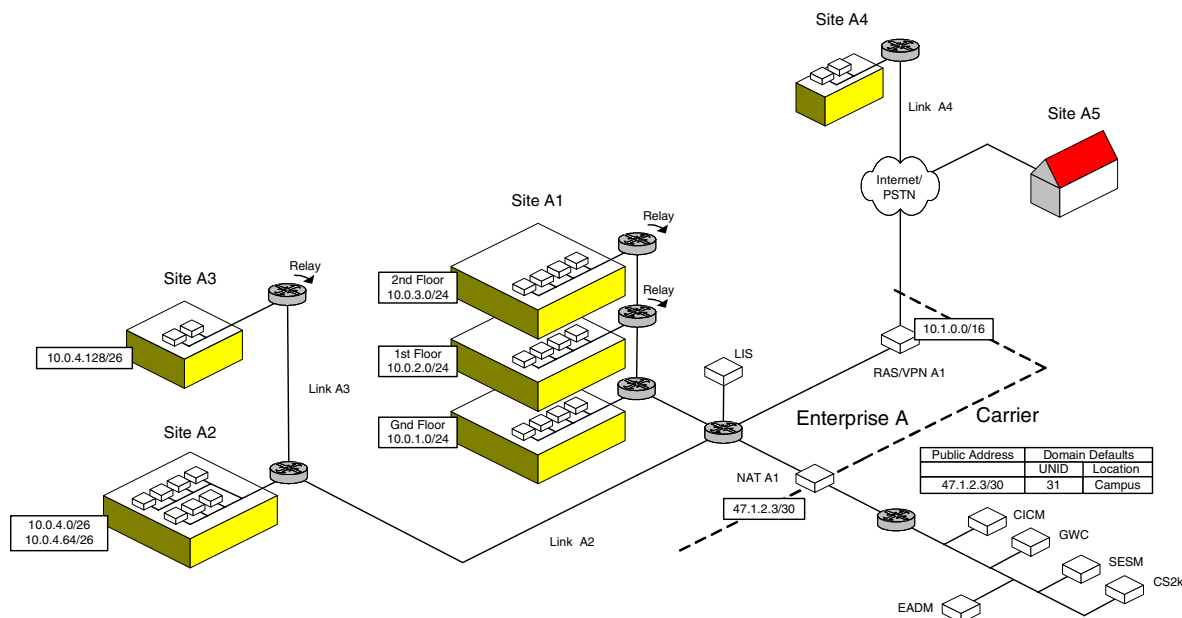
The EADM determines how emergency calls from telephony clients should be handled and sends this information to the Call Server. To accomplish this, the EADM correlates data from the LIS and the telephony client controller and uses its own network topology data to determine what emergency call handling information to send to the Call Server. In addition, the EADM handles Emergency Response Location (ERL) management and Automatic Location Identification (ALI) entry updates to the ALI Database.

In the CICM ECS Location Identification solution the EADM receives the Location Identification information the gateway controller, e.g. the GWC, not the telephony client controller, e.g. the CICM. Included in the Location Identification information reported by the GWC to the EADM are the telephony client's public IP address, private IP address, MAC address and a way to uniquely identify the client on the Call Server. The EADM correlates this information with the information from the LIS. The EADM can then update the call server with emergency call routing for the telephony client and decide whether to use the Location Identification information reported by the GWC or use Location Identification information from its own database.

CICM Carrier ECS solution reference network



Enterprise ECS solution reference network



Operation overview

The CICM ECS Location Identification solution allows location identification information to be configured at the network level and reported through the network, ultimately being reported to an ECS application. Each component can process the information as required, e.g. the GWC uses the UNID in call processing for NAT traversal.

[“Propagation of Location Identification information during user registration \(Client to CICM\)”](#) on page 1048 and [“Propagation of Location Identification information during user registration \(CICM to Location Recipient\)”](#) on page 1049 show how the Location Identification information is requested and reported through the network when a user logs in to a CICM telephony client.

The CICM can specify which Location Identification parameters are required, e.g. civil location descriptor, geographic location descriptor and unique network id.

The CICM telephony client requests the Location Identification options from the DHCP Server. The DHCP Server may have none or only some of the options configured. Only the configured Location Identification options will be returned by the DHCP Server to the CICM telephony client.

In the case of the CICM telephony soft client the user can define the location identification as part of the login interface.

If a Location Identification options is requested by the CISM but not made available by the DHCP Server the CISM telephony client will respond to the CISM with the appropriate Unistim command containing no information.

The CISM will always request the MAC Address from the CISM telephony client.

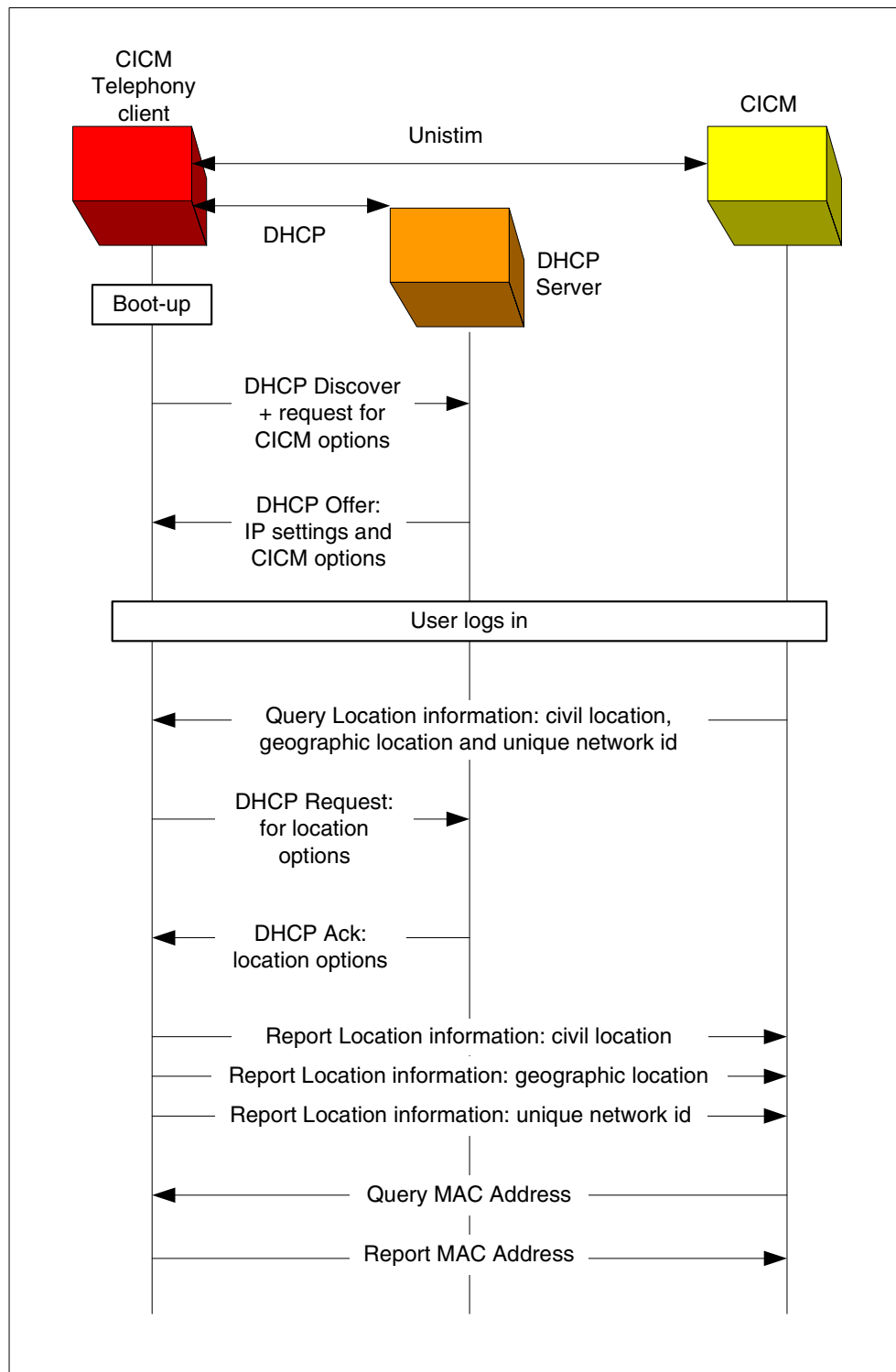
Once all of the Location Identification information has been collected from the CISM telephony client the CISM registers the successful user login with the GWC via a H.248 location change event of the terminal location package.

The GWC uses this event to trigger an audit of the H.248 location identification package for the termination, to collect the Location Identification information.

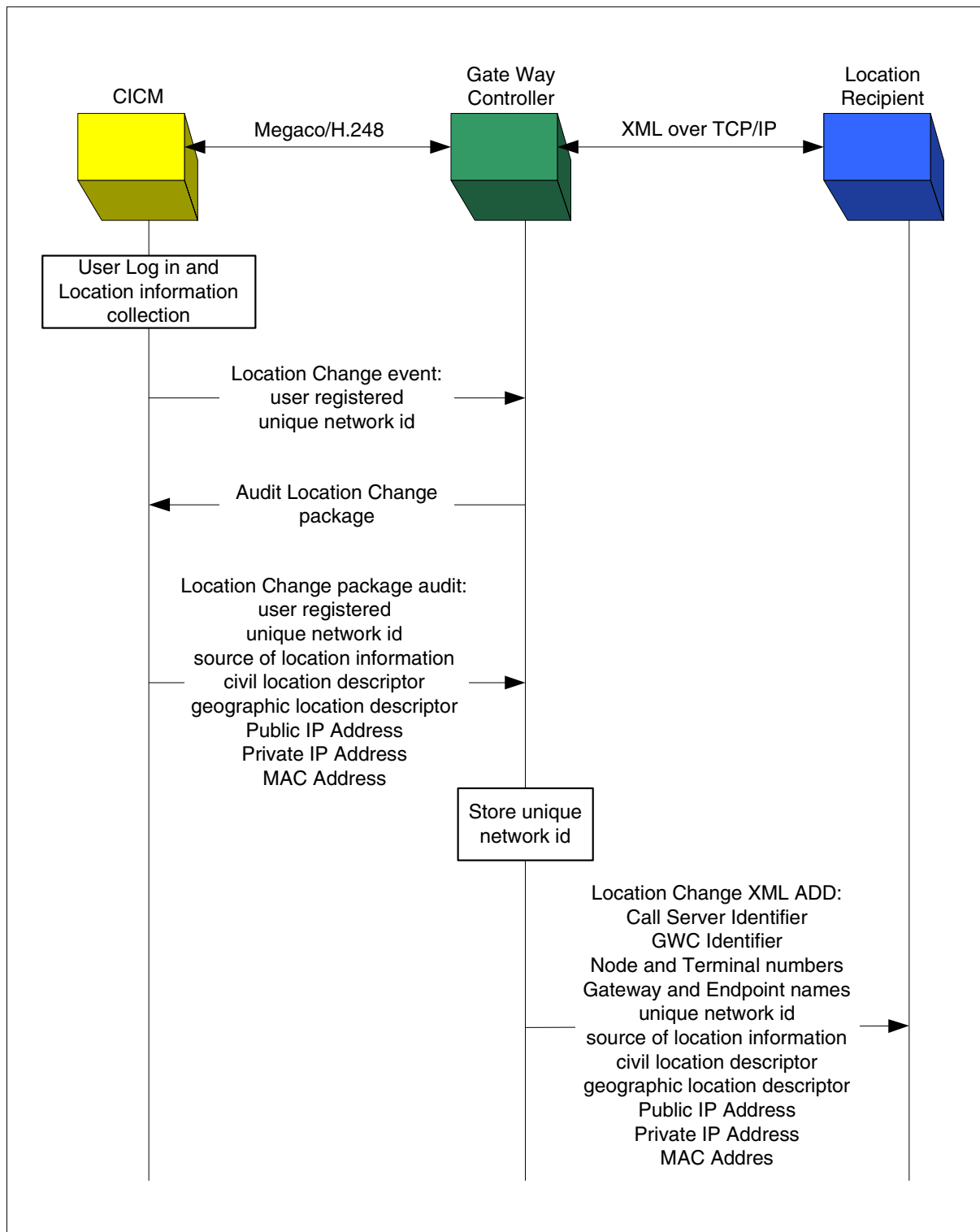
The CISM responds to the audit with an H.248 audit message for the termination containing all the available Location Identification information.

The GWC uses the Unique Network Id for call processing and so stores the value internally. The GWC uses the Location Identification information received from CISM for the termination to build a Location Change XML structure to send to the Location Recipient application.

The Location Change XML structure is sent to the Location Recipient application over a TCP/IP connection that the GWC maintains.

Propagation of Location Identification information during user registration (Client to CICM)

Propagation of Location Identification information during user registration (CICM to Location Recipient)



Interfaces

The following sections describe how the location identification information is reported from the CICM telephony client through the network.

DHCP

The CICM telephony client requests the Location Identification information from the DHCP server. This is achieved by implementing the IETF GEOPRIV working group DHCP options for civil and geographic location identification. Please refer to references [1] and [2].

The DHCP option numbers are TBD.

The DHCP options will be requested from the DHCP server in a DHCP request. The DHCP server will respond with a DHCP acknowledge, containing all the requested options that are configured against the scope.

Unistim

Unistim (Unified Networks IP Stimulus) is a Nortel Networks defined protocol for Internet Terminals (IP phones) used for VoIP (Voice over Internet Protocol) telephony services.

The information required for the ECS location identification solutions is:

- Public IP Address
- Private IP Address
- MAC Address
- Civil Location description
- Geographic Location description
- Unique Network Id

The Public and Private IP Addresses are required for the CICM to manage a telephony client and so are already reported to the CICM prior to this activity.

This activity implemented Unistim commands to request and report the following information.

- MAC Address
- Civil Location description
- Geographic Location description
- Unique Network Id

Requesting the MAC Address

A CICM telephony client's MAC address is required because it is reported to the GWC along with other location identification information by the CICM.

Prior to this activity the i2004 happens to provide the terminal MAC address as part of the unique hardware id in the Internet Terminal (IT) to Network Intelligence (NI) Hardware ID Basic Command in response to the Basic Manager Query (H/W Id). However, the unique hardware id provided by CICM soft client (M3650) does not contain the terminal MAC address. Therefore a new MAC address specific request command was necessary. The Unistim Query MAC Address command from CICM does not have any parameters.

The Query MAC Address is introduced as a NI to IT command for the Basic Manager.

Query MAC Address (0F XX)

7	6	5	4	3	2	1	0
SOURCE		RESERVED	ADDRESS				
LENGTH							
COMMAND							

1st Byte; Command header:

- Source = 0 (originated by NI)
- Address = 0x1A (Basic Manager)

2nd Byte; Length:

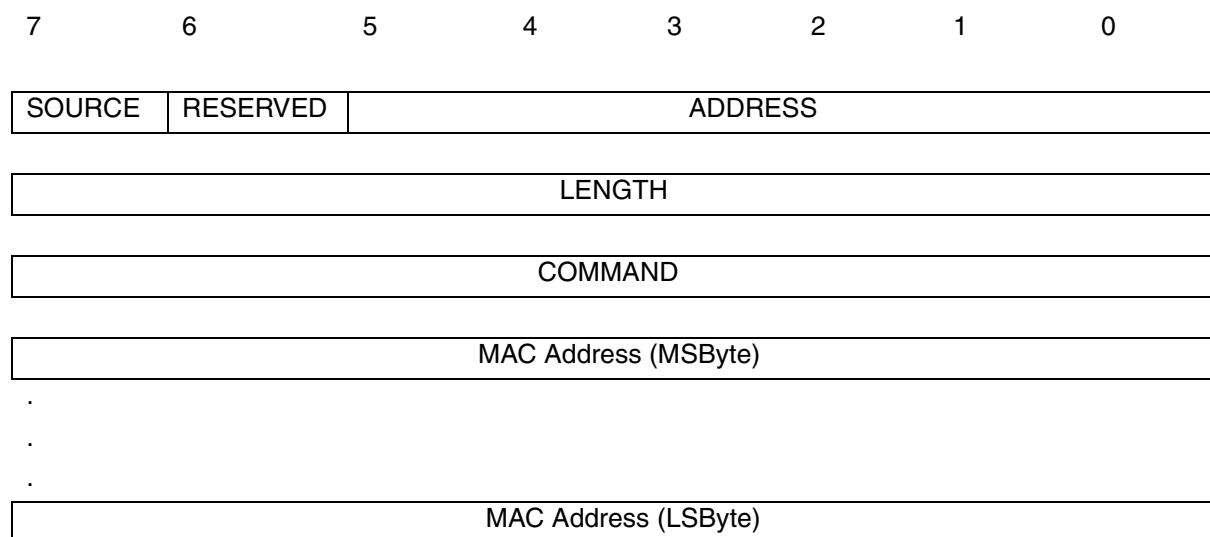
- Length = 0x03 (3 bytes)

3rd Byte; Command contents:

- Command = 0x0F (Query MAC address)

Reporting the MAC Address

The CICM telephony client responds to the 'query MAC' command with a 'MAC information report' command containing the clients MAC address. This is a new 'IT to NI' command for the Basic Manager.

MAC Information report (10 XX XX XX .. XX)

1st Byte; Command header:

- Source = 1 (originated by IT)
- Address = 0x1A (Basic Manager)

2nd Byte; Length:

- Length = 0x09 (9-Bytes, 3-Byte header + 6-Byte MAC address)

3rd Byte; Command contents:

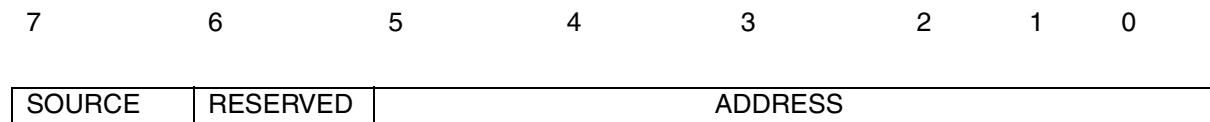
- Command = 0x10 (MAC Address report)

4th Byte; Command contents: MAC Address (MSByte)

9th Byte; Command contents: MAC Address (LSByte)

Requesting the Location Identification information

To request the Location Identification information from the telephony client the CICM sends a new Unistim 'query location' command. Within the command the CICM can specify which location identification parameters are required, i.e. unique network id, civil location description and geographic location description. The Query Location Unistim command is a new 'NI to IT' command for the Basic Manager.

Query Location (0E XX)

LENGTH							
COMMAND							
RESERVED	RESERVED	RESERVED	RESERVED	RESERVED	GLOC	LOC	UNID

1st Byte; Command header:

- Source = 0 (originated by NI)
- Address = 0x1A (Basic Manager)

2nd Byte; Length:

- Length = 0x04 (4 bytes)

3rd Byte; Command contents:

- Command = 0x0E (Query Location)

4th Byte; Command contents: indicates which information is being requested

- UNID = 1 if Unique Network Id is required, otherwise UNID = 0
- LOC = 1 if Location descriptor is required, otherwise LOC = 0
- GLOC = 1 if the Geographical Location descriptor is required, otherwise GLOC = 0

Reporting the Location Identification information

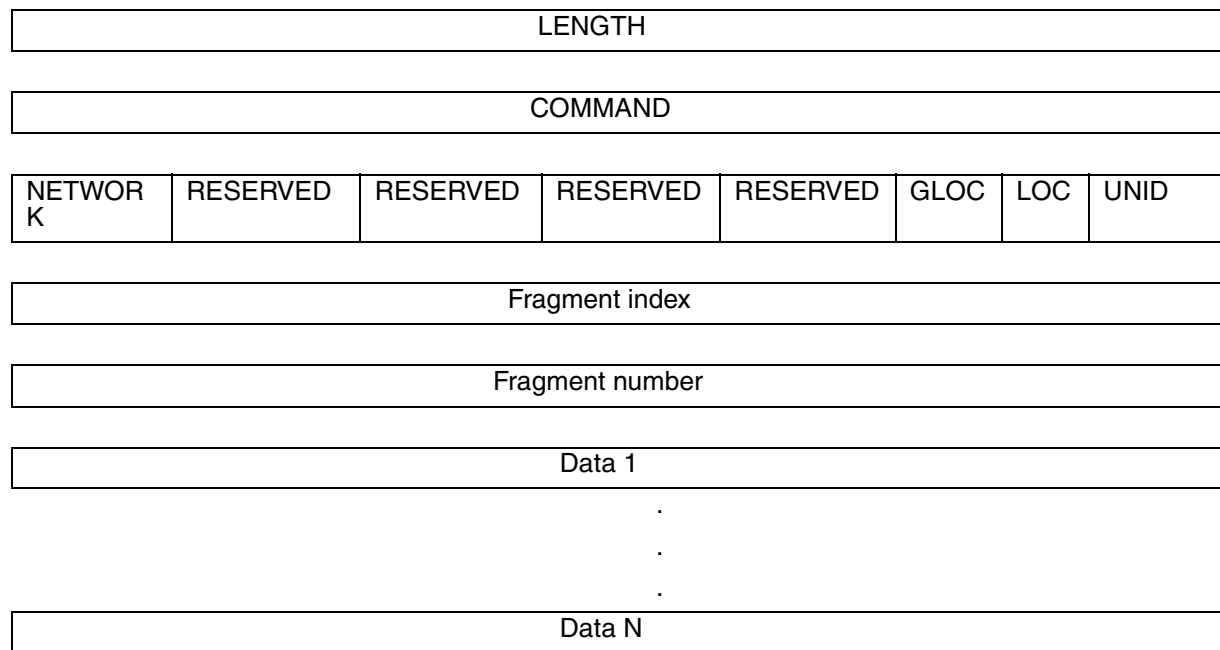
The CICM telephony client responds to the 'query location' command with a separate 'location information report' command for each requested parameter. This command includes fields for the parameter id, length and value.

The location descriptor may too large to fit into a single Unistim command, maximum length is 255-bytes, therefore the 'location information report' message supports fragmentation. In the case where the location descriptor is larger than the maximum size to fit into a single Unistim 'Location Information report' command the telephony client will fragment the location descriptor and the CICM will rebuild the location descriptor.

The Location Information report Unistim command is a new 'IT to NI' command for the Basic Manager.

Location Information report (0F XX XX XX .. XX)

7	6	5	4	3	2	1	0
SOURCE		RESERVED		ADDRESS			



1st Byte; Command header:

- Source = 1 (originated by IT)
- Address = 0x1A (Basic Manager)

2nd Byte; Length:

- Length = variable

3rd Byte; Command contents:

- Command = 0x0F (Location Information report)

4th Byte; Command contents: indicates which information is being report, either:

- UNID = 1 if Unique Network Id is reporting in this command; LOC and GLOC must equal 0
- LOC = 1 if Location descriptor is reporting in this command; UNID and GLOC must equal 0
- GLOC = 1 if geographic location descriptor is reporting in this command; UNID and LOC must equal 0
- NETWORK = 1 if the location information is provided by the network. If NETWORK = 0, the location information has been provided by the user.

Note: For the UNID, NETWORK must always be 1.

Note: Location Identification information reported by an i200x etherset will always have NETWORK equal to 1.

Note: NETWORK can only equal to 0 for the Location Identification information reported by the CICM telephony soft client if the DHCP server did not provide Location Identification information.

5th Byte; Command contents:

- Fragment index – the index of the command within the fragmented command

6th Byte; Command contents:

- Fragment Number – the total number of fragments required to report the location identification data.

7th Byte; Command contents:

- Data 1 – first byte of the Location Information data.

Nth Byte; Command contents

- Data N – last byte of the Location Information data.

Note: The Unique Network Id (UNID) is always 4-Bytes, therefore the Unistim UNID Location Information report command has Length of 7, Fragment index of 1 and Fragment Number of 1.

Note: If the Location Descriptor is less than 249-Bytes (maximum command size minus Unistim Location Information report command header, e.g. 255-bytes – 6-bytes) then the Fragment index is 1 and Fragment Number is 1

If a parameter is requested but not available, e.g. was not provided by the DHCP server, then the terminal responds with a 'location information report' message for the parameter specifying a Length of 6, i.e. the Unistim Location Information report command header with no data.

H.248

Prior to this activity, the location change event of the terminal location H.248 package was implemented to report the Unique Network ID (UNID) for the CICM telephony client from the CICM to the GWC. This event is reported after a user has successfully logged into a client. The reported Unique Network ID is used for network policy services. This event and operation is maintained by this activity. The location change event is used to trigger an audit of the location identification package, which is an extension of the terminal location package.

The location change event contains two parameters:

- reg, a Boolean used to indicate whether the termination is being registered to, or un-registered from, the unique network id (locid).
- locid, a String used to represent the unique network id (locid)

When a user logs in to a CICM telephony client the CICM sends a location change event with reg=true and the locid.

When a user logs out from a CICM telephony client the CICM sends a location change event with reg=false and loc of 0.

Northbound to Location Recipient

The GWC collects the CICM ECS Location Identification information from the CICMs that it controls. The Location Identification information is required by the Location Recipient, the GWC only uses UNID of the ECS Location Identification information. The Location Identification information is reported by the GWC to the Location Recipient in a proprietary XML format. The XML structure is generated from the information received in the H.248 Location Identification package audit message and termination/endpoint information held in the GWC.

The information required by the Location Recipient is given in the following table:

Location Identification parameters

Parameter	XML tag	Description	Format	Example
Call Server Identifier	csid (attribute of LocChange element)	Used to identify the Call Server that provides call processing for the CICM telephony client	String	CS2K_LONDON
GWC Identifier	gwcid (attribute of LocChange element)	Used to identify the Gateway Controller that provides call processing and management for the CICM telephony client	String	GWC-1
Node number	node (attribute of terminal element)	The number the Call Server uses to uniquely identify the CICM node.	Numeric	4
Terminal number	term (attribute of terminal element)	The number the Call Server uses to uniquely identify the CICM telephony client on the node.	Numeric	1
Gateway name	gw (attribute of terminal element)	The name of the gateway, used in the GWC and GWC-EM	String	cicm
Endpoint name	ep (attribute of terminal element)	The name of the endpoint on the gateway, used in the GWC and GWC-EM.	Numeric	1

Unique Network ID	unid	Uniquely identifies the middle-box, NAT or LBL that CICM telephony client network is behind.	Numeric	45
Source of Location Information	src	Whether the location descriptors were provided by the Network, e.g. DHCP Server, or by the User, e.g. the M6359 CICM softclient	String	network
Civil Location Descriptor	civil	The civil location of the CICM telephony client	String	
Geographic Location Descriptor	geo	The geographic location of the CICM telephony client	String	
Public IP Address	pubip	The public IP address of the CICM telephony client	String	
Private IP Address	privip	The private IP address of the CICM telephony client	String	
MAC Address	mac	The MAC address of the CICM telephony client	String	

XML messages

Several XML messages are required to support the reporting of location identification data to the location recipient and to maintain the integrity of the data in the location recipient.

New Location identification data (ADD)

When the GWC receives location identification data from the CICM for a newly registered termination it creates an ADD XML structure and sends it to the location recipient.

The H.248 Location Identification package audit from the CICM does not identify if this is the first time the location identification information is being reported for the termination; therefore the GWC uses an internal flag to indicate whether the location identification information has been successfully reported to the Location Recipient. If the flag is false, an ADD XML message is sent to the Location Recipient containing the Location identification information.

The internal GWC per termination 'location identification' flag is set when the ADD XML message is successfully sent to the Location Recipient.

An example ADD XML structure:

```
<?xml version='1.0'?>
<LocChange csid="CS2K_LONDON" gwcid="GWC-1">
  <ADD>
    <terminal node="4" term="1" gw="cicm" ep="1">
```

```
<unid>45</unid>
<src>network</src>
<civil>xxxxxxxxxxxxxxxxxxxxxxxxxxxx</civil>
<geo>xxxxxxxxxxxx</geo>
<pubip>47.165.168.100:2000</pubip>
<privip>10.0.1.16:5000</privip>
<mac>0E-18-4F-93-AC-01</macc>
</terminal>
</ADD>
<LocChange>
```

Changed Location identification data (CHANGE)

If the GWC receives location identification data from the CICM for a termination that has already successfully reported location identification to the Location Recipient, the GWC generates a CHANGE XML structure and sends it to the location recipient.

An example CHANGE XML structure:

```
<?xml version='1.0'?>
<LocChange csid="CS2K_LONDON" gwcid="GWC-1">
  <CHANGE>
    <terminal node="4" term="1" gw="cicm" ep="1">
      <unid>45</unid>
      <src>network</src>
      <civil>xxxxxxxxxxxxxxxxxxxxxxxxxxxx</civil>
      <geo>xxxxxxxxxxxx</geo>
      <pubip>47.165.168.100:2000</pubip>
      <privip>10.0.1.16:5000</privip>
      <mac>0E-18-4F-93-AC-01</macc>
    </terminal>
  </CHANGE>
</LocChange>
```

Remove Location Identification data (REMOVE)

When a user logs out of a CICM telephony client the location identification information is no longer required or reliable. The CICM reports the user log out in a H.248 location change event. When the GWC receives this event it resets the stored unique network id and sends a 'remove' XML structure to the location recipient to indicate that the location identification information for the termination/endpoint is no longer valid.

An example REMOVE XML structure:

```
<?xml version='1.0'?>
<LocChange csid="CS2K_LONDON" gwcid="GWC-1">
  <REMOVE>
    <terminal node="4" term="1" gw="cicm" ep="1">
    </terminal>
  </REMOVE>
</LocChange>
```

The internal GWC 'location identification' flag is reset so that any subsequent location identification information received from the CICM is treated as new information.

Synchronize Location Identification data (SYNC)

The location recipient sends this message when it requires the location data to be synchronized.

An example SYNC XML structure:

```
<?xml version='1.0'?>
  <LocChange>
    <SYNC/>
  </LocChange>
```

On receipt of the synchronize message the GWC recovers the Location Identification information for every termination by auditing the Location Identification package for every registered CICM telephony client termination. For unregistered endpoints a REMOVE message will be sent to the location recipient.

Connection Keep-alive (KEEPALIVE)

The TCP/IP connection established by the GWC has a time-out, e.g. if no data is sent over the connection for 2 hours the GWC drops the connection. To prevent the connection from being dropped due to this timeout a timer is used.

If the timer reaches a predefined time, e.g. 1 hour, the GWC sends a 'keep alive' XML structure to the Location Recipient to keep the connection alive. The timer is reset each time data is sent on the connection. The location recipient will ignore the 'keep alive' XML structure.

An example KEEPALIVE XML structure:

```
<?xml version='1.0'?>
  <LocChange csid="CS2K_LONDON" gwcid="GWC-1">>
    <KEEPALIVE/>
  </LocChange>
```

Connection status message (STATUS)

The location recipient sends this message to check that the connection is still active.

An example STATUS XML structure:

```
<?xml version='1.0'?>
  <LocChange>
    <STATUS/>
  </LocChange>
```

The STATUS message will be ignored by the Location Identification application on the GWC.

SNMP

A new SNMP MIB has been introduced to send the Location Identification configuration from the GWC Element Manager to the GWC. Please refer to ["Appendix x: GWC-LOCATION-CHANGE-REPORTING-MIB"](#) on page 1075.

Logs and Alarms

This feature introduces a new alarm and corresponding log.

Alarm Signals

Alarm condition	Alarm signal	NEW/CHANGED/DELETED/RELOCATED
Unable to establish a connection to Location Recipient.	GWC 314	NEW

An example of the GWC314 log follows.

```
CS2K1 *** GWC314 JUN30 11:02:37 0586 TBL GWC Fault
Location: GWC-213-UNIT-0
NotificationID: 3
State: Raise
Category: Processing Error
Cause: Communications subsystem failure
Time: Jun 30 11:09:58 2004
Component Id: GWC=GWC-213-UNIT-
0;Version=GI070B0;Unit=unit_0;Software=LocIdRep
Specific Problem: Location Id Reporting connection <88.53.45.223> has failed
- attempting recover
Description: Location Id Reporting connection failure
```

Feature Configuration and Activation

There are several places within the Call Server network that require configuring to enable the CICM ECS Location Identification functionality.

DHCP Server

The DHCP Server must be configured with the DHCP options for the GEOPRIV civil location identification, GEOPRIV geographic location identification and unique network id.

Please refer to references [1] and [2].

CICM telephony clients

Ethersets (i200x)

The Etherset (i200x) must be configured to use full or partial DHCP configuration to enable the CICM ECS Location Identification functionality.

The i200x requires firmware level TBD.

Soft client (M6350)

The CICM soft client has been modified to provide the user with an interface to specify their civil location description when logging in.

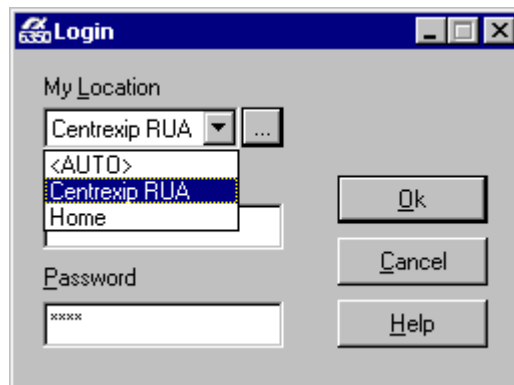
The CICM soft client has also been modified to allow the user to specify automatic server selection. If this is selected the soft client retrieves the CICM and Location Identification options from the DHCP server. Meaning that the user is not required to specify the server address.

The CICM telephony softclient must be at release 7.

Entering location description

The user log in process has been changed so that the user is prompted to enter a location description. An example is given in the following figure:

CICM Soft client login GUI



The GUI may provide a list of previously entered locations, which a user can choose from, or enter a new location. An example is given in the following figure:

CICM Soft client Location edit GUI.

6350 Edit Location

SOME TEXT DESCRIBING THIS DIALOG

Location Shortcut Name: Centrexip RUA

Personal Name (optional): user in the Centre

Company/Dept: nortel networks

MailStop/Office/Cube: centrexip lab

Floor: ground

Building: MOP-3

Address Line 1: Maidenhead Office Park

Address Line 2: Westacott Way

Address Line 3: Maidenhead

Address Line 4:

Postcode/Zip: SL7 9XX

County/State: Berks

Country: United Kingdom

[GPS/MAP]Position: 52 deg N 1deg W

New

Delete

Apply

Cancel

Help

Enabling automatic server selection

An existing part of the soft client login GUI is the 'Server settings' window. In this window the user specifies the server settings to use. Prior to this activity only manual server selection was available, requiring the user to enter the address of the server. A new option has been provided which allows the user to choose 'automatic server selection'. An example is shown in the following figure.

CICM Soft client server settings GUI

Choosing 'automatic server selection' means that the server settings are requested from the DHCP server. The Location identification parameters will be requested as part of the DHCP request.

The civil location descriptor provide by the DHCP server will take precedence over the user defined civil location descriptor.

The CICM soft client reports the location identification information to the CICM when requested.

The soft client can only report the unique network id to the CICM if it was provide by the DHCP server. If the unique network id is requested by the CICM and manual server settings were used, the soft client will response with an empty UNID location information report command.

When reporting the civil and geographic location description to the CICM the soft client indicates whether the information was provided by the network or user defined. This is because a network provided location descriptor might be considered more reliable.

CICM Element Manager

The CICM ECS Location Identification functionality on the CICM is activated via the CICM Element Manager.

The CICM Element Manager always the operator to configure a default civil location description and unique network id against a network domain profile. If a CICM telephony client registers with the CICM, but does not provide either the civil location description or unique network id, the default value is taken from the network domain profile.

GWC Element Manager

The CICM ECS Location Identification functionality on the GWC is activated via the GWC Element Manager GUI.

Configuring the Location Recipient

The destination for the Location Identification information, e.g. the Location Recipient, is configured in the GWC Element Manager. The Location Recipient is configured in the Location Recipient tab of the Network Devices section of the Network panel. The default value for the Location Recipient IP Address and Port number is <not configured>. Refer to the following figure.

To configure the Location Recipient press the change button. This opens to 'Add Location Recipient' window. Refer to [“Add Location Recipient window” on page 1066](#).

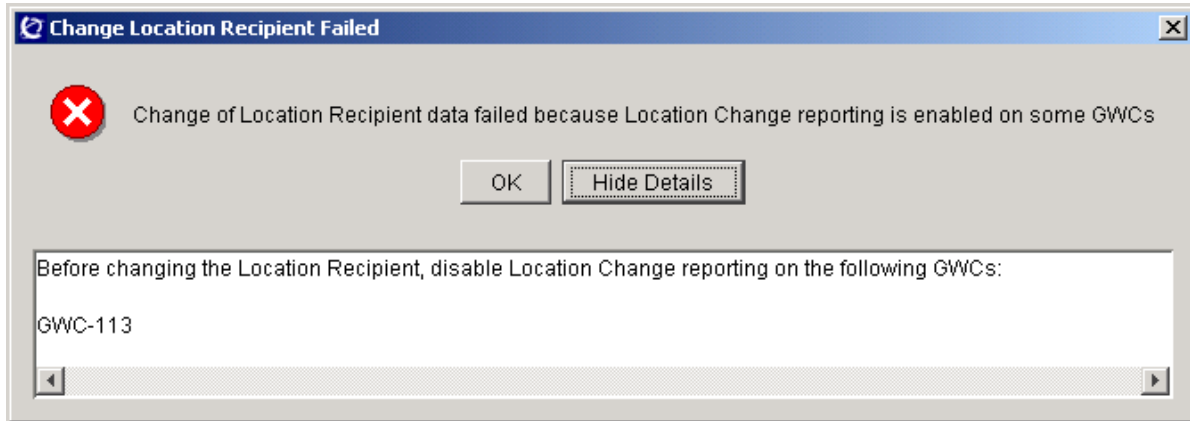
GWC Element Manager Network Panel**Add Location Recipient window**

The format of the IP Address is <0-255>.<0-255>.<0-255>.<0-255> and the format of the port is any number in the range 0 to 65535, the Add Location Recipient window will only allow the user to enter data in the correct format.

Once the data has been entered the OK button is pressed to submit the data.

The Location Recipient values cannot be changed if the Location Recipient is associated with a GWC. The following figure gives an example of the error message.

Change Location Recipient failure window



To unconfigure the Location Recipient the change button is pressed, then in the Add Location Recipient window the reset button is used to enter the default values, e.g. <not configured>, and OK is pressed to submit the data.

Activating the Location Change reporting on the GWC

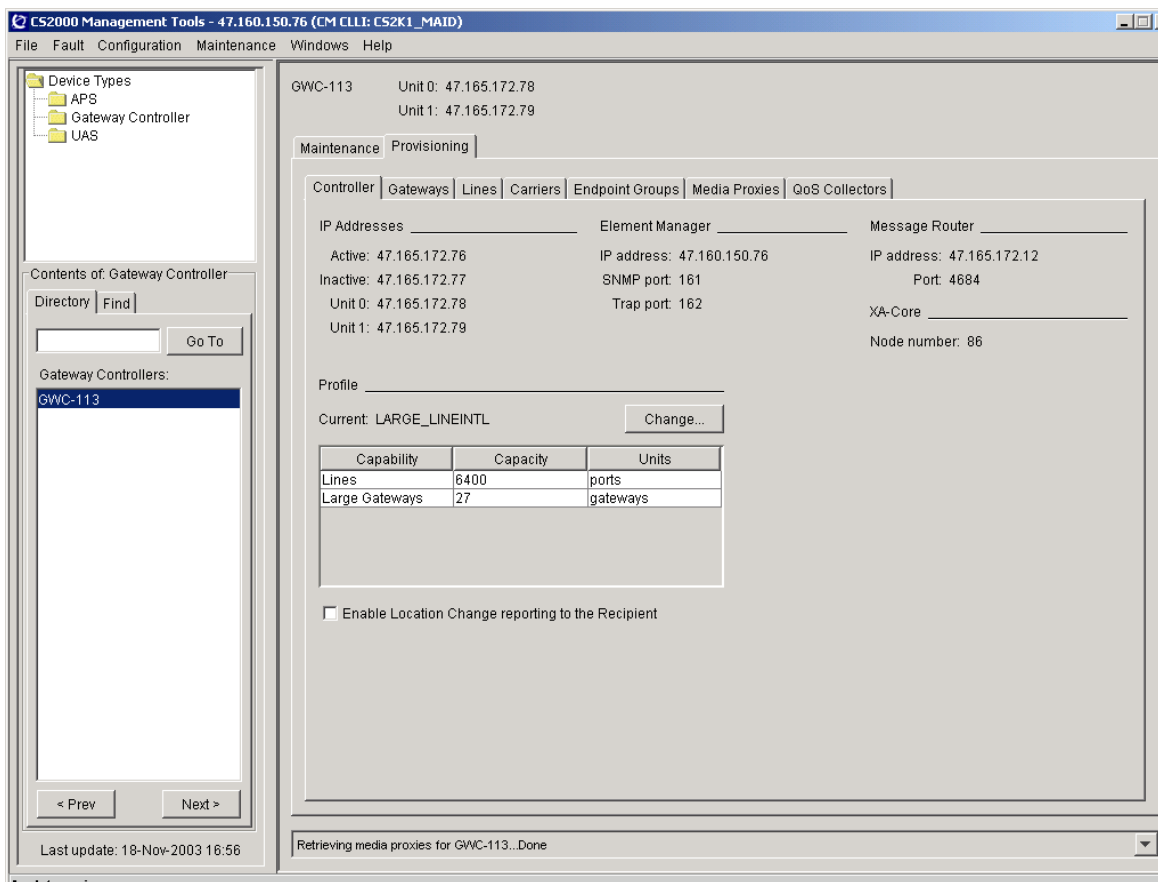
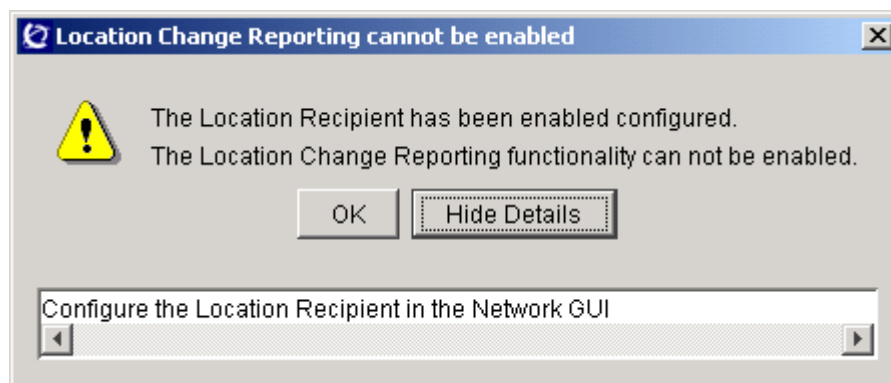
The Location Change reporting from a GWC to the Location Recipient is activated via a checkbox in the GWC controller-provisioning panel. Refer to [“GWC Controller provisioning panel” on page 1068](#).

The checkbox is only available for ‘large line gateway’ GWC profiles.

The checkbox cannot be checked if a Location Recipient has not been configured. Please refer to for an example of the error message.

When the checkbox is checked the GWC Element Manager sends the Location Recipient configuration values to the GWC via SNMP. A ‘status’ parameter is also sent to the GWC, this has the value ‘enabled’.

When the checkbox is unchecked the GWC Element Manager sends the ‘status’ parameter to the GWC, this has the value ‘disabled’.

GWC Controller provisioning panel**Location Change reporting checkbox error****GWC Location Identification reporting application operation**

This section describes the operation of the Location Identification reporting application on the GWC. The application is responsible for:

- Interfacing with the H.248 application, this includes:

- Notification on receiving a H.248 terminal location package location change event for a termination.
 - Sending an audit request on the H.248 location identification package for a termination.
 - Notification on receiving a H.248 location identification package audit.
- Queuing Location Identification information to be sent to the Location Recipient.
- Recovery and auditing of Location Identification information.
- Establishing and maintaining the TCP/IP connection to the Location Recipient.

The Location Identification reporting is enabled for a GWC in the GWC Element Manager. (Refer to section [].)

The GWC Element Manager enables Location Identification reporting on the GWC via SNMP.

When the Location Identification reporting application is enabled it does the following:

- Initializes the queue, recovery and audit mechanisms
- Establishes a TCP/IP connect to the configured Location Recipient

Once the Location Identification reporting application has been initialized it can:

- Accept notifications from the H.248 application
- Send audit requests to H.248 application
- Accept XML from the Location Recipient TCP/IP connection
- Send XML structures to the Location Recipient TCP/IP connection

The operation of the GWC Location Identification reporting application for an initial user login is described in section [].

If the TCP/IP connect cannot be established to the Location Recipient the Location Identification reporting application queues the Location Identification information to be sent. Once the connection is established the queued Location Identification information is processed and sent to the Location Recipient.

If the queue overflows, the recovery indicator is set for the termination. The Location Identification reporting application regularly audits the recovery

indicators for all terminations. If the audit detects a set recovery indicator for a termination it initiates an audit of the H.248 Location Identification package for the termination.

While the TCP/IP connection is not established the Location Identification reporting applications does not use the Location identification information audit/recovery procedures.

The GWC Location Identification reporting applications operates until instructed to stop by the GWC Element Manager.

Hardware requirements

None.

Software Requirements or Dependencies

SESM must be at release 7.
GWC must be at release 7.
CICM must be at release 7.
CICM EM must be at release 7.
CICM soft client must be at release 7.
i200x must be at firmware release TBD.

Limitations and restrictions

To be identified.

Interactions

None.

Glossary

Term	Description
CICM	Centrex IP Client Manager
CLI	Calling Line Identifier
CS2K	Call Server 2000
DHCP	Dynamic Host Configuration Protocol
EADM	Emergency Application & Data Manager
ECS	Emergency Call Services
FN	Functional Description
GEOPRIV	Geographic Location/Privacy
GWC	Gateway Controller
IEFT	Internet Engineering Task Force
IP	Internet Protocol
IT	Internet Terminal

LIS	Location Information Server
NAT	Network Address Translator
NI	Network Intelligence
MAC	Media Access Control
Megaci/H.248	Media Gateway Control
RAS	Remote Access Services
SN07	Succession software release 7
TDM	Time Division Multiplexing
UNID	Unique Network Identifier
Unistim	Unified Networks IP Stimulus Protocol
VoIP	Voice over IP
VPN	Virtual Private Network

References

- [1] draft-ietf-geopriv-dhcp-civil-00.txt, June 27, 2003 -
<http://www.ietf.org/internet-drafts/draft-ietf-geopriv-dhcp-civil-00.txt>
- [2] draft-ietf-geopriv-dhcp-lci-option-02.txt, Aug 21st, 2003 -
<http://www.ietf.org/internet-drafts/draft-ietf-geopriv-dhcp-lci-option-02.txt>
- [3] Enterprise Emergency Call Service Architecture Specification -
http://livelinkott.ca.nortel.com/livelink/livelink.exe/5146119/E911_Architecture_Spec.doc?func=doc.Fetch&nodeid=5146119

Appendices

Appendix x: H.248 Location Identification package description

H.248.x Location Identification Reporting Package

Summary

This document defines a package that provides Termination Location Identification reporting for H.248.

Scope

This document defines a package that provides Termination Location Identification reporting for H.248. The support of this package is optional.

References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references

listed below. A list of the currently valid ITU-T Recommendations is regularly published.

ITU-T Recommendation H.248.1 (05/2002), Gateway Control Protocol
[DHCP Option for Civil Location](#)
[Dynamic Host Configuration Protocol Option for Location Configuration Information for GEOPRIV](#)

Definitions

-

Abbreviations

MG Media Gateway
MGC Media Gateway Controller

Location Identification reporting Package

PackageID: locId (0x00??)

Version: 1

Extends: tl

This package defines Termination Location Identification reporting for IP Terminals.

Properties

Unique Network Id

PropertyID: locid (0x0001)

Description: Reports the Unique Network Id (middle-box id) of an IP Terminal for location identification purposes. This is the unique global id assigned to a middle-box when it is configured in 'CS2000 Management Tools'.

Type: String

Possible Values: Any value of meaning between the MG and MGC. Default value is an empty String.

Defined In: Termination State Descriptor

Characteristics: Read only.

Location

PropertyID: loc (0x0002)

Description: Reports the civil location of an IP Terminal.

Type: String

Possible Values: Format specified in IETF GEOPRIV working group civil location Internet draft, draft-ietf-geopriv-dhcp-civil-00.txt, dated June 27, 2003. Default value is an empty String.

Defined In: Termination State Descriptor

Characteristics: Read only

Geographic Location

PropertyID: gloc (0x0003)

Description: Reports the geographic location of an IP Terminal.

Type: Octet String
Possible Values: Format specified in IETF GEOPRIV working group geographic location Internet draft, draft-ietf-geopriv-dhcp-lci-option-02.txt, dated August 21, 2003. Default value is an empty String.
Defined In: Termination State Descriptor
Characteristics: Read only

Source of Location information

PropertyID: src (0x0004)
Description: Identifies whether the network or the user provided the civil and geographic location information.
Type: Enumeration
Possible Values: Not Applicable (0x0001), Network (0x0002), User (0x0003). Default value is 0x0001. If the civil location (loc) or geographic location (gloc) properties are present then this property must contain a non-default value.
Defined In: Termination State Descriptor
Characteristics: Read only

Public IP Address

PropertyID: pubAddr (0x0005)
Description: Reports the public IP address of an IP Terminal for location identification purposes.
Type: Octet String
Possible Values: Default value is an empty String. If the civil location (loc) or geographic location (gloc) properties are present then this property must contain a non-default value.
Defined In: Termination State Descriptor
Characteristics: Read only

Private IP Address

PropertyID: privAddr (0x0006)
Description: Reports the private IP address of an IP Terminal for location identification purposes.
Type: Octet String
Possible Values: Default value is an empty String. If the civil location (loc) or geographic location (gloc) properties are present then this property must contain a non-default value.
Defined In: Termination State Descriptor
Characteristics: Read only

MAC Address

PropertyID: macAddr (0x0007)
Description: Reports the MAC address of an IP Terminal for location identification purposes.
Type: Octet String.
Possible Values: MAC address encoded in hex. Default value is an empty String. If the civil location (loc) or geographic location (gloc) properties are

present then this property must contain a non-default value.

Defined In: Termination State Descriptor

Characteristics: Read only

Events

Identification Change

EventID: idChg (0x0001)

Description: Reports that location identification information has changed and reports the new location identification property values.

EventsDescriptor parameters:

None

ObservedEventsDescriptor parameters:

Events Parm Name

ParameterID: reg (0x0001)

Type: BOOLEAN

Possible values: TRUE, FALSE

Description: Indicates whether the termination is registering or unregistering terminal location information.

ParameterID: locid (0x0002)

Type: String

Possible values: Any value of meaning between the MG and MGC. Default value is an empty String.

Description: Reports the Unique Network Id (middle-box id) of an IP Terminal for location identification purposes.

ParameterID: loc (0x0003)

Type: String

Possible values: Format specified in IETF GEOPRIV working group civil location Internet draft, draft-ietf-geopriv-dhcp-civil-00.txt, dated June 27, 2003. Default value is an empty String.

Description: Reports the civil location of an IP Terminal.

ParameterID: gloc (0x0004)

Type: Octet String

Possible values: Format specified in IETF GEOPRIV working group geographic location Internet draft, draft-ietf-geopriv-dhcp-lci-option-02.txt, dated August 21, 2003. Default value is an empty String.

Description: Reports the geographic location of an IP Terminal.

ParameterID: src (0x0005)

Type: Enumeration

Possible Values: Not Applicable (0x0001), Network (0x0002), User (0x0003). Default value is 0x0001. If the civil location (loc) or geographic location (gloc) properties are present then this property must contain a non-default value.

Description: Identifies whether the network or the user provided the civil and geographic location information. Default value is an empty String.

ParameterID: pubAddr (0x0006)

Type: Octet String

Possible values: Default value is an empty String. If the civil location (loc) or geographic location (gloc) properties are present then this property must

contain a non-default value.

Description: Reports the public IP address of an IP Terminal for location identification purposes.

ParameterID: privAddr (0x0007)

Type: Octet String

Possible values: Default value is an empty String. If the civil location (loc) or geographic location (gloc) properties are present then this property must contain a non-default value.

Description: Reports the private IP address of an IP Terminal for location identification purposes.

ParameterID: macAddr (0x0008)

Type: Octet String

Possible values: MAC address encoded in hex. Default value is an empty String. If the civil location (loc) or geographic location (gloc) properties are present then this property must contain a non-default value.

Description: Reports the MAC address of an IP Terminal for location identification purposes.

Signals

None

Statistics

None

Procedures

These are the procedures.

Appendix x: GWC-LOCATION-CHANGE-REPORTING-MIB

```
-- DMS Call Server GateWay Controller Location Change Reporting MIB
```

```
GWC-LOCATION-CHANGE-REPORTING-MIB DEFINITIONS ::= BEGIN
```

```
    IMPORTS
```

```
        OBJECT-TYPE, MODULE-IDENTITY, enterprises, IpAddress
```

```
        FROM SNMPv2-SMI
```

```
        DisplayString, RowStatus
```

```
        FROM SNMPv2-TC;
```

```
--
```

```
-- Define the location of this MIB within the MIB tree
```

```
--
```

```
nortel OBJECT IDENTIFIER ::= { enterprises 562 }
```

```
voip OBJECT IDENTIFIER ::= { nortel 28 }
```

```
ptn OBJECT IDENTIFIER ::= { voip 0 }
```

```
serviceControl OBJECT IDENTIFIER ::= { ptn 1 }
```

```
legacyCallServer OBJECT IDENTIFIER ::= { serviceControl 4 }
```

```
lcsGateWayController OBJECT IDENTIFIER ::= { legacyCallServer 1 }
```

```
--
-- Define the elements in the GWC Location Change Reporting MIB
--

gwcLocationChangeReportingMIB MODULE-IDENTITY
    LAST-UPDATED "200210090000Z"    -- October 9, 2003
    ORGANIZATION "Nortel DMS Call Server"
    CONTACT-INFO "David Johnson
        Nortel Networks Inc.
        Maidenhead Office Park, Westacott Way
        Maidenhead, BERKS, UK, SL6 3QH
        Phone: 01628 431218
        email: davidjoh@nortelnetworks.com"
    DESCRIPTION "The MIB module defines information about
        the Location Change Reporting
        data provisioning supported
        by the GateWay Controller (GWC)."
```

::= { lcsGateWayController 24 }

```
locationChangeReportingStatus OBJECT-TYPE
    SYNTAX          INTEGER{
        disable (0),
        enable  (1)
    }
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION     "A boolean value indicating whether Location Change Reporting
        is enabled or disabled on a per GWC base. By default, Location
        Change Reporting is disabled."
    DEFVAL { 0 }
    ::= { gwcLocationChangeReportingMIB 1 }
```

```
locationChangeReportingPort OBJECT-TYPE
    SYNTAX Integer32(0..65535)
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION     "Location Change Reporting Location Recipient Port, the range
        is from 1024 to 65535."
    DEFVAL { 0 }
    ::= { gwcLocationChangeReportingMIB 2 }
```

```
locationChangeReportingIpAddress OBJECT-TYPE
    SYNTAX IpAddress
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION     "Location Change Reporting Location Recipient IpAddress."
    DEFVAL { '00000000'h }
    ::= { gwcLocationChangeReportingMIB 3 }
```

```
locationChangeReportingErrorMessage OBJECT-TYPE
```

```
SYNTAX DisplayString (SIZE(1..128))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "Error Message holds a descriptive error message
    in case of an snmp failure of the last operation."
 ::= { gwcLocationChangeReportingMIB 4 }

locationChangeReportingErrorType OBJECT-TYPE
    SYNTAX INTEGER { information      (0),
                    warning          (1),
                    error            (2) }
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "This value contains the type of error that occurred on
        the last SET failure on any variable in the gateWayTable.
        The combination of this type and the error message give
        the manager enough information to process the failure."
    ::= { gwcLocationChangeReportingMIB 5 }

END
```



Product = CS2000

A00003576 -- Trunk Security (IAC)

Functional Description

This feature enables the IP Security (IPSec) capability for the following GWC trunking profiles:

- TRUNKNA
- TRUNKINTL

The IPSec provisioning GUI is modified/enhanced as follows:

- in the “IPSec Profile” panel, the “SA renew thresh” field (which was previously expressed as a percentage of SA lifetime) is changed to “Grace Period (seconds)”.
- a “Comment” field is added to the “Connection Policy” panel. When a connection policy is added, the user can enter descriptive comments in the “Comment” field. These descriptive comments provide an extra level of detail or history regarding that specific connection policy.
- the option to enter the Kerberos service key in hexadecimal format, as well as the currently supported PEM format.
- showing (1) the Kerberos panel and (2) the “KERBEROS” option in the “IPSec Profile” panel “Key Negotiation” field, only if the Kerberos capability is included for that GWC profile.

The IPSec portion of the Gateway Controller on-line help panels are enabled.

Hardware Requirements or Dependencies

Not applicable.

Software Requirements or Dependencies

Not applicable.

Limitations and restrictions

Not applicable.

Interactions

Not applicable.

Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema _____

User Interface _____

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

Glossary

Term	Description
GWC	Gateway Controller
IPSEC	IP Security
SA	Security Association
PEM	Base 64
SESM	Succession Element Sub-Element Manager
TRUNKINTL	International Trunk (<i>GWC profile</i>)
TRUNKNA	North American Trunk (<i>GWC profile</i>)

Product = CS 2000

A00003613 -- SSPFS: CBM Configuration Parameters (PT-IP)

Functional Description

This feature adds three configuration parameters to the existing SSPFS configuration, which will be configured via the existing “cli” tool:

CM Internet Protocol (IP) Address: The address by which the CM may be reached. This address should be reachable by the SSPFS through VLAN's, which are defined in the network topology.

Login Greeting: A string that will be displayed to remote telnet users before they attempt to login.

System Location: A string defining the physical location of the SSPFS Server

New menu options for each of these parameters will be added to the existing SSPFS “cli” tool.

Applicable customer facing sections

Fault Management:

Not Applicable	<u>N/A</u>
Logs	<u>N/A</u>
Alarms	<u>N/A</u>

Configuration:

Not Applicable	<u>N/A</u>
Data Schema/MIBs	<u>N/A</u>
User Interface	<u>X</u>
GUI	<u>N/A</u>
Element Management	<u>N/A</u>
Security	<u>X</u>
Service Order	<u>N/A</u>
SOC	<u>N/A</u>
Office Parameters	<u>N/A</u>
Upgrades impact	<u>N/A</u>

Accounting	<u>N/A</u>
Performance	<u>N/A</u>
Operational Measurements	<u>N/A</u>
Performance Measurements	<u>N/A</u>

Hardware Requirements or Dependencies

No new hardware or hardware dependencies are introduced.

Software Requirements or Dependencies

No new customer software or firmware dependencies are introduced in this feature.

Limitations and restrictions

No limitations or restrictions visible to any user are planned as part of this feature.

Interactions

No interactions between this feature and existing features.

Configuration for A00003613

Hardware and Software Requirements

SSPFS platform software and supported hardware are required for this feature.

Initial Configuration

These new parameters are optional to SSPFS, and will be configured after the initial install or upgrade of SSPFS.

Office / Subnet parameters (OP/SP) (CM & SESM)

Not Applicable to this feature.

Upgrade Impact

No upgrade impacts.

Data schema (DS) (CM, MIBS, RDB)

Not Applicable to this feature.

Service Orders (SO) (CM & SESM)

Not Applicable to this feature.

Software optionality control (SOC)

Not Applicable to this feature.

Element Management

New/modified GUIs

Not Applicable to this feature.

GUI information

Not Applicable to this feature.

CLUI Interface

The existing SSPFS “cli” menu tool will be updated to configure the three new parameters. Details of this are described in the User interface changes section.

User interface changes

Directory: Configuration/ OAMP Application Configuration

Directory description

This existing menu level contains commands to configure switch specific settings that are used by OAMP Applications.

Accessing directory: OAMP Application Configuration

Access to directory or MAP level and return to CI

As with all menus in the “cli” tool, the enters “x” to exit to the higher level menu.

Command: cm_conf (Configure CM IP Address)

Command type: Listed MENU

Command target: Other, SSPFS system

Command availability: RES

Command description

This command will allow the user to configure enter or change the CM IP address. The CM IP address parameter will also be displayed in the CLI Menu level “View”, “software configuration” and the capt_gather tool.

Command syntax

This command only takes one parameter, which is an IP address. The IP address must be of the format “0-255.0-255.0-255.0-255”.

<CommandName> command parameters and variables (Continued)

Command	Parameters and variables
Configure CM IP Address	IP address of the CM

Qualifications and warnings

User must be root to change this value.

Responses

Enter the CM IP Address (default: <address>)

This prompts the user for the new CM IP Address. If an address is already configured, it will be displayed in the prompt as the default value. If the user just presses enter, the default value will be taken for this parameter.

User confirmation

After a user enters valid parameters for this command, they will be prompted:

```
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

This allows the user to review their entry and confirm they want to change these parameters.

ERROR: IP Address <address> is not valid

The IP address enter was not of a valid format, the user will be prompted to re-enter the IP address.

Must be root to use this tool

A non-root user is attempting to change the IP address. The command will exit. The user should become root and re-enter the command.

Example

Example of changing the CM IP Address (user input in bold):

```
=== Executing "cm_conf"
CM IP:          10.14.71.3
Enter the CM IP Address (default: 10.14.71.3):
10.14.71.5
CM IP:          10.14.71.5
Enter "ok" to commit changes
Enter "quit" to exit
```

```
Enter anything else to re-enter settings
ok
```

```
=== "cm_conf" completed successfully
```

Command: cm_unconf (Unconfigure CM IP Address)

Command type: Listed MENU

Command target: Other, SSPFS system

Command availability: RES

Command description

This command will allow the user to unconfigure the CM IP address. This is used if the CM IP address is no longer needed, or can be automatically determined via application software (such as systems with OC-3 core connectivity).

Command syntax

This command only takes no parameters.

<CommandName> command parameters and variables (Continued)

Command	Parameters and variables
Unconfigure CM IP Address	none

Qualifications and warnings

User must be root to change this value.

User confirmation

After a user enters valid parameters for this command, they will be prompted:

```
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

This allows the user to review their entry and confirm they want to change these parameters.

Must be root to use this tool

A non-root user is attempting to unconfigure the IP address. The command will exit. The user should become root and re-enter the command.

Example

Example of changing the CM IP Address (user input in bold):

```
=== Executing "cm_unconf"
CM IP:          10.14.71.3
CM IP address will be unconfigured
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
ok
=== "cm_unconf" completed successfully
```

Directory: Configuration / Login Session

Directory description

This existing menu level contains commands to configure login parameters

Accessing directory: Login Session

Access to directory or MAP level and return to CI

As with all menus in the "cli" tool, the enters "x" to exit to the higher level menu.

Command: telnet_greeting (Telnet Login Greeting)

Command type: Listed MENU

Command target: Other, SSPFS system

Command availability: RES

Command description

This command will allow the user to configure enter or change the message shown to users before they attempt to login to this server. This text message may contain multiple lines and has no size limit. This may contain information about this system and or warnings to un-authorized users. On fresh installs or upgrades from older loads, the default message will be "Authorized use only, activities logged".

Command syntax

This command only takes one parameter, which is a text field.

<CommandName> command parameters and variables (Continued)

Command	Parameters and variables
Configure telnet login greeting	Message to be displayed to users before they attempt to login

Qualifications and warnings

User must be root to change this value.

Responses

Enter the Telnet Login Greeting Message. Enter a blank line to end the message.

This prompts the user for the Telnet Login Greeting. If a greeting is already configured, it will be displayed above this prompt. If the user just enters a blank line, the Login Greeting Message will be cleared.

User confirmation

After a user enters valid parameters for this command, they will be prompted:

```
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

This allows the user to review their entry and confirm they want to change these parameters.

Must be root to use this tool

A non-root user is attempting to change the Telnet Login Greeting address. The command will exit. The user should become root and re-enter the command.

Example

Example shown is changing the greeting from the default (user input in bold):

```
=== Executing "telnet_greeting"
```

```
Telnet Login Greeting Message:  Authorized use only,
activities logged
```

```
Enter the Telnet Login Greeting Message.
Enter a blank line to end the message:
```

```
Private Database, Authorized users only
```

```
Telnet Login Greeting Message:  Private Database,
Authorized users only
```

```
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

```
ok
```

```
=== "telnet_greeting" completed successfully
```

Directory: Configuration / Location Configuration

Directory description

This new menu level contains commands to configure system parameters. The current time zone command “chg_tz (Change Timezone)” will be moved to this level. The new command “sys_loc (System Location)” will also be at this level.

Accessing directory: Location Configuration

Access to directory or MAP level and return to CI

As with all menus in the “cli” tool, the enters “x” to exit to the higher level menu.

Command: sys_loc (System Location)

Command type: Listed MENU

Command target: Other, SSPFS system

Command availability: RES

Command description

This command will allow the user to configure enter or change a text string describing the system location. On fresh installs or upgrades from older loads, this string will be empty by default. The System Location parameter will also be displayed in the CLI Menu level “View”, “software configuration” and the capt_gather tool.

Command syntax

This command only takes one parameter, which is a text field.

<CommandName> command parameters and variables (Continued)

Command	Parameters and variables
Configure System Location	A line of text describing the system's physical location

Qualifications and warnings

User must be root to change this value.

Responses

Enter the System Location (default: <location>)

This prompts the user for the System Location. If this is already configured, the current value will be displayed and set as the default choice.

User confirmation

After a user enters valid parameters for this command, they will be prompted:

```
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

This allows the user to review their entry and confirm they want to change these parameters.

Must be root to use this tool

A non-root user is attempting to change the system location. The command will exit. The user should become root and re-enter the command.

Example

Example of changing the CM IP Address (user input in bold):

```
=== Executing "sys_loc"

System Location:          NC RTP Lab 4

Enter the CM IP Address (default: NC RTP Lab 4) : NC RTP
Lab 5

System Location:          NC RTP Lab 5

Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
ok

=== "sys_loc" completed successfully
```

Security

Only the Login Greeting has any security implications. The greeting should not reveal any system information and if often used to inform persons that only authorized or employee use is allowed. As other Nortel products have this same mechanism, we anticipate customers will have a Login Greeting message established.

Configuration Walkthrough

These parameters may be configured at any time. On SSPFS system which will use the CBM applications, these parameters must be set. These parameters are not required on other SSPFS systems. However their use should be encouraged.

Product = CS 2000

A00003617 -- AlarmD Integration (PT-IP)

Functional Description

This feature serves the following purposes:

- 1** Use alarmD as the reporting (writing to customer logs and lighting alarm lights) and storage mechanism for all platform related alarms.
- 2** In addition to existing fault monitors, provide new monitors that will monitor the following system components.
 - CPU load average
 - Memory usage
 - Swap space

In addition to this, the existing file system monitor will be enhanced to monitor a lot more than just file system usage.

- 3** It will provide interfaces to turn on, turn off and query alarm lights on Netra 1400 and N240 platforms. A command line interface to do the same will also be provided.
- 4** A command to query all the faults on a system (an aggregate view of the system) will be included. This command can be invoked from command line or through the cli interface.

Applicable customer facing sections

Fault Management

Not applicable	_____
Logs	___X___
Alarms	___X___

Configuration

Not applicable	_____
Data Schema/MIBs	_____
User Interface	___X___
GUI	_____
Element Management	_____

Security	_____
Service Order	_____
Office Parameters	_____
SOC	_____
Upgrades impact	_____
Accounting (includes AMA billing)	_____
Not Applicable	___X___
Billing changes	_____
Performance	_____
Not Applicable	___X___
Operational Measurements	_____
Performance Measurements	_____

Hardware Requirements or Dependencies

Certain components of this feature will be supported only on field grade hardware.

When an alarm is raised or cleared, the corresponding alarm light will be turned on and off only on T1400s and N240s.

Logs will be generated on other platforms. However, the turning on, turning off and querying the state of a light will be supported only on T1400s and N240s.

Software Requirements or Dependencies

No requirements identified at this time.

Limitations and restrictions

None

Interactions

A00001953 - Common Platform Capabilities - introduced a set of fault monitors. The reporting mechanism used by these monitors was through two separate calls. The first call was to write a customer log. The second was to turn on/ off an alarm light. The state of a fault was not maintained.

As part of this feature, alarmD will be used to write logs and light a light as part of a single call. It will also store the state of a fault associated with a particular monitor. These faults will be aggregated to provide a blanket view of the system at an instant in time. Existing monitors (the ones provided as part

of A00001953) will be modified to make use of the capability that alarmD provides.

Fault Management for A00003617

Logs

CPU Related Logs

Log related to a Major Alarm

3X20 ** SPFS310 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Equipment

Cause: CPU Load Average threshold exceeded

ProbableCause: thresholdCrossed

ComponentId: CPU

Description: CPU load average is 6.3

Recovery Action: Check System for run away processes.

Log related to Minor Alarm

3X20 * SPFS310 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Equipment

Cause: CPU Load Average threshold exceeded

ProbableCause: thresholdCrossed

ComponentId: CPU

Description: CPU load average is 4.3

Recovery Action: Check System for runaway processes.

Log associated with a clear

3X20 SPFS310 JUL17 22:20:05 0812 INFO SPFS Fault Cleared

Location: SSPFS - <hostname>

Time: Thu Jul 17 22:20:04 EDT 2003

State: Cleared

Category: Equipment

Component Id: CPU

Description: No CPU problems reported at this time

Swap Space

Logs Related to Major Alarms

3X20 ** SPFS310 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Equipment

Cause: Swap Space usage threshold exceeded

ProbableCause: thresholdCrossed

ComponentId: SwapSpace

Description: Less than 20% of swap space available

Recovery Action: Contact Support.

Logs Related To Critical Alarms

3X20 ** SPFS310 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Equipment

Cause: Swap Space usage threshold exceeded

ProbableCause: thresholdCrossed

ComponentId: SwapSpace

Description: Less than 10% of swap space available

Recovery Action: Contact Support.

Logs Related To Clears

3X20 SPFS310 JUL17 22:20:05 0812 INFO SPFS Fault Cleared

Location: SSPFS - <hostname>

Time: Thu Jul 17 22:20:04 EDT 2003

State: Cleared

Category: Equipment

Component Id: Swap Space

Description: Over 20% of swap space available.

Memory Usage

Logs Related to Minor Alarms

3X20 * SPFS310 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Equipment

Cause: Memory usage threshold exceeded

ProbableCause: thresholdCrossed

ComponentId: Memory

Description: Scan Rate Exceeded 20

Recovery Action: Contact Support

Logs Related to Major Alarms

3X20 ** SPFS310 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Equipment

Cause: Memory usage threshold exceeded

ProbableCause: thresholdCrossed

ComponentId: Memory

Description: Scan Rate Exceeded 50

Recovery Action: Contact Support

Logs Related To Clears

3X20 SPFS310 JUL17 22:20:05 0812 INFO SPFS Fault Cleared

Location: SSPFS - <hostname>

Time: Thu Jul 17 22:20:04 EDT 2003

State: Cleared

Category: Equipment

Component Id: Memory

Description: Reported Scan Rate is less than 20. No memory problems reported at this time.

File System Monitor

Logs Related To Major Alarms

3X20 ** SPFS350 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Software

Cause: FileSystem Not mounted

ProbableCause: SHM: check probable cause

ComponentId: FSMon

Description: Filesystem <mountpoint> not mounted

Recovery Action: Contact Support.

3X20 ** SPFS350 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Software

Cause: File System usage threshold exceeded

ProbableCause: thresholdCrossed

ComponentId: FSMon

Description: Less than 20% of <Filesystem> available

Recovery Action: Remove files from <Filesystem>

Critical Alarms

3X20 *** SPFS350 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Software

Cause: File system usage threshold exceeded

ProbableCause: thresholdCrossed

ComponentId: FSMon

Description: Less than 10% of <File System> available

Recovery Action: Remove files immediately from <Filesystem>

3X20 *** SPFS350 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Software

Cause: File system write failed

ProbableCause: fileError

ComponentId: FSMon

Description: O_SYNC write to <File System> Failed

Recovery Action: Contact support

3X20 *** SPFS350 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Software

Cause: File system read failed

ProbableCause: fileError

ComponentId: FSMon

Description: O_DIRECT read from <File System> failed

Recovery Action: Contact Support.

Minor Alarm

3X20 * SPFS350 JUL17 14:53:12 0093 TBL SPFS Fault

Location: SSPFS - <hostname>

Time: Thu Jul 17 14:53:11 EDT 2003

State: Raised

Category: Software

Cause: File System usage threshold exceeded

ProbableCause: thresholdCrossed

ComponentId: FSMon

Description: Less than 25% of <Filesystem> available

Recovery Action: Remove files from <Filesystem>

Alarm Clears

3X20 SPFS350 JUL17 22:20:05 0812 INFO SPFS Fault Cleared

Location: SSPFS - <hostname>

Time: Thu Jul 17 22:20:04 EDT 2003

State: Cleared

Category: Software

Component Id: FSMon

Description: No File System related problems reported at this time.

Cli interface to query platform state.

A cli interface to query the “state” of the system will be made available.

The interface will allow the user to query a comprehensive state of the system (this includes information about all monitors registered with AlarmD) or just the pieces that have faults tagged against them; both will be available.

Both these commands can be invoked either from cli or directly from the command line.

The output of these commands has not been defined fully yet. In time, this document will be updated to reflect the output of these commands.

The anticipated output looks like this:

The cli interface to these commands will be as shown below:

Step 1: Type in cli

```
> cli
```

This brings up the following menu:

Command Line Interface

- 1 - View
- 2 - Configuration
- 3 - Other

- X - exit

select - 2

Step 2: Select choice 2 (Configuration) from the menu. This will bring up the following options.

Platform Monitor Status

- 1 - all Monitor
- 2 - faults

Configuration

- 1 - NTP Configuration
- 2 - Apache Proxy Configuration
- 3 - DCE Configuration
- 4 - OAMP Application Configuration
- 5 - CORBA Configuration
- 6 - IP Configuration
- 7 - DNS Configuration
- 8 - Syslog Configuration
- 9 - Database Configuration
- 10 - NFS Configuration
- 11 - Bootp Configuration

- 12 - Restricted Shell Configuration
- 13 - Security Services Configuration
- 14 - Login Session
- 15 - Location Configuration
- 16 - Cluster Configuration
- 17 - Succession Element Configuration
- 18 - snmp_poller (SNMP Poller Configuration)

X - exit

select - 17

Step 3: Select 17 (Succession element configuration). That will bring up the following menu

Succession Element Configuration

- 1 - RESMON Application Configuration
- 2 - NPM Application Configuration
- 3 - PSE Application Configuration
- 4 - OMPUSH Application Configuration

X - exit

select - 1

Step 4: Select 1 (Resmon Application configuration).

RESMON Application Configuration

- 1 - queryFaults (Query all faults on the box)
- 2 - enableLocalLogs (Enable Local Logging Of Faults)
- 3 - disableLocalLogs (Disable Local Logging Of Faults)

X - exit

select - 1

Step 5: Select 1 (Query Faults).

If there are no alarms on the box the output will look like this

=== Executing “queryFaults”

Alarm database does not contain Faulted Nodes

=== “queryFaults” completed successfully

If alarms are raised, the output will look like this (sample output)

```
** SPFS310 NOTICE: bge2: link down
```

```
Network Interface down
```

```
Tue Mar 30 17:31:58 2004
```

```
** SPFS310 NOTICE: bge0: link down
```

```
Network Interface down
```

```
Tue Mar 30 17:32:02 2004
```

Cli interface to turn off local logging

Run through steps 1-4 from [“Cli interface to query platform state.”](#) on page 1099.

In the RESMON Application Configuration menu, select 3 (disableLocalLogs).

RESMON Application Configuration

1 - queryFaults (Query all faults on the box)

2 - enableLocalLogs (Enable Local Logging Of Faults)

3 - disableLocalLogs (Disable Local Logging Of Faults)

X - exit

select - 3

This will print out the following message:

=== Executing “disableLocalLogs”

=== “disableLocalLogs” completed successfully

Cli option to turn ON local logging

Run through steps 1-4 from [“Cli interface to query platform state.”](#) on page 1099.

In the RESMON Application Configuration menu, select 3 (disableLocalLogs).

RESMON Application Configuration

1 - queryFaults (Query all faults on the box)

2 - enableLocalLogs (Enable Local Logging Of Faults)

3 - disableLocalLogs (Disable Local Logging Of Faults)

X - exit

select - 2

This will print out the following message:

=== Executing “enableLocalLogs”

=== “enableLocalLogs” completed successfully

Glossary

Term	Description
FSMon	File System Monitor
AlarmD	The fault reporting utility that will be provided as part of the SSPFS
CPU	Central Processing Unit
CPU Load	The number of processes on the “ready” queue (that is, processes that are not blocked waiting for IO, but are in a “run” state).
15 minute Load average	The average CPU load over 15 minutes
NIC	Network interface card.

Product = CS 2000

A00003618--SSPFS: High Availability Enhancements (PT-IP, AAL2)

Functional Description

This feature will enhancement the existing SSPFS High Availability framework in the following ways:

- *Application Groups may have unique IP Address*: This allows for IEMS and SESM co-residency and provides a framework for future application co-residency.

- *Expanded HA API*: complete set of C++ and command line tools for applications which needs to interface with the HA framework, such as CBM and NPM.
- *Cluster Software upgrade*: A newer version of the cluster software from Continuous Computing Corporation is introduced. This provides enhanced “split-brain” resolution and memory mapped file handling required by SBA.
- *Enhanced Ethernet interface fail over*: This will introduce Continuous Computing Corporation's UpLink product to provide faster Ethernet interface fail over on both simplex and HA cluster SSPFS system. On simplex systems, this removes the use of Solaris IP multipathing. Solaris IP multipathing required two test IP Addresses, which will no longer be needed, reducing the number of IP Addresses required by SSPFS.
- *Non-replicated application file systems*: This gives applications a new option to have their file systems not replicated by the HA software, required by the CBM applications.
- *Cluster state change notification to applications*: applications may register to be called when a cluster state change occurs (such as a swact).
- *User option to disable cluster fail over*: a new option is added to the existing “cli” tool which allows users to disable cluster fail over (or swact) as needed.

Applicable customer facing sections

Fault Management:

Logs N/A

Alarms N/A

Configuration:

Data Schema/MIBs N/A

User Interface X

GUI N/A

Element Management N/A

Security N/A

Service Order N/A

SOC N/A

Office Parameters N/A

Upgrades impact X

Accounting:

Billing changes N/A

Performance:

Operational Measurements N/A

Performance Measurements N/A

Hardware Requirements or Dependencies

No new hardware or hardware dependencies are introduced. All existing field grade SSPFS hardware will work with the Ethernet interface fail over enhancement.

Software Requirements or Dependencies

No new customer viable software or firmware dependencies are introduced in this feature. All software introductions are contained in the SSPFS load.

Limitations and restrictions

No limitations or restrictions that is visible to any user are planned as part of this feature.

Interactions

Interactions between this feature and several existing features. Several of the enhancements are specifically for the CBM and NPM applications.

Glossary

Term	Description

Configuration for A00003618

Hardware and Software Requirements

SSPFS platform software and supported hardware are required for this feature.

Initial Configuration

This feature will introduce changes to the SSPFS installation tool to support application specific IP address configuration. These changes will be mirrored in the post-install “cli” tool IP configuration tool discussed below. The menus and behavior for settings IP addresses will be the same at install as in the post-install “cli” tool.

Office / Subnet parameters (OP/SP) (CM & SESM)

Not Applicable to this feature.

Upgrade Impact

The details of a HA cluster upgrade from SN06.2 to SN07 are addressed in a separate activity, corrective caf in SN07, A00004860. However, this feature will alter the Ethernet interface fail over on upgrade (which will 'free up' test addresses in simplex systems) as well as introduce a new version of the cluster software.

Data schema (DS) (CM, MIBS, RDB)

Not Applicable to this feature.

Service Orders (SO) (CM & SESM)

Not Applicable to this feature.

Software optionality control (SOC)

Not Applicable to this feature.

Element Management

New/modified GUIs

Not Applicable to this feature.

GUI information

Not Applicable to this feature.

CLUI Interface

The existing SSPFS “cli” menu tool will be updated. Details of this are described in the User interface changes section.

User interface changes

Directory: Configuration/ IP Configuration

Directory description

This existing menu level contains commands to configure the system's IP network settings

Accessing directory: IP Configuration

Access to directory or MAP level and return to CI

As with all menus in the “cli” tool, the user enters “x” to exit to the higher level menu.

Command: conf_test (Configure IP Multipathing Test Addresses)

Command type: Listed MENU

Command target: Other, SSPFS system

Command availability: RES

Command description

This command will be removed. The functionality provided by this command will be replaced by UpLink. UpLink configuration will be completely automated.

Command syntax

N/A

Qualifications and warnings

N/A.

Responses

N/A.

Command: config_ip (Configure System IP Addresses)

Command type: Listed MENU

Command target: Other, SSPFS system

Command availability: RES

Command description

This command will allow the user to configure the public IP addresses on both simplex and HA cluster systems.

Command syntax

This command is interactive.

Qualifications and warnings

User must be root to configure the system IP address(es).

Responses

User confirmation

After a user enters valid parameters for this command, they will be prompted:

```
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

This allows the user to review their entry and confirm they want to change these parameters.

Application association with additional IP address

If the user chooses to configure an additional IP address, then that address must be associated with a particular application. The user will be prompted for the “name” of that application. This application name should match the servman application group name for this application.

In SN07, the only valid combined system, that will require multiple virtual IP addresses, is a system that will support both IEMS and CS2M. So, in SN07, the only reasonable option will be ‘items’.

Must be root to use this tool

A non-root user is attempting to configure the IP address. The command will exit. The user should become root and re-enter the command.

Cluster restart order message

After a successful IP change on an HA cluster system, the cluster units must be restarted in a particular order. This message is given to the user:

The network changes have been made, however the cluster requires a restart of both units. The units must be restarted in the below order.

- 1) Login as root on the console of the standby unit and shut it down with the command: "shutdown -i 0 -y".
- 2) After the standby unit has shutdown, restart the active unit with the command: "shutdown -i 6 -y".
- 3) After the restart is complete, the new network settings are in effect.
- 4) Boot the standby unit with the command "boot".

Example

Example of changing the IP Addresses on a cluster (user input in bold). Notice that the current values are indicated in brackets.

***** There will be no error checking on the application string that is entered...the string must be entered accurately. The only check will be to ensure that an alpha-numeric literal is entered. *****

=== Executing "config_ip"

```
Enter the hostname for this cluster [znc0s0jy] znc0s0jx
Enter primary cluster ip address for znc0s0jx [47.142.108.199] 47.142.108.11
Configure additional cluster ip address ? [yes] yes
Enter additional cluster ip address for znc0s0jx [47.142.108.201] 47.142.108.12
Enter application for cluster ip address 47.142.108.12 [iems] iems
Configure additional cluster ip address ? [no]
Enter ip address for unit zero [47.142.108.220] 47.142.108.7
Enter ip address for unit one [47.142.108.221] 47.142.108.8

Enter "ok" to commit changes
Enter "quit" to exit
```

Enter anything else to re-enter settings
ok

=== "config_ip" completed successfully

Directory: Configuration / Cluster configuration

Directory description

This existing menu level contains configuration commands and directories.

Accessing directory: Configuration / cluster configuration

Access to directory or MAP level and return to CI

As with all menus in the “cli” tool, the user enters “x” to exit to the higher level menu.

Command: disable_failover (Disable cluster node Fail over)

Command type: Listed MENU

Command target: Other, SSPFS system

Command availability: RES

Command description

This command **MUST** be run from the ACTIVE node in the cluster. This command will allow the user to disable a cluster fail over. (activity will remain on current node of the cluster, data will still be replicated).

Command syntax

This command takes one parameter, but is interactive. If a user enters this command a series of other questions will be asked to allow user to disable or re-enable failover.

Qualifications and warnings

User must be root to change this value.

Responses

Cluster Fail over is manually disabled.

This informs the user that HA fail over has been manually disabled. A Customer log entry will be generated to indicate this state ‘transition’.

User confirmation

After a user enters valid parameters for this command, they will be prompted:

```
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

This allows the user to review their entry and confirm they want to change these parameters.

Must be root to use this tool

This message appears when a non-root user is attempting to disable fail over. The command will exit. The user should become root and re-enter the command.

Example

Example shown (user input in bold):

Command: req_failover (manual request to failover)

Command type: Listed MENU

Command target: Other, SSPFS system

Command availability: RES

Command description

This command **MUST** be run from the **ACTIVE** node in the cluster. This command will allow the user to perform/initiate a cluster fail over. (all applications on the active node will stop, and the Active node will give up activity).

Command syntax

This command takes no parameters. If a user enters this command a series of other questions will be asked to confirm the operation.

Qualifications and warnings

User must be root to change this value.

Responses**Cluster Failover initiated**

This informs the user that HA fail over has been manually disabled. A Customer log entry will be generated to indicate this state 'transition'.

User confirmation

After a user enters valid parameters for this command, they will be prompted:

*** Warning: This command will initiate a cluster switch of activity ***

Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings

This allows the user to review their entry and confirm they want to change these parameters.

Must be root to use this tool

This message appears when a non-root user is attempting to disable fail over. The command will exit. The user should become root and re-enter the command.

Example

Example shown (user input in bold):

Security

N/A

Configuration Walkthrough

N/A.

Product = CS 2000

A00003630 -- TGCP for the Cable Market (IAC)

Functional Description

The TGCP for the Cable Market feature implements the Trunking Gateway Control Protocol (TGCP) for ISDN User Part (ISUP) and Per Trunk Signaling (PTS) trunk groups on the Succession Call Server 2000 (CS2K). Specifically, this activity provides:

- incoming and outgoing interconnection from a North American End Office (EO) to the Public Switch Telephone Network (PSTN) using ISUP trunk groups.
- incoming and outgoing interconnection from a North American EO to the PSTN for Operator Services.
- incoming interconnection from a North American EO to the PSTN for Emergency Services.

ISUP Inter-Toll (IT) and Access To Carrier (ATC) trunks are supported for interconnection to the PSTN. Multi-Frequency (MF) Operator (OP) trunks are supported for interconnection to a Local Exchange Carrier (LEC) operator

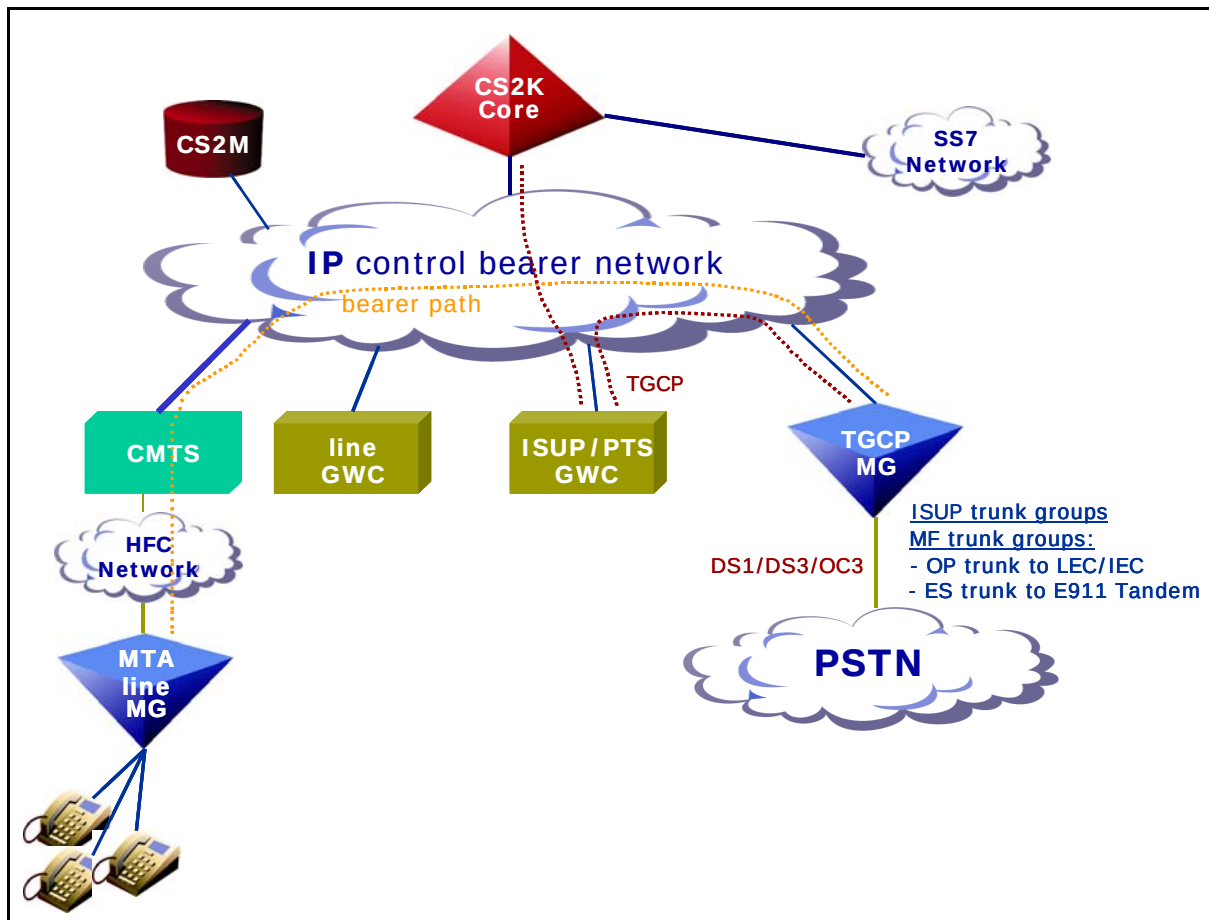
system. MF Emergency Service (ES) and OP trunks are supported for interconnection to an Emergency 911 (E911) Tandem switch.

The ISUP and MF trunk interconnection capability provided by this activity is supported for the North American Integrated Access - Cable (IAC) solution.

The following figure illustrates the CS2K network components relevant to this activity. PSTN interconnection is provided using ISUP and MF trunks configured on a Gateway Controller (GWC) peripheral type. TGCP is supported between the GWC and the Media Gateway (MG). A third party gateway vendor is providing the Media Gateway functionality. Development on the Media Gateway is beyond the scope of this activity. The goal of this activity is to achieve TGCP third party gateway compliancy on the CS2K.

This activity describes the necessary changes on the Core, GWC, and Call Server 2000 Manager (CS2M) to support ISUP IT, ISUP ATC, MF OP, and MF ES trunk signaling and associated services on a TGCP MG. External signaling transparency is provided for the ISUP and MF trunks configured on a GWC. Additionally, limited service transparency is provided as described in this document. The Core, GWC, and CS2M changes are provided as part of the SN07 software release.

IP Cable Network Configuration



Operator and 911 call *originations* are supported for agents configured on the following MG types:

- Multimedia Terminal Adapter (MTA) line MGs (line agents)

Refer to the solutions specifications for Integrated Access Cable for the complete list of line MGs supported in the SN07 release.

Operator and 911 call originations are **not** supported with MGs other than those listed above. However, there are service interactions that may result in the conferencing or transfer of an OP or ES trunk into a call with an agent other than those listed above. This activity supports interoperability with the following agent types when a service interaction¹ results in a connection with either an OP or ES trunk:

- Dynamic Packet Trunk (DPT)

1. Examples of service interactions include, but are not limited to, three-way calling and call transfer. Call forwarding is excluded. Call forwarding to an OP or ES trunk is not supported.

- ISUP trunk
- PRI trunk
- line

Interworking between TGCP MGs and the Universal Audio Server (UAS) is supported for providing media services such as voice announcements.

Functional Description

Operator Services Interconnection

Interconnection from the CS2K EO to a LEC operator switch is provided using MF OP trunk types.

Traditional Bell and Modified Operator Services Signaling (MOSS) are supported. Both signaling types provide two stage signaling:

	stage 1	stage 2
Traditional Bell	KP+called number+ST/STP/ST2P/ST3P	KP+I ^a +7 digit ANI+ST
Modified OSS	KP+called number+ST/STP/ST2P/ST3P	KP+II+7 digit ANI+ST/STP ^b

a. A single information (I) digit is provided with Traditional Bell, two information (II) digits with MOSS.

b. ST is signaled for LEC call completions. STP is signaled for IEC call completions and is provided for completeness.

To configure an OP trunk for Traditional Bell signaling, field EA in table TRKGRP must be provisioned as 'N'. To configure an OP trunk for MOSS signaling, fields EA and EAOSS must be provisioned as 'Y' and 'N' in table TRKGRP respectively.

The capabilities listed below are supported by this activity. For these capabilities, transparency is provided with the legacy switching system:

- LEC interconnection
- Traditional Bell signaling
- MOSS
- Busy Line Verification (BLV)
- Operator Barge-In (BI)
- Operator Ringback
- Operator Recall
- Outgoing OP trunk

- Incoming OP trunk support for BLV and BI
- Hold types of Term Hold and No Hold
- MF signaling
- Reversal ANI request type
- Flexible ANI (FANI) digits - applies to MOSS only
- Intercept calls

The key *exclusions* for this activity are listed below. For a complete list of restrictions and limitations, refer to section [“Limitations and restrictions” on page 1127](#).

- Coin control signals
- DP and DTMF² address signaling
- Exchange Access Operator Services Signaling (EAOSS)
- 2-way OP trunks

Table control restrictions are added by this activity to enforce the SN07 restrictions for MF OP trunks. Refer to the Configuration customer facing section of this document for more information on these restrictions.

Emergency Services Interconnection

Interconnection from the CS2K EO to an E911 tandem switch is provided using MF ES or MF OP trunk types. In SN07, only an *outgoing* MF ES trunk type or an *outgoing* MF OP trunk type is supported. For call completions from the E911 tandem switch back to the CS2K EO, Signaling System Number 7 (SS7) trunks must be configured.

Two stage Traditional Bell signaling is supported on the OP trunk type as described in section [“Operator Services Interconnection” on page 1115](#). Two stage Traditional Bell signaling is supported on the ES trunk type, providing the called number (i.e. 911) and Automatic Number Identification (ANI) digits to the E911 tandem switch as follows:

	stage 1	stage 2
Traditional Bell	KP+911+ST	KP+I+7 digit ANI+ST

The capabilities listed below are supported by this activity for both the OP and ES trunk types (unless noted otherwise). For these capabilities, transparency is provided with the legacy switching system:

2. Restriction applies to DTMF signaling of the called and ANI address digits. DTMF signaling related to pressing keys on the originating line's keypad is supported.

- E911 tandem interconnection
- Ringback
- Outgoing ES and outgoing OP trunk [only]
- Hold type of Term Hold
- MF signaling
- Reversal ANI request type

In addition to the list above, ES trunk types provide specific capabilities that are controlled through provisioning in table TRKGRP. The following TRKGRP capabilities are also supported by this activity for the ES trunk type:

- Audible Ringing:
Field AUDRING specifies whether audible ringing should be applied to the originator. The values Y and N are supported by this activity.
- Automatic Number Identification (ANI) Type:
Field ANI specifies what type of outpulsing to provide on the ES trunk. Only a value of “ANISPILL” is supported by this activity. “ANISPILL” specifies the called digits (i.e. 911) should be outpulsed followed by the ANI digits.
- Switch Hook Status:
Field SWST specifies the action taken when the switch detects the originating subscriber has gone onhook. Only a value of “DC” is supported by this activity. “DC” provides an onhook signal towards the E911 tandem when the originating subscriber goes onhook.
- Calling Line Identification:
Field CLI specifies whether CLI logs should be generated by the switch. The values Y and N are supported by this activity.
- Abandon Hold Time:
Field ABNHLDTM ensures ANI outpulsing completes in the event the calling party goes onhook prior to the completion of outpulsing. A timer value, in seconds, is specified. All timer values are supported by this activity.
- Special Billing Directory Number:
Field SPBDN controls whether to signal the calling number or special billing number as the ANI digits for line originations. The values Y and N are supported by this activity for this field.

The key *exclusions* for this activity are listed below. For a complete list of restrictions and limitations, refer to section [“Limitations and restrictions” on page 1127](#).

- B911 interconnection
- DP and DTMF³ address signaling
- Incoming and 2-way ES trunks and OP trunks

Table control restrictions are added by this activity to enforce the SN07 restrictions for MF ES trunks. Refer to the Configuration customer facing section of this document for more information on these restrictions.

ISUP interconnection to PSTN

Interconnection from the CS2K EO to the PSTN is provided using ISUP IT or ISUP ATC trunk types.

The key *exclusions* for this activity are listed below. For a complete list of restrictions and limitations, refer to section [“Limitations and restrictions” on page 1127](#).

- Digit collection on ISUP trunks

Provisioning

The provisioning in Succession CS2K is distributed among several interfaces:

- the CS2M is used to provision GWC nodes, register MGs with GWCs, and bulk provision endpoints (i.e., by carrier);
- the CS2K core can be used to provision GWC node data and trunk related data; and
- OSSGate can also be used to provision trunk related data, register MGs with GWCs, and bulk provision endpoints by carrier.

GWC Node Provisioning

The CS2M is used to provision trunking GWC nodes with TGCP ISUP and MF trunks. The provisioning of the GWC includes:

- updating table SERVRINV on the CS2K core;
- configuring TGCP MGs on the GWC; and
- provisioning carriers/endpoints on the GWC.

New GWC Exec Lineup

Upon adding a GWC node, table SERVRINV is updated with the GWC node data including node number, tone data, and exec line-up data. A new exec line-up, GWCABEX, is created for the GWC. The new exec line-up is provisionable in table SERVRINV and applies to a term type of ABTRK. This exec line-up must be provisioned in table SERVRINV for GWCs that support MF OP and/or ES trunks.

3. Restriction applies to DTMF signaling of the called and ANI address digits. DTMF signaling related to pressing keys on the originating line's keypad is supported.

Refer to the Configuration section of this document for further information on the new exec line-up.

The CS2M interface for configuring GWC nodes allows the selection of the GWCABEX exec line-up for TRUNKNA (N.A. trunking) GWCs. Refer to the Configuration customer facing section of this document for further information on the CS2M.

Configuring TGCP MGs

TGCP MGs are registered with a GWC via the CS2M. For this activity, the CS2M interface for associating an MG with a GWC is expanded to include the TGCP protocol type and a new gateway profile name.

Refer to the Configuration section of this document for further information on the CS2M.

GWC Endpoint Provisioning

The CS2M provides the capability to provision endpoints of a GWC on a carrier basis (i.e., 24 or 31 endpoints). The endpoints on a GWC must be provisioned prior to adding the tuple entries in table TRKMEM. The CS2M provides a list of terminal identifiers which must be entered in the tuple for table TRKMEM.

For GWCs supporting TGCP MGs, CS2M permits provisioning carriers of 24 endpoints at a time. The carrier naming convention follows the TGCP convention outlined below.

TGCP Endpoint Naming Convention

The TGCP endpoint naming convention follows the standards proposed in the PKT-SP-TGCP-I05-030728 TGCP Specification. The format supports a DS-0 channel endpoint type on a trunking gateway:

- **ds/<unit-type1>-<unit #>/<unit-type2>-<unit #>/.../<channel #>** where
 - **<unit-type>** is defined to be one of “s”, “su”, “oc3”, “ds3”, “e3”, “ds2”, “e2”, “ds1”, and “e1”;
 - **<unit #>** is a decimal value referring to the particular instance of <unit-type>;
 - **<channel #>** is a decimal value indicating the channel number at the lowest level in the hierarchy (e.g., DS-0); and
 - **ds** is fixed, identifying the endpoint naming scheme.

For SN07, the CS2M and GWC support TGCP MGs with DS1 interfaces, OC3 interfaces containing channelized DS3 and DS1 levels, and DS3 interfaces with channelized DS1 levels as defined in the following table.

TGCP MG interfaces and Endpoint Naming

TGCP MG Interface	Endpoint Naming Convention
DS1 interface	ds/ds1-#/#
OC3 interface with DS3 and DS1 levels	ds/oc3-#/ds3-#/ds1-#/#
DS3 interface with DS1 level within a logical processor (or slot)	ds/s-#/ds3-#/ds1-#/#
DS3 interface without DS1 framing	ds/s-#/ds3-##

Refer to the Configuration section of this document for further information on the CS2M.

Trunk Group Provisioning

GWC ISUP and MF trunk related data is provisioned on the CS2K core using the same data tables as for legacy TDM trunks, namely tables CLLI, TRKGRP, TRKSGRP, TRKOPTS, and TRKMEM (ISUP trunks also require tables ISUPDEST and C7TRKMEM to be provisioned). Additionally, a new option is added in table TRKOPTS which must be assigned to OP and ES trunks groups provisioned on a GWC.

When provisioning an MF trunk group on a GWC, there are no restrictions regarding the distribution of the trunk members. An MF trunk group may be configured with trunk members spanning one or more GWCs or spanning one or more MGs. The trunk group can consist of any number of channels on a DS1 (e.g. 1, 5 or 24 channels).

MF trunk groups consisting of trunk members distributed across different peripheral types, such as a GWC and DTC, are **not** supported.

There are no restrictions regarding provisioning ISUP trunk groups on a GWC. Hybrid ISUP trunk groups are supported.

ISUP and MF trunk groups on the same GWC are supported. ISUP and MF trunk groups on the same MG are supported (the MG vendor is responsible for supporting ISUP and MF trunk groups on the same MG).

Table TRKOPTS

A new trunk group option, GWCPTSTK, is added in table TRKOPTS. This option identifies PTS packet trunks that provide connectivity between the

packet network and the PSTN. Option GWCPTSTK must be provisioned against the MF OP or ES trunk group CLLI *after* provisioning table TRKGRP and *prior* to adding trunk members in table TRKMEM.

The GWCPTSTK option is used to restrict trunk group, subgroup, and member capabilities incompatible with GWC PTS trunks. This option cannot be added to a trunk group with the trunk group and subgroup restrictions listed in section “Limitations and restrictions” on page 1127.

This option can not be added to a trunk group that has pre-existing entries in table TRKMEM⁴. Additionally, this option can not be removed until all entries in table TRKMEM have been deleted.

The GWCPTSTK option contains a single sub-option, PRELOADANI. This sub-option identifies PTS packet trunk groups which support a call model that allows the ANI digits to be sent from the Core to the GWC without receiving an ANI request from the far-end. The MG is responsible for handling the ANI request and responding with the ANI digits stream.

Refer to the Configuration section of this document for further information on the new trunk group option.

Table TRKGRP

The tuple entry in table TRKGRP for ISUP IT, ISUP ATC, MF OP, and MF ES trunks remains unchanged. However, restrictions are added to table TRKGRP to prevent the activation of capabilities not supported on GWC MF trunks in the SN07 release. Refer to section “Limitations and restrictions” on page 1127 and the Configuration section of this document for further information.

Table TRKSGRP

With an IP network configuration, the responsibility of providing low-level MF signaling requirements is delegated to the MG (e.g., A/B bit transition). As a result, data currently provisioned in table TRKSGRP is not applicable to OP and ES trunks configured on a GWC. Specifically, the IDGTIME and TRKGRDTM fields in table TRKSGRP are not used by the CS2K. The MG is expected to comply with GR-505 and GR-506 regarding MF timings. Refer to the MG provisioning guidelines for further information related to administering this data.

Restrictions are added to table TRKSGRP to prevent the activation of capabilities not supported on GWC MF trunks in the SN07 release. Refer to section “Limitations and restrictions” on page 1127 and the Configuration section of this document for further information.

4. This can occur only if an attempt is made to add option GWCPTSTK to a trunk group with members on a peripheral type other than a GWC, such as a DTC.

Table TRKMEM

The tuple entry in table TRKMEM for a GWC peripheral type requires a node number and terminal number be entered⁵. The terminal numbers are obtained when the endpoints are provisioned on the GWC using the CS2M. Endpoint provisioning must be completed prior to provisioning table TRKMEM. Refer to section “GWC Endpoint Provisioning” on page 1119 for further information.

The option GWCPTSTK must be provisioned in table TRKOPTS prior to adding MF OP or ES trunk members in table TRKMEM. Table control for table TRKMEM enforces this restriction. Additionally, if option GWCPTSTK exists on a trunk group, table control disallows the addition of trunk members on peripheral types other than a GWC, such as a DTC.

Refer to the Configuration section of this document for further information on the table TRKMEM restrictions.

OSSGate

OSSGate provides a machine interface for provisioning components within Succession. The main functionality of OSSGate is to act as a gateway to the Node, Carrier, Trunk, and Line provisioning applications and the Trunk Maintenance application.

OSSGate supports provisioning of tables TRKSGRP and TRKMEM for ISUP and MF trunks on GWCs. OSSGate is subject to the provisioning restrictions described in sections “Table TRKSGRP” on page 1121 and “Table TRKMEM” on page 1122.

For carrier provisioning, OSSGate supports the naming convention of TGCP described in section “GWC Endpoint Provisioning” on page 1119.

Refer to the Configuration section of this document for further information on OSSGate.

Echo Cancellation

Echo cancellation must be applied from the TDM side of the network. This is because any delay that enters the packet network can become too long for the echo cancellers on the MGs to handle.

In the SN07 release for OP and ES trunk groups, echo cancellation is always performed by the MG. With TGCP, the MG always performs echo cancellation by default.

Table control restrictions are added to table TRKSGRP to reflect that external echo cancellation is always applied by the MG. Table control enforces field

5. Changes to table TRKMEM to support a GWC PMTYPE were provided in a previous Succession release.

ESUPR be provisioned as “N” and field ECSTAT be provisioned as either “EXTERNAL” or “INTERNAL”. ECSTAT set to “INTERNAL” indicates that the echo cancellation is performed in the MG; ECSTAT set to “EXTERNAL” indicates that the echo cancellation is performed on the TDM trunk. See NTP NN10068-461 “Upgrading the GWC” for further details.

For GWC ISUP trunks in SN07, echo cancellation is performed by the MG based on trunk data (i.e., ECSTAT field in table TRKSGRP) unless the echo cancellation info in the ISUP messages (e.g., IAM, ACM, CPG) indicate that it has already been performed between the CS2K and the source of the echo.

TGCP Package Requirements

The TGCP packages used to support ISUP, MF OP, and MF ES trunks in the SN07 release include:

- ISUP Trunk (IT) Package
- MF FGD Operator Services (MO) Package
- MF Terminating Protocol (MT) Package

Trunk Maintenance

In the IP network architecture, the MG owns the physical hardware. The DS1 carrier is no longer owned or maintained by the CS2K. As a result, the maintenance behavior of ISUP and MF trunks configured on a GWC is changed.

CS2K Trunk States

The trunk state of carrier failure (CFL) has a new definition for trunks configured on a GWC. The CFL trunk state indicates the circuit on the MG is out-of-service. The CS2K places a trunk into the CFL state when a TGCP RestartInProgress (RSIP) message with a RestartMethod of “forced” is received from the MG. Recovery from the CFL state back to an IDLE state only occurs if the MG notifies the CS2K the circuit is back in service. The MG notifies the CS2K a circuit is back in service by sending an RSIP with a RestartMethod of “restart”.

In the packet cable architecture, the Media Gateway Controller (MGC) does not have knowledge of the reason the MG has taken one or more circuits out of service. There could be a card failure, carrier failure or a maintenance action being performed on the circuit by the MG. The reason for the removal of a circuit from service is beyond the scope of the CS2K.

The CS2K supports receiving an RSIP on an individual endpoint, carrier, or gateway basis. If a carrier failure occurs on the MG, the MG may send twenty-four individual RSIP messages or one RSIP message on the carrier to the CS2K.

Trunk Test Position (TTP)

Limited maintenance is supported at the TTP level of the MAP for TGCP MF trunks provisioned on a GWC. Restrictions also apply to the MANUAL, MONITOR and DATA levels of the MAP (accessed through the “Level_” command on the TTP). Refer to the following table for a summary of the commands supported and not supported in the SN07 release.

TTP Level Command Summary

Level	Supported Commands	Unsupported Commands
TTP	Quit, BSY ^a (with optional states INB, MB), RTS, BSY ALL, FRIs, Post_, Hold, NEXT, Level_, <i>TST</i> , <i>Ckt_</i>	BSY ^b (with optional state SB), SEIZE , CktInfo , CktLoc, TrnsIvf_, StkSdr_, Pads
MONITOR ^c	Quit, Post_, BSY, RTS, Hold, NEXT, FRIs, <i>TST</i> , <i>MonTalk</i> ,	MONPOST, MONLINK, CktMon , CPos_ , RLS
MANUAL	Quit, Post_, BSY, RTS, Hold, NEXT, <i>LOSS</i> , <i>TGEN</i> , <i>TST</i> , <i>Noise</i> , <i>TDET</i> , <i>Hset</i>	OP_ , Jack_, SGNL , CallTrf, RLS
DATA	Quit, Post_, BSY, RTS, Hold, NEXT, FRIs, <i>BERT_</i>	Seize , BTerm_ , RLS

a. BSY at all levels is supported only with optional states INB and MB.

b. BSY with optional state SB is blocked at all levels.

c. MONITOR level is inaccessible if GWC MF trunk is posted and no InterWorking (IW) bridges are available.

Several of the unsupported commands in the above table are prevented by existing maintenance restrictions added in a prior release. This activity implements only those restrictions required above the existing maintenance restrictions (shown in **bold** text in the table), e.g., the output pulse command (**OP_**) is not supported at the MANUAL level of the MAP.

Several supported commands (shown in *italics* text in the table) are dependent on the availability of certain components in the IAC solution. Test line tests of trunk connections (*TST* command at the TTP, MONITOR and MANUAL levels) require appropriate test line facilities on the Audio Controller⁶. The other TTP commands require Interworking (IW) bridges to provide the necessary functionality. These hardware dependencies also apply for manual test line trunk tests performed from the Automated Test Trunk (ATT) level of the MAP.

Maintenance support at the TTP MAP level for TGCP ISUP trunks is subject to the same set of supported/unsupported commands listed in Table “TTP Level Command Summary” on page 1124, with the exception of the MF restricted commands (shown in **bold** text) which are supported for ISUP. In

6. The availability of test line facilities on the Audio Controller are indicated by the office parameter EXTERNAL_GATEWAY_TEST_LINES in table OFCVAR on the core.

addition, any existing restrictions at the C7TTP MAP level for GWC ISUP trunks also apply to TGCP ISUP trunks.

Refer to the Configuration section of this document for further information on the restrictions added by this activity.

Trunk Maintenance Manager (TMM)

Trunk maintenance for ISUP and MF trunks is supported through TMM. TMM is an existing trunk maintenance application which uses an interface provided by CS2M. The following TMM maintenance commands are supported:

- POST by gateway name, trunk group/CLLI, or carrier;
- BSY, BSY INB, RTS, FRLS, and Query Endpoint State (QES) on posted set.

The Post by Carrier supports the carrier naming convention of TGCP described in section “GWC Endpoint Provisioning” on page 1119.

Trunk Audits

The trunk audits for PTS trunks on legacy peripherals are changed as necessary to align with the new behavior for PTS trunks configured on a GWC.

Automatic recovery actions are no longer performed on PTS trunks in CFL state. Placement into and out of the CFL state is strictly controlled by notification from the MG (as discussed in section “[CS2K Trunk States](#)” on [page 1123](#)). Enhancements are provided to audits both on the core and GWC.

Trunk audits of GWC ISUP trunks was added in a prior Succession release.

Initialization

When the GWC is initially brought into service it awaits notification from the MG that it is inservice and ready to process calls. The trunks transitions from a PMB state to a CFL state⁷ at this time. Upon receipt of an RSIP (with a RestartMethod of “restart”) on the gateway from the MG indicating the MG is inservice, the CS2K begins the process of bringing all CFL trunks into an inservice state. This process includes setting the trunk state to IDL and sending an acknowledgement of the RSIP to the MG. The MG begins scanning for seizures (e.g., remote make busy, call setups) from the far-end (note that seizure-state changing events are persistent in TGCP).

Note that following a restart if the MG has a number of endpoints (e.g., channels) out of service, the GWC/CS2K is unaware of this.

7. Note trunks in the MB or INB state are unaffected. Trunks remain in these states until manually brought into service via the TTP or TMM.

The GWC is also capable of handling RSIPs on a trunk/endpoint basis. However, to minimize the number of messages generated, it is recommended the MG send an RSIP on the gateway when coming inservice.

Swacts and Restarts

This activity provides support for CS2K core restarts, CS2K core swacts, GWC node restarts, and GWC swacts.

For core reload and cold restarts or GWC cold swact and node restarts, all MF calls on the GWC(s) are taken down. The CS2K initiates the necessary cleanup of resources on the MG using TGCP signaling. The same behavior applies to warm restarts on the core and warm swacts on the GWC with one exception, stable MF calls on the GWC(s) remain active. ISUP and MF calls in the answered state are considered stable on the CS2K core.

This activity also supports norestart swact, restartswact and abortswact on the CS2K core.

IP Network loss between the GWC and MG

The GWC monitors its connection to the MG by sending a heartbeat message (in the form of an AuditEndpoint (AUEP) message wildcarded on the gateway) every 10 seconds in the absence of any other messaging between the GWC and MG. A heartbeat loss is detected if after 40 seconds no acknowledgement to the heartbeat message is received by the GWC from the MG.

Upon detecting heartbeat loss, the GWC transitions the trunks on the MG to a CFL state and begins sending heartbeat messages every 2 minutes. During this period, if the GWC receives any message from the MG, the GWC/CS2K begins the process of trunk recovery by: deleting all connections on the MG; and re-starting the regular heartbeat message with the MG.

QoS Reporting

QoS reporting on the GWC is supported to measure voice quality. The TGCP end-of-connection statistics are reported by the MG to the GWC. The GWC collects and transfers the end-of-connection statistics to a QoS Collector Application (QCA) server, where they are correlated with the billing records.

Accounting

Transparency is provided with the Automatic Message Accounting (AMA) records generated for the legacy billing system. No changes are required by this activity.

Fault Management

Transparency is provided with the trunk related Operational Measurements (OM), Logs and Alarms supported for the legacy OA&M system. No changes are required by this activity.

Hardware Requirements or Dependencies

This activity has the following hardware dependencies:

- The MG functionality is provided by a third party gateway vendor supporting TGCP as described in the PKT-SP-TGCP-I05-030728 TGCP specification.
- Test Line tests of TGCP MG trunk connections to the PSTN require an Audio Controller (AC), an UAS, and a SAGE 945RTS testhead unit to perform tests.

Software Requirements or Dependencies

This activity enhances the CS2K core, GWC, and CS2M to support a TGCP MG hosting ISUP IT, ISUP ATC, MF OP, and MF ES trunks as described in the previous sections. The SN07 software load is required on the CS2K core. The GC070 software load is required in the GWC. The PNM07 software load is required on the CS2M.

Limitations and restrictions

The TGCP PKT-SP-TGCP-I05-030728 TGCP specification limits support of MF trunk interconnection to a LEC Access Tandem. Interconnection to an Inter-Exchange Carrier (IEC) operator system is not supported.

The CS2K supports manual busy (ManBusy⁸) of ISUP and MF trunks configured on a GWC. The MO package of the TGCP PKT-SP-TGCP-I05-030728 TGCP specification does not support sending a busy signal from the GWC to the MG. When a ManBusy is performed on MF trunks hosted on a TGCP MG, the trunks will go CFL.

IAC (hybrid) configurations involving TDM elements are not supported in SN07.

IAC configurations involving APG components are not supported in SN07. Without APGs, limited support of DPTs is provided: services on DPTs requiring digit collection or applying tones are not supported.

The following limitations and restrictions apply to *both* MF OP and MF ES trunks:

- Hybrid trunk groups are not supported. A trunk group containing members on a GWC can not include members on any other legacy peripheral type (e.g. DTC).
- MF trunks are not supported on a GWC with lines, DPTs, or ACs.
- Test trunk calls are not supported.

8. i.e., BSY MB from the TTP MAP level

- The outpulse (OP_) command at the MANUAL level of MAPCI is not supported.
- Field OPULSTYP in table TRKSGRP is restricted to 'MF'.
- Only wink start trunks are supported. Field OSTARTSG in table TRKSGRP is restricted to 'WK'.
- Echo cancellation is always provided by the MG. Field ESUPR is restricted to 'N'. Field ECSTAT in table TRKSGRP is restricted to 'EXTERNAL' or 'INTERNAL'.
- Coin control signals are not supported. A coin control signal, if sent from the far-end, will be ignored. Field CCONT in table TRKSGRP is restricted to 'NO'. Although coin control is not applicable to ES trunks, field CCONT is still restricted to 'NO'.
- Only Ringback signal of 'MW' is supported in the CS2K. Field RNGBCK in table TRKSGRP is restricted to 'NO' or 'MW'.

The MG is responsible for handling the ringback signal sent from the far-end. The CS2K will process all ringback requests as a 'MW' ringback request.

- This activity supports operator and 911 *originations* **only** for **line** MGs approved for deployment with the Integrated Access Cable solutions.

Operator and 911 originations on PRI, ISUP, and DPT trunks are not supported.

Service interactions may result in the conferencing or transfer of an OP or ES trunk into a call. This activity supports interoperability with the following agent types when a service interaction⁹ results in a connection with either an OP or ES trunk:

- DPT
- ISUP trunk
- PRI trunk
- line

- Interworking with legacy peripherals is not supported.
- Call forwarding to OP and ES trunks is not supported.

The following limitations and restrictions apply to MF OP trunks only:

- Exchange Access Operator Services Signaling (EAOSS) is not supported. Field EAOSS in table TRKGRP is restricted to 'N'.

9. Examples of service interactions include, but are not limited to, three-way calling and call transfer. Call forwarding is excluded. Call forwarding to an OP or ES trunk is not supported.

- Hold type of joint hold is not supported. Field HOLDTYPE in table TRKGRP is restricted to 'TERMHOLD' or 'NOHOLD'.
- Only ANI request types of reversal is supported. Field ANI_REQUEST in table TRKGRP is restricted to 'REV'.

The following limitations and restrictions apply to *MF ES trunks only*:

- B911 interconnection is not supported. An ES trunk group is supported for E911 Tandem interconnection *only*.
- Incoming and two-way trunks are not supported. Field DIR in tables TRKGRP and TRKSGRP is restricted to 'OG'.
- Field ANI in table TRKGRP is restricted to 'ANISPILL'. The value 'ANISPILL' signals the dialed digits (i.e., 911) followed by the ANI digits. The values 'NOANI' and 'OUTPULSE' are not supported.
- The switch hook status field, SWST, in table TRKGRP is restricted to 'DC'. The value 'DC' signals an onhook towards the E911 tandem when the originating subscriber goes onhook. The values 'AC' and 'ADC' are not supported.

Note the switch hook status tone field, SWSTTN, in table TRKGRP is only applicable when field SWST is set to 'AC' or 'ADC'. Therefore, field SWSTTN is ignored.

- The forced disconnect timing field, FDISCTIM, in table TRKGRP is restricted to '0'. Forced disconnect timing is not supported.
- The disconnect tone type field, DISCTON, in table TRKGRP is specific to B911. This field is not supported. The value provisioned for this field is ignored.
- The integrity tone time field, INTT, in table TRKGRP is specific to B911. This field is not supported. The value provisioned for this field is ignored.
- Field BILLDN in table TRKGRP is not supported. This field is PRI specific and 911 originations on PRI trunks are not supported. The value provisioned for this field is ignored.

The following limitations and restrictions apply to *both ISUP IT and ATC trunks*:

- feature interactions involving digit collection are not supported including, but not limited to:
 - CFRA
 - DISA
 - AIN

Interactions

This activity supports interactions between ISUP IT, ISUP ATC, MF OP, and MF ES trunks and the following line based services:

- Three way calling
- Call Transfer
- Call Forwarding (all variations except CFRA)¹⁰
- Call Waiting

Transparency with the legacy DMS service set is provided for these services. The same service interactions and restrictions that exist with legacy MF OP and ES trunks also apply to MF OP and ES trunks configured on a GWC.

This activity supports interoperability with the following agent types when a service interaction, such as three way calling or call transfer, results in a connection with either an OP or ES trunk:

- DPT
- ISUP trunk
- PRI trunk
- line

Applicable customer facing sections

Fault Management

Logs	__N/A__

Alarms	__N/A__

Configuration

Data Schema	__X__

User Interface	__X__

Element Management	__N/A__

Security	__N/A__

Service Order	__N/A__

Office Parameters	__N/A__

Accounting (includes AMA billing)	__N/A__

10. Call forwarding for operator and 911 is not supported in the legacy switching system. Attempts to call forward to operator or 911 is blocked by the switch software. CS2K is consistent with legacy and blocks attempts to call forward.

Performance (includes operational measurements) __N/A__

Glossary

Term	Description
AIN	Advanced Intelligent Network
AMA	Automatic Message Accounting
ANI	Automatic Number Identification
APG	Anchor Packet Gateway
ATT	Automated Test Trunk
AUEP	AuditEndpoint
B911	Basic 911
BI	Barge-In
BLV	Busy Line Verification
CAS	Channel Associated Signaling
CFL	Carrier Failure
CFRA	Call Forward Remote Access
CLI	Calling Line Identification
CMTS	Cable Modem Termination System
CS2K	Call Server 2000
CS2M	Call Server 2000 Manager
DISA	Direct Inward Service Access
DMS	Digital Multiplex System
DN	Directory Number
DP	Dial Pulse
DPT	Dynamic Packet Trunk
DTC	Digital Trunk Controller
E911	Emergency 911
EAOSS	Exchange Access Operator Services Signaling
EO	End Office
ES	Emergency Service

Term	Description
FGC	Feature Group C
GWC	Gateway Controller
HFC	Hybrid Fiber Coax
I	Information (I) digit
IAC	Integrated Access - Cable
IEC	Inter-Exchange Carrier
IETF	Internet Engineering Task Force
II	Information (II) digits
IP	Internet Protocol
ISUP	ISDN User Part
LEC	Local Exchange Carrier
MAP	Maintenance and Administration Position
MF	Multi-Frequency
MG	Media Gateway
MGC	Media Gateway Controller
MOSS	Modified Operator Services Signaling
MTA	Multimedia Terminal Adapter
OM	Operational Measurement
OP	Operator
PPVM	Peripheral Processor Virtual Machine
PRI	Primary Rate Interface
PTS	Per Trunk Signaling
PSTN	Public Switched Telephone Network
QCA	QoS Collector Application
QoS	Quality of Service
RSIP	ReStartInProgress
SS7	Signaling System Number 7
TDM	Time Division Multiplex
TGCP	Trunking Gateway Control Protocol

Term	Description
TMM	Trunk Maintenance Manager
TTP	Trunk Test Position
UAS	Universal Audio Server

Configuration for A00003630

Hardware and Software Requirements

It is assumed the hardware and software installation of the CS2K is complete with the SN07 load lineup for the CS2K core, GWC, and CS2M. The MG is provided by a third party gateway vendor supporting TGCP as described in the PKT-SP-TGCP-I05-030728 TGCP Specification. Additionally, CS2M and OSSGate is initialized and available for provisioning data related to this activity.

Initial Configuration

Refer to section [“Configuration Walkthrough” on page 1154](#).

Office/Subnet parameters (OP/SP) (CM & SESM)

No new office parameter or subnet parameter is introduced by this activity.

Upgrade Impact

Dump and Restore

None

Element Management Upgrade

Since TGCP profile is a new gateway profile introduced in SN07, there is no upgrade work required to upgrade existing TGCP gateways to the ones with the new profile.

However, through this feature, all the 5 existing PVG profiles are collapsed into one profile -- PVG.

PVG15K
PVG15K_1000
PVG15K_PARTIAL
PVG7K
PVG_VSP3

All existing PVG gateway profiles share the same information other than the maximum reserved endpoints. The new PVG profile is defined to have the maximum reserved endpoints to be the maximum of all the ones defined in the existing PVG profiles.

Similarly, all the following “Motorola” profiles are collapsed into one profile -- “MOTOROLA”.

MOTOROLAMTA_1
MOTOROLAMTA_2
MOTOROLAMTA_4

All the following four “TouchTone” profiles are collapsed into one profile -- “TOUCHTONE”.

TOUCHTONE_NN01_1
TOUCHTONE_NN01_2
TOUCHTONE_NN01_3
TOUCHTONE_NN01_4

All the following “MediaTrix” profiles are collapsed into one profile -- “MEDIATRIX”.

MEDIATRIX_LINE_GW_24
MEDIATRIX_LINE_GW_4

All the following “ASKEY” profiles are collapsed into one profile -- “ASKEY”.

ASKEY_LINE_GW_12
ASKEY_LINE_GW_30
ASKEY_LINE_GW_4

All the following “CVX” profiles are collapsed into one profile -- “CVX”.

CVX1800_2688
CVX600_612

All the following “ARRIS” profiles are collapsed into one profile -- “ARRIS”.

ARRIS_TOUCHTONE_NN01_4
ARRIS_TOUCHTONE_NN02_4

All the following “PVG” profiles are collapsed into one profile -- “PVG_APG”.

PVG_APG
PVG_APG_VSP3

Because of the collapse activity, upgrade plug-ins are written to upgrade all the existing gateways to reference their new respective gateway profile.

Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
NORTEL-GWC-COMMON-TC	changed	unchanged
SERVRINV	changed	unchanged
TRKGRP	changed	unchanged
TRKSGRP	changed	unchanged
TRKOPTS	changed	unchanged
TRKMEM	changed	unchanged

Table/MIB/Remote Database Schema information

Name: NORTEL-GWC-COMMON-TC

Nortel GWC Common attributes MIB

Functional description

This MIB is used for defining all the supported gateway protocols.

In this MIB, a new protocol “TGCPPROTOCOL” is added in the supported protocol list for the field “GWCDDeviceProtocol” as shown below. The rest of the MIB stays the same.

GWCDDeviceProtocol ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

“Represents device protocol type defined in gwcdtype.h and callpdefs.h on the Gateway Controller. The module gwcdtype.h,
enum gw_protocols {NIL_PROTOCOL, NCS_PROTOCOL, ASPEN, DSMCC, MEGACO, MGCP, TGCPPROTOCOL, FILLER3_PROTOCOL, GWCRESERVED, DQOSPROTOCOL, MGCP_PLUS, H323}.”

SYNTAX INTEGER {nilprotocol (0),
 ncsprotocol (1),
 aspen (2),
 dsmcc (3),
 megaco (4),
 mgcp (5),
 tgcpprotocol (6),
 filler3protocol (7),
 gwcreerved (8), -- GWC internal use only
 dqosprotocol (9),
 mgcpplus (10),
 h323 (11)}

Usage sequence and implications (CM Only)

Not Applicable

Size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
NORTEL-GWC-COMMON-TC	0	115000	

Fields/OIDs

The following table lists fields/OIDs for **NORTEL-GWC-COMMON-TC**.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GWCDDeviceProtocol	Changed	N/A	TGCP PROTOCOL	When provisioning a TGCP gateway, TGCP protocol information needs to be sent down to the GWC device from SESM.

Datafill example

When sending SNMP set to the GWC device, GWCDDeviceProtocol should be set to 12 for provisioning TGCP gateways.

GWCDDeviceProtocol = 6;

Translation verification other tools

Not Applicable

Name: SERVINV

Server Inventory table

Functional description

This activity adds a new exec line-up, GWCABEX, for GWC node types. The new exec line-up is specific to Succession End Office and Tandem Per Trunk Signaling (PTS) trunk types configured on a GWC node type. For GWCs configured with MF OP and/or ES trunk group members, GWCABEX must be provisioned with the **ABTRK** TRMTYPE in table SERVINV.

Usage sequence and implications (CM Only)

Current datafill order unchanged by this activity.

Size

The size of this table is unchanged by this activity.

Fields/OIDs

The following table lists fields for table SERVINV changed by this activity. The configuration information for all other fields in table SERVINV are unchanged.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SRVREXEC	changed	TRMTYPE	unchanged	The TRMTYPE subfield is unchanged. This activity adds a new EXEC entry for the existing TRMTYPE of ABTRK .
		EXEC	GWCABEX	The new exec line-up, GWCABEX, is added. For GWCs configured with either OP or ES trunk group members, GWCABEX must be provisioned with a TRMTYPE ABTRK .

Datafill example

The following example shows sample datafill for table SERVINV.

```

SRVRNAME      SRVRADDR
SRVRTONE      SRVROPTS
-----
              GWC      0      IP 47 174 66 4
              (      ABTRK  GWCABEX)
NORTHAM      $

```

Table release history update

The following information is added to table SERVRINV:

exec line-up GWCABEX added to field SRVREXEC

Supplementary information

Tuples in table SERVRINV should not be added or changed via manual table control commands. Provisioning of this table should be performed using CS2M GWC node provisioning.

The modifications to table SERVRINV is a shared requirement with activity A00003506. See activity A00003506 for further details.

Translation verification other tools

Not applicable.

Name: TRKGRP

Trunk Group Table

Functional description

This activity introduces new provisioning restrictions in table TRKGRP for MF OP and ES trunk groups configured on a GWC. The restrictions apply when the trunk group is assigned the GWCPTSTK option in table TRKOPTS and the trunk group tuple is changed in table TRKGRP.

Supported GWC MF Trunk Group Types for TGCP MG

TrunkGroup Type	Supported Services
OP	Operator Services
ES	Emergency Services

Usage sequence and implications (CM Only)

When provisioning MF OP and ES trunk group members on a GWC, the following sequence of table provisioning is required.

1. table CLLI
2. table TRKGRP

3. table TRKOPTS, option GWCPTSTK
4. table TRKSGRP
5. table TRKMEM

Size

The size of this table is unchanged by this activity.

Fields/OIDs

Not Applicable

Datafill example

Not Applicable

Table release history update

The following information is added to table TRKGRP:

Restrictions added for GWC MF OP and ES trunk groups.

Supplementary information

When MF OP or ES trunk group data is changed in table TRKGRP, table control determines if option GWCPTSTK is provisioned in table TRKOPTS. GWCPTSTK identifies PTS packet trunk groups that provide connectivity between the packet network and the PSTN. If option GWCPTSTK is provisioned, table control performs error checking to ensure the TRKGRP data is provisioned correctly. The following table lists the new error messages that may be generated by table control.

TRKGRP Restrictions

Trunk Type	Error Messages
OP	"GWCPTSTK option exists in table TRKOPTS. DIR must be IC or OG." "GWCPTSTK option exists in table TRKOPTS. ANITYPE must be REV." "GWCPTSTK option exists in table TRKOPTS. EAOSS must be N."
ES	"GWCPTSTK option exists in table TRKOPTS. DIR must be OG." "GWCPTSTK option exists in table TRKOPTS. ANI must be ANISPILL." "GWCPTSTK option exists in table TRKOPTS. SWST must be DC." "GWCPTSTK option exists in table TRKOPTS. FDISCTIM must be 0."

The modifications to table TRKGRP is a shared requirement with activity A00003506. See activity A00003506 for further details.

Translation verification other tools

Not Applicable

Name: TRKSGRP

Trunk Subgroup Table

Functional description

This activity introduces new provisioning restrictions in table TRKSGRP for MF OP and ES trunk groups configured on a GWC. The restrictions apply when the trunk group is assigned the GWCPTSTK option in table TRKOPTS and adding or changing the trunk subgroup tuples in table TRKSGRP.

Usage sequence and implications (CM Only)

When provisioning MF OP and ES trunk group members on a GWC, the following sequence of table provisioning is required.

1. table CLLI
2. table TRKGRP
3. table TRKOPTS, option GWCPTSTK
4. table TRKSGRP
5. table TRKMEM

Size

The size of this table is unchanged by this activity.

Fields/OIDs

Not Applicable

Datafill example

Not Applicable

Table release history update

The following information is added to table TRKSGRP:

Restrictions added for GWC MF OP and ES trunk groups.

Supplementary information

When MF OP or ES trunk groups are provisioned or tuples are changed in table TRKSGRP, table control determines if option GWCPTSTK is provisioned in table TRKOPTS. GWCPTSTK identifies PTS packet trunk groups that provide connectivity between the packet network and the PSTN. If option GWCPTSTK is provisioned, table control performs error checking to ensure the TRKSGRP data is provisioned correctly. [“TRKSGRP Restrictions” on page 1141](#) lists the new error messages that may be generated by table control.

TRKSGRP Restrictions

TRKSGRP Field	Error Messages
OP, ES	"GWCPTSTK option exists in table TRKOPTS. CCONT must be NO." "GWCPTSTK option exists in table TRKOPTS. OPULSTYP in table TRKSGRP must be MF for this trunk type." "GWCPTSTK option exists in table TRKOPTS.OSTARTSG in table TRKSGRP must be WK for this trunk type." "GWCPTSTK option exists in table TRKOPTS. SGRPVAR must be STD." "GWCPTSTK option exists in table TRKOPTS. RNGBCK must be MW." "GWCPTSTK option exists in table TRKOPTS. ESUPR must be N." "GWCPTSTK option exists in table TRKOPTS. ECSTAT must be INTERNAL or EXTERNAL."

Provisioning of this table may also be performed using OSSGate. The error checking described above is performed on TRKSGRP data enter through OSSGate.

The modifications to table TRKSGRP is a shared requirement with activity A00003506. See activity A00003506 for further details.

Translation verification other tools

Not Applicable

Name: TRKOPTS

Trunk Options Table

Functional description

A new trunk group option, GWCPTSTK, is added to table TRKOPTS. GWCPTSTK identifies PTS packet trunk groups that provide connectivity between the packet network and the PSTN. In the SN07 release, GWCPTSTK is supported with all GWC PTS supported trunk group types configured on a GWC. This option must be provisioned prior to configuring MF OP and/or ES trunk group members in table TRKMEM.

Additionally, this activity adds a sub-option, PRELOADANI, to the GWCPTSTK trunk group option. PRELOADANI sub-option identifies PTS packet trunks which support a call model that allows the ANI digits to be sent from the Core to the GWC prior to receiving any ANI request from the far-end.

Usage sequence and implications (CM Only)

When provisioning MF OP and ES trunk group members on a GWC, the following sequence of table provisioning is required.

1. table CLLI
2. table TRKGRP

3. table TRKOPTS, option GWCPTSTK
4. table TRKSGRP
5. table TRKMEM

Table TRKOPTS may be provisioned following table TRKSGRP. Table control restrictions enforce table TRKOPTS be provisioned after table TRKGRP and before table TRKMEM.

Size

The size of this table is unchanged by this activity.

Fields/OIDs

The following table lists fields for TRKOPTS that are changed by this activity.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTKEY	changed	CLLI	unchanged	The CLLI subfield is unchanged. Provision the OP or ES trunk group CLLI.
		OPTION	GWCPTSTK	The new option GWCPTSTK is added. For MF OP and ES trunks configured on a GWC, this option must be provisioned.
OPTION	changed	OPTION	GWCPTSTK	The new option GWCPTSTK is added. For PTS trunks configured on a GWC, this option must be provisioned.
		PRELOAD ANI	Y/N	The new sub-option PRELOADANI is added. For GWC PTS trunks which support a call model that allows the ANI digits to be sent from the Core prior to receiving an ANI request, the field must be to Y.

Datafill example

The following example shows sample datafill for table TRKOPTS.

OPTKEY	OPTINFO
PTSCLLI	GWCPTSTK GWCPTSTK N

Table release history update

The following information is added to table TRKOPTS:

Option GWCPTSTK added for GWC PTS trunk groups.

Supplementary information

Option GWCPTSTK identifies PTS packet trunk groups that provide connectivity between the packet network and the PSTN. This option applies to all GWC PTS trunk group types supported in the SN07 release. Table control in table TRKOPTS blocks the addition of this option to a non-supported trunk type (see activity A00003506 for the list of supported PTS trunk types on a GWC). The following error message will result:

“GWCPTSTK cannot be assigned for the following reasons:”

“It is not supported with this trunk type.”

This option cannot be added for PTS trunk groups if there is existing datafill in either table TRKGRP or table TRKSGRP not supported on the GWC. If this error occurs when provisioning GWCPTSTK in table TRKOPTS, the tuple entry in table TRKGRP and/or table TRKSGRP must be changed. See [“TRKGRP Restrictions” on page 1139](#) and [“TRKSGRP Restrictions” on page 1141](#) for the list of restrictions.

This option cannot be added to a supported PTS trunk group that contains members on a peripheral type other than a GWC. PTS trunk groups on a GWC can not consist of members on different peripheral types, such as a GWC and DTC (hybrid PTS trunk groups are not supported). A check is made of other trunk members already present in table TRKMEM prior to assigning the GWCPTSTK option. If members are present it is assumed they do not have a PMTYPE of GWC, since the option isn’t assigned yet. The following error will result:

“GWCPTSTK cannot be assigned for the following reasons:”

“Trunk Members exist in table TRKMEM”

This option cannot be deleted from table TRKOPTS until all members on the trunk group have been deleted from table TRKMEM. The following error will result:

“GWCPTSTK cannot be deleted for the following reasons:”
“Trunk Members exist in table TRKMEM”

The PRELOADANI sub-option applies only to GWC PTS trunk group types of OP and ES. The PRELOADANI sub-option cannot be set to “Y” for other GWC PTS trunk group types (see activity A00003506 for the list of supported PTS trunk types on a GWC).

Translation verification other tools

Not Applicable

Name: TRKMEM

Trunk Member Table

Functional description

This activity introduces new provisioning restrictions in table TRKMEM for MF OP and ES trunks groups configured on a GWC.

Usage sequence and implications (CM Only)

When provisioning MF OP and ES trunk group members on a GWC, the following sequence of table provisioning is required.

1. table CLLI
2. table TRKGRP
3. table TRKOPTS, option GWCPTSTK
4. table TRKSGRP
5. table TRKMEM

Size

The size of this table is unchanged by this activity.

Fields/OIDs

Not Applicable

Datafill example

Not Applicable

Table release history update

The following information is added to table TRKMEM:

Restrictions added for GWC MF OP and ES trunk groups.

Supplementary information

Table control for table TRKMEM determines if the option GWCPTSTK is provisioned in table TRKOPTS. If option GWCPTSTK is provisioned, table control performs error checking to ensure the TRKMEM data is provisioned correctly (see [“TRKMEM Restrictions” on page 1145](#)).

TRKMEM Restrictions

TRKMEM Action	Error Messages
Attempt to ADD member with GWC PMTYPE to PTS group without GWCPTSTK option.	TBD
Attempt to ADD member with non-GWC PMTYPE to PTS group with GWCPTSTK option	TBD
Attempt to Change PMTYPE from GWC to non-GWC.	TBD
Attempt to CHANGE PMTYPE from Non-GWC to GWC	TBD

Provisioning of this table may also be performed using OSSGate. The error checking described above is performed on TRKMEM data enter through OSSGate.

The modifications to table TRKMEM is a shared requirement with activity A00003506. See activity A00003506 for further details.

Translation verification other tools

Not Applicable

Service Orders (SO) (CM & SESM)

Service Order unchanged by this activity.

Software optionality control (SOC)

Not Applicable. There is no SOC control for this activity.

Element Management

New/modified GUIs

GUI name	NEW, CHANGED, or DELETED
Associate Gateway	Changed
Add GWC	Changed

GUI information

GUI name: Add GW

Associate Gateway Dialog

Functional description

Associate Gateway Dialog is a graphic tool that provides the crafts person with the ability to associate a gateway. For this activity, a TGCP gateway can be associated via the Associated Gateway Dialog from CS2M GUI.

GUI usage and implications

There is no requirement to datafill the Associate Gateway Dialog in a specific order.

GUI size

New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Add GW	0	10	64k

GUI fields

The following table lists fields for the Associate Gateway Dialog.

- Gateway Name
- Gateway IP Address
- Gateway Controller Name
- Gateway Profile Name
- Reserved Terminations
- Protocol Type
- Protocol Port

- Protocol Version

GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Gateway Profile Name	Changed	N/A	TGCP	When adding a TGCP gateway, the TGCP gateway profile should be selected from the provided profile list.	GWC-GW-MIB

Usage example

The following example shows sample datafill or menu selection for GUI Associate Gateway Dialog:

Associate Media Gateway

Gateway name:

Gateway IP address:

Gateway controller name:

Gateway profile name:

Reserved terminations:

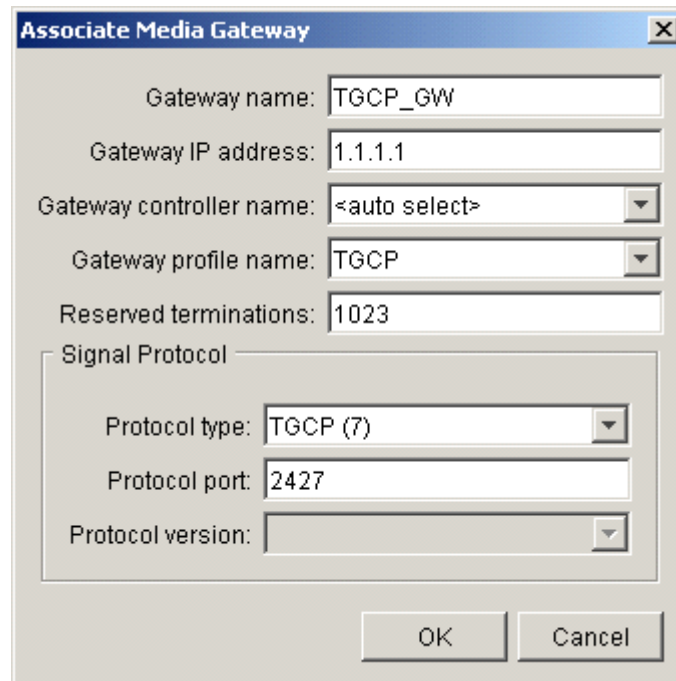
Signal Protocol

Protocol type:

Protocol port:

Protocol version:

OK Cancel



The image shows a Windows-style dialog box titled "Associate Media Gateway". It contains several input fields and dropdown menus. The fields are: "Gateway name" with the value "TGCP_GW", "Gateway IP address" with the value "1.1.1.1", "Gateway controller name" with a dropdown menu showing "<auto select>", "Gateway profile name" with a dropdown menu showing "TGCP", and "Reserved terminations" with the value "1023". Below these is a section titled "Signal Protocol" which contains three fields: "Protocol type" with a dropdown menu showing "TGCP (7)", "Protocol port" with the value "2427", and "Protocol version" with a dropdown menu. At the bottom right of the dialog are "OK" and "Cancel" buttons.

OSSGate Interface

The following is an example of an XML input file when using OSSGate interface to datafill a TGCP gateway.

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <assocMG usn="1" version="1.0">
        <Parameters>
          <mgUIName>mg1.nortel.net</mgUIName>
          <mgProfileName>TGCP_GW</mgProfileName>
          <mgIpAddr>47.49.23.43</mgIpAddr>
          <mgProtocolType>12</mgProtocolType>
          <mgProtocolVersion>1.0</mgProtocolVersion>
          <mgProtocolPort>2427</mgProtocolPort>
          <gwcUIName>GWC-0</gwcUIName>
        </Parameters>
      </assocMG>
    </Methods>
  </Command>
</CommandList>
```

GUI name: Add GWC

Add Gateway Controller Dialog

Functional description

Add Gateway Controller Dialog is a graphic tool that provides the crafts person with the ability to add a gateway controller.

When PTS functionality is provided, a different TRUNK profile needs to be selected to provision different EXEC types in the XACore.

GUI usage and implications

There is no requirement to datafill the Add Gateway Controller Dialog in a specific order.

GUI size

New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Add GWC	0	10	64k

GUI fields

The following table lists fields for the Add Gateway Controller Dialog.

- Gateway Controller Name
- Gateway Controller Active IP Address
- Message Router IP Address
- Gateway Controller Profiles
- Tone Data
- Exec Data
- Type List

GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Gateway Controller Profile Name	Changed	N/A	TRUNKNA	When PTS functionality is provided, TRUNKNA needs to be selected when adding a GWC	GWC-GWC-MIB
EXEC Type	Changed	N/A	(DTCEX, PRAB) (GWCABEX, ABTRK)	When PTS functionality is provided, EXEC type needs to include ABTRK	

Usage example

The following example shows sample datafill or menu selection for GUI Add Gateway Controller Dialog:

The screenshot shows the 'Add Gateway Controller' dialog box with the following fields and values:

- Gateway controller name: GWC-6
- Gateway controller active IP address: 47.142.128.64
- Message router IP address: 47.142.128.24
- Gateway controller profiles: TRUNKNA_PTS (selected in a dropdown menu)
- Profile Data Information section:
 - Tone data: NORTHAM
 - Exec data: DTCEX PRAB (selected in a dropdown menu)
 - Type list: 8 (selected in a dropdown menu)

At the bottom are 'OK' and 'Cancel' buttons.

This screenshot is identical to the one above, but the 'Type list' dropdown menu is expanded, showing two options: 'DTCEX PRAB' and 'DTCEX AB250'. 'DTCEX PRAB' is currently selected.

OSSGate Interface

The only method of adding a gateway controller is through GUI. There is no XML interface for it.

Command interface changes**Directory: TTP****Directory description**

Trunk Test Position (TTP) is changed. New restrictions are added at this MAP level for MF OP and ES trunk groups provisioned on a GWC.

Accessing directory: TRKS**Access to directory or MAP level and return to CI**

To access TTP for the CI environment enter “mapci;mtc;trks;ttp”

To return to the CI environment enter “quit all”.

Supplementary information

New restrictions are added to the TTP level of the MAP for MF OP and ES trunks configured on a GWC.

The “Seize” and “Cktinfo” commands are not supported for MF OP and ES trunks configured on a GWC. The following error message is displayed if an attempt is made to execute these commands:

“Action not supported on GWC trunks.”

The “TST” and “Ckt” commands require certain Succession components to support MF OP and ES trunks configured on a GWC. The following error message is displayed if an attempt is made to execute these commands without the available components:

“Action not supported on GWC trunks.” or

“No IW SPM IP Bridges Available to Perform Action.”

Directory: MONITOR**Directory description**

MONITOR is changed. New restrictions are added at this MAP level for MF OP and ES trunk groups provisioned on a GWC.

Accessing directory: TTP**Access to directory or MAP level and return to CI**

To access MONITOR for the CI environment enter “mapci;mtc;trks;ttp;level monitor”

To return to the CI environment enter “quit all”.

Supplementary information

New restrictions are added to the MONITOR level of the MAP for MF OP and ES trunks configured on a GWC.

The “CktMon”, “CPos_”, and “RLS” commands are not supported for MF OP and ES trunks configured on a GWC. The following error message is displayed if an attempt is made to execute these commands:

“Action not supported on GWC trunks.”

The “TST” and “MonTalk” commands require certain Succession components to support MF OP and ES trunks configured on a GWC. The following error message is displayed if an attempt is made to execute these commands without the available components:

“Action not supported on GWC trunks.” or
“No IW SPM IP Bridges Available to Perform Action.”

MONITOR level is not accessible for posted MF OP and ES trunks configured on a GWC if Succession IW bridges are not available. The following error message is displayed if an attempt is made to enter the MONITOR map level without the available components:

“No IW SPM IP Bridges Available to Perform Action.”

Directory: MANUAL**Directory description**

MANUAL is changed. New restrictions are added at this MAP level for MF OP and ES trunk groups provisioned on a GWC.

Accessing directory: TTP**Access to directory or MAP level and return to CI**

To access MANUAL for the CI environment enter “mapci;mtc;trks;ttp;level manual”

To return to the CI environment enter “quit all”.

Supplementary information

New restrictions are added to the MANUAL level of the MAP for MF OP and ES trunks configured on a GWC.

The “OP_”, “SGNL”, and “RLS” commands are not supported for MF OP and ES trunks configured on a GWC. The following error message is displayed if an attempt is made to execute these commands:

“Action not supported on GWC trunks.”

The “Loss”, “TGEN”, “TST”, “Noise”, “TDET”, and “HSET” commands require certain Succession components to support MF OP and ES trunks configured on a GWC. The following error message is displayed if an attempt is made to execute these commands without the available components:

“Action not supported on GWC trunks.” or

“No IW SPM IP Bridges Available to Perform Action.”

Directory: DATA**Directory description**

DATA is changed. New restrictions are added at this MAP level for MF OP and ES trunk groups provisioned on a GWC.

Accessing directory: TTP**Access to directory or MAP level and return to CI**

To access DATA for the CI environment enter “mapci;mtc;trks;ttp;level datattp”

To return to the CI environment enter “quit all”.

Supplementary information

New restrictions are added to the DATA level of the MAP for MF OP and ES trunks configured on a GWC.

The “Seize”, “BTerm_”, and “RLS” commands are not supported for MF OP and ES trunks configured on a GWC. The following error message is displayed if an attempt is made to execute these commands:

“Action not supported on GWC trunks.”

The “BERT_” command require certain Succession components to support MF OP and ES trunks configured on a GWC. The following error message is displayed if an attempt is made to execute this command without the available components:

“Action not supported on GWC trunks.” or
“No IW SPM IP Bridges Available to Perform Action.”

Security

Not covered by this activity. See activity A00003576.

Configuration Walkthrough

Following is a high-level walkthrough of the steps required to provision MF OP and ES trunk groups on a GWC.

1. Add the GWC node using the CS2M GWC EM. The CS2M GWC EM will provision table `SERVRINV` on the CS2K core. The new exec line-up, **GWCABEX**, must be selected when provisioning the GWC node.
2. Provision the TGCP MG(s) using the CS2M GWC EM. The gateway profile name that should be provisioned for a TGCP MG is “**tbd**¹¹”. Additionally, TGCP protocol must be specified.

When provisioning the TGCP MGs, the GWC name must be entered. In the SN07 release, MF OP and ES trunks must be configured on a GWC reserved for PTS trunks only. The GWC name must be entered to prevent the GWC EM from discovering an incorrect GWC.

3. Provision the TGCP MG endpoints on the GWC using the CS2M GWC EM. The endpoint names and terminal numbers returned by the GWC EM should be noted. The terminal numbers are required for provisioning table `TRKMEM` on the CS2K core.
4. Provision table `CLLI` with the OP and/or ES trunk group cli.
5. Provision table `TRKGRP` with the OP and/or ES trunk group data. Note the table control restrictions described in [“TRKSGRP Restrictions” on page 1141](#).
6. Provision the `GWCPTSTK` option for MF OP and/or ES trunk group cli in table `TRKOPTS`.
7. Provision table `TRKSGRP` with the OP and/or ES trunk subgroup data. Note the table control restrictions described in [“TRKSGRP Restrictions” on page 1141](#).
8. Provision table `TRKMEM` with the OP and/or ES trunk group members. The terminal number information provided by the CS2M GWC EM is required when entering tuples in table `TRKMEM`. Note the table control restrictions described in section [“Name: TRKMEM” on page 1144](#).

Following is a high-level walkthrough of the steps required to provision TGCP ISUP IT and/or ATC trunk groups on a GWC.

11. The profile name can not be confirmed at this time, but will be updated when the activity is completed.

1. Add the GWC node using the CS2M GWC EM. The CS2M GWC EM will provision table SERVINV on the CS2K core.
2. Provision the TGCP MG(s) using the CS2M GWC EM. The gateway profile name that should be provisioned for a TGCP MG is “**tbd**¹²”. Additionally, TGCP protocol must be specified.

When provisioning the TGCP MGs, the GWC name must be entered. The GWC name must be entered to prevent the GWC EM from discovering an incorrect GWC.
3. Provision the TGCP MG endpoints on the GWC using the CS2M GWC EM. The endpoint names and terminal numbers returned by the GWC EM should be noted. The terminal numbers are required for provisioning table TRKMEM on the CS2K core.
4. Provision table CLLI with the ISUP IT and/or ATC trunk group clii.
5. Provision table TRKGRP with the ISUP IT and/or ATC trunk group data.
6. Provision table TRKSGRP with the ISUP IT and/or ATC trunk subgroup data.
7. Provision table TRKMEM with the ISUP IT and/or ATC trunk group members. The terminal number information provided by the CS2M GWC EM is required when entering tuples in table TRKMEM.
8. Provision table ISUPDEST with the C7 routeset for the ISUP IT and/or ATC trunk subgroups.

Provision table C7TRKMEM with the C7 circuit ID code (CIC) for the ISUP IT and/or ATC trunk group members.

Product = CS 2000

A00003667 -- SESM NB Alarm Interface Changes required for OSS (UA-IP)

Functional Description

This SN07 feature modifies some of the existing functionality in the SESM alarm system. Primarily, it refines and updates the CORBA interface to include data that enhances the usability of the alarm notifications. This includes a resynchronization mechanism, improved performance, and a change to the data passed to include additional alarm information.

12. The profile name can not be confirmed at this time, but will be updated when the activity is completed.

The majority of these changes do not impact the customer as they are transparent to the user. The customer areas impacted include:

- SESM Alarm GUI - removal of acknowledge and de-acknowledge interface. This change is discussed in the configuration section.
- SESM Syslog Alarm Feed - this feed will be disabled by default as the primary northbound feed will be CORBA notifications to the IEMS. The resulting Nortel Standard or SCC2 logs should be identical to those generated in previous releases. This change is discussed in the configuration section.
- Change to alarm log generated when SESM cannot communicate with a managed device. Previously, the log was owned by the device, now it will be a SESM alarm and will be a major instead of a critical. This change is discussed in the fault management section.
- Creation of a log to identify when SESM is encountering difficulties generating CORBA notifications for alarm events. This change is discussed in the fault management section.
- Creation of a log upon startup and shutdown of SESM.

Hardware Requirements or Dependencies

N/A - No new hardware is required.

Software Requirements or Dependencies

The change to the interface requires that all clients of the SESM alarm system are upgraded to be able to continue to use the alarm notifications. Without being upgraded, existing clients of the alarm system notifications will not function.

Limitations and restrictions

With this feature, the SESM alarm GUI no longer allows alarm acknowledgements. This ability is present in the IEMS alarm GUI and all alarm acknowledgements should be done there.

Interactions

N/A

Applicable customer facing sections

Fault Management

Logs ☒

Alarms ☒

Configuration

Data Schema ☐

User Interface	_____
Element Management	_____X_____
Security	_____
Service Order	_____
Office Parameters	_____
Accounting (includes AMA billing)	_____
Performance (includes operational measurements)	_____

Fault Management for A00003667

Fault management strategy

There are three changes to the existing SESM fault management structure.

One is the elimination of the SESM alarm acknowledgement function. This is removed because the alarm acknowledgements are being handled at the IEMS level of alarm management. This change will apply to the SESM alarm GUI clients. It is discussed briefly below and more fully in the configuration section.

The second is the update of the SESM communications alarm previously “owned” by the device. The alarm was raised as an alarm from the device that SESM could not communicate with. This was an inaccurate representation of the source of the alarm as the device itself may not have any alarm condition. The alarm was also a critical and this was inaccurate as it did not necessarily mean an outage was occurring or imminent. The alarm has been changed to a major to reflect that the current condition could cause an outage.

The third is the generation of logs on SESM. One each is generated upon startup and shutdown and one when SESM cannot generate alarm notification events. These logs will be sent via the syslog to the SDM.

Fault management tools and utilities

There are two SESM alarm GUI’s. One shows active alarms on the managed devices and the other shows the alarm history. On the active alarm GUI, the ability to acknowledge an alarm will be removed. This function is handled by the IEMS alarm GUI. By removing it, there is no confusion whether an alarm is acknowledged or not.

The only change to the alarm GUI’s will be the removal of the acknowledge options in the active alarm manager and the removal of the “show acknowledged” check box on the alarm history window.

Logs

Explanation

The CMT500 log is generated by the SESM alarm system to indicate the system is initializing.

Format

```
COMPACT2 CMT500 JUN30 11:01:55 0580 INFO CMT INFO Init
CS2K Management Tools Alarm Manager Initialization.
```

Cause – SESM server is restarting.

Action – None.

Interfaces – this is generated by the SESM alarm system via syslog.

Field descriptions

N/A

Action

N/A

Associated Operational Measurements or Performance Measurements

N/A

Additional information

N/A

Explanation

The CMT501 log is generated by the SESM alarm system upon shutdown.

Format

```
COMPACT2 CMT501 JUN30 11:01:55 0580 INFO CMT INFO Shutdown
CS2K Management Tools Alarm Manager Shutting Down.
```

Cause – SESM Server has been shutdown.

Action – A SESM administrator should ensure that the server was intentionally shutdown and that it is being restarted.

Interfaces – this is generated by the SESM alarm system via syslog.

Field descriptions

N/A

Action

A SESM administrator should ensure that the server was intentionally shutdown and that it is being restarted.

Associated Operational Measurements or Performance Measurements

N/A

Additional information

N/A

Explanation

The CMT 502 log is generated by the SESM alarm system to inform northbound alarm clients that alarm notifications cannot be generated. This log will be sent via the SSPFS syslog feed to the customer log.

Format

```
COMPACT2 CMT502 JUN30 11:01:55 0580 INFO CMT INFO
CS2K Management Tools Alarm Manager failed to raise alarm
notification due to CORBA failure. Please check CORBA status on
CS2K Management Tools server.
```

The is just a sample of how the log might look. The final format will be provided prior to IT.

Cause – CORBA communications on the SESM server or within SESM are failing.

Action – A SESM administrator should check the communications on the SESM server.

Interfaces – this is generated by the SESM alarm system via syslog.

Field descriptions

N/A

Action

The SESM administrator should determine the status of the CORBA communications on the SESM server and the network connectivity of that machine.

Associated Operational Measurements or Performance Measurements

N/A

Additional information

This log is intended for users of the SESM CORBA alarm notifications to inform the user that events cannot be generated.

Alarms

There is one change to an existing alarm. The alarm was previously a device owned alarm represented as GWC398 or UAS398 and was a critical alarm. It has been changed to be owned by the CMT and will be a major alarm now.

This is the new format of the communication error log. Changed fields in bold.

COMPACT2 ** **CMT302** JUN30 11:01:55 0580 TBL **CMT** Fault

Location: SNMP_NE_Poller

NotificationID: 0

State: Raise

Category: Communications

Cause: Communications subsystem failure

Time: Jun 30 11:01:55 2003

Component Id: SNMP Device Poller;Device=rtpsUASa;DeviceID=0x0000006
3000000a12f8e5952

Specific Problem: SNMP Timeout

Description: CMT Unable to communicate with managed device

Severity – Major, as it may indicate a network issue or an issue with the device itself, and it could lead to an outage.

Cause – SNMP poller cannot communicate to the network device

Duration – will remain active until communications are reestablished to the device being polled

Action – have a network administrator determine the cause of the SNMP timeout to the device

Interfaces – this is generated by the SNMP poller on SESM

Configuration for A00003667

Hardware and Software Requirements

No change due to this feature.

Initial Configuration

No change due to this feature.

Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

Upgrade Impact**Dump and Restore**

N/A

Element Management Upgrade

This feature introduces a new mechanism for sending SESM alarm logs northbound. Previously this was handled via syslog to the SDM. In this release, it can be handled by CORBA notifications to the IEMS.

For customers that use IEMS in SN07, the syslog generation should be turned off to avoid duplication of the alarm logs. This cannot be turned off over the upgrade because some customers will not have IEMS in SN07. So this should be a manual step post-installation.

To turn the SESM syslog generation off:

- 1) As root on the SESM server: > cd /opt/nortel/NTsesm/admin/bin/
- 2) Run: ./configure
- 3) Select option 5: SESM logging configuration (syslog, sesm debug log)
- 4) Select option 3: SESM Alarm Logging configuration
- 5) Enter n
- 6) Exit the configuration tool
- 7) Restart the SESM application: ./ptmctl restart

In the case of new installations, this northbound syslog generation will still be turned on by default. To turn this off for customers with IEMS, the same commands listed above should be run post installation.

Data schema (DS) (CM, MIBS, RDB)

N/A

Service Orders (SO) (CM & SESM)

N/A

Software optionality control (SOC)

N/A

Element Management

New/modified GUIs

New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
SESM Alarm Manager	Changed
SESM Alarm History	Changed

GUI information

GUI name: SESM Alarm Manager and Alarm History

Functional description

The Alarm Manager is the SESM GUI used to monitor active alarms in on devices it manages. It receives CORBA notifications when new alarms occur or when existing alarms are cleared. Because of the addition of IEMS and its alarm manager, the alarm acknowledgment feature is no longer required at this level. Alarms should be acknowledged at the network management level.

Alarm History is the SESM GUI used to view all alarms received by the system (to save disk space, old alarms are cleared after some preconfigured time period, usually 1 week). This GUI shows both active and cleared alarms.

GUI usage and implications

Because of the addition of IEMS and its alarm manager, the alarm acknowledgment feature is no longer required at this level. Alarms should be acknowledged at the network management level.

In the Alarm Manager, the ability to acknowledge and de-acknowledge the alarms will be removed. In the Alarm History, the check box to filter on acknowledged alarms will be removed so as to not be confusing.

GUI size

N/A

GUI fields

N/A

Usage example

N/A

GUI release history update

N/A

Supplementary information

N/A

CLUI Interface

N/A

Command interface changes

N/A

Security

N/A

Configuration Walkthrough

N/A

Product = CS 2000**A00003698 -- Razor Gateway Requirements for Trunking (PT-IP)*****Functional Description***

This feature provides an extension to the existing CALLTRAK/TRMTRACE functionality found on the Core. Currently there isn't a way to initiate a Trmtrace to capture incoming SIP based calls. This shortcoming is addressed by functionality delivered to the Core, GWC, and the Session Server network elements.

This feature is primarily targeted to Customer Support groups like GNPS. While the tool will be available in the field, due to the impact of running a Calltrak session on the capacity of the field office, it should not be done on a regular basis or at high traffic levels.

Background information

Previous releases of the Calltrak/Trmtrace functionality provided the interfaces required to turn on and off the GateWay Controller Trmtrace functionality. Prior to SIP based calls, the Core was able to start the Trmtrace on the GWC for a new call and so capture the trace from the beginning of the call. For SIP calls, this was no longer sufficient. The Core found out about SIP calls too late in the Call sequence to start the trmtrace. Also, the SIP GWC that would be used for a SIP call was not always pre-defined. These shortcomings are addressed by the functionality delivered by this feature.

The Session Server and the Core will now be able to track and initiate the Trmtrace on a SIP call for both incoming and outgoing SIP trunks. The user will only need to know the trunk group CLI for that SIP trunk (or Access Link) in order to capture the GWC Trmtrace from the beginning. The Session Server will also capture (locally) the SIP messages and GCP messages used in the life of the traced call.

Overview and Core information

The following is an overview of a typical tracing session.

- 1 Using the Calltrak interface, the user will select the SIP trunk (using the DPT select option). (No Changes to functionality)
- 2 The user will then start the calltrak trace. This has the following behavior:
 - a. The selected DPT trunk (in this case a SIP trunk) is noted and a 'setup' message is sent to a sip GWC.
 - b. The SIP GWC sends the setup message to each NGSS.
 - c. Each NGSS starts its trace on the selected trunk group/Link.
- 3 First call starts (either in the Core or NGSS).
 - a. The origination point sends a 'start_trmtrace' message to the selected SIP GWC.
 - b. The selected GWC initialized the trmtrace module to capture the trmtrace information on the supplied TID.
 - c. The selected GWC will also initialize a buffer to capture the messages (GCP messages specifically).
- 4 Other calls may or may not start/stop during this time.
- 5 First call Stops (either in the Core or the NGSS, based on which started it and knows it is being traced).
 - a. The release is sent followed by the 'stop_trmtrace' message for that TID.
 - b. The GWC stops the trmtrace for that TID (but doesn't touch other in-progress tracing).
- 6 More of the other calls...
- 7 The user stops the calltrak trace.
 - a. The setdown message is sent to the arbitrary SIP GWC.
 - b. GWC forwards the message to each NGSS
 - c. Each NGSS stops in-progress call trmtraces and responds to the GWC with a list of stopped trmtrace descriptions (i.e., like in the core output: GWC 9, TID 17...) for each TID that was traced on.

- d. This GWC then collects all responses and sends one or more unsolicited message to the core with this information.
 - e. Core outputs the list of stopped trmtrace messages to the user (using existing interface).
- 8 User is able to retrieve the captured information from the appropriate network elements in the GWC list and the NGSS.

There are no new Core interfaces. The current CallTrak and TRMTRACE interfaces are utilized along with the SELECT DPT option. Once a SIP trunk group is SELECTed, the TRMTRACE ON and START commands will work together to initiate the functionality.

Every effort is made to keep the user interfaces the same where they existed previously. For example the CallTrak interface to select a SIP based trunk is unchanged (the SELECT DPT option is utilized) and no other option needs to be set.

GWC information

The GateWay Controller interface to display the captured trmtrace information will be the same (trmtrc, dumpall). There will also be another interface to display the captured GCP messages. The following is an example:

From the GWC Telnet session (or PMDEBUG session, although that is very slow and is not recommended):

```
GWCUP>GCPDebug
```

```
DUMPmessages,Enable,Disable,DElete
```

```
GCPDebug>DUMPmessages
```

This will output the collected information in the following way:

Timestamp TID Direction

The Timestamp and TID will allow correlation with the TRMtrc;Printout;DUMPAll output that could be used to display all the TRMTRC information collected by the EDI interface.

The other commands are more for debugging. The Enable command will turn on the collection functionality, selecting all TIDs. The Disable command will turn off data collection. The DElete command will remove all the collected data.

Each entry in the output will contain the GCP message contents.

The above assumes that the terminal is connected via telnet (as the pmdebug interface will be too slow to display all the information in a reasonable amount of time).

NGSS information

The Session Server will only have a file that needs to be looked at to collect the information that is captured. The file is located in the application traces directory:

/opt/apps/logs

And the filename is:

NGSS_trmtrace.txt

The file will never be deleted automatically by the tool (unless it is very old and the partition has reached its upper limit - see limitations section), so the craft will always have to ensure to remove the file after collecting the information. The file can be looked at using on board tools like 'cat', 'vi', and 'more'. Also the file could be copied off board for downstream use.

The file will contain SIP messages, GCP messages, and basic call flow information like timestamp, direction of message, and callID. This information will be presented in ASCII format (indented to provide readability).

Hardware Requirements or Dependencies

Customer offices without the Session Server will not have the functionality delivered by this feature.

Software Requirements or Dependencies

The Session Server feature, A00003280 (SP2K Debug and Tracing) must be available. Also, certain other features developed for the Session Server will be required (Call Processing support, etc.) as well.

Limitations and restrictions

The feature will only apply to offices with the Session Server, SIP application. The VRDN support will not be implemented with this feature.

There will be a limitation on the file size in use on the NGSS. The upper limit of the NGSS_trmtrace.txt file will be 10 Mb. The upper limit of the /opt/apps/logs directory will be 100 Mb. This will be enforced within the trace server application (see Activity A00003280).

Interactions

N/A

Applicable customer facing sections

Fault Management

Logs _____N

Alarms _____N

Configuration

Data Schema _____N

User Interface _____N

Element Management _____N

Security _____N

Service Order _____N

Office Parameters _____N

Accounting (includes AMA billing) _____N

Performance (includes operational measurements) _____N

Glossary

Term	Description
NGSS	Another acronym for the Session Server
GWC	GateWay Controller
SIP	In-band signally protocol, RFC 2962
VRDN	GWC that provides the SIP session server functionality, to be replaced by the NGSS.

Product = CS 2000

A00003711 -- CS2000 SUPPPORT FOR GateWay Inter Machine Trunk (GWIMT) ON Passport Voice Gateway (UA-IP)

Functional Description

This activity provides a limited set of gateway services on the long distance application of Succession Communication Server 2000 with a partial compliance of ITU-T Recommendation Q.767 Blue Book version signaling protocol and ITU-T Recommendation Q.764 White Book version) (ISUP92) signaling protocol (international use only). This functionality is supported on

the IMT GLOBAL trunk agency which are provisioned as gateway trunk agents¹³. This feature supports interworking the gateway trunk agency with a set of supported national long distance signalling agencies.

Functional overview

Background

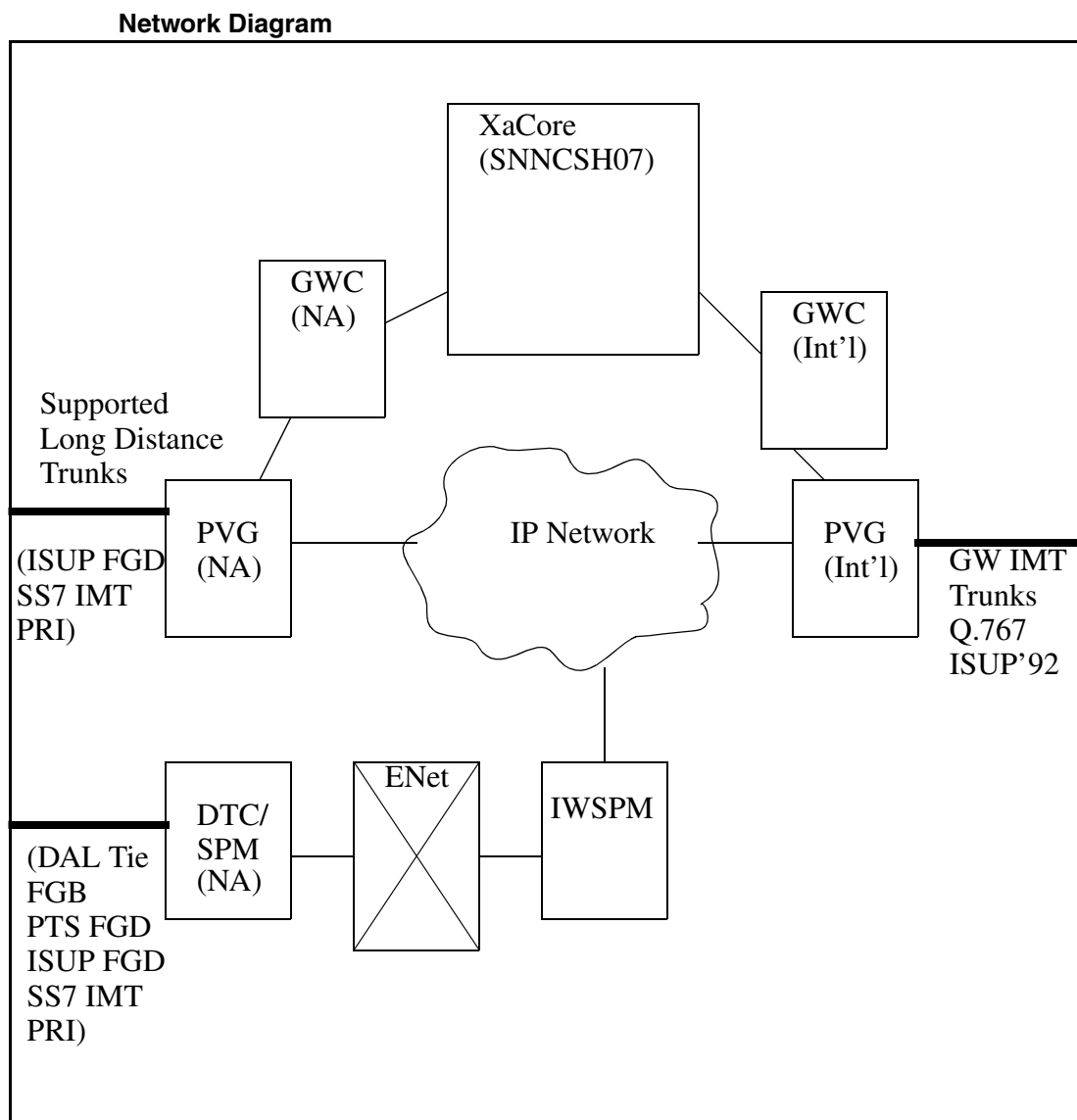
The IMT Global trunk agency on the Succession CS2000 is enhanced to support a limited set of gateway services and a partial compliance of ITU-T Recommendation Q.767 Blue Book version (Q.767) and an international use of ITU-T Recommendation Q.764 White Book version (ISUP92).

This feature allows Inter-eXchange Carriers (IXC) in World Zone-1 countries to provide limited gateway services on the Succession Communication Server 2000 operating as a UCS DMS-250 with either Q.767 or ISUP92 protocols.

Network Overview

This feature allows the IXCs to connect Succession CS2000 directly to foreign exchanges in the international network with either Q.767 or ISUP92 protocol signalling. This feature supports interworking gateway trunk agency with a set of existing UCS national trunk agencies. The following diagram shows the network connectivity for gateway trunk on Succession CS2000.

13. IMT trunk agent in Table TRKGRP provisioned with NETSPEC field value of GLOBAL and new table TRKGRP option GWYTRK



Supported Gateway services

The limited set of gateway functionality is supported by this feature on the Succession CS2000 and is only applicable in the World Zone-1 (WZ-1) market. The new functionality introduced by this feature includes:

- Introduction of new option GWYTRK in table TRKGRP to provision the IMT GLOBAL trunks agents as gateway trunks.
- Support for Q.767 and ISUP92 (international use) signalling protocol on the IMT GLOBAL trunk agency with GWYTRK option.
- Message Compatibility and Parameter compatibility procedures on gateway trunks with ISUP92 protocol.

- Interworking between ISUP92/Q.767 gateway trunks and supported national long distance trunk agencies:
 - IMT Inter
 - IMT Intra
 - FGD SS7
 - FGD PTS¹⁴
 - UCS PRI
 - FGB^{<Superscript>14}
 - DAL TIE^{<Superscript>14 15}
- Support of direct termination and transit 15-digit IDDD calls.
- Support direct termination and transit Code 11 and Code 12 calls (operator assisted calls).
- Support of tie-route connection between Succession CS2000 Communication Servers within WZ-1 using ISUP92/Q.767 gateway trunks.
- Mapping of new cause values defined in ITU-T Recommendation Q.850 received on ISUP92 to normal_unspecified on non-ISUP92 trunks.
- Introduction of new protocol Q.767 in table CSEMAP and TMTMAP for ISUP92/Q.767 gateway trunk agents.
- Calling Party Category (CPC) screening, routing, and override.
- Data calls
- Test calls
- Supporting Q.767 and ISUP92 gateway trunks as terminating agents for Carrier AIN (AIN) calls on supported national long distance trunk agents.
- Support of table C7UPTMR for Q.767 and ISUP92 gateway trunks
- New SOC option GIMT0003 to control gateway services.

Feature description

Enhancements to IMT Global trunk agency

The existing IMT Global trunk agency is enhanced to provide gateway services. Gateway trunks are provisioned in table TRKGRP as IMT Global trunks, with GWYTRK option selected.

14. PTS trunks supported only in hybrid configuration

15. Supported DAL TIE pulse type of MF and DT and start signal of WINK.

The GWYTRK option prompts for two fields SERVCC and C11C12PT. The field SERVCC identifies the serving country code of the foreign exchange in which the gateway trunk is connected. The field C11C12PT provides a pretranslator name for Code 11 and Code 12 calls received on the gateway trunk agency. Please refer to section 1.4.3 Gateway Services for applications of these fields.

On the gateway trunks, two versions of SS7 protocol for international use are supported:

- ISUP92

ISUP92 refers to partial compliance to ITU-T Recommendation Q.764 White Book version that is provided by this feature. The ISUP92 protocol is provisioned in table TRKSGRP with protocol CCITT version ISUP92 and variant V1.

- Q.767

Q.767 refers to ITU-T Recommendation Q.767 BlueBook version that is provided by this feature. The Q.767 protocol is provisioned in table TRKSGRP with protocol CCITT version BLUE and variant V1.

Message Protocols

The following sections describe the support for limited set of Q.767 and ISUP92 protocols that this feature provides.

Support for ISUP92 protocol

This feature provides the following support for ISUP92 protocol agencies:

1. Allows IMT Global trunks to be provisioned as ISUP92 trunks in table TRKSGRP with protocol CCITT, version ISUP92 and variant V1 (hereafter referred to as ISUP92 gateway trunk).
2. This feature introduces a new option GWYTRK for IMT Global agents in table TRKGRP. This option enables gateway functionality on the ISUP92 trunks and provisions the trunk for international use of the ISUP92 protocol.
3. Message Compatibility Parameter (MCP) processing as per the ISUP92 recommendations in Q.764, Section 2.9.5.2 - 2.9.5.4
4. Parameter Compatibility Parameter (PCP) processing as per the ISUP92 recommendations in Q.764, Section 2.9.5.2 - 2.9.5.4
5. Mapping of new cause values received on ISUP92 trunks to Normal unspecified (31) if the other trunk in the call is one of the other supported trunk agencies.

For more information see “APPENDIX A: Messages and Parameters Supported on ISUP92” on page 1223.

Handling of Unexpected messages received on ISUP92

An unexpected or out of sequence message is a message which is supported, and is valid, but has been received when it is not expected in the call.

If such messages are received, the following applies:

- If a Release (REL) message is received for a circuit which is idle, it is acknowledged with a Release Complete message.
- If a Release Complete message is received relating to an idle circuit, it is ignored.
- If any other message is received relating to an idle circuit, a reset message is sent.

In general, unexpected messages received relating to call processing busy circuit, are ignored with the following qualifications:

- Release message and any circuit supervision messages are accepted and processed at any time during the call.
- After sending an IAM, and prior to receiving an ACM or CON, only REL and CPG messages are accepted. Receipt of any other message causes a release sequence to be initiated.
- After a Release message is received, any other call-related messages are discarded.
- If a Release Complete message is received relating to a busy circuit for which a Release message has not been sent, the circuit is released and a Release message sent.
- Blocking messages may be received at any time.

MCP/PCP processing

Compatibility procedures

The compatibility procedures¹⁶ described below have been designed to ensure predictable network behavior, when the switch receives unrecognized signaling information. Refer to ISUP92 Q.761-Q.764 for a more detailed explanation of the compatibility procedures.

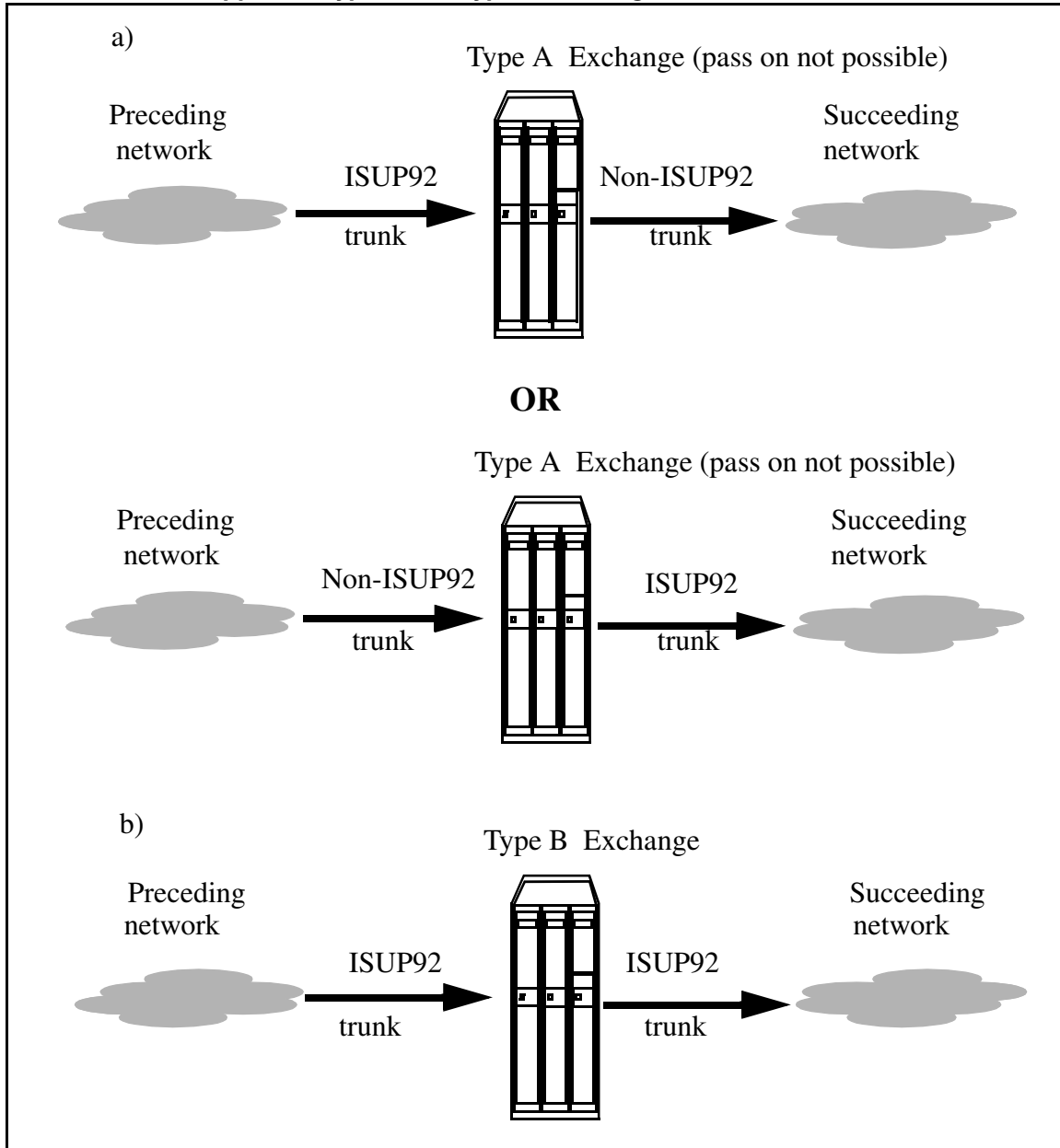
The ISUP92 recommendation Q.764, Section 2.9.5.3, recommends that if a message arrives that is unrecognized, or contains unrecognized parameters, the switch follows a compatibility procedure. Two new optional parameters provide the functionality of the compatibility procedure: the message and parameter compatibility parameters.

16. In this document MCP means Message Compatibility information Parameter and PCP means Parameter Compatibility information Parameter.

Operation of the CS2000 as a Type A and Type B exchange

The Succession CS2000 interprets compatibility procedures found in compatibility parameters according to the type of exchange. The Succession CS2000 behaves as a Type B exchange when both trunks (the originating and terminating trunks) in the call are ISUP92 gateway trunks; otherwise, Succession CS2000 behaves as a Type A exchange (pass on not possible). Succession CS2000 does not support behaving as a Type A exchange (pass on possible).

Examples of Type A and Type B exchanges supported by Succession CS2000 are given in the following figure.

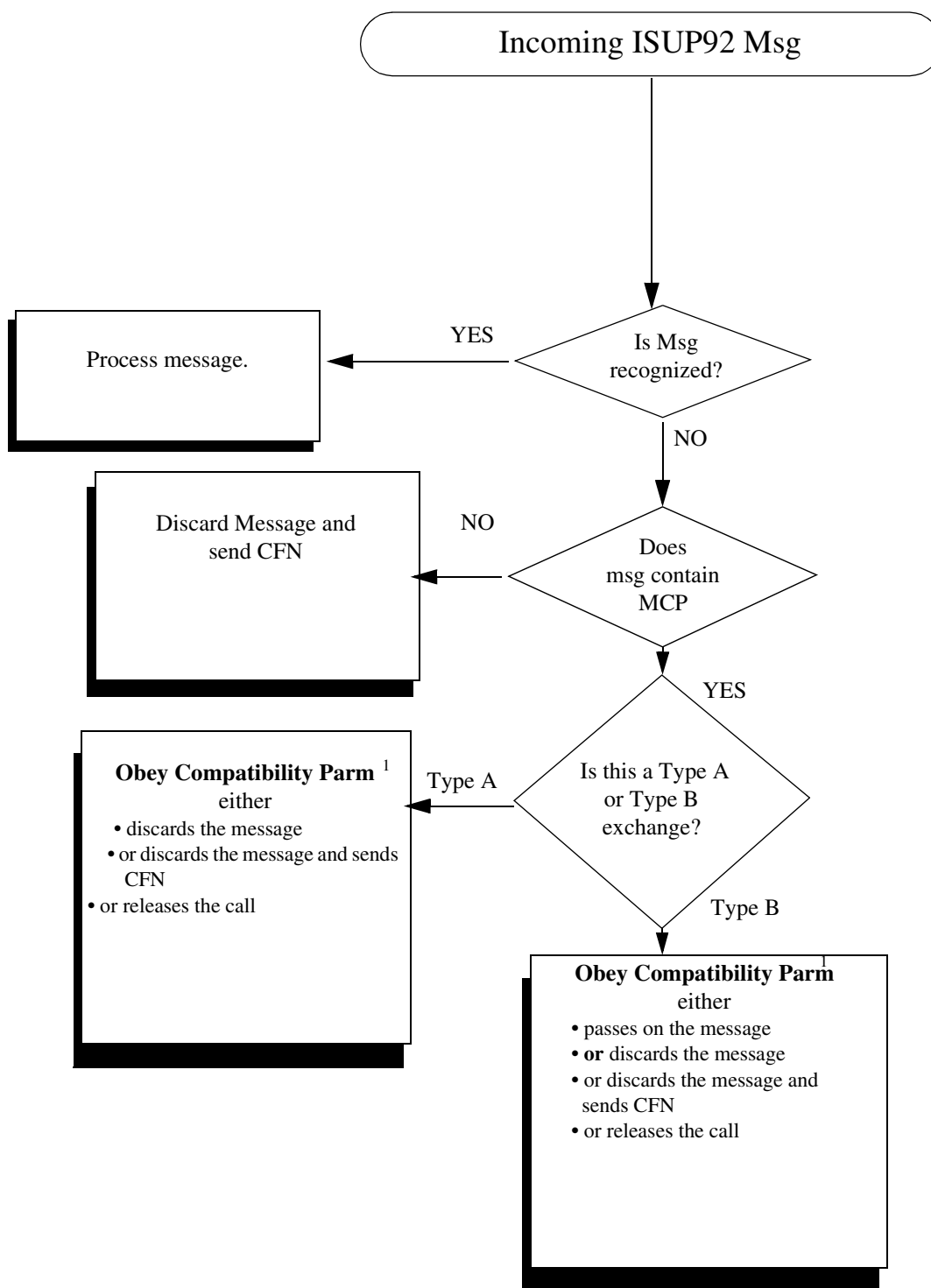
.Supported Type A and Type B exchanges**Message Compatibility Parameter Procedure**

The MCP information pertains to the procedure to be followed, if the switch does not recognize an incoming message. Compatibility procedures can be applied at either a Type A or Type B exchange.

This feature provides the functionality to scan any unrecognized message received from an ISUP92 trunk for the optional MCP. If the message contains the parameter, the Succession CS2000 obeys the parameter. If there is no MCP in an unrecognized message, the switch discards the message and returns a confusion message. All CFN messages generated as a result of MCP processing contain appropriate cause and diagnostic information.

When the Succession CS2000 acts as a Type A exchange, it may receive an ISUP92-compliant Network Resource Message (NRM). The NRM is not one of the minimum set of mandatory messages that the Succession CS2000 must recognize, as stated in the ISUP92 recommendation Q.761, Table 3. Upon receipt of this message at the Succession CS2000, the switch scans the NRM for the optional MCP. If the switch finds the parameter, it applies the message compatibility parameter procedure for Type B exchange. The following figure shows a flowchart of the procedure followed upon receipt of an ISUP92 message at the Succession CS2000.

Flow chart for Message Compatibility Parameter Procedures

ISUP '92 Message Compatibility:

Note 1: Decision on next process is based on the instruction indicator in MCP as described in ISUP92 recommendation Q.764 Section 2.9.5.

Note:

As a Type B exchange, the Succession CS2000 may transit an unrecognized message. As a Type A exchange, the Succession CS2000 does not transit an unrecognized message.

The following tables explain how the switch interprets the instruction indication's bit patterns to execute the subsequent process. This is based on ISUP92 recommendation Q.764, Section 2.9.5.

Message Compatibility for a Type A exchange (pass on not possible)

Bits								Meaning
H	G	F	E	D	C	B	A	
X	X	X	X	X	X	1	X	Release Call
X	X	X	0	0	X	0	X	Release Call
X	X	X	1	0	0	0	X	Discard Message
X	X	X	1	0	1	0	X	Discard Message and send CFN ^a
X	X	X	X	1	0	0	X	Discard Message
X	X	X	X	1	1	0	X	Discard Message and send CFN ^a

a. CFN messages contain an appropriate cause value and diagnostic information.

Message Compatibility for a Type B exchange

Bits								Meaning
H	G	F	E	D	C	B	A	
X	X	X	X	X	X	1	1	Release Call
X	X	X	X	0	X	0	1	Pass on Message
X	X	X	X	1	0	0	1	Discard Message
X	X	X	X	1	1	0	1	Discard Message and send CFN ^a
X	X	X	X	X	X	X	0	Pass on Message

a. CFN messages contain an appropriate cause value and diagnostic information.

where bit A is Transit at Intermediate Exchange Indicator,

0 = Transit interpretation

1 = End node interpretation

Only type B exchanges examine this indicator. If it is set to “Transit Interpretation”, the other indicators are ignored. If it is set to “End Node Interpretation”, the following actions are performed.

bit B is Release Call Indicator,

0 = Do not release

1 = Release call

bit C is Send Notification Indicator,

0 = Do not send

1 = Send notification

bit D is Discard Message Indicator,

0 = Do not discard message

1 = Discard message

bit E is Pass On Not Possible Indicator,

0 = release call

1 = discard information

bits F-G are spare bits,

bit H is Extension Indicator, and

X means a don't care value.

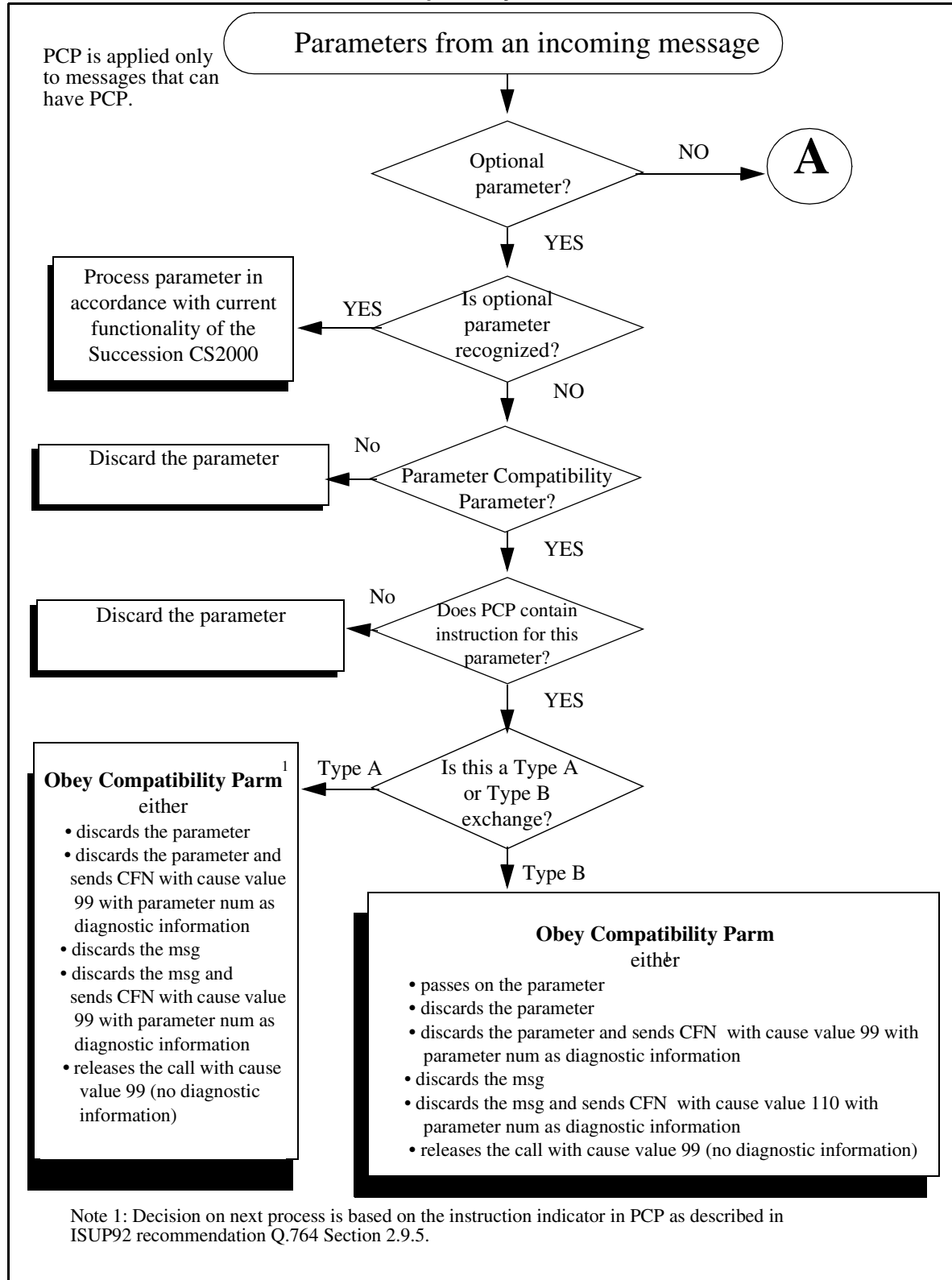
Parameter Compatibility Parameter Procedure

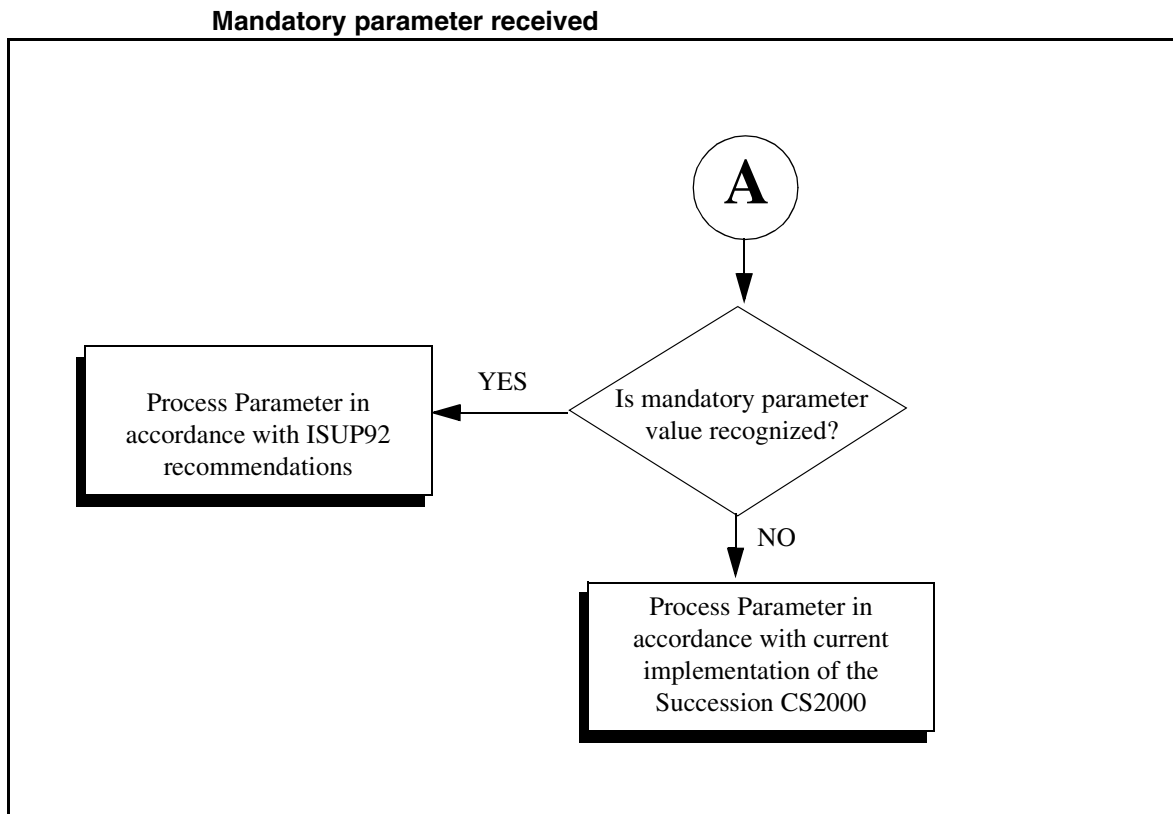
The PCP contains information pertaining to the procedure the Succession CS2000 follows if it recognizes an incoming message, but it does not recognize one of the parameters contained in that message. The switch can only treat optional parameters as unrecognized parameters, since it always recognizes mandatory parameters.

This feature allows the Succession CS2000 to scan messages for the optional PCP when it receives the messages from an ISUP92 trunk. If the switch finds a PCP within the message, it obeys the instruction of the parameter. Please refer to Figure 4 and Figure 5 for the procedure the switch follows when it receives unrecognized information in messages that can have PCP.

All CFN messages generated as a result of PCP processing contain appropriate cause and diagnostic information. The Diagnostic Information includes all the parameters that caused PCP processing to be invoked.

ISUP '92 Parameter Compatibility Procedure





If the Succession CS2000 receives a mandatory parameter with an unrecognized value, it functions as specified in the Q.764 recommendations. If the switch receives a recognized optional parameter with an unrecognized value, it functions as specified in the Q.764 recommendations.

If the Succession CS2000 receives a message containing an unrecognized optional parameter without related parameter compatibility information, the switch discards the parameter and allows the call to proceed.

Table 3 and Table 4 explain how the Succession CS2000 interprets the PCP instruction based on ISUP92 recommendation Q.764, Section 2.9.5. See Figure 4 and Figure 5 for detail. This feature uses the following approach for PCP implementation.

- For IAM message if the instruction indicates **discard message OR discard message and send notification**, it is treated as equivalent to **release call**.
- For IAM message If more than one instruction is received for a parameter, the most severe instruction that was received is applied. This is achieved by performing the logical OR operation of all instructions per parameter.

- If an instruction contains multiple indicators, the precedence followed depends on the type of exchange.

For type A exchange, the precedence (higher to lower) is

- release call
- discard parameter and send notification
- discard parameter
- pass on

For type B exchanges, the indicator precedence followed for:

- BIT A is set to 0 i.e. Transit_node Interpretation is
 - pass on (If BIT A is set to 0 i.e. Transit_node Interpretation) PCP along with the parameters included in the PCP parameter are tandemed, unless another PCP instruction contravenes this indication, in which case the end_node interpretation precedence would be followed.
- BIT A is set to 1 i.e. End_node Interpretation is
 - release call
 - discard parameter and send notification
 - discard parameter
 - pass on
- If more than one PCP is received, the PCP that was received first is used.
- In the REL message, only discard / pass on parameter instructions are applicable.
- The PCP parameter itself is tandemed only if the type of exchange is type B.

The following tables explain how the switch interprets the PCP instruction based on ISUP92 recommendation Q.764, Section 2.9.5.

Parameter Compatibility for a Type A exchange (pass on not possible)

Bits								Meaning
H	G	F	E	D	C	B	A	
X	X	X	X	X	X	1	X	Release the call
X	X	X	X	1	0	0	X	Discard the message ^a
X	X	X	X	1	1	0	X	Discard the message and send CFN ^b
X	X	X	1	0	X	0	X	Discard the parameter ^c

Bits								Meaning
H	G	F	E	D	C	B	A	
X	0	0	0	0	X	0	X	Release the call
X	0	1	0	0	0	0	X	Discard the message ^a
X	0	1	0	0	1	0	X	Discard the message and send CFN ^b
X	1	0	0	0	X	0	X	Discard the parameter ^c
X	1	1	0	0	X	0	X	Release the call

- a. If the message is the IAM message, the switch releases the call.
- b. CFN messages contain an appropriate cause value and diagnostic information. If the message is the IAM message, the switch releases the call and returns no CFN.
- c. If bit C is set, the switch returns a CFN message. CFN messages contain an appropriate cause value and diagnostic information.

Parameter Compatibility for a Type B exchange

Bits								Meaning
H	G	F	E	D	C	B	A	
X	X	X	X	X	X	1	1	Release the call
X	X	X	X	1	0	0	1	Discard the message ^a
X	X	X	X	1	1	0	1	Discard the message and send CFN ^b
X	X	X	1	0	X	0	1	Discard the parameter ^c
X	X	X	X	X	X	X	0	Pass on the parameter
X	X	X	0	0	X	0	1	Pass on the parameter

- a. If the message is an IAM, the switch releases the call.
- b. CFN messages contain an appropriate cause value and diagnostic information. If the message is an IAM, the switch releases the call and returns no CFN.
- c. If bit C is set, the switch returns a CFN message. CFN messages contain an appropriate cause value and diagnostic information.

bit A means that is transited at Intermediate Exchange Indicator

0 = Transit interpretation
1 = End node interpretation

Only type B exchanges examine this indicator. If the exchange sets it to Transit Interpretation, the other indicators are ignored. If the exchange is set to End Node Interpretation, the switch performs the following actions:

bit B is Release Call Indicator
0 = Do not release
1 = Release call
bit C is Send Notification Indicator
0 = Do not send
1 = Send notification
bit D is Discard Message Indicator
0 = Do not discard message
1 = Discard message
bit E is Discard Parameter Indicator
0 = Do not discard parameter (pass on)
1 = Discard parameter
bits F-G are pass on not possible indicator:
00 = Release the call
01 = Discard the message
10 = Discard the parameter
11 = Release the call
bit H is Extension Indicator

If pass on is set (bit D = 0 or bit E = 0) but not possible, then bits C, F and G are examined.

Support for Q.767

This feature provides the following support for Q.767 protocol agencies:

1. Allows IMT Global trunks to be provisioned as Q.767 gateway trunks in table TRKSGRP with protocol CCITT, variant v1 and version BLUE (hereafter referred to as Q.767 trunk).
2. This feature introduces a new option GWYTRK for IMT Global agents in table TRKGRP. This option enables limited gateway functionality on the Q.767 trunks and provisions the trunk for international use of Q.767 protocol on Succession CS2000.

For more information see “Appendix B: Messages and Parameters Supported on Q.767” on page 1236.

Handling of Unrecognized & Unexpected messages For Q.767

All messages that are not included in table 32 (*Appendix B: Messages and Parameters Supported on Q.767*) are considered as unrecognized messages and are treated as per ITU - T Blue Book Q.767 section 4.1.1. Unrecognized messages are discarded without disrupting normal call handling. No logs are produced for unrecognized messages.

An unexpected or out of sequence message is a message which is supported, and is valid, but has been received when it is not expected in the call.

If such messages are received in the Q.767 to Q.767 case, the following applies:

- If a Release (REL) message is received for a circuit which is idle it is acknowledged with a Release Complete message.
- If any other message is received relating to an idle circuit a reset message is sent.
- If a Release Complete message is received relating to an idle circuit it is ignored.

In general, unexpected messages received relating to call processing busy circuit are ignored with the following qualifications:

- Release message and any circuit supervision messages are accepted and processed at any time during the call.
- After sending an IAM, and prior to receiving an ACM or CON, only REL and CPG messages are accepted. Receipt of any other message causes a release sequence to be initiated.
- After a Release message is received, any other call-related messages are discarded.
- If a Release Complete message is received relating to a busy circuit for which a Release message has not been sent, the circuit is released and a Release message sent.
- Blocking messages may be received at any time.

Q.767/ISUP92 Cause value handling

This feature enhances the keys into table TMTMAP and table CSEMAP to include a new protocol Q.767 for calls originating/terminating on Q.767 and ISUP92 trunk agents.

For calls that release at terminator first with a cause value other than *Normal call clearing* (cause value of 16), Succession CS2000 accesses table CSEMAP with the originating trunk agent protocol and the cause value. The cause value is mapped to an extended treatment value when the fields RTEADV and RECOL are set to 'N' in table CSEMAP.

This extended treatment value along with the trunk agent protocol is then used to access table TMTMAP to determine the action to be taken for the call. For calls in which Succession CS2000 have applied a treatment, the applied treatment along with the protocol of the trunk agent is used to access table TMTMAP to derive the action to be taken for the call.

For calls with an action of local treatment (table TMTMAP field TMTPROC value of either LOCAL, ISLOCAL, or INTLOCAL), existing Succession CS2000 functionality is applied.

For calls with an action of non-local treatment (table TMTMAP field TMTPROC value of NOLOCAL) and originated on Q.767 or ISUP92 trunk agents, the carrier is responsible to properly provision the Q.767 protocol in table TMTMAP to reflect the proper location field value of INTL_NET (*International network*) to reflect the generation of the location took place in the international network.

The following excerpt is from ITU-T Recommendation Q.850 which identifies the proper handling of the location field in the CAUSE parameter for international exchanges:

- i) If the event causing the generation of the location field takes place in an international exchange (i.e. incoming or outgoing or international transit exchange) the location is set to *International network*.

For calls originating on UCS trunk agent and has terminated to Q.767 or ISUP92 trunk agent, the CS2000 modifies the LOCATION field derived from table TMTMAP with the LOCATION field value of INTL_NET (*International network*) to reflect the generation of the location took place in the international network.

For calls originating on UCS trunk agent and has **not** successfully routed to a Q.767 or ISUP92 trunk agent or has terminated to a UCS trunk agent, the existing table TMTMAP functionality is utilized and the location field is not modified.

For type A exchanges (ISUP92 trunk agents interworking with non-ISUP92 trunk agents), the CS2000 maps the following ISUP92 cause values to *normal*, *unspecified* (Cause value 31) prior to accessing table CSEMAP and also CS2000 maps the following ISUP92 cause values from table TMTMAP to *normal*, *unspecified* (Cause value 31) prior to sending the CAUSE value for non-local treatments:

- Preemption (T1.619) (8 or CSE_8)
- Pre-emption Circuit reserved for re-use (9 or CSE_9)
- Subscriber absent (20 or CSE_20)
- User information discarded (43 or CSE_43)
- No Preempt Circuit Available (46 or CSE_46)
- Incompatible Agents (53 or CSE_53)
- Inconsistency in designated info (62 or CSE_62)
- Non-existent CUG (90 or CSE_90)
- Message with unrecognized parameter discarded (110 or CSE_110)

For type B exchanges (ISUP92 trunk agent interworking with ISUP92 trunk agent), the CS2000 does not perform the ISUP92 cause value mappings to *normal unspecified* (Cause value 31) as performed on type A exchanges.

Mapping of ISUP92 cause values for non-ISUP92 trunks

The following table summarizes the mapping of ISUP92 cause values for non-ISUP92 trunks.

Mapping of ISUP92 cause values for non-ISUP92 trunks

Release Incoming Trunk	CSEMAP Cause	Release Outgoing Trunk	Outgoing Cause
ISUP92	ISUP92 Cause	ISUP92	CSEMAP Cause Value
ISUP92	Non-ISUP92 Cause	ISUP92	CSEMAP Cause Value
ISUP92	ISUP92 Cause	Q767	Normal Unspecified
ISUP92	Non-ISUP92 Cause	Q767	CSEMAP Cause Value
ISUP92	ISUP92 Cause	UCS Agent	Normal Unspecified
ISUP92	Non-ISUP92 Cause	UCS Agent	CSEMAP Cause Value
Q767	ISUP92 Cause	ISUP92	Normal Unspecified
Q767	Non-ISUP92 Cause	ISUP92	CSEMAP Cause Value
Q767	ISUP92 Cause	Q767	Normal Unspecified
Q767	Non-ISUP92 Cause	Q767	CSEMAP Cause Value
Q767	ISUP92 Cause	UCS Agent	Normal Unspecified
Q767	Non-ISUP92 Cause	UCS Agent	CSEMAP Cause Value
UCS Agent	ISUP92 Cause ^a	Q767	Normal Unspecified
UCS Agent	ISUP92 Cause ^a	ISUP92	Normal Unspecified
UCS Agent	Non-ISUP92 Cause	Q767	CSEMAP Cause
UCS Agent	Non-ISUP92 Cause	ISUP92	CSEMAP Cause

a. CSEMAP does not differentiate between CCITT coding standard or National coding standard.

Q.767 and ISUP92 Protocol Timers

This feature allows flexibility to set timers per trunk sub-group basis for the Q.767/ISUP92 trunks. Table TRKSGRP field TMRNAME value provides the index into Table C7UPTMR. Table C7UPTMR allows to set timers based on a per trunk sub-group basis. If the TMRNAME field is not provisioned, then the default values are used.

For more information see “Appendix C: Q.767/ISUP92 Timers” on page 1243.

Q.118 Timer

This feature does not support suspend (SUS) and resume (RES) functionality on the ISUP92/Q.767 trunk agency. The gateway functionality is required to tandem any received SUS or RES messages (when the appropriate indicators indicate the message is network initiated) and not process these messages when the originating agency is Gateway trunk. For other originating agencies the existing suspend-resume functionality is performed. For this reason, Q.118 timer in section 4.3.2 in ITU Q.118 recommendation is not supported. Timer value associated with T6 is ignored and the timer is not set which corresponds to a infinite timer value.

Gateway services**Supported calltypes**

The Q.767/ISUP92 gateway trunks support the following calltypes:

- direct termination and transit IDDD calls
- direct termination and transit international operator assisted calls
- direct termination and transit Code 11/Code 12 calls

All calltypes are handled as automatic service calls. This feature also supports tie-route connections between two Succession CS2000 Communication Servers using the ISUP92/Q.767 trunk agency.

This feature supports 15-digit IDDD requirements for both the called party number and the calling party number. The ISUP92/Q.767 trunk agency supports receiving and outpulsing two Nature of Address (NOA) values for both calling party number and called party number based on below mentioned supported calltypes:

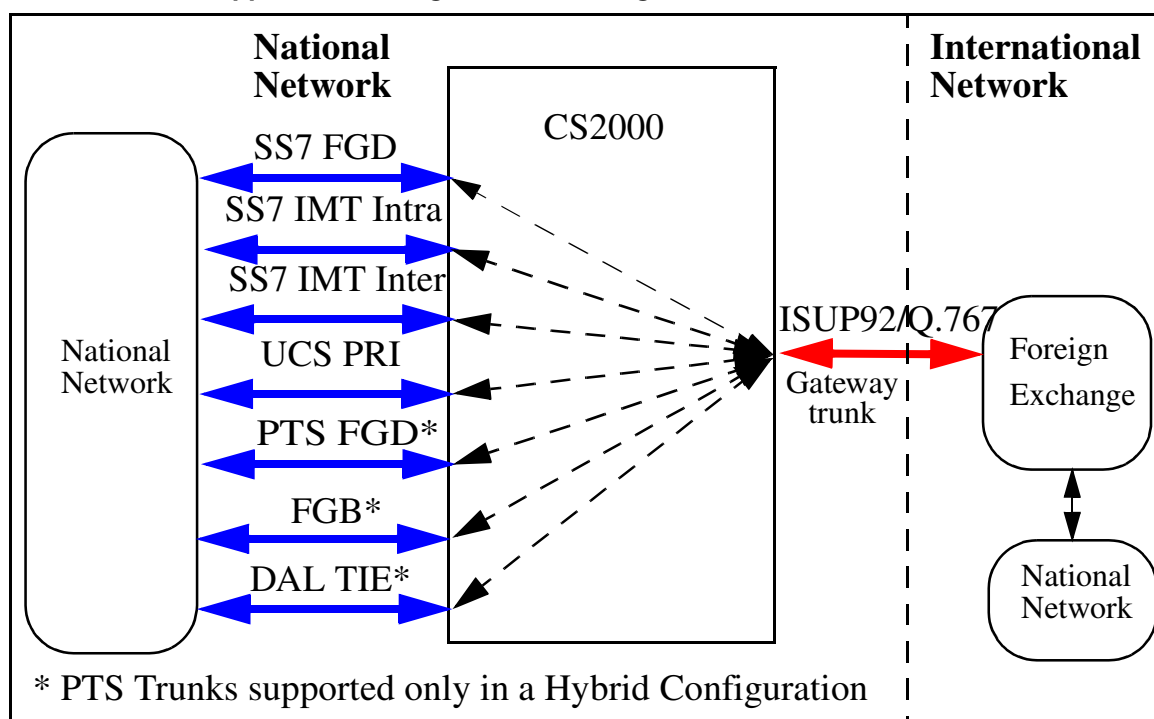
- National significant number (0000011)
 - direct termination IDDD calls
 - direct termination operator assisted calls
 - direct termination Code 11/Code 12 calls
- International significant number (0000100)
 - transit IDDD calls
 - transit operator assisted calls
 - transit Code 11/Code 12 calls

The Q.767/ISUP92 gateway trunks are used to inter-connect to foreign exchanges. The table TRKGRP GWYTRK option field SERVCC identifies the serving country code of the foreign exchange. The foreign exchange provides the international interface for the national network of the serving country code.

The Succession CS2000 provides the international interface for the national network associated with the table OFCVAR parameter OFC_SERVING_CC. Table OFCVAR parameter OFC_SERVING_CC is provisioned with the country code that is associated with the country that resides the Succession CS2000. This feature is only supported in WZ-1 countries; therefore, the only supported country code for the office parameter OFC_SERVING_CC is 1. The supported UCS trunk agents are associated with the country code of the office parameter OFC_SERVING_CC.

The following figure illustrates the supported trunk agencies interworking and the international interface between the national network being served by Succession CS2000 and the international network.

Supported trunk agent interworkings

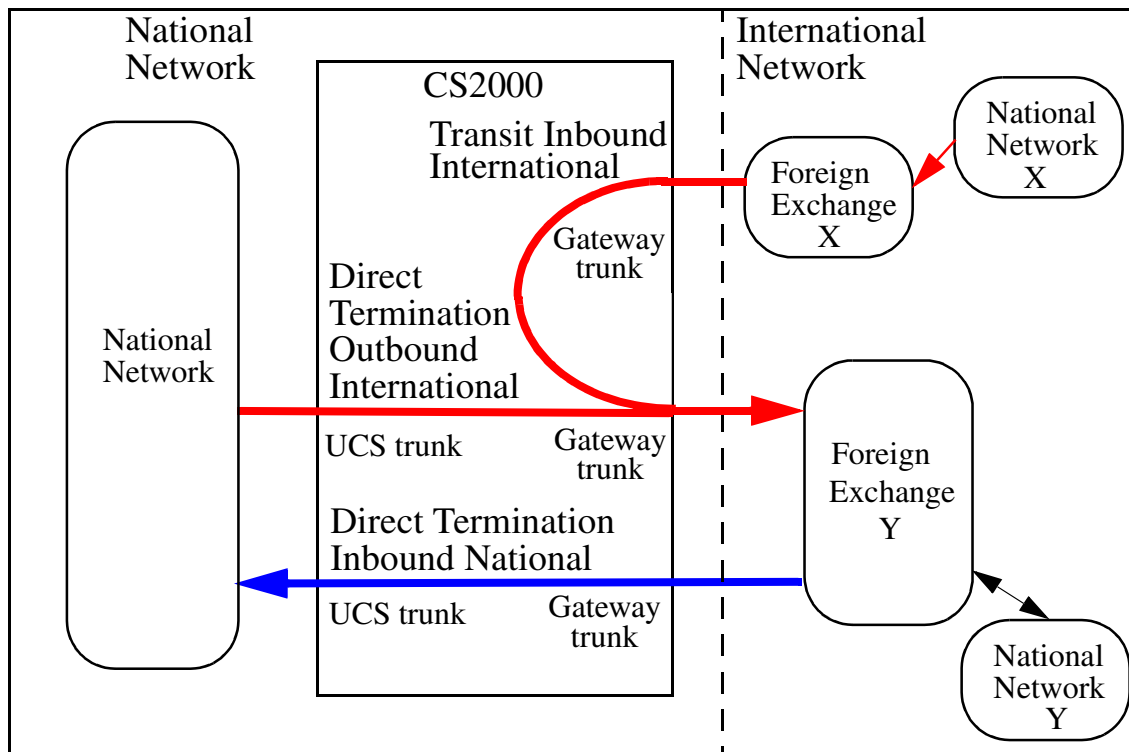


Direct Termination calls

Direct termination outbound international calls pertains to IDDD calls which are routed to a foreign exchange which serves the country code prefixed to the called number. The foreign exchange would serve the national network of the country code. For direct termination outbound international (IDDD) calls, the call would be routed to a ISUP92/Q.767 trunk which is connected to the foreign exchange that serves the country code prefixed on the called number.

Direct termination inbound national calls pertain to national calls routed from a foreign exchange which are destined for the country (serving country code) in which the Succession CS2000 resides. For direct termination inbound national calls, the call would be routed (via translations) to the supported UCS agents. The supported UCS agents are associated with the national network of the serving country code. Figure 7 illustrates supported direct termination calltypes.

Direct Termination calltypes



Direct Termination Outbound International:

For direct termination outbound international calls, the call origination occurs on one of the supported UCS trunk agents or a ISUP92/Q.767 trunk agency (in the case of a transit inbound international call from a foreign exchange) and terminates to a ISUP92/Q.767 trunk agency where the call is typed as an international (IDDD) call. The terminating ISUP92/Q.767 trunk agency is connected to the foreign exchange serving the country code prefixed on the called number. For the call to be classified as a direct termination outbound international call, the serving country code (table TRKGRP GWYTRK option field SERVCC) that is associated with the terminating ISUP92/Q.767 trunk agency would be EQUAL to the country code prefixed on the called number.

For originations on the supported UCS agents, this feature supports existing international (IDDD) translations (IP and IN translations) and existing Carrier AIN functionality to allow the call to be routed to the terminating ISUP92/Q.767 trunk agency. For originations on ISUP92/Q.767 trunk agency, this feature supports existing international (IDDD) translations (IP and IN translations) to allow the call to be routed to the terminating ISUP92/Q.767 trunk agency.

For more information see “Appendix D: Call Information (IAM message) for Gateway Calltypes” on page 1246. “Appendix E: Callflow diagram” and “Appendix F: Datafill examples” for more details on DMS250 processing of direct termination outbound international calls.

Direct Termination Inbound National:

For direct termination inbound national calls, the connected foreign exchange routes the call as a national call to the Succession CS2000 via ISUP92/Q.767 trunk agency. For the call to be classified as a direct termination inbound national call, the Succession CS2000 would call type the call as a national call (via table STDPRTCT CT selector with CALLFEAT of OFFNET or table STDPRTCT S/T selectors).

The ISUP'92/Q.767 trunk agency would utilize table TYP2PRTM to derive the pretranslator name (to access table STDPRTCT) based on the received called party number NOA. This feature supports the following pretranslation selectors from table STDPRTCT:

- CT selector (calltype of OFFNET)
- S selector
- T selector

The other pretranslation selectors are not supported.

This feature supports existing national translation system (HNPACONT). This feature supports the following translation routing selectors from table HNPACONT:

- S route selector
- N route selector
- T route selector (supported UCS routing tables)
- SX route selector
- TRMT route selector

The other translation routing selectors are not supported.

The outgoing call information is updated based on the information/translations derived/performed by the Succession CS2000.

For more information see “Appendix D: Call Information (IAM message) for Gateway Calltypes” on page 1246. “Appendix E: Callflow diagram” and “Appendix F: Datafill examples” for more details on DMS250 processing of direct termination inbound national calls.

Transit calls

Transit calls pertain to international calls which are routed to a foreign exchange (gateway) which does not serve the country based on the country code prefixed on the called number. This foreign exchange would then route the call as either a direct termination inbound national call or a transit outbound international call to another foreign exchange that is serving the country code prefixed on the called number.

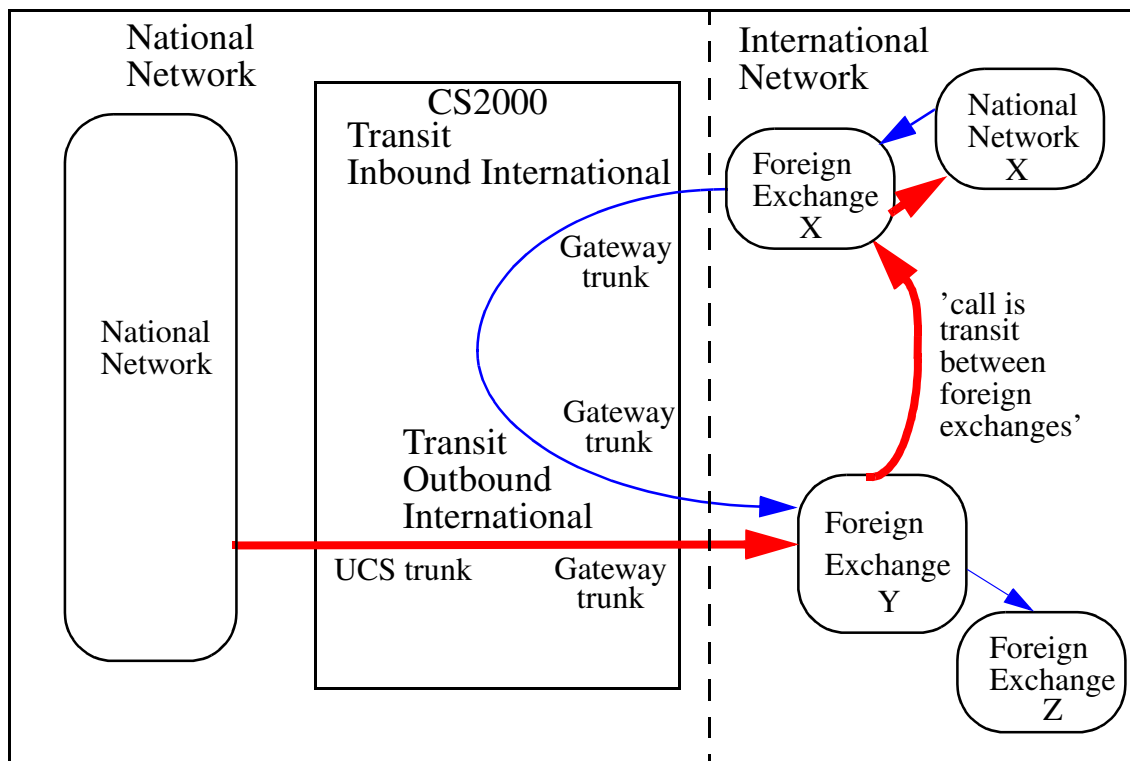
Transit inbound national call pertains to national calls (gateway serving the country code prefixed on the called number) which were transit through a foreign exchange that did not serve the country code of the subscriber (calling party number) and terminates to the serving country code of the Succession CS2000. Transit inbound national calls are handled in the same manner as direct termination inbound national call.

For more information see “Appendix D: Call Information (IAM message) for Gateway Calltypes” on page 1246. “Appendix E: Callflow diagram” and “Appendix F: Datafill examples” for more details on CS2000 processing of transit calls.

Transit Outbound International

For transit outbound international calls, the call origination occurs on either the supported UCS agents or ISUP92/Q.767 trunk agency and the call is typed as an international (IDDD) call. Transit outbound international (IDDD) calls could have originated from the national network serving the Succession CS2000 (originated on supported UCS agents) or from a foreign exchange using the Succession CS2000 as a transit foreign exchange (gateway) where the incoming call is a transit inbound international call and the outgoing call is a transit outbound international call.

The following figure illustrates transit outbound international calls coming from either the national network (origination on supported UCS trunk agent) or international network (origination on ISUP92/Q.767 trunk agent).

Transit outbound international call type

For ISUP92/Q.767 trunk agency originations existing international translations (IP and IN translations) is supported and for supported UCS agents originations existing international translations (IP and IN translations or Carrier AIN) are supported.

The ISUP92/Q.767 trunk agency would utilize table TYP2PRTM to derive the pretranslator name (to access table STDPRCT) based on the received called party number NOA.

International translations would have routed the call to a ISUP92/Q.767 trunk agency. For the call to be classified as a transit outbound international call, the terminating trunk agent is an ISUP92/Q.767 trunk agent and the serving country code (table TRKGRP option GWYTRK field SERVCC) for ISUP92/Q.767 trunk agent is NOT EQUAL to the country code prefixed on the called number.

Operator calls

This feature supports following types of operator assisted calls:

- Inbound national OA calls (Direct)
- Outbound international OA calls (Direct & Transit)

- Inbound national Code 11 and Code 12 calls (Direct)
- Outbound international Code 11 and Code 12 calls (Direct & Transit)

Inbound National OA calls (Direct)

Calls originating on Q.767/ISUP92 gateway trunk agents, are identified as inbound national operator assisted (OA) call via pretranslations (in table STDPRTCT, subtable STDPRT, S selector with TYPCALL field value of OA or T selector with TYPCALL field value of OA). The S and T selector by default call type the call as a national call (OFFNET). Succession CS2000 treats inbound national OA call (S and T selectors with TYPCALL value of OA in table STDPRTCT) as direct termination inbound national calls except the CPC value is not modified (unless modified by the SX routing selector via table RTEATTR) in the outgoing call information (ISUP or PRI trunk terminations).

Inbound national OA calls can also use the CT selector with CALLFEAT value of OFFNET to pretranslate the call. The CT selector with CALLFEAT value of OFFNET has the option of using the new option CPCSCRN to perform CPC screening, routing, or override the incoming CPC but the call is treated as a direct termination inbound national call.

The carrier is responsible to append any WZ-1 prefix digits.

For more information see “Appendix D: Call Information (IAM message) for Gateway Calltypes” on page 1246. “Appendix E: Callflow diagram” and “Appendix F: Datafill examples” for detail on CS2000 processing of inbound national OA calls.

Outbound international OA calls (Direct & Transit)

Direct termination outbound international OA and Transit outbound international OA calls originate on supported UCS agents or Q.767/ISUP92 gateway trunk and terminate on Q.767/ISUP92 gateway trunk. These calls are identified as international operator assisted call via NT selector with TYPCALL field value of OA in table STDPRTCT, subtable STDPRT.

The NT selector call types the call as an international call. Succession CS2000 treats outbound international OA call (NT selector in table STDPRTCT) as either a direct termination outbound international call or a transit outbound international call based on the comparison between the country code prefixed on the called number and the serving country code (table TRKGRP option GWYTRK field SERVCC) of the terminating Q.767/ISUP92 gateway trunk agent. For either case, the CPC value is not modified (unless modified by the SX routing selector via table RTEATTR or the NT selector option CPCSCRN functionality). The NT selector option CPCSCRN in table STDPRTCT provides the optionality to perform CPC screening, CPC routing, and CPC override for calls originating on Q.767/ISUP92 gateway trunk agents.

For more information see “Appendix D: Call Information (IAM message) for Gateway Calltypes” on page 1246. “Appendix E: Callflow diagram” and “Appendix F: Datafill examples” for details on CS2000 processing of outbound international OA calls.

Code 11/Code 12 calls:

An operator can place international calls to other operators by including Code 11 (Hexadecimal B) or Code 12 (Hexadecimal C) in called number. Code 11 (‘B’) is used internationally to signify Directory Assistance and Code 12 (‘C’) is used to indicate General Operator Assistance.

Outbound International Code 11/12 calls (Direct & Transit)

These calls originate either on Gateway trunk or UCS Agents and terminate on Gateway trunk.

In WZ-1, code 11 digit (B) and code 12 digit (C) are commonly translated to “121” and “131” respectively. For outbound international Code 11 and Code 12 calls, the national operator includes 121 or 131 in place of the Code 11 or Code 12 digit in the called number. The international exchange would then convert the 121 and 131 to Code 11 digit (B) and Code 12 digit (C), respectively.

The called number contents from a national operator position could have the following format (Recommendation Q.107):

<01> + <country code> + <extra digit> + <121 or 131> + <digits>

- ‘01’: WZ-1 prefix digits for international operator assisted calls
- extra digit: (Optional) extra digit designating the incoming international exchange is used in cases where more than one incoming international exchange can be reached in the country of destination. (It is recognized that some existing equipment does not permit the insertion of the extra digit)
- digits: (Optional) number of a particular operator position or group of positions

For calls originating on Q.767/ISUP92 gateway trunk agents, the CS2000 scans the called number for the Code 11 and Code 12 digits. If the Code 11 or Code 12 digits exist in the called number, the Succession CS2000 replaces these digits in the called number with 121 or 131, respectively along with prefixing the called number with 0 or 01 based on the NOA of the called number. Succession CS2000 uses the pretranslator name from table TRKGRP option GWYTRK option field C11C12PT to access table TYP2PRTM along with the NOA of the called number.

The IAM called number contents from a foreign operator position via foreign exchange could have the following format (Recommendation Q.107):

<country code> + <extra digit> + <code 11 or code 12> + <digits> + #F

- extra digit: (Optional) extra digit designating the incoming international exchange is used in cases where more than one incoming international exchange can be reached in the country of destination. (It is recognized that some existing equipment does not permit the insertion of the extra digit)
- digits: (Optional) number of a particular operator position or group of positions

The Succession CS2000 would treat the call as either a direct termination outbound international OA call or transit outbound international OA call based on the comparison between the country code prefixed on the called number and the serving country code (table TRKGRP option GWYTRK field SERVCC) of the terminating Q.767/ISUP92 gateway trunk agent. For either case, the CPC value is not modified (unless modified by the SX routing selector via table RTEATTR or by NT selector option CPCSCRN in table STDPRTCT).

The carrier is responsible to remove any WZ-1 prefix digits and perform digit manipulation (via translations) to convert the 121 and 131 digits to Code 11 digit and Code 12 digit, respectively.

For more information see “Appendix D: Call Information (IAM message) for Gateway Calltypes” on page 1246. “Appendix E: Callflow diagram” and “Appendix F: Datafill examples” for details on DMS250 processing of outbound international code 11/12 calls.

Inbound National Code 11/12 calls (Direct)

These calls originate on Gateway trunk and terminate on UCS agent.

For calls originating on Q.767/ISUP92 gateway trunk agents, the CS2000 scans the called number for the Code 11 and Code 12 digits. If the Code 11 or Code 12 digits exist in the called number, the Succession CS2000 replaces these digits in the called number with 121 or 131, respectively. Also, Succession CS2000 prefixes digit(s) 0/01 based on the incoming NOA. Succession CS2000 uses the pretranslator name from table TRKGRP option GWYTRK option field C11C12PT to access table TYP2PRTM along with the NOA of the called number.

The IAM called number contents from a foreign operator position via foreign exchange could have the following format (Recommendation Q.107):

<extra digit> + <code 11 or code 12> + <digits> + #F

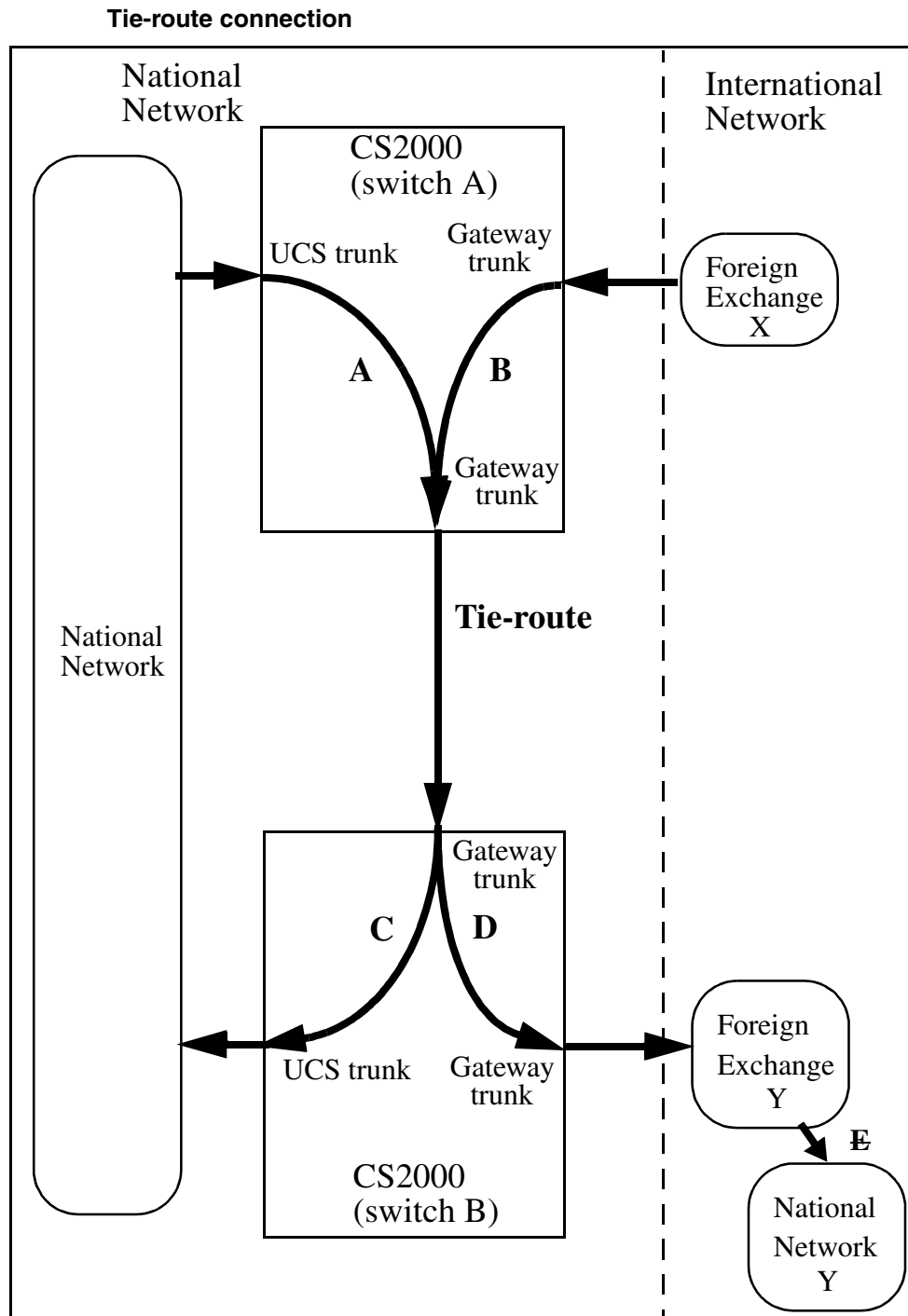
- extra digit: (Optional) extra digit designating the incoming international exchange is used in cases where more than one incoming international exchange can be reached in the country of destination. (It is recognized that some existing equipment does not permit the insertion of the extra digit)
- digits: (Optional) number of a particular operator position or group of positions

The Succession CS2000 would treat direct termination inbound national code 11 or code 12 call as a direct termination inbound national OA call based on pretranslations.

For more information see “Appendix D: Call Information (IAM message) for Gateway Calltypes” on page 1246. “Appendix E: Callflow diagram” and “Appendix F: Datafill examples” for details on DMS250 processing of inbound national code 11/12 calls.

Tie-route support

Tie-route connections are used when the carrier has more than one switch with the gateway functionality. These switches would be directly connected to each other via gateway trunk agency. The tie-route connection may be used by the carrier to route calls between the switches based on which switch has the available connection to the destination foreign exchange or the destination national network. The following figure illustrates the supported tie-route connection between two CS2000 Communication Servers.



The carrier would be expected to use the national backbone to tandem any national traffic within the carrier's network or within the national network. The tie-route connection could be used to route the following gateway calltypes:

- direct termination inbound national calls (connection B to connection C)
- direct termination outbound international calls (connection A to connection D)
- any transit outbound international calls (connection B to connection D)

Please refer to Section "Appendix G: Tie-route Connection Example" on page 1277. for example on tie-route connection.

Calling Party Category (CPC) handling

New table CPCSCRN is implemented to provide the following functionality:

- CPC screening
- CPC routing
- CPC override

Table CPCSCRN is only accessible by ISUP92 and Q.767 gateway trunk agencies. Table CPCSCRN is accessed as a two part key with the NT/CT option CPCSCRN index value (CPCINDEX) and the incoming call CPC value (0 to 255). If the tuple is not present in table CPCSCRN, the call is allowed to continue.

A new Table STDPRTCT option CPCSCRN is added to NT selector for the DD and OA type of call (TYPCALL field) and CT selector with CALLFEAT of OFFNET. CPCSCRN option requests for an index value (0 to 255).

Table STDPRTCT CT selector

Selector	CALLFEAT	MINDIGS	MAXDIGS	NOPREDIGS	OPTIONS
CT	OFFNET	0 TO 18	0 TO 18	0 to 7	CPCSCRN

Table STDPRTCT NT selector

Selector	TYPCALL	NOPREDIG	TRANSYS	OPTIONS
NT	DD	0 to 7	IP,IN	CPCSCRN
NT	OA	0 to 7	IP,IN	CPCSCRN

TYPCALL can have the following values:

DD: Direct Dial

OA: Operator Assisted

NP: Nil type of call (CPCSCRN option is not available for this value)

NL: No prefix local (CPCSCRN option is not available for this value)

CT/NT option CPCSCRN

Options	CPCSCRN Index
CPCSCRN	0 to 255

Table CPCSCRN contains three fields:

- Action:
 - Continue: allows the call to proceed
 - Block: routes the call to treatment
- Override STS:
 - N: STS is not overridden
 - Y: STS is overridden with provisioned STS. Table control prompts for STS when Override STS is set to 'Y'.
- Override CPC:
 - N: CPC is not overridden
 - Y: CPC is overridden with provisioned CPC. Table control prompts for CPC value (0 to 15) when Override CPC is set to 'Y'.

Table CPCSCRN

FIELD NAME	RANGE OF VALUES	STATUS	DEFAULT VALUES
CPCINDEX	{0 TO 255}	NEW	N/A
CPC	Alphanumeric character string, which are mapped to range 0-255. The first 16 values are same as given in table 36. Other values are from CPC_16 to CPC_255.	NEW	N/A
ACTION	{ACTION_CONTINUE, ACTION_BLOCK}	NEW	ACTION_CONTINUE
OVRDSTS	{Y, N}	NEW	N
STS	{000 TO 999}	NEW	N/A
OVRDCPC	{Y, N}	NEW	N
CPC	Alphanumeric character string, which are mapped to range 0-15. The values are same as given in table 10.	NEW	N/A

Table CPCSCRN CPC values

CPCSCRN CPC value	Integer value of CPC
UNKNOWN	0
OP_FRENCH	1
OP_ENGLISH	2
OP_GERMAN	3
OP_RUSSIAN	4
OP_SPANISH	5
CPC_6	6
CPC_7	7
CPC_8	8
OP_NATIONAL	9
SUBSCRIBER1	10
PRIORITY	11
DATA	12
TEST	13
NON_VOICE	14
PAYPHONE	15

The field *Action* is used to screen the incoming CPC value based on the CPCSCRN index value obtained from the new CT/NT option CPCSCRN in table STDPRTCT and the incoming CPC value. The field ACTION either allows the call to continue or blocks the call by routing the call to Call Not Allowed (CNAD) treatment.

The field *OVRDSTS* is used to provide a new STS value for the call when the *Override STS* value is set to 'Y'. If the value is set to 'N', table CPCSCRN does not prompt for a new STS value and the last derived STS value is used for the call.

The field *OVRDCPC* is used to override the incoming CPC value with a new CPC value for the call when *Override STS* value is set to 'Y'. If the value is set to 'N', table CPCSCRN does not prompt for a new CPC value and the incoming CPC value is maintained for the call.

The following CPC values were extracted from ITU-T Recommendation Q.767 section 3.11:

00000000 : Unknown
 00000001 : operator, language French
 00000010 : operator, language English
 00000011 : operator, language German
 00000100 : operator, language Russian
 00000101 : operator, language Spanish
 00000100 : available to Administrations
 to for selecting a particular
 00001000 : language by a mutual agreement
 00001001 : reserved (see Recommendation Q.104) (Note)
 00001010 : ordinary calling subscriber
 00001011 : calling subscriber with priority
 00001100 : data call (voice band data)
 00001101 : test call
 00001110 : spare
 00001111 : payphone
 00001000 :
 to spare
 11011111 :
 11100000 : reserved
 to for
 11111110 : national use
 11111111 : spare

Example datafill:

Table STDPRTCT, subtable STDPRT

0117 0117 NT DD 3 IP (CPCSRCN 1)\$

Table CPCSRCN is accessed with the CPCINDEX value of 1 along with the call CPC value of 2 (OP_ENGLISH).

Table CPCSRCN

1 OP_ENGLISH CONT Y 611 Y OP_SPANISH

For a call with the CPC value of 2 (OP_ENGLISH), the call is allowed to continue (ACTION_CONTINUE), the STS for the call is updated to 611, and the CPC for the call is updated with a value of OP_SPANISH (5).

The call CPC is also allowed to be overridden by using the SX selector during translations of the call. The SX selector provides the index to access table RTEATTR. The REPLACE field in Table RTEATTR is enhanced to prompt for a CPC value. Table-10 provides table RTEATTR CPC values.

The CPC value replaces the CPC value for the Calling Party Category parameter in the outgoing IAM on the trunk provisioned against the SX selector. This functionality is only available for Q.767 and ISUP92 gateway trunk agents.

Table RTEATTR CPC values

RTEATTR CPC value	Integer value of CPC
UNKNOWN	0
OP_FRENCH	1
OP_ENGLISH	2
OP_GERMAN	3
OP_RUSSIAN	4
OP_SPANISH	5
CPC_6	6
CPC_7	7
CPC_8	8
OP_NATIONAL	9
SUBSCRIBER1	10
PRIORITY	11
DATA	12
TEST	13
NON_VOICE	14
PAYPHONE	15

Example datafill:

Table HNPACONT, subtable RTEREF

```
724 (SX GITU1E1AN03 CPC_OVRD) $
```

CPC_OVRD is the index into table RTEATTR.

Table RTEATTR

```
CPC_OVRD $ $ CPC SUBSCRIBER1
```

The outgoing CPC value is set to SUBSCRIBER1

Satellite Restrictions

This feature supports the existing Succession CS2000 satellite functionality for the ISUP92/Q.767 trunk agent to enable double satellite hop restriction. Double satellite hop restriction is invoked when the terminating trunk agent TRKSGRP field SAT is provisioned with a value of 'Y'.

Double satellite hop restriction:

For originating calls on the Succession CS2000 which have an indication that the call has been previously involved in a satellite connection (via originating trunk agent table TRKSGRP field SAT with a value of 'Y' and/or the Nature of Connection with an indication of at least one satellite circuit in the connection), the Succession CS2000 restricts the call from terminating on a trunk agent with an indication of a satellite connection (via terminating trunk agent table TRKSGRP field SAT value of 'Y'). Succession CS2000 performs route advance to the next available route in the route list.

Gateway (ISUP92/Q.767) satellite indication:

The value of table TRKSGRP field SAT is interpreted as below:

- Table TRKSGRP field SAT:

N: No satellite circuit in the connection

Y: Satellite circuit in the connection

The value of 'Satellite indicator' in 'Nature of Connections parameter' is interpreted as below:

- Nature of Connection (reflected as 'O/G ind.' below tables):

00: No satellite circuit in the connection

01: One satellite circuit in the connection

10: Two satellite circuit in the connection

11: spare

UCP Inter/Intra ISUP IMT satellite indication:

The value of table TRKSGRP field SAT is interpreted as below:

- Table TRKSGRP field SAT:

N: No satellite circuit in the connection

Y: One satellite circuit in the connection

The value of 'Satellite indicator' in 'Nature of Connections parameter' is interpreted as below:

- Nature of Connection (reflected as 'O/G ind.' below tables):

00: No satellite circuit in the connection

01: One satellite circuit in the connection

10: Two satellite circuit in the connection

11: Three or more satellite circuits in the connection

- I3PA (II digits reflects satellite connection):

II digits (Facility code) of I3PA dialplan is a two digit value reflecting the following information:

calltype (first digit of facility code)

- 0x: national calls
- 2x: COS
- 56: data call

second digit of facility code

- queued at previous switch
- satellite at previous switch

SS7 FGD satellite indication:

The value of table TRKSGRP field SAT is interpreted as below:

- Table TRKSGRP field SAT:

N: No satellite circuit in the connection

Y: One satellite circuit in the connection

The value of 'Satellite indicator' in 'Nature of Connections parameter' is interpreted as below:

- Nature of Connection (reflected as 'O/G ind.' below tables):

00: No satellite circuit in the connection

01: One satellite circuit in the connection

10: Two satellite circuit in the connection

11: Three or more satellite circuits in the connection

UCS PRI, PTS FGD, FGB, DAL TIE satellite indication:

These trunk agencies are only supported on land-base transmission medium and do not provide any type of outgoing indicator that a satellite was involved in the call.

ISUP 'Satellite indicator' values in the outgoing IAM

The following table gives the value of 'ISUP Satellite indicator' in 'Nature of Connection Parameter' in outgoing IAM.

***Note:** Please note that, call is ROUTE ADVANCED until a terminator with SAT set to N (not equipped with satellite), for all other combination of values which are not listed in Table12, Table13 and Table 14.*

ISUP 'Satellite indicator' values for Gateway terminating to UCS agent

Originator		Terminator						
Gateway		SS7 IMT			SS7 FGD		Gateway	
I/C ind.	Trks grp	Trks grp	O/G ind.	I3PA Satel. ind.	Trks grp	O/G ind.	Trks grp	O/G ind.
00	N	N	00	N	N	00	N	00
00	Y	N	01	Y	N	01	N	01
00	N	Y	01	Y	Y	01	Y	01
01	N	N	01	Y	N	01	N	01
01	Y	N	01	Y	N	01	N	01
10	N	N	10	Y	N	10	N	10

ISUP 'Satellite indicator' values for Gateway terminating to UCS agent

Originator		Terminator						
Gateway		SS7 IMT			SS7 FGD		Gateway	
10	Y	N	10	Y	N	10	N	10
11	N	N	10	Y	N	10	N	10
11	Y	N	10	Y	N	10	N	10

ISUP 'Satellite Indicator' values for UCS agent terminating to Gateway

Originator		Terminator	
FGD SS7/ IMT SS7		Gateway	
I/C ind.	Trks grp	Trks grp	O/G ind.
00	N	N	00
00	N	Y	01
00	Y	N	01
01	N	N	01
01	Y	N	01
10	N	N	10
10	Y	N	10
11	N	N	10
11	Y	N	10

ISUP 'Satellite Indicator' values for UCS PTS/PRI agent terminating to Gateway

Originator	Terminator	
PTS/PRI	Gateway	
Trks grp	Trks grp	O/G ind.
N	N	00
N	Y	01
Y	N	01

Test calls on Gateway Trunks.

Test lines are used to test trunk connections to other offices, both local and toll. Test Line Tests (TLT) are run under the control of the calling office, and can be initiated either manually from the Trunk Test Position (TTP) level or automatically from the Automatic Trunk Test (ATT) level of Maintenance & Administration Position (MAP). TLT can test both the originating and terminating ends of trunks, and can be used to simulate most conditions that may arise under normal operating conditions.

Test calls are defined as calls originating from test facilities on the near end switch, going over the trunk to be tested and finally terminating on test equipment of far end switch. This feature supports test calls on Q.767/ISUP92 gateway trunk for the following testlines:

- T100 (Balanced Termination testline)
- T101¹⁷ (Communication testline)
- T102 (Milliwatt testline)

Test facilities, supported by this feature include ATT, and the TST and OP commands of the TTP MAP level. ATR originated test calls are not supported by this feature.

17. T101 testline is supported only in a hybrid configuration.

Please refer to Section “ Appendix H: Test Call” on page 1280. for more details on test calls.

Data Calls on Gateway Trunks.

This feature supports data calls for calls originating and/or terminating on Q.767/ISUP92 gateway trunk agencies. Data calls are supported on the following bearer services:

- 64kbps Unrestricted
- 56kbps

Following matrix shows the interworking supported by this feature for data calls:

Interworking Matrix For Data calls

	Terminating Agency							
Orig. Agency	Gateway	UCP Intra	UCP Inter	FGD SS7	FGD PTS	UCS PRI	FGB	DAL TIE
Gateway	X	X	X	X	X	X	X	X
UCP Intra	X							
UCP Inter	X							
FGD SS7	X							
FGD PTS	X							
UCS PRI	X							
FGB	X							
DAL TIE	X							

Please refer to Section “ Appendix I: Data Call” on page 1288. for more details on data calls.

ECAN support

Echo Canceller support is integrated into the PVG for ISUP92/Q.767.

Following section describes the messaging and office configuration for ECAN.

Please refer to Section “ Appendix J: ECAN” on page 1296.

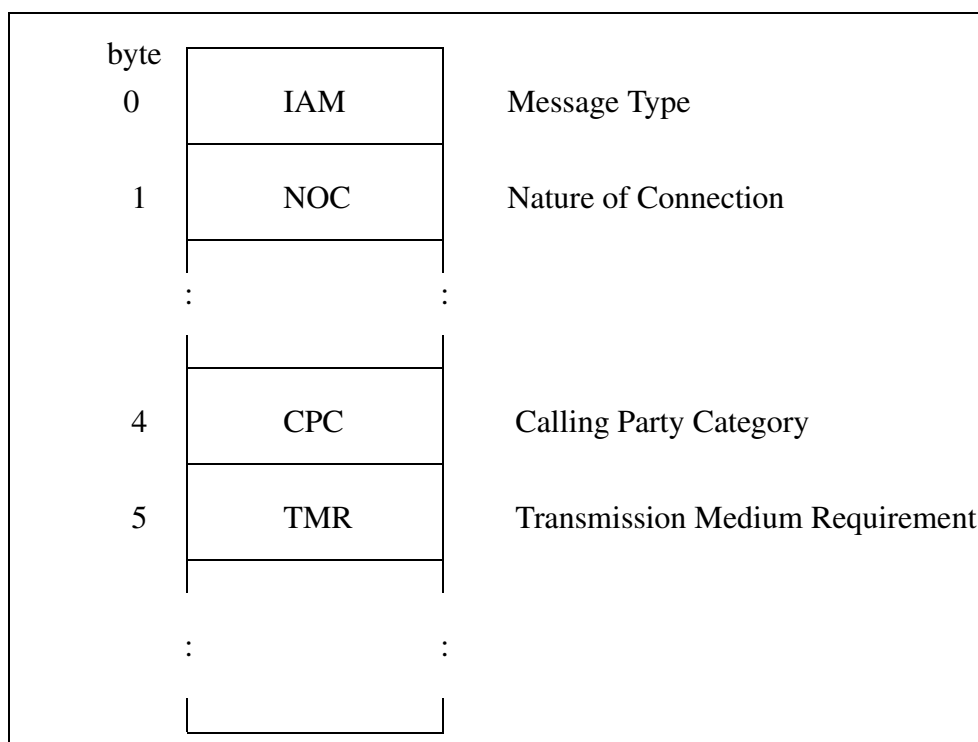
Echo Control Messaging

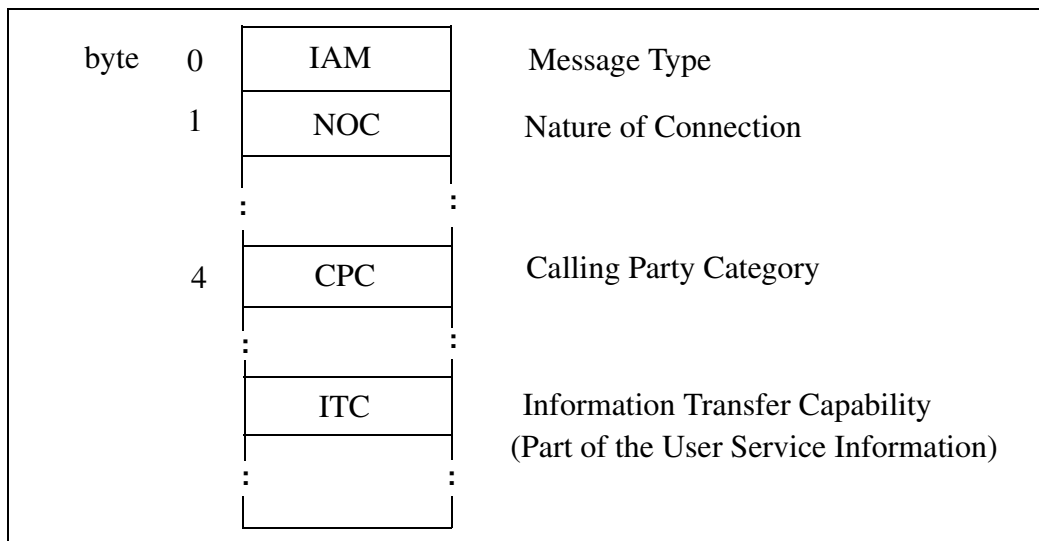
In relation to the ISUP messaging protocol, echo canceller control operates according to the following picture. The echo control information in the first forward-going message and the first backward-going message per call is used for the duration of that call.

Typically the IAM is the first forward-going message, and the ACM is the first backward-going message. However, a CON, CPG or ANM may also be sent as the first backward-going message. The logic to enable / disable the EC in backward-going message is described in more detail later.

Forward Address Parameter for Echo Cancellation (IAM)

IAM Message for Q.767/ISUP92



IAM Message for UCS ISUP**Nature of Connection (For both UCS and Q.767/ISUP92)**

H	G	F	E	D	C	B	A
			X				

E = Echo Control

0 - outgoing half echo device not included

1 - outgoing half echo device included

Transmission Medium Requirement (For Q.767/ISUP92 only)

H	G	F	E	D	C	B	A
						X	X

0000 0000 = speech

0000 0011 = 3.1 kHz audio

0000 0010 = 64 kb/s data call

Information Transfer Capability (For UCS only)

H	G	F	E	D	C	B	A
			X	X	X	X	X

00000 = speech

01000 = Unrestricted digital Information - data call

10000 = 3.1 kHz audio

Data Call:

If the TMR or ITC in USI parameter in the incoming IAM indicates that it is a data call, the echo controllers at the incoming and outgoing exchange remains OFF for the duration of the call, regardless of the echo control bit in any message.

Backward Call Indicator (ACM, CON, CPG, ANM)

The backward call indicator is included in ACM, CON, CPG and ANM messages for both ITU protocol and UCS protocol.

Echo cancel indication bit in Backward call indicator

H	G	F	E	D	C	B	A	
								BCI LSB
		X						BCI MSB

BCI MSB

0000 0000 = incoming half echo device not included

0010 0000 = incoming half echo device included

Indication of an incoming echo canceller included by a transit switch is given in the BCI of the ACM, CON, CPG or ANM. The BCI of the ACM and the CON is mandatory but is optional in the ANM and CPG.

The EC information in the first backward-going protocol message (e.g. ACM, CON, CPG or ANM) per call is used to notify EC status to the transit switch. EC information in the later messages is ignored. So, two cases may occurred during the call processing. In most cases, EC-bit is a mandatory part of the messages. However, in the case where EC-bit is optional and is not present, the next message is examined. In all cases, by the time the call reaches to the answer stage (after received ANM), at least one message with EC-bit should be sent to both trunks in the incoming and outgoing directions.

Table TRKSGRP

Echo canceller control is provided on a trunk subgroup basis, in table TRKSGRP. No checking is done in table control to ensure that all trunks in this subgroup do in fact have echo cancelling equipment present. Three fields pertain to echo canceller control:

- **ECSTAT** -this should be datafilled '**INTERNAL**' to allow the echo canceller to be used by call processing when required. If left at the default of 'UNEQ', the canceller remains OFF at all times.
- **ABCNTL** - this should be datafilled '**NONE**' to indicate that the echo canceller does not monitor the trunk's AB bits for activation information.

A-LAW/U-Law Conversion

The Succession CS2000 should be configured to use u-law PCM encoding in world zone-1. The ISUP92/Q.767 trunk agencies are only supported on E1 spans using A-law PCM encoding. The PVG will perform A-law to u-law conversion as required.

PCM encoding conversion on a per call basis is enabled, if transmission medium requirement parameter indicates speech and 3.1 kHz (PCM encoding conversion requirements is based on Q.764 section 2.1.1.3 b). The user information layer 1 protocol identification field of the user service information (USI) parameter in IAM must reflect the proper PCM encoding:

'Recommendation G.711 u-law' for supported UCS SS7 trunk agents (SS7 FGD, SS7 IMT Intra, and SS7 IMT Inter) and 'Recommendation G.711 A-law' for the ISUP92/Q.767 trunk agent. For UCS PRI trunk agent, user information layer 1 protocol identification field of the Low layer compatibility element in the Q.931 Setup must reflect 'Recommendation G.711, u-law speech'.

For 64K unrestricted data calls, the conversion between A-law and u-law PCM encoding on a per call basis is disabled. The user information layer 1 protocol identification field must reflect the proper PCM encoding value as stated in the previous paragraph.

Overlap Sending

Gateway trunks support overlap sending and that the field OVRLAP in table TRKSGRP is required to be set to enter overlap sending. If a 'F' digit is not received on called number when field OVRLAP in table TRKSGRP is set to 'Y', CS2000 will wait based on T35 timer value (if table C7UPTMR is not used, then default value is 5 seconds) for a subsequent address message (SAM) prior to processing the called number. If SAM is not received within the T35 time, CS2000 will proceed processing the called number.

CS2000 does not support overlap receiving and will always outpulse the called number in 'ENBLOC' format.

ISUP92/Q.767 interworking with supported national trunk agencies.

The supported CS2000 trunk agencies interworking with Q.767/ISUP92 trunks:

- SS7 IMT Inter (UCP)
- SS7 IMT Intra (UCP)
- FGD SS7 (UCP)
- FGD PTS¹⁸
- UCS PRI
- FGB¹⁸
- DAL TIE^{18 19}

The following interworkings are supported by this feature:

Interworkings Supported

Originating Agency	Terminating Agency
ISUP92	ISUP92
Q.767	Q.767
ISUP92	Q.767
Q.767	ISUP92
ISUP92/Q.767	IMT Intra
ISUP92/Q.767	IMT Inter
ISUP92/Q.767	DAL TIE

18. PTS trunks supported only in a hybrid configuration

19. Supported DAL TIE pulse type of MF and DT and start signal of WK.

Interworkings Supported

Originating Agency	Terminating Agency
ISUP92/Q.767	FGB
ISUP92/Q.767	FGD PTS
ISUP92/Q.767	FGD SS7
ISUP92/Q.767	PRI
FGD SS7	ISUP92/Q.767
FGD PTS	ISUP92/Q.767
FGB	ISUP92/Q.767
IMT Intra	ISUP92/Q.767
IMT Inter	ISUP92/Q.767
DAL TIE	ISUP92/Q.767
PRI	ISUP92/Q.767

Interworking between UCP ISUP & ISUP92 /Q.767

The supported UCP ISUP²⁰ messages that are interworked to ISUP92/Q.767 are:

- Address Complete Message (ACM)
- Answer Message (ANM)
- Initial Address Message (IAM)
- Release (REL)

The supported ISUP92/Q.767 messages that are interworked to UCP ISUP are:

- Address Complete Message (ACM)
- Answer Message (ANM)
- Connect Message (CON)
- Initial Address Message (IAM)
- Release (REL)

For details on interworking between UCP ISUP & ISUP92 /Q.767 Please refer to Section “ Appendix K: UCP ISUP & ISUP92/Q.767 Interworking” on page 1300.

20. UCP ISUP protocol on Succession CS2000 is implemented on IMT and SS7 FGD agents.

Interworking ISUP92/Q.767 with PTS agents

The supported ISUP92/Q.767 messages that are interworked to PTS agencies are:

- Address complete message (ACM)
- Answer message (ANM)
- Initial Address message (IAM)
- Release message (REL)
- Release complete message (RLC)

For details on interworking between PTS agents & ISUP92/Q.767 Please refer to Section “ Appendix L: Interworking of ISUP92/Q.767 with PTS agents” on page 1327..

Interworking with PRI agents**UCS PRI & ISUP92/Q.767 Message Interworking**

The supported UCS PRI messages that interwork to ISUP92/Q.767 are:

- Setup Message (SETUP)
- Alerting Message (ALERT)
- Progress Message (PROG)
- Connect Message (CONN)
- Disconnect Message (DISC)
- Release Message (REL)
- Release complete Message (REL COM)

The supported ISUP92/Q.767 messages that interwork to UCS PRI are:

- Address Complete Message (ACM)
- Answer Message (ANM)
- Connect Message (CON)
- Initial Address Message (IAM)
- Release Message (REL)
- Release Complete Message (RLC)

For details on interworking between UCS PRI and ISUP92/Q.767 Please refer to Section “ Appendix N: Interworking between ISUP92/Q.767 and UCS PRI” on page 1333.

Interworking between ISUP92 and Q.767 protocols

This feature supports interworking between ISUP92 trunks and Q.767 trunks.

All the Messages except the following is interworked between ISUP92 and Q.767. These messages are supported only on ISUP92 trunks. The below messages on Q.767 trunk are considered as unrecognized messages and are treated as per ITU - T Blue Book Q.767 section 4.1.1. Unrecognized messages are discarded without disrupting normal call handling. No logs are produced for unrecognized messages.

- Confusion Message (CFN)
- Facility Request Message (FAR) != 02
- Facility Reject Message (FRJ)
- Facility Accept Message (FAA)
- User to User Information Message (USR)

All the Parameters except the following are supported in Q.767. These parameters are supported only on ISUP92 trunks. On Q.767 trunks they are discarded.

- Redirecting Number
- Redirection Information
- Redirection Number
- Parameter compatibility information
- Message compatibility information
- Call Diversion information

The other interworking issues are:

- Mapping of new cause values: For information on this issue please refer to section 1.4.2.3.
- Handling of MCP and PCP parameters: For more information on this issue, please refer to section 1.4.2.1.2.

Optionality

The functionality provided by this feature is controlled by SOC option GIMT0003.

Data schema (DS)

This feature introduces the following two new tables:

- CPCSCRN
- CCTABLE

The following tables are modified by this feature:

- TRKGRP
- TRKSGRP
- STDPRTCT
- RTEATTR
- CSEMAP
- TMTMAP

This feature introduces one new office variable - OFC_SERVING_CC in OFCVAR.

Please refer to the “Data Schema Changes (DS)” section of this feature document (A00003711) for more details about this.

AMA/Billing information (AM)

This feature supports UCS13 CDR template. The fields are captured as per the existing support, except the following fields:

INCINTL: This field is set based on the ‘Nature of Address’ in ‘Calling Party Address’ parameter. If the ‘Nature of Address’ in ‘Calling Party Address’ parameter is set to ‘Intl_sig_number’ then the field is set to ‘Y’.

CLGPTYNO: This field captures up to most significant 15 digits calling party address digits received in the ‘Calling Party Address’ parameter of IAM.

CALLEDNO: This field captures most significant 15 digits of called party address used in translations.

DIALEDNO: This field captures most significant 15 digits of called party address after pretranslations.

OUTPULNO: This field captures most significant 15 digits of outpulsed number. If translations insert a ‘B’ or ‘C’ digits in the outpulsed number then these digits will be represented by ‘*’ and ‘#’ in the TBCD digit format respectively.

PREDIG: Three bits defining dialed prefix digits. For Code11 and Code12 calls, this field captures ‘0’.

CNPREDIG: The called number prefix digits. For Code11 and Code 12 calls, this field captures ‘0’.

Feature impact

Interactions

Hardware Requirements or Dependencies

GWIMT trunks are supported via dedicated PVG VSPs and international carrier (E1 or STM-1) interfaces. PVG VSPs for GWIMT trunks are separate from any VSPs which may be used to provide trunking to the national network in world zone 1. GWIMT PVG VSPs must also be controlled by one or more dedicated Gateway Controllers.

Software Requirements or Dependencies

GWIMT is supported initially in the Succession North American Combo load SNNCSH07; the corresponding GWC load supporting GWIMT trunks in this release is the international GC070 variant (GI070).

Limitations and restrictions

- GWIMT trunks are not supported on DTC type peripherals in SNNCSH07. Only PVG based GWIMT trunks are supported.
- Echo Cancellation is provided by the PVG VSP under this activity. Support for external echo cancelers is not provided.
- Carrier AIN calls can terminate to GWIMT trunks, however calls originating on GWIMT trunks do not encounter Carrier AIN (CAIN) triggers.
- CLI screening on ISUP92/Q.767 gateway trunk agency is not supported.
- Gateway trunk agencies (ISUP92/Q.767) supports only ADDR dialplan. This restriction is provided as datafill restriction.
- When option GWYTRK is datafilled in table TRKGRP, the fields CLIREQ and CLISCRN must be set to N. This is also implemented as datafill restriction.
- Local Number Portability (LNP) is not support on ISUP92/Q.767 gateway trunk agency.
- The maximum number of called number digits supported by this feature is 15 (15-digit IDDD) excluding the end-of-digit signal (F).
- The maximum number of calling number digits supported by this feature is 15 (15-digit IDDD) excluding the end-of-digit signal (F).
- The feature implements only a limited set of GSP features, on Succession CS2000 in the role of a UCS DMS-250 switch.
- Support for ISUP92 and Q.767 protocols are subject to partial compliance as stated within this feature.

- This feature support only internal echo cancellers, in which case ESUPR field should be set to N, ECSTAT field should be set to INTERNAL, and ABCNTL field should be set to NONE in table TRKSGRP.
- For transit inbound code 11/code 12 calls a maximum of 14 called party address digits are supported.
- For code 11/code 12 calls, only one code 11 or code 12 signal code is supported in the called party address digits stream.
- RLT functionality is not supported by this feature. This includes support of RLT option on ISUP92/Q767 agencies and interworking of ISUP92/Q767 agencies with RLT trunk agents.
- CGETS functionality, including IAM priority, is not supported on GWIMT trunks.

Interactions

CIC routing/CIC delivery

The feature doesn't support CIC routing on ISUP92 and Q.767 trunks. CIC routing on UCS agents are supported as per the existing functionality.

The TNS/CIP parameters received on ISUP92/Q.767 gateway agencies are discarded. In the case when ISUP92/Q.767 gateway trunks are terminating agencies, these parameters are not delivered.

AX0205 'UCS TRKGRP NOA Enhancements'

Feature AX0205 'UCS Trunkgroup NOA Enhancements' enhances Nature of address delivery in called party address parameter of outgoing IAM. This feature affects the INBOUND direct termination calls terminating on Inter/Intra network ISUP IMTs.

The NOA outputted in called party address parameter of outgoing IAM for these calls is the value of OUTNOA datafilled in table TRKGRP. Please refer to feature AX0205 for more details.

Carrier AIN

ISUP92/Q.767 trunk agency as an originator

Carrier AIN functionality is not supported on an incoming call on a ISUP92/Q.767 trunk agency.

ISUP92/Q.767 trunk agency as a terminator

The ISUP92/Q.767 trunk agency is supported as a terminating agent for incoming calls on the supported CS2000 agencies that are CAIN capable. Any PICs, TDPs, triggers and EDPs supported on the originating CS2000

agencies, are supported by this feature with the following restrictions.

- Any Carrier AIN SS7 parameters that are not supported within the ISUP92/Q.767 trunk agency protocol is not delivered/included in any outgoing messages on the ISUP92/Q.767 trunk agency.
- Direct termination routing to the terminating ISUP92/Q.767 trunk agency is supported via table TERM RTE only.
- The terminating call model is not supported.

User-To-User Parameter Mapping

Reference feature document AD9067 'Support for User to User Parameter' for proper requirements when mapping of the User to User parameter is required.

Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema _____

User Interface _____

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

References

- A59007112, "Up to 128ms ECAN (Echo Cancellation) on IW-SPM IP"
- A00000284, "Packet Trunking IP AAL2 test Line Testing Utilizing the UAS and SAGE"
- A59038503, "Test Trunk Support via IW-SPM-IP"
- AR2020 - DMS300 - ISUP92
- AM0115, "UCS PRA on DMS-250".
- AD1614, "DMS-250 PRA Application Guide".
- AD9067, "Support For UUI Parameters".

- AM0184, “Access Transport PRI/SS7 DDOC”
- AD8792, “Route Based Outgoing Parameter Modifications”.
- AD6849, “UCS ANI Delivery Enhancements”.
- ITU-T Recommendation Q.850 (March 1993)
- ITU-T Recommendation Q.767 Blue Book version (February 1991)
- ITU-T Recommendation Q.761-764 White Book version (March 1993)

Glossary

Term	Description
GWIMT	Gateway Inter Machine Trunk
PVG	Passport Voice Gateway
BSS	Bearer Service Selection
CAS	Channel Associated Signalling
CAIN	Carrier Advanced Intelligent Networks
CCITT	Consultative Committee on International Telephony and Telegraphy
CCS7	Common Channel Signaling No. 7
CDR	Call Detail Record
CGETS	Carrier GETS
CIC	Carrier Identification Code
CLI	Calling Line Identification
CSP	Communications System Platform
CPC	Calling Party Category
DAL	Direct Access Link
DDOC	Design Document
DMS	Digital Multiplexing System
DTC	Digital Trunk Controller
DTCI	Digital Trunk Controller International
DTCO	Digital Trunk Controller Overseas
EC	Echo Canceler
ECC	Echo Canceler Controller
EDP	Electronic Data Processing

Term	Description
EOPS	Enhanced Operator Services
FGB	Feature Group B
FGD	Feature Group D
FSD	Feature Specification Document
GETS	Government Emergency Telecommunications Service
GWC	Gateway Controller
IMT	Inter Machine Trunk
ISUP	ISDN User Part
ITU	International Telecommunications Union
LEC	Local Exchange Carrier
MCP	Message Compatibility Procedure
NORTEL	Northern Telecom
NWM	Network Management
PIC	Point In Call
PCM	Pulse Code Modulation
PCP	Parameter Compatibility Procedure
PSN	Programmable Service Node
PTS	Per-Trunk Signaling
RLT	Release Link Trunk
SOC	Software Optionality Control
SS7	Signaling System No. 7
TDP	Telelocator Data Protocol
TRKGRP	Trunk Group Table
TRKSGRP	Trunk Signaling Group Table
TRM	Transmission Resource Management
UCP	Universal Carrier Protocol
UCS	Universal Carrier Services
UIFN	Universal International Freephone Number
VPN	Virtual Private Network

Term	Description
XPM	eXtended Peripheral Module

APPENDIX A: Messages and Parameters Supported on ISUP92

Messages and Parameters that are supported on ISUP92 trunks are listed in the following tables in this section.

International ISUP92 message base

The table below represents the list of recognized messages for an international ISUP92 trunk at the Succession CS2000.

Note: S/R means Send/Receive. Dis/CFN means Discard and send CFN (confusion message)

Note: P/T/D means Process (Process the message), Tandem (Tandem message across network) and Discard (Discard and ignore the message) respectively.

International ISUP92 parameter base

International ISUP92 Messages recognized by the Succession CS2000

Acronym	Message Name	Send/Receive/ Dis/CFN	Process/ Tandem/Discard
ACM	Address complete	S/R	P
ANM	Answer	S/R	P
BLO	Blocking	S/R	P
BLA	Blocking Acknowledgment	S/R	P
CPG	Call Progress	S/R	T
CGB	Circuit Group Blocking	R	P
CGBA	Circuit Group Blocking Acknowledgment	S	P
GRS	Circuit Group Reset	S/R	P
GRA	Circuit Group Reset Acknowledgment	S/R	P
CGU	Circuit Group Unblocking	R	P
CGUA	Circuit Group Unblocking Acknowledgment	S	P
CON	Connect	S/R	P
COT	Continuity	S/R	P
CFN	Confusion	S/R	P

International ISUP92 Messages recognized by the Succession CS2000

Acronym	Message Name	Send/Receive/ Dis/CFN	Process/ Tandem/Discard
CCR	Continuity Check Request	S/R	P
FAA	Facility Accepted	Dis/CFN	Discard
FAR	Facility Request	R ^a	Discard/ Tandem
FRJ	Facility Reject	^b Dis/CFN	Discard
FOT	Forward Transfer	S/R	T
IAM	Initial Address	S/R	P
INR	Information Request	S ^c	T
REL	Release	S/R	P
RLC	Release Complete	S/R	P
RSC	Reset Circuit	S/R	P
RES	Resume	S/R	T ^d
SAM	Subsequent Address	S/R	P
SUS	Suspend	S/R	T ^e
UBL	Unblocking	S/R	P
UBA	Unblocking Acknowledgment	S/R	P
USR	User-to-user information	Dis/CFN	Discard

a. If FAR != 02 is received, the Succession CS2000 discards the FAR and returns.

If FAR = 02 (user-to-user service), the Succession CS2000 tandems the FAR

b. If FRJ is received, the Succession CS2000 discards the FRJ and returns CFN with cause value 97 with FRJ as the diagnostic information.

c. There is no call processing done for this message, the Succession CS2000 tandems this message. Succession CS2000 always delivers the CLI in enbloc format. If an incomplete CLI is received, the Succession CS2000 does not generate INR msg but instead discards the calling party parameter.

d. RES msg is tandemmed only if the Resume indicator is set to network initiated and the message is received on the terminator after the ANM, and the originator agency does not support existing Succession CS2000 Suspend/Resume functionality. For all other cases it is discarded.

e. SUS msg is tandemmed only if the suspend indicator is set to network initiated and the message is received on the terminator after the ANM, and the originator agency does not support existing Succession CS2000 Suspend/Resume functionality. For all other cases it is discarded.

The Succession CS2000 supports the following parameters for the given supported messages in accordance with ISUP92 for the Succession CS2000 exchange.

Notations used are:

F = mandatory fixed length parameter

V = mandatory variable length parameter

O = optional parameter

The proprietary and national parameters are discarded unless specified.

When the Succession CS2000 generates a REL or CFN message, the location field of the cause parameter is set to 'International Network'. If the REL message is generated using table TMTMAP, the location field of the cause parameter is taken from the 'location' field of the table entry. Please refer to section 1.4.2.3 for more details on cause handling.

'ISUP92 minimum set' refers to the recommended minimum set of parameters to be supported for each supported message based on ITU-T Recommendation Q.761 White Book version table 4 for international use.

Initial Address Message (IAM)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the IAM message as shown in the following table. All parameters not contained in this table are subject to the rules of the PCP procedures.

> Parameters supported in the IAM Message ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Nature Of Connection Indicators	F	Process	ISUP92 minimum set
Forward Call Indicators	F	Process	ISUP92 minimum set
Calling Party's Category	F	Process	ISUP92 minimum set
Transmission Medium Requirement (TMR)	F	Process	ISUP92 minimum set supported values ^a .
Called Party Number	V	Process	ISUP92 minimum set
Access Transport	O	Tandem	ISUP92 minimum set
Calling Party Number	O	Process	ISUP92 minimum set
Closed User Group Interlock Code	O	Tandem	ISUP92 minimum set
Connection Request	O	Discard	

> Parameters supported in the IAM Message ISUP92

Parameter Name	Type	Action	Notes
End of Optional Parameters	O	Process	ISUP92 minimum set
Generic Notification	O	Discard	
Generic Number	O	Discard	
Generic Reference	O	Discard	
Location Number	O	Discard	
MLPP Precedence	O	Discard	
Optional Forward Call Indicators	O	Tandem	ISUP92 minimum set
Original Called Number	O	Tandem	ISUP92 minimum set
Origination ISC Point Code	O	Discard	
Parameter Compatibility Information	O	See Section 1.4.2.1.2	
Propagation Delay Counter	O	Discard	
Redirecting Number	O	Tandem	ISUP92 minimum set
Redirection Information	O	Tandem	ISUP92 minimum set
Transmission Medium Requirement Prime	O	Discard	
User service information	O	Process	ISUP92 minimum set
User Service Information prime	O	Discard	
User teleservice information	O	Discard	
User-to-user Indicators	O	Tandem	ISUP92 minimum set
User-to-user information	O	Tandem	ISUP92 minimum set
Call reference	O	Discard	National use only
Generic digit	O	Discard	National use only

> Parameters supported in the IAM Message ISUP92

Parameter Name	Type	Action	Notes
Network specific facility	O	Discard	National use only
Remote operations	O	Discard	National use only
Service activation	O	Discard	National use only
Transit network selection	O	Discard	National use only

a. Supported values are Speech, 64 Kbit/s unrestricted, and 3.1 KHz audio

Address complete message (ACM)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the IAM message as shown in the following table. All parameters not contained in this table are subject to the rules of the PCP procedure.

Parameters supported in the ACM Message ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Backward call indicators	F	Process	ISUP92 minimum set
Optional backward call indicators	O	Process	ISUP92 minimum set
Cause indicators	O	Tandem	ISUP92 minimum set
User-to-user indicators	O	Tandem	ISUP92 minimum set
User-to-user information	O	Tandem	ISUP92 minimum set
Access transport	O	Tandem	ISUP92 minimum set
Generic notification Indicator	O	Tandem	ISUP92 minimum set
Transmission medium used	O	Tandem	ISUP92 minimum set
Echo control information	O	Tandem	ISUP92 minimum set
Access delivery information	O	Tandem	ISUP92 minimum set

Parameters supported in the ACM Message ISUP92

Parameter Name	Type	Action	Notes
Redirection number	O	Tandem	ISUP92 minimum set
Parameter compatibility information	O	Tandem	ISUP92 minimum set
Call diversion information	O	Tandem	ISUP92 minimum set
Redirection number restriction	O	Tandem	ISUP92 minimum set
End of optional parameters	O	Tandem	ISUP92 minimum set
Call reference	O	Discard	National use only
Network specific facility	O	Discard	National use only
Remote operations	O	Discard	National use only
Service activation	O	Discard	National use only

Answer message (ANM)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the ANM message as shown in the following table. All parameters not contained in this table are subject to the rules of the PCP procedure.

Parameters supported in the ANM Message ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Backward call indicators	O	Tandem	ISUP92 minimum set
Optional backward call indicators	O	Tandem	ISUP92 minimum set
User-to-user indicators	O	Tandem	ISUP92 minimum set
User-to-user information	O	Tandem	ISUP92 minimum set
Connected number	O	Tandem	ISUP92 minimum set
Access transport	O	Tandem	ISUP92 minimum set

Parameters supported in the ANM Message ISUP92

Parameter Name	Type	Action	Notes
Access delivery information	O	Tandem	ISUP92 minimum set
Generic notification indicator	O	Tandem	ISUP92 minimum set
Parameter compatibility information	O	Tandem	ISUP92 minimum set
Call history information	O	Tandem	ISUP92 minimum set
Generic number	O	Tandem	ISUP92 minimum set
Transmission medium used	O	Tandem	ISUP92 minimum set
Redirection number	O	Tandem	ISUP92 minimum set
Echo control information	O	Tandem	ISUP92 minimum set
Redirection number restriction	O	Tandem	ISUP92 minimum set
End of optional parameters	O	Tandem	ISUP92 minimum set
Call reference	O	Discard	National use only
Network specific facility	O	Discard	National use only
Remote operations	O	Discard	National use only
Service activation	O	Discard	National use only

Call progress message (CPG)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the CPG message as shown in the following table. All parameters not contained in this table are subject to the rules of the PCP procedure.

Parameters supported in the CPG Message ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Event information	F	Process	ISUP92 minimum set
Backward call indicators	O	Tandem	ISUP92 minimum set
Optional backward call indicators	O	Tandem	ISUP92 minimum set
Cause indicators	O	Tandem	ISUP92 minimum set
User-to-user indicators	O	Tandem	ISUP92 minimum set
User-to-user information	O	Tandem	ISUP92 minimum set
Access transport	O	Tandem	ISUP92 minimum set
Redirection number	O	Tandem	ISUP92 minimum set
Transmission medium used	O	Tandem	ISUP92 minimum set
Access delivery information	O	Tandem	ISUP92 minimum set
Generic notification indicator	O	Tandem	ISUP92 minimum set
Parameter compatibility information	O	Tandem	ISUP92 minimum set
Call diversion information	O	Tandem	ISUP92 minimum set
Redirection number restriction	O	Tandem	ISUP92 minimum set
End of optional parameters	O	Tandem	ISUP92 minimum set
Call reference	O	Discard	National use only
Network specific facility	O	Discard	National use only
Remote operations	O	Discard	National use only
Service activation	O	Discard	National use only

Connect message (CON)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the CON message as shown in the following table. All parameters not contained in this table are subject to the rules of the PCP procedure.

Parameters supported in the CON Message ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Backward call indicators	F	Process	ISUP92 minimum set
Optional backward call indicators	O	Tandem	ISUP92 minimum set
User-to-user indicators	O	Tandem	ISUP92 minimum set
User-to-user information	O	Tandem	ISUP92 minimum set
Access transport	O	Tandem	ISUP92 minimum set
Generic notification Indicator	O	Tandem	ISUP92 minimum set
Parameter compatibility information	O	Tandem	ISUP92 minimum set
Call history information	O	Tandem	ISUP92 minimum set
Generic number	O	Tandem	ISUP92 minimum set
Transmission medium used	O	Tandem	ISUP92 minimum set
Redirection number	O	Tandem	ISUP92 minimum set
Echo control information	O	Tandem	ISUP92 minimum set
Redirection number restriction	O	Tandem	ISUP92 minimum set
Access delivery information	O	Tandem	ISUP92 minimum set
Connected number	O	Tandem	ISUP92 minimum set

Parameters supported in the CON Message ISUP92

Parameter Name	Type	Action	Notes
End of optional parameters	O	Tandem	ISUP92 minimum set
Call reference	O	Discard	National use only
Network specific facility	O	Discard	National use only
Remote operations	O	Discard	National use only
Service activation	O	Discard	National use only

Facility Accept (FAA) & Facility Request Messages (FAR)

The Succession CS2000 discards FAA Messages and sends Confusion message on an ISUP92 trunk. If FAR != 02, is received, the DMS-250 discards the FAR. If FAR with facility indicator set to User-to-User service (00000010), is received, the DMS-250 tandems the FAR.

Continuity Message (COT)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the COT message as shown in the following table. The proprietary and national use parameters are not supported.

Parameters supported in the COT Message on ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Continuity Indicators	F	Tandem	ISUP92 minimum set

Circuit Group ReSet (GRS) & circuit Group Reset Acknowledge messages (GRA)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the GRS & GRA messages as shown in the following table. The proprietary and national use parameters are not supported.

Parameters supported in the GRS & GRA Messages on ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Range and Status	V	Process	ISUP92 minimum set

User-to-User Information Message (USR)

The Succession CS2000 discards USR Messages and sends Confusion message on an ISUP92 trunk.

Facility Reject message (FRJ)

The Succession CS2000 discards the FRJ and returns CFN with cause value 97 with FRJ as the diagnostic information.

Circuit Group blocking (CGB), block ACK(CGBA), unblocking (CGU), unblock ack (CGUA) messages.

The Succession CS2000 on an ISUP92 trunk supports the mandatory parameters in the CGB, CGBA, CGU, CGUA messages as shown in the following table. The CGB, CGBA, CGU, or CGUA messages do not have optional parameters.

Parameters supported in the CGB,CGBA,CGU,CGUA Messages on ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Circuit group supervision msg type indicator	F	Process	ISUP92 minimum set
Range and Status	V	Process	ISUP92 minimum set

Blocking (BLO), block ack (BLA), Continuity check request (CCR), unblock (UBL), unblock ack (UBA), Reset circuit (RSC) messages.

The Succession CS2000 on an ISUP92 trunk supports the mandatory parameters in the BLO, BLA, CCR, UBL, UBA, RSC messages as shown in the following table. The BLO, BLA, CCR, UBL, UBA, RSC messages do not have optional parameters.

Parameters supported in the BLO, BLA, CCR, UBL, UBA, RSC Messages on ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	

Confusion Message (CFN)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the CFN message as shown in the following table.

Parameters supported in the CFN Message on ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Cause Indicators	V	Process	ISUP92 minimum set
End of Optional Parameters	O	Process	ISUP92 minimum set

Release Message (REL)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the CON message as shown in the following table. All parameters not contained in this table are subject to the rules of the PCP procedure.

Parameters supported in the REL Message ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Cause Indicators	F	Process	ISUP92 minimum set
Automatic congestion level	O	Discard	The switch handles this parameter on a link-by-link basis. If received, the parameter is removed from the message and not transited.
User-to-user indicators	O	Tandem	ISUP92 minimum set
User-to-user information	O	Tandem	ISUP92 minimum set
Access transport	O	Tandem	ISUP92 minimum set
Parameter compatibility information	O	Tandem	ISUP92 minimum set
Redirection number restriction	O	Tandem	ISUP92 minimum set
Access delivery information	O	Tandem	ISUP92 minimum set

Parameters supported in the REL Message ISUP92

Parameter Name	Type	Action	Notes
End of optional parameters	O	Tandem	ISUP92 minimum set
Network specific facility	O	Discard	National use only
Signalling Point Code	O	Discard	National use only
Redirection Number	O	Discard	National use only
Redirection Information	O	Discard	National use only

Release Complete Message (RLC)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the RLC message as shown in the following table. Parameters not contained in this table are treated as unrecognized parameters.

Parameters supported in the RLC Message on ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Cause Indicators	O	N/A	ISUP92 minimum set
End of Optional Parameters	O	N/A	ISUP92 minimum set

Forward Transfer Message (FOT)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the FOT message as shown in the following table. All parameters not contained in this table are treated as unrecognized parameters.

Parameters supported in the FOT Message on ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
End of Optional Parameters	O	Tandem	ISUP92 minimum set
Call reference	O	Discard	National Use only

Suspend (SUS) & Resume (RES) Messages

The Succession CS2000 on an ISUP92 trunk supports the parameters in the SUS & RES messages as shown in the following table. All parameters not contained in this table are treated as unrecognized parameters.

Parameters supported in the SUS & RES Message on ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Suspend/Resume indicators	F	Tan-dem/Dis-card ^a	ISUP92 minimum set
End of Optional Parameters	O	Process	ISUP92 minimum set
Call reference	O	Discard	National Use only

a. If the Suspend/ Resume indicator (in the SUS/RES message) is set to network initiated and the message is received on the terminator after the ANM, the message is Tandemed. For all other cases it is Discarded.

Subsequent Address Message (SAM)

The Succession CS2000 on an ISUP92 trunk supports the parameters in the SAM message as shown in the following table.

Parameters supported in the SAM Message on ISUP92

Parameter Name	Type	Action	Notes
Message Type	F	Process	ISUP92 minimum set
Subsequent number	V	Process	ISUP92 minimum set
End of Optional Parameters	O	Process	ISUP92 minimum set

Appendix B: Messages and Parameters Supported on Q.767

Messages and Parameters that are supported on Q.767 trunks are listed in the Tables in this section. Messages and parameters marked for national use, are discarded

International Q.767 Message Base

The Table below represents the list of recognized messages for an international Q.767 trunk at the DMS-250 exchange.

Note: S/R means Send/Receive.

Note: P/T means Process (Process the message), Tandem (Tandem message across network) respectively.

International Q.767 Messages recognized by the Succession CS2000

Acronym	Message Name	Send/Receive	Process/ Tandem
ACM	Address complete	S/R	P
ANM	Answer	S/R	P
BLO	Blocking	S/R	P
BLA	Blocking Acknowledgment	S/R	P
CPG	Call Progress	S/R	T
CGB	Circuit Group Blocking	R	P
CGBA	Circuit Group Blocking Acknowledgment	S	P
GRS	Circuit Group Reset	S/R	P
GRA	Circuit Group Reset Acknowledgment	S/R	P
CGU	Circuit Group Unblocking	R	P
CGUA	Circuit Group Unblocking Acknowledgment	S	P
CON	Connect	S/R	P
COT	Continuity	S/R	P
CCR	Continuity Check Request	S/R	P
FOT	Forward Transfer	S/R	T
IAM	Initial Address	S/R	P
INR	Information Request	S ^a	P
REL	Release	S/R	P
RLC	Release Complete	S/R	P
RSC	Reset Circuit	S/R	P
RES	Resume	S/R ^b	T
SAM	Subsequent Address	S/R	P
SUS	Suspend	S/R ^c	T
UBL	Unblocking	S/R	P

International Q.767 Messages recognized by the Succession CS2000

Acronym	Message Name	Send/Receive	Process/ Tandem
UBA	Unblocking Acknowledgment	S/R	P

a. There is no call processing done for this message, the DMS-250 tandems this message. DMS-250 always delivers the CLI in enbloc format. If an incomplete CLI is received, the DMS-250 does not generate INR msg but instead discards the calling party parameter.

b. If the Resume indicator (in the RES message) is set to network initiated and the message is received on the terminator after the ANM, and the originator agency does not support existing DMS-250 Suspend/Resume functionality, the message is Tandemed. For all other cases it is Discarded.

c. If the Suspend indicator (in the SUS message) is set to network initiated and the message is received on the terminator after the ANM, and the originator agency does not support existing DMS-250 Suspend/Resume functionality, the message is Tandemed. For all other cases it is Discarded

International Q.767 Parameter Base

The Succession CS2000 supports the following parameters for the given supported call processing messages in accordance with Q.767 recommendation for the DMS-250 exchange.

F = mandatory fixed length parameter

V = mandatory variable length parameter

O = optional parameter

The proprietary and national use parameters are discarded.

‘Q.767 minimum set’ refers to the recommended minimum set of parameters to be supported for each supported message based on ITU-T Recommendation Q.767 Blue Book version tables C-5 to C-28.

Initial Address Message (IAM)

The Succession CS2000 on an Q.767 trunk supports the parameters in the IAM message as shown in the following table. All parameters not contained in this table are discarded.

Parameters supported in the IAM Message at Q.767

Parameter Name	Type	Action	Notes
Message Type	F	Process	Q.767 minimum set

Parameters supported in the IAM Message at Q.767

Parameter Name	Type	Action	Notes
Nature Of Connection Indicators	F	Process	Q.767 minimum set
Forward Call Indicators	F	Process	Q.767 minimum set
Calling Party's Category	F	Process	Q.767 minimum set
Transmission Medium Requirement (TMR)	F	Process	Q.767 minimum set
Called Party Number	V	Process	Q.767 minimum set
Access Transport	O	Tandem	Q.767 minimum set
Calling Party Number	O	Process	Q.767 minimum set
Closed User Group Interlock Code	O	Tandem	Q.767 minimum set
End of Optional Parameters	O	Process	Q.767 minimum set
Optional Forward Call Indicators	O	Tandem	Q.767 minimum set
User service information	O	Process	Q.767 minimum set
User-to-user information	O	Tandem	Q.767 minimum set
Call reference	O	Discard	National use only
Generic digit	O	Discard	National use only
Network specific facility	O	Discard	National use only
Remote operations	O	Discard	National use only
Service activation	O	Discard	National use only
Transit network selection	O	Discard	National use only

Address Complete (ACM), Answer Message (ANM), Call Progress (CPG), Connect (CON), Release (REL) Messages.

The parameters supported in these messages are given in Table 35. All the parameters shown in table 35 are tandemed.

Parameters supported in ACM, CPG, ANM, CON and REL messages

Message	Parameters tandemed
ACM	Optional Backward Call Indicators, Cause Indicator, User to user indicators ^a , User to user information, Access Transport
CPG	Optional Backward Call Indicators, Backward Call Indicators, User to user information, Access Transport
ANM	Backward Call Indicators, Connected Number ^a , User to user information, Access Transport
CON	Connected Number ^a , Backward call indicator, User to user indicators, User to user information, Access Transport
REL	User to user information. Automatic congestion Level ^b

a. It is tandemed only if it is valid as per Q767 recommendations.

b. It is processed as per Q767 recommendations and is not tandemed.

Continuity Message (COT)

The Succession CS2000 on an Q.767 trunk supports the parameters in the COT message as shown in the following table.

Parameters supported in the COT Message on Q.767

Parameter Name	Type	Action	Notes
Message Type	F	Process	Q.767 minimum set
Continuity Indicators	F	Tandem	Q.767 minimum set

Circuit Group ReSet (GRS) & circuit Group Reset Acknowledge messages (GRA)

The Succession CS2000 on an Q.767 trunk supports the parameters in the GRS & GRA messages as shown in the following table.

Parameters supported in the GRS & GRA Messages on Q.767

Parameter Name	Type	Action	Notes
Message Type	F	Process	Q.767 minimum set
Range and Status	V	Process	Q.767 minimum set

Circuit Group blocking (CGB), block ack (CGBA), unblocking (CGU), unblock ack (CGUA) messages.

The Succession CS2000 on an Q.767 trunk supports the mandatory parameters in the CGB, CGBA, CGU, CGUA messages as shown in the following table. The CGB, CGBA, CGU, or CGUA messages do not have optional parameters.

Parameters supported in the CGB,CGBA,CGU,CGUA Messages on Q.767

Parameter Name	Type	Action	Notes
Message Type	F	Process	Q.767 minimum set
Circuit group supervision msg type indicator	F	Process	Q.767 minimum set
Range and Status	V	Process	Q.767 minimum set

Blocking (BLO), block ack (BLA), Continuity check request (CCR), unblock (UBL), unblock ack (UBA), Reset circuit (RSC) messages.

The Succession CS2000 on an Q.767 trunk supports the mandatory parameters in the BLO, BLA, CCR, UBL, UBA, RSC messages as shown in the following table. The BLO, BLA, CCR, UBL, UBA, RSC messages do not have optional parameters.

Parameters supported in the BLO, BLA, CCR, UBL, UBA, RSC Messages on Q.767

Parameter Name	Type	Action	Notes
Message Type	F	Process	Q.767 minimum set

Release Complete Message (RLC)

The Succession CS2000 on an Q.767 trunk supports the parameters in the RLC message as shown in the following table. Parameters not contained in this table are treated as unrecognized parameters and discarded.

Parameters supported in the RLC Message on Q.767

Parameter Name	Type	Action	Notes
Message Type	F	Process	Q.767 minimum set
Cause Indicators	O	N/A	Q.767 minimum set
End of Optional Parameters	O	N/A	Q.767 minimum set

Forward Transfer Message (FOT)

The Succession CS2000 on an Q.767 trunk supports the parameters in the FOT message as shown in the following table. Parameters not contained in this table are treated as unrecognized parameters.

Parameters supported in the FOT Message on Q.767

Parameter Name	Type	Action	Notes
Message Type	F	Process	Q.767 minimum set
End of Optional Parameters	O	Tandem	Q.767 minimum set
Call reference	O	Discard	National Use only

Suspend (SUS) & Resume (RES) Messages

The Succession CS2000 on an Q.767 trunk supports the parameters in the SUS & RES messages as shown in the following table. Parameters not contained in this table are treated as unrecognized parameters.

Parameters supported in the SUS & RES Message on Q.767

Parameter Name	Type	Action	Notes
Message Type	F	Process	Q.767 minimum set
Suspend/Resume indicators	F	Tandem/ discard ^a	Q.767 minimum set
End of Optional Parameters	O	Process	Q.767 minimum set

Parameters supported in the SUS & RES Message on Q.767

Parameter Name	Type	Action	Notes
Call reference	O	Discard	National Use only

a. If the Suspend/ Resume indicator (in the SUS/RES message) is set to network initiated and the message is received on the terminator after the ANM, the message is Tandemed. For all other cases it is Discarded.

Subsequent Address Message (SAM)

The Succession CS2000 on an Q.767 trunk supports the parameters in the SAM message as shown in the following table.

Parameters supported in the SAM Message on Q.767

Parameter Name	Type	Action	Notes
Message Type	F	Process	Q.767 minimum set
Subsequent number	V	Process	Q.767 minimum set
End of Optional Parameters	O	Process	Q.767 minimum set

Appendix C: Q.767/ISUP92 Timers**Q.767/ISUP92 Timers for International use**

(ISUP/Q.767) /Q.118	Cause of initiation	Table C7UPTMR timer	Range (default value)
T1 4-15 s	When release message is sent	NQ764T1	1-60 s (15 s)
T2 3 min	When suspend request controlling exchange receives suspend (user) message	NQ764T2	1-240 s (180 s)
T3	Not used on the international interface		
T4	Not used on the international interface		
T5 1 min	When initial release message is sent	NQ764T5	1-180 s (60 s)

Q.767/ISUP92 Timers for International use

(ISUP/Q.767) /Q.118	Cause of initiation	Table C7UPTMR timer	Range (default value)
T6 Q.118	When controlling exchange receives suspend (network)	NQ764T6	1-240 s (90 s)
T7 20-30 s	When the latest address message is sent	NQ764T7	1-60 s (20 s)
T8 10-15 s	When transit or incoming international exchange receives initial address message requiring continuity check on this circuit, or indicates that continuity check has been performed on a previous circuit	NQ764T8	1-60 s (15 s)
T9 Q.118 2-4 min	When national controlling or outgoing international exchange receives ACM ^a	Q.118	120-240 s (180 s)
T10 4-6 s	When last digit is received in interworking situations	NQ764T10	1-30 s (5 s)
T11 15-20 s	When latest address message is received in interworking situations	NQ764T11	1-60 s (15 s)
T12 4-15 s	When blocking message is sent	NQ764T12	1-60 s (10 s)
T13 1 min	When initial blocking message is sent	NQ764T13	1-180 s (60 s)
T14 4-15 s	When unblocking message is sent	NQ764T14	1-60 s (10 s)
T15 1 min	When initial unblocking message is sent	NQ764T15	1-180 s (60 s)
T16 4-15 s	When reset circuit message is sent not due to the expiry of Timer T5	NQ764T16	1-60 s (10 s)
T17 1 min	When initial reset circuit message is sent	NQ764T17	1-180 s (60 s)
T18 4-15 s	When group blocking message is sent	NQ764T18	1-60 s (10 s)

Q.767/ISUP92 Timers for International use

(ISUP/Q.767) /Q.118	Cause of initiation	Table C7UPTMR timer	Range (default value)
T19 1 min	When initial group blocking message is sent	NQ764T18	1-180 s (60 s)
T20 4-15 s	When group unblocking message is sent	NQ764T20	1-60 s (10 s)
T21 1 min	When initial group unblocking message is sent	NQ764T21	1-180 s (60 s)
T22 4-15 s	When circuit group reset message is sent	NQ764T22	1-60 s (10 s)
T23 1 min	When initial circuit group reset message is sent	NQ764T23	1-180 s (60 s)
T24 < 2 s	When check tone is sent	NQ764T24	0.1-2.0 s (1 s)
T25 1-10 s	When initial continuity check failure is detected	NQ764T25	1-30 s (10 s)
T26 1-3 min	When second or subsequent continuity check failure is detected	NQ764T26	1-240 s (120 s)
T27 4 min	When continuity check failure indication is received	NQ764T27	1-300 s (240 s)
T28	Not used on the international interface		
T29 300-600 ms	Congestion indication received when T29 not running	Not implemented	
T30 5-10 s	Congestion indication received when T29 not running	Not implemented	
T31	Not used on the international interface		
T32	Not used on the international interface		
T33	Not used on the international interface		

Q.767/ISUP92 Timers for International use

(ISUP/Q.767) /Q.118	Cause of initiation	Table C7UPTMR timer	Range (default value)
T34	Not used on the international interface		
T35 15-20 s	At receipt of the latest digit and before the minimum or fixed number of digits have been received	NQ764T35	1-60 s (20 s)
T36 10-15 s	When transit or incoming international exchange receives continuity check request message	NQ764T8	1-60 s (15 s)

a. This timer is not used for answer timing. Instead field LCDDUR in table TRKGRP1 is used for answer timing purpose. The value of LCDDUR for terminating trunk provides the answer timing. The range of this field is 0-60, supporting up to 60 minutes. If the value is 0, then no answer timing is done on this switch and call continues.

Appendix D: Call Information (IAM message) for Gateway Calltypes

This Appendix describes the pertinent information in the ISUP IAM message as it pertains to the supported Gateway Calltypes:

- Direct Termination Outbound International
- Direct Termination Inbound National
- Transit Outbound International

Direct Termination Outbound International

The CS2000 would calltype the call as a international (IDDD) call and perform the following gateway functions on the outgoing call information (Initial Address message (IAM)):

- Called party number parameter (Refer ITU-T Recommendation Q.107)
 - set Nature of Address (NOA) to value of national significant number (0000011)
 - called number format (15-digit IDDD + F)(<true Country Code>+<NN>+F)
 - strip any international prefix ('011' for WZ1 format)
 - Strip the country code digits.
 - end-of-digit (#F) is suffixed to the called number
 - called number is delivered using enbloc format
- Calling party number parameter (if received in originating call informa-

- tion)
 - Nature of Address (NOA) would be set to International significant number (0000100)
 - Calling party number would be prefixed with the serving country code of CS2000 (per office basis) Note: maximum of 15-digit is supported.
 - existing CLI (ANI) delivery functionality is used to determine if calling party parameter is delivered.
- Calling party category (CPC) parameter
 - CPC value would be set to (00001010) 'ordinary calling subscriber' only if the CPC value has not been overridden by the CPCSCRN option and has a value associated with 'not used' values as defined in recommendation Q.767 section C.3.9. The 'not used' values are:
 - 00000000: calling party's category unknown at this time
 - 00001001: reserved (see Recommendation Q.104)
 - 11100000
 - to
 - 11111110: spare for national use
- Forward Call Indicator parameter
 - Bit A (National/international call indicator) would have been set to value of 0 'call to be treated as a national call'

Direct Termination Inbound National

For direct termination inbound national calls, the ISUP92/Q.767 gateway trunk agency would expect to receive the following call information (Initial Address message (IAM)) from the preceding foreign exchange:

- Called party number parameter
 - Nature of Address (NOA) would have been set to value of National significant number (0000011)
 - called number format (10-digit NN + F)
 - called number would contain WZ-1 national number (10-digit).
 - If end-of-digit (#F) is suffixed to the called number, CS2000 would strip end-of-digit prior to accessing table STDPRTCT.
 - For incomplete called number (called number not suffixed with end-of-digit ('F' digit)) Succession CS2000 waits for subsequent address message (SAM) until the Succession CS2000 receives either an end-of-digit or time-out occurs waiting for SAM prior to proceeding with translations.
- Calling party number parameter
 - Nature of Address (NOA) would have been set to International significant number
 - Calling party number would have been prefixed with the country code of the subscriber. Maximum of 15 digits are supported (based on 15-digit IDDD format). Most significant digits exceeding 15 digits is removed from the calling party number.

- If end-of-digit (#F) is suffixed to the calling party number, CS2000 would remove the end-of-digit.
- If an incomplete calling party number is received (calling party number incomplete indicator (NI) is 'incomplete', CS2000 would discard the calling party number.
- Calling party category (CPC) parameter
 - CPC value would have been set to (00001010) 'ordinary calling subscriber' depending on calltype (DDD, OA)
- Forward Call Indicator parameter
 - If Bit A has not been set to value of '0' (call to be treated as an national call), CS2000 would set Bit A to value of '0' (Recommendation Q.767 section C.3.20).

Transit Outbound International

For transit inbound international calls, the gateway trunk agency would have received the following initial call information (Initial Address message (IAM)) where the preceding foreign exchange would have performed the following function on the initial call information in the IAM:

- Called party number parameter
 - Nature of Address (NOA) would have been set to value of International significant number (0000100)
 - called number format (15-digit IDDD + F)
 - called number would contain WZ-1 national number (10-digit).
 - If end-of-digit (#F) is suffixed to the called number, CS2000 would strip end-of-digit prior to accessing table STDPRTCT.
 - For incomplete called number (called number not suffixed with end-of-digit ('F' digit)) Succession CS2000 waits for subsequent address message (SAM) until the Succession CS2000 receives either an end-of-digit or time-out occurs waiting for SAM prior to proceeding with translations.
- Calling party number parameter
 - Nature of Address (NOA) would have been set to International significant number
 - Calling party number would have been prefixed with the country code of the subscriber. Maximum of 15 digits are supported (based on 15-digit IDDD format).
 - If end-of-digit (#F) is suffixed to the calling party number, CS2000 would remove the end-of-digit.
 - If an incomplete calling party number is received (calling party number incomplete indicator (NI) is 'incomplete', CS2000 would discard the calling party number.
- Forward Call Indicator parameter
 - If Bit A has not been set to value of '1' (call to be treated as an international call), CS2000 would set Bit A to value of '1' (Recommendation

Q.767 section C.3.20).

The CS2000 would calltype the call as a international (IDDD) call and perform the following gateway functions on the outgoing call information (Initial Address message (IAM)):

- Called party number parameter (Refer Recommendation Q.107)
 - called number format (15-digit IDDD + F)
 - strip any international prefix based on the national dialing plan
 - Nature of Address (NOA) would have been set to value of International significant number (0000100)
 - called number would have been prefixed with proper country code by the subscriber
 - end-of-digit (#F) is suffixed to the called number
 - CS2000 delivers the called number in enbloc.
- Calling party number parameter (if delivered based ANI delivery functionality)
 - Nature of Address (NOA) is set to International significant number (0000100)
 - If call originated on Q.767/ISUP92 gateway trunk agent, Succession CS2000 assumes the country code has been prefixed on the calling party number by the preceding foreign exchange. If call originated on UCS agent, the OFC_SERVING_CC office parameter value is prefixed on the calling party number. Note: maximum of 15 digits is supported.
- Calling party category (CPC) parameter
 - CPC value would be set to (00001010)'ordinary calling subscriber' only if the CPC value has not been overridden by the CPCSCRN option and has a value associated with 'not used' values as defined in recommendation Q.767 section C.3.9. The 'not used' values are:
 - 00000000: calling party's category unknown at this time
 - 00001001: reserved (see ITU-T Recommendation Q.104)
 - 11100000
 - to
 - 11111110: spare for national use
- Forward Call Indicator parameter
 - If Bit A has not been set to value of '1' (call to be treated as an international call), CS2000 would set Bit A to value of '1' (Recommendation Q.767 section C.3.20).

Appendix E: Callflow diagram

The following figures illustrate the call flow for the gateway functionality. The shaded boxes indicate the functionality provided by this feature.

Gateway functionality call flows

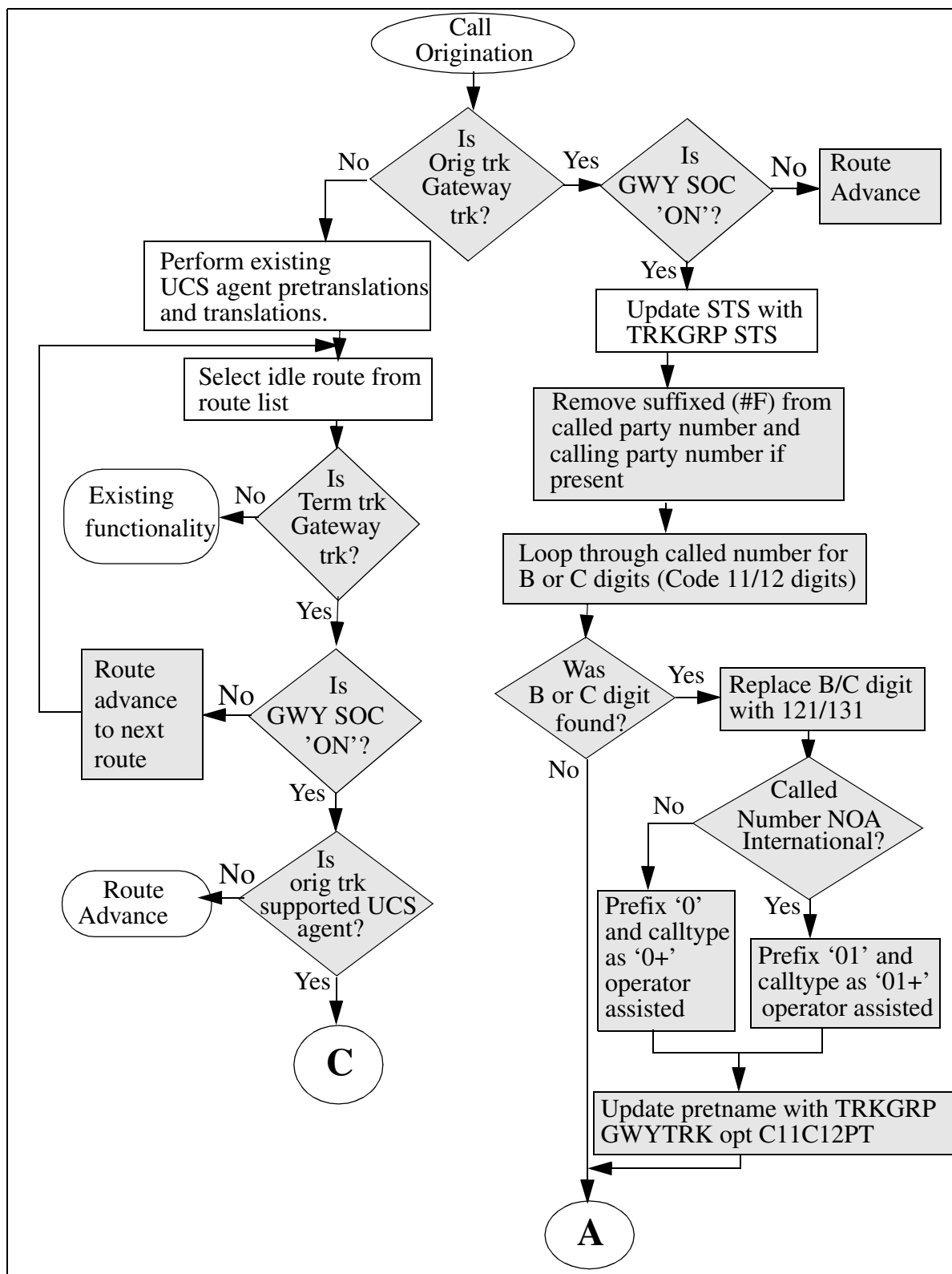


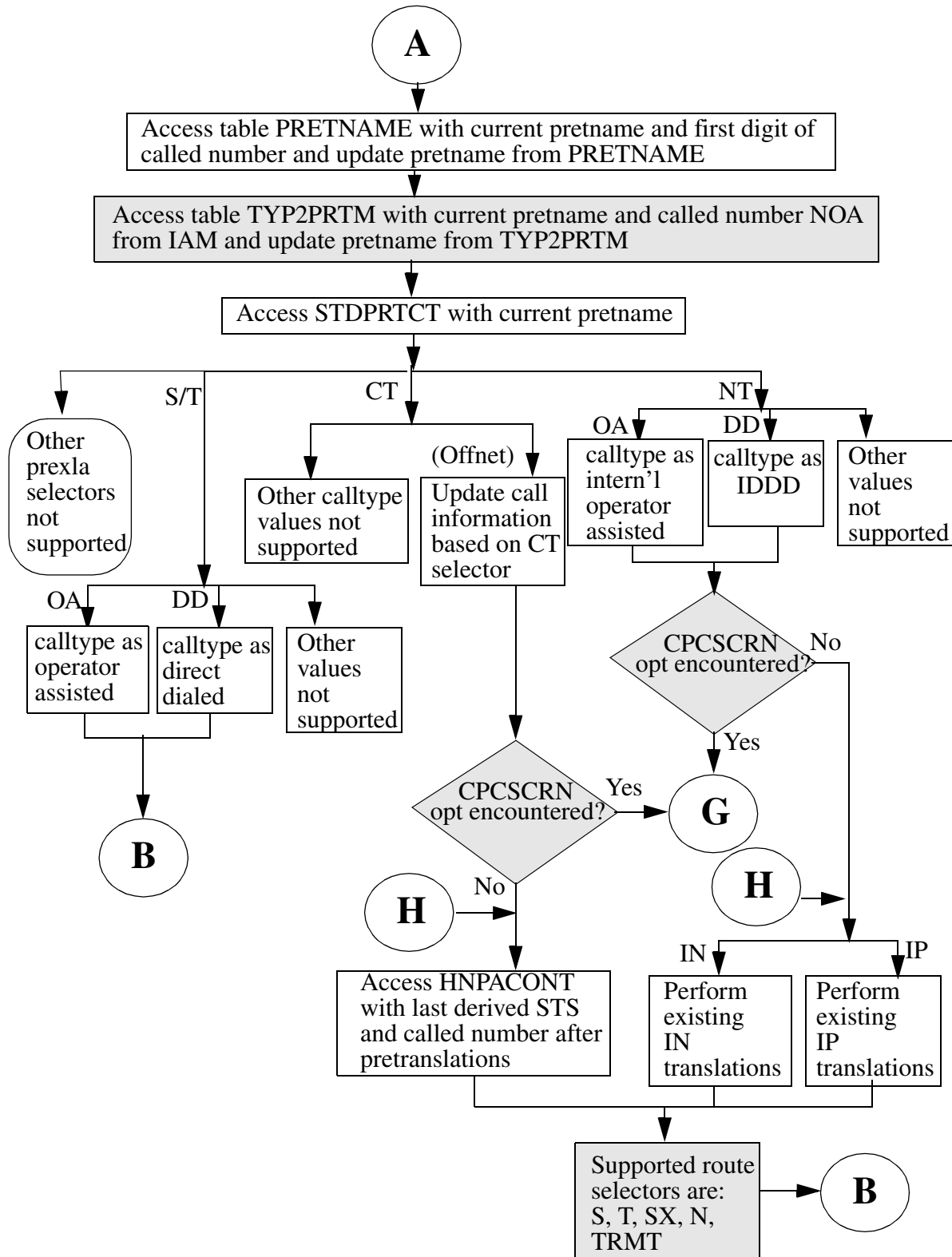
Figure 1 Gateway functionality call flows (continued)

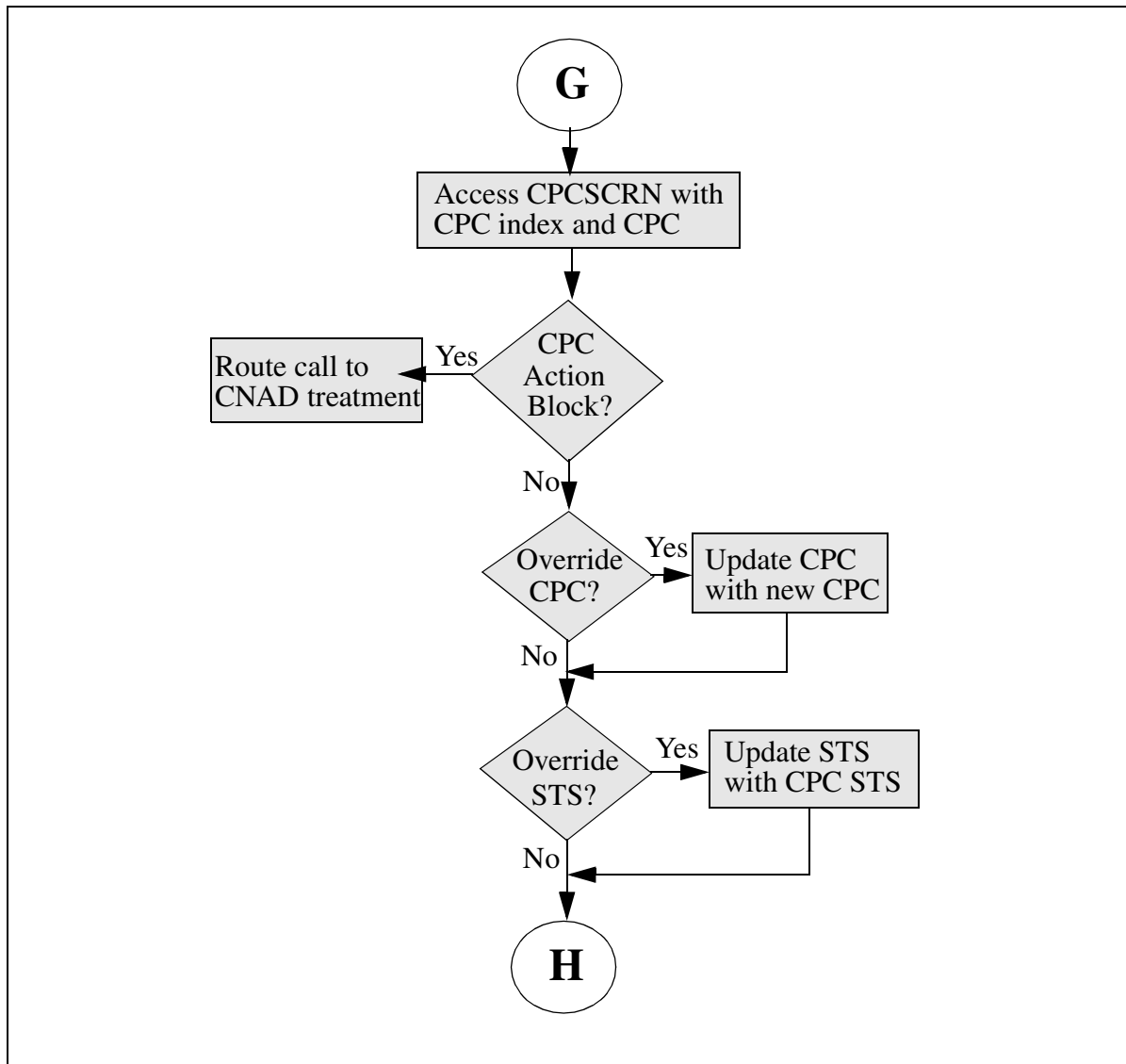
Figure 2 Gateway functionality call flows (continued)

Figure 3 Derive outpulsed number calltype

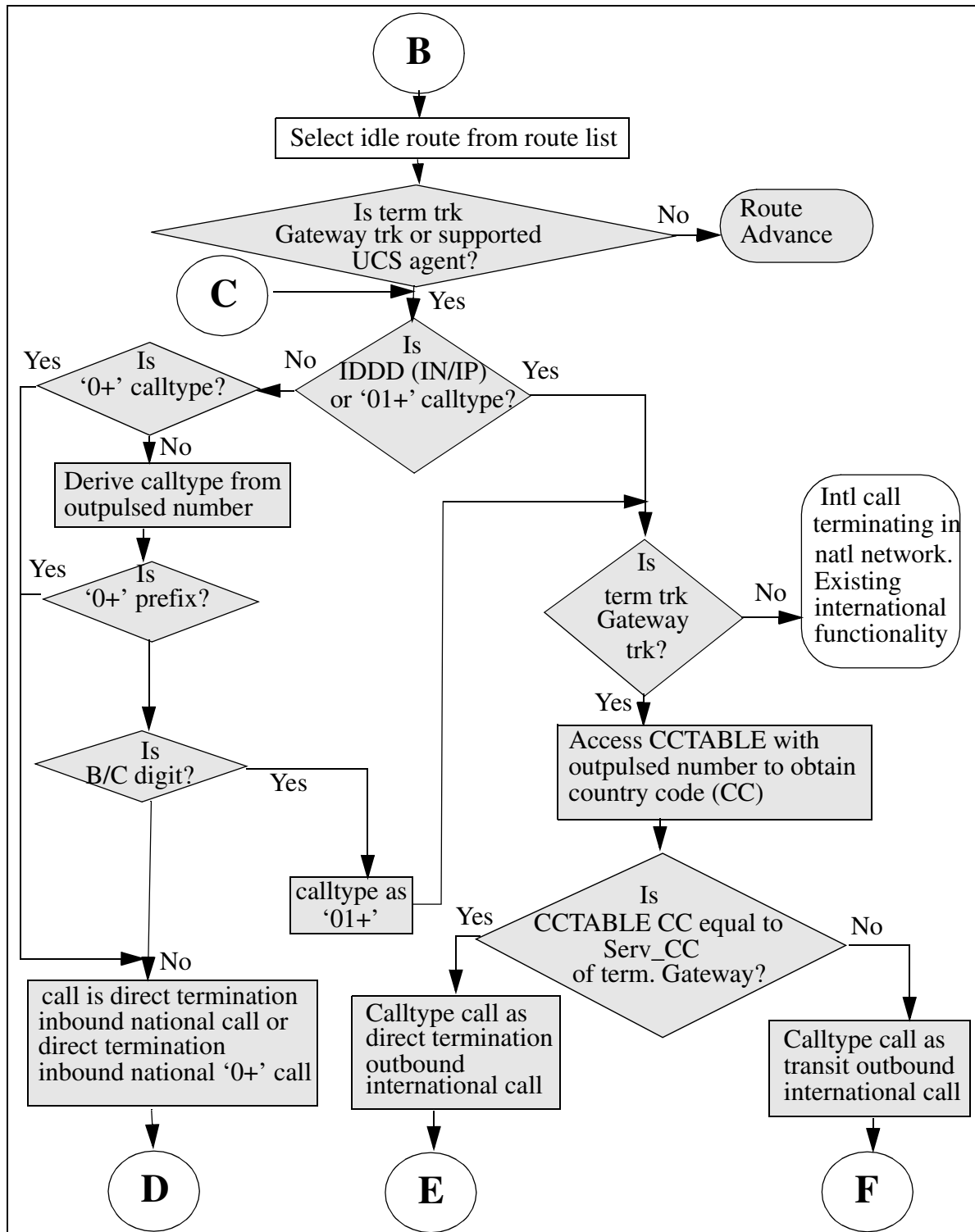


Figure 4 Gateway functionality call flows (Continued)

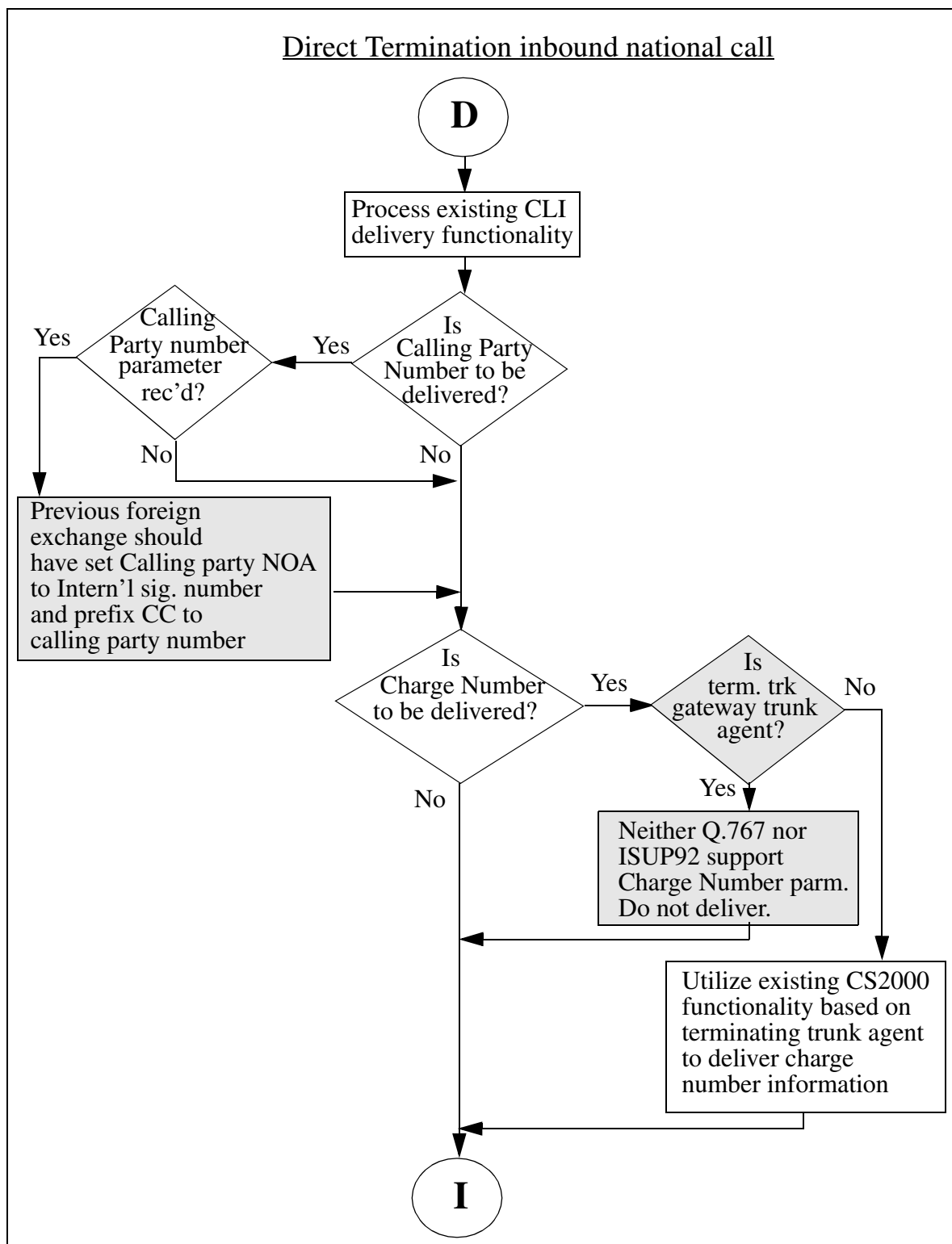


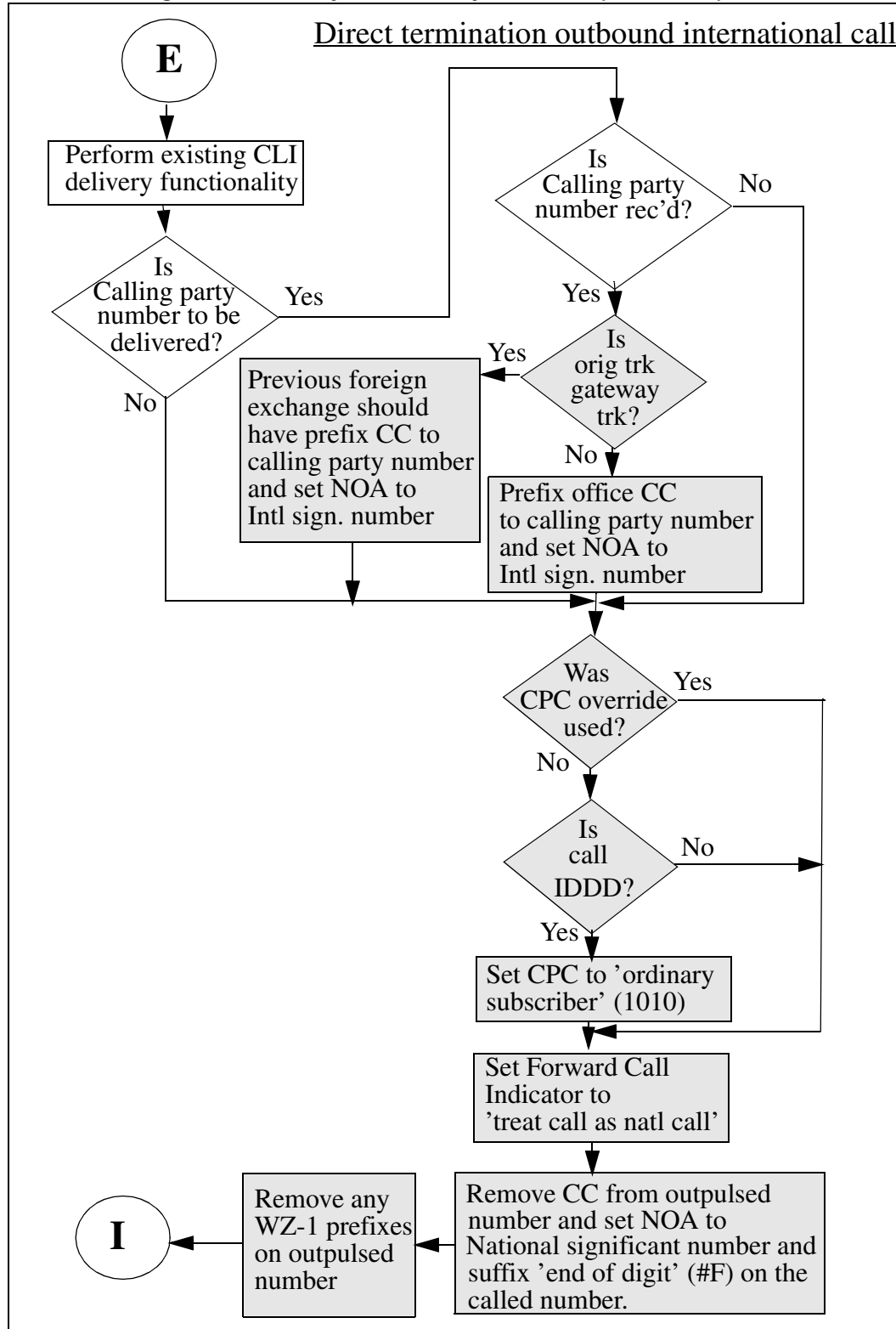
Figure 5 Gateway functionality call flows (Continued)

Figure 6 Gateway functionality call flows (Continued)

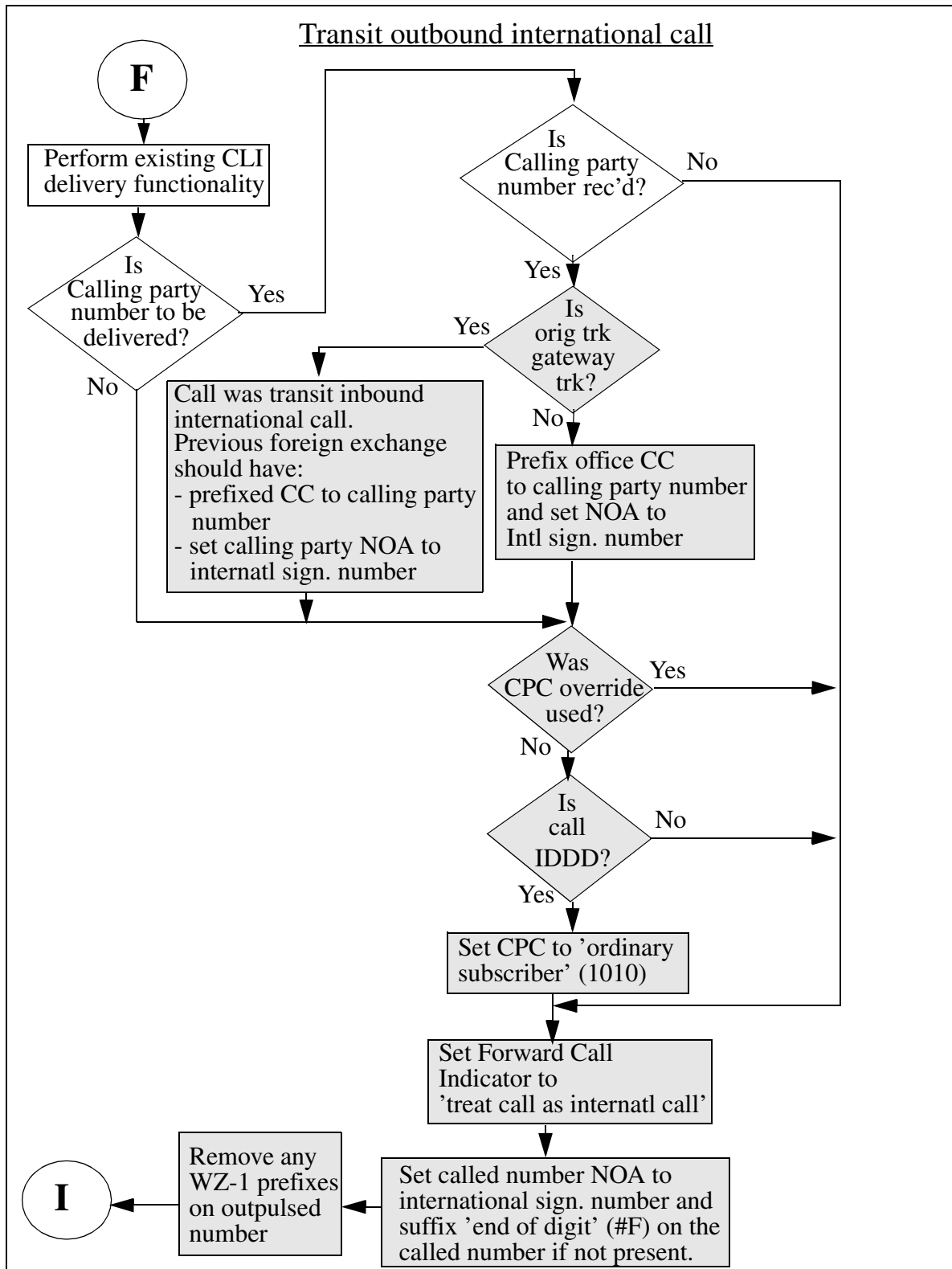
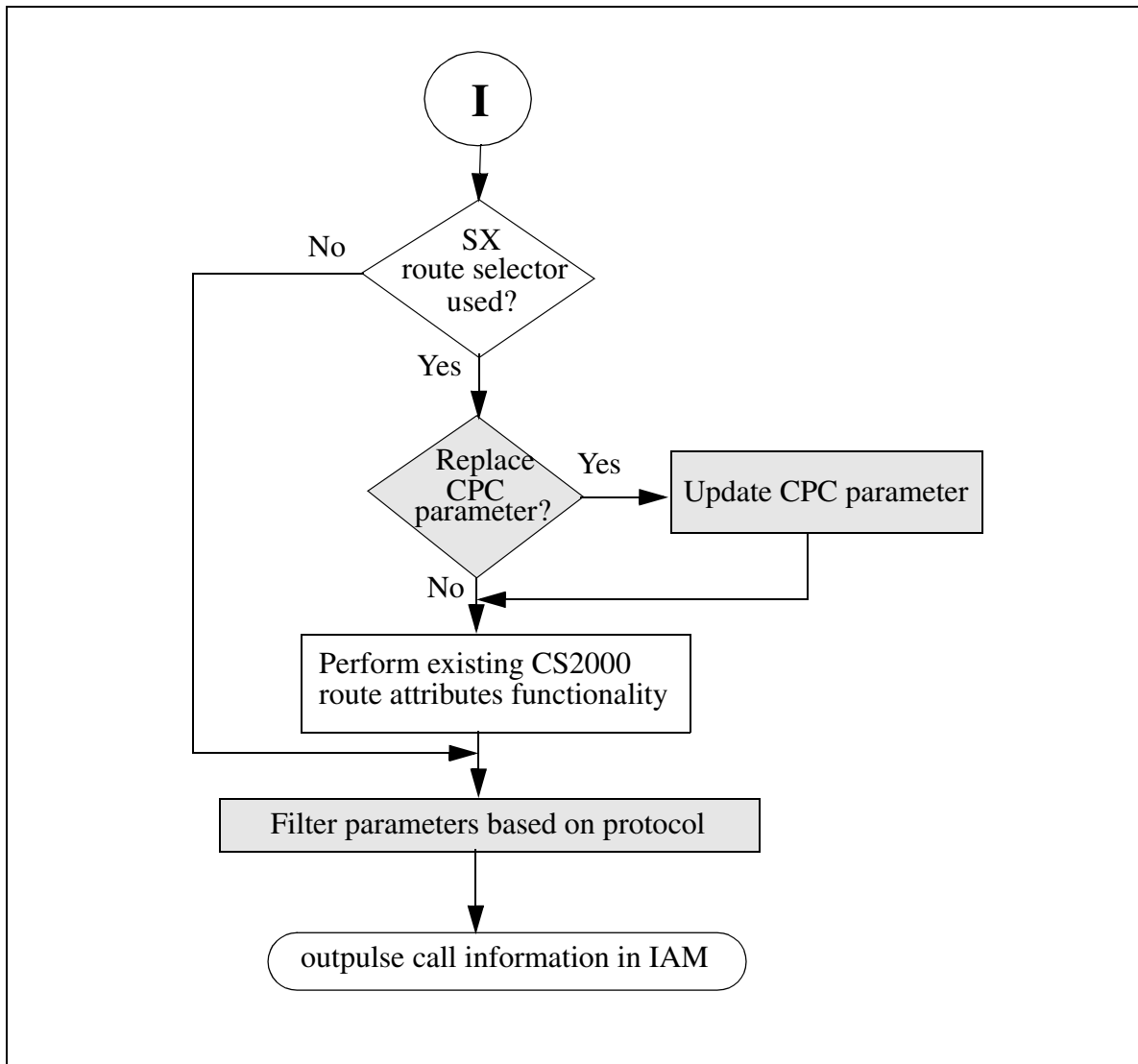


Figure 7 Gateway functionality call flows (Continued)

Appendix F: Datafill examples

This appendix describes example datafill for the different types of calls supported by this feature.

Direct Inbound National Call.

This is an example of a direct inbound national call where a foreign exchange routes a call destined for US to a CS2000 in WZ-1. The CS2000 calltypes the call as a national call and routes the call to a US national trunk agency as a direct inbound national call.

Originating Trunk: Gateway Trunk

IAM msg:

NOA= National (3)

Called Number = 2142221234F

CPC=0

FCI bit A = 0 (National)

TABLE: TRKGRP

GWYTRK1 IMT 40 NPDGP NCIM 0 2W **GWY** MIDL 16 7 16 16
UCSGWAY NIL C N NONE 4 ALWAYS ADDR 286 0 GLOBAL N N N
VOICE_DATA MANUAL 4 160 214 0 (**GWYTRK 772 IMT**) \$

TABLE: TRKSGRP

GITU1E1AN01 0 DS1SIG C7UP 2W N Y UNEQ ACTIVEA **CCITT** THRH
0 DMSNODE Y Y **V1 BLUE** \$ NIL CIC

TABLE: TYP2PRTM

GWY NATL GWY

TABLE: PARTOSTS

00 286 786

TABLE: STDPRTCT²¹

GWY (1) (0)

subtable STDPRT

2142221234 21 CT OFFNET 7 10 0 \$

TABLE: HNPACONT

786 Y 999 10 (2) (1) (0)

subtable HNPACODE

214 214 HNPA 0

222 222 LRTE 222

subtable RTEREF

222 (\$ D UCS_Agency) \$

Since the terminator is a existing agent (national agent) the call is calltyped as a direct inbound national call.

If terminating UCS_Agency is an SS7 trunk (INTER/INTRA IMT, SS7 FG D) etc., Outgoing IAM is as follows.

IAM msg:

NOA= National (3)

Outpulsed Number = 2142221234

21. 'F' is removed from the Called Number prior to entering table STDPRTCT.

CPC=0

FCI bit A = 0 (National)

Transit Inbound International Call.

This is an example of a transit inbound international call where a foreign exchange is routing a call destined for Panama (country code of '507') to a CS2000 in WZ-1. The CS2000 routes the call to a foreign exchange in Mexico as a transit outbound international call.

Originating Trunk: Gateway Trunk

IAM msg:

Called number NOA = International (4)

Called Number = 507+7242212345+F

CPC=0

FCI bit A = 1 (International)

TABLE: TRKGRP

GWYTRK1 IMT 40 NPDGP NCIM 0 2W **GWY** MIDL 16 7 16 16
UCSGWAY NIL C N NONE 4 ALWAYS ADDR 286 0 GLOBAL N N N
VOICE_DATA MANUAL 4 160 214 0 (**GWYTRK 772 IMT**) \$

TABLE: TRKSGRP

GITU1E1AN01 0 DS1SIG C7UP 2W N Y UNEQ ACTIVEA **CCITT** THRH
0 DMSNODE Y Y **V1 BLUE** \$ NIL CIC

TABLE: TYP2PRTM

GWY INTL GWY

TABLE: PARTOSTS

00 286 786

TABLE: STDPRTCT²²

GWY (1) (0)

subtable STDPRT

5077242212345 508 NT DD 3 IP (CPCSCRN 1)\$

TABLE: CPCSCRN

CPCINDEX	CPC	ACTION	OVRDSTS	STS
1	UNKNOWN	ACTION_C ONTINUE	Y	611

- Table CPCSCRN was accessed with the CPCINDEX value from table STDPRTCT, CPCSCRN option and the calling party category (CPC) value of '0' (UNKNOWN) from the IAM.

- The corresponding tuple is to take the action of 'ACTION_CONTINUE' and override the STS with '611'.

TABLE: STS2CCDB

786 UCS786

TABLE: CTCODE

UCS786 7724 7724 RTE (PF 0) (MM 7 15) (DEST 724) \$

TABLE: CTRTE

22. 'F' is removed from the Called Number prior to entering table STDPRTCT.

UCS786 724 (SX GWYTRK2 CPC_OVRD²³) \$

TABLE CCTABLE

5070 5079 507

TABLE: RTEATTR

KEY	INCLUDE	EXCLUDE	REPLACE	OPTION
CPC_OVRD	\$	\$	(CPC SUBSCRIBER1)	\$

TABLE: TRKGRP

GWYTRK2²⁴ IMT 40 NPDGP NCIM 0 2W GIMT MIDL 16 7 16 16
 UCSGWAY NIL C N NONE 4 ALWAYS ADDR 286 0 GLOBAL N N N
 VOICE_DATA MANUAL 4 160 214 0 (**GWYTRK 52 IMT**) \$

TABLE: TRKSGRP

GWYTRK2 0 DS1SIG C7UP 2W N Y UNEQ ACTIVEA **CCITT** THRH 0
 DMSNODE Y Y **V1 ISUP92** \$ NIL CIC

TABLE: OFCVAR

OFC_SERVING_CC 001

Outpulsed IAM:

- Since GWYTRK2 serving country code (SERV-CC) is not equal to the called number country code ('507'), the call is calltyped as a transit outbound international call. The call is being routed to a trunk to a foreign exchange in Mexico (country code '52') as a transit call to Panama (country code '507').

23. CPC_OVRD is an index into table RTEATTR.

24. It is an ISUP92 gateway trunk

called number = 507+7242212345+F

Called number NOA is set to International significant number due to calltype of transit outbound international call.

CPC = 10 Ordinary Subscriber (via table RTEATTR)

Direct Outbound International Call.

This is an example of direct outbound international call where an international call destined for Mexico (country code '52') originated from US national network and is routed to the CS2000. The CS2000 calltypes the call as a international call and routes the call to a gateway trunk which connects to a foreign exchange in Mexico as a direct outbound international call.

Originating Trunk: Any Supported UCS Agency. (SS7 IMT for this example)

Called Party Number = 011+52+8775221234

If Originating Trunk is an SS7 trunk then IAM contains

Called Party Number NOA= International (4)

Calling Party Number = 2146112211

Calling Party Number NOA= National (3)

CPC = UNKNOWN

TABLE: TRKGRP

```
IMTTRK1 IMT 40 NPDGP NCIT 0 2W IMT MIDL 16 7 16 16 NILIDX NIL
S N NONE 4 ALWAYS ADDR 111 0 INTER N VOICE_DATA NONE 4 160
214 0 $
```

TABLE: STDPRTCT

IMT (1) (0)

subtable STDPRT

011528775221234 011528775221234 NT DD 3 IN \$

TABLE: CCTR

8775221234 T 711 3 15 T OFRT 101 Y

TABLE CCTABLE

52 52 52

TABLE OFRT:

101 (SX GWYTRK1 CPC_OVRD)

TABLE: RTEATTR

KEY	INCLUDE	EXCLUDE	REPLACE	OPTION
CPC_OVRD	\$	\$	(CPC SUBSCRIBER1)	\$

TABLE: OFCVAR

OFC_SERVING_CC 001

TABLE: TRKGRP

GWYTRK2²⁵ IMT 40 NPDGP NCIM 0 2W GIMT MIDL 16 7 16 16
UCSGWAY NIL C N NONE 4 ALWAYS ADDR 286 0 GLOBAL N N N
VOICE_DATA MANUAL 4 160 214 0 (**GWYTRK 52 IMT**) \$

Note: Since Terminating trunk is a Gateway trunk with the same country code as given by table CCTABLE, this is Direct Termination Outbound call.

Outpulse IAM:

called number = 8775221234+F

25. It is an ISUP92 gateway trunk

Called number NOA = National²⁶ (3).

Calling Party Number = 1+2146112211 (Country Code from table OFCVAR is prefixed)

Calling Party Number NOA = International²⁷ (4).

CPC = SUBSCRIBER1 (via Table RTEATTR)

Transit Outbound International Call.

This is an example of a transit outbound international call where a international call destined for Panama (country code '507') originated from US national network and is routed to the CS2000 in WZ-1. The CS2000 calltypes the call as an international call and routes the call to a gateway trunk which connects to a foreign exchange in Mexico as a transit outbound international call.

Originating Trunk: Any Supported UCS Agency. (FGB for this example)

Called Party Number = 011+507+7242212345

Calling Party Number = 2146112211

CPC = SUBSCRIBER1 (Default value)

TABLE: TRKGRP

```
ONTTRK1 ONAT 50 NPDGP NCOF 0 2W ONT MIDL 16 7 16 16 7 7 OT 7
0 214 S 7 FGBC 111 MANUAL 214 0 NOAUTHS NONE 0 Y 1 NONE 00
IMMEDIATE VOICE_DATA 160 $
```

TABLE: PARTOSTS

```
00 111 611
```

TABLE: STDPRTCT

```
ONT (1) (0)
```

```
subtable STDPRT
```

```
0115077242212345 0115077242212345 NT DD 3 IP $
```

26. NOA is set to national significant number since the call is direct termination outbound call.

27. NOA is set to international significant number due to the calltype of direct terminating outbound call and the originator is a UCS national agent

TABLE: STS2CCDB

611 UCS611

TABLE: CTCODE

UCS611 5077 5077 RTE (PF 0) (MM 7 15) (DEST 722) \$

TABLE: CTRTE

UCS611 722 (S D GWYTRK2) \$

TABLE CCTABLE

5070 5079 507

TABLE: OFCVAR

OFC_SERVING_CC 001

TABLE: TRKGRP

GWYTRK2 IMT 40 NPDGP NCIM 0 2W GIMT MIDL 16 7 16 16
UCSGWAY NIL C N NONE 4 ALWAYS ADDR 286 0 GLOBAL N N N
VOICE_DATA MANUAL 4 160 214 0 (**GWYTRK 52 IMT**) \$

Note: Since Terminating trunk is a Gateway trunk with the different country code as given by table CCTABLE, this is Transit Outbound International call.

TABLE: TRKSGRP

GWYTRK2 0 DS1SIG C7UP 2W N Y UNEQ ACTIVEA **CCITT** THRH 0
DMSNODE Y Y **V1 ISUP92** \$ NIL CIC

TABLE: OFCVAR

OFC_SERVING_CC 001

Outpulsed IAM:

Since GWYTRK2 serving country code (SERV_CC) is not equal to the called number country code ('507'), the call is calltyped as a transit outbound international call. The call is being routed to a trunk to a foreign exchange in Mexico (country code of '52') as a transit call to Panama (country code '507').

called number = 507+7242212345+F

Called number NOA = International²⁸ (4).

Calling Party Number = 1+2146112211 (Since the originator is a UCS national agent, Country Code from table OFCVAR is prefixed)

Calling Party Number NOA = International²⁹ (4).

CPC = SUBSCRIBER1

Inbound National OA Calls (Direct)

This is an example of a direct inbound national OA call where a foreign exchange routes a call destined for US to a CS2000 in WZ-1. The CS2000 calltypes the call as a national OA call and routes the call to a US national trunk agency as a direct inbound national OA call.

Originating Trunk: Gateway Trunk

IAM msg:

NOA= National (3)

Called Number = 2142221234F

CPC=0

FCI bit A = 0 (National)

TABLE: TRKGRP

```
GWYTRK1 IMT 40 NPDGP NCIM 0 2W GWY MIDL 16 7 16 16
UCSGWAY NIL C N NONE 4 ALWAYS ADDR 286 0 GLOBAL N N N
VOICE_DATA MANUAL 4 160 214 0 (GWYTRK 772 IMT) $
```

28. NOA is set to international significant number due to calltype of transit outbound international call.

29. NOA is set to international significant number due to calltype of transit outbound international call and the originator is a UCS national agent.

TABLE: TRKSGRP

GITU1E1AN01 0 DS1SIG C7UP 2W N Y UNEQ ACTIVEA **CCITT** THRH
0 DMSNODE Y Y **V1 BLUE** \$ NIL CIC

TABLE: TYP2PRTM

GWY NATL GWY

TABLE: STDPRTCT³⁰

GWY (1) (0)

subtable STDPRT

2142221234 21 T OA 0 OFRT 741 8 11 NONE

TABLE: OFRT

237 (SX IMT741C7DR12 ENG_OP)

TABLE: RTEATTR

ENG_OP \$ \$ (CPC OP_ENGLISH)

Since the terminator is a existing agent (national agent) the call is calltyped as a direct inbound national OA call.

If terminating UCS_Agency is an SS7 trunk (INTER/INTRA IMT, SS7 FG D) etc., Outgoing IAM is as follows.

IAM msg:

NOA= National (3)

30. 'F' is removed from the Called Number prior to entering table STDPRTCT.

Outpulsed Number = 2142221234

CPC=2 (op_english)

FCI bit A = 0 (National)

Direct Outbound International OA Call

This is an example of direct outbound international OA call where an international OA call destined for Mexico (country code '52') originated from US national network and is routed to the CS2000. The CS2000 calltypes the call as a international OA call and routes the call to a gateway trunk which connects to a foreign exchange in Mexico as a direct outbound international OA call.

Originating Trunk: Any Supported UCS Agency. (SS7 IMT for this example)

Called Party Number = 011+52+8775221234

If Originating Trunk is an SS7 trunk then IAM contains

Called Party Number NOA= International (4)

Calling Party Number = 2146112211

Calling Party Number NOA= National (3)

CPC = UNKNOWN

TABLE: TRKGRP

IMTTRK1 IMT 40 NPDGP NCIT 0 2W IMT MIDL 16 7 16 16 NILIDX NIL
S N NONE 4 ALWAYS ADDR 111 0 INTER N VOICE_DATA NONE 4 160
214 0 \$

TABLE: PARTOSTS

00 111 611

TABLE: STS2CCDB

611 UCS611

TABLE: STDPRTCT

IMT (1) (0)

subtable STDPRT

011528775221234 011528775221234 NT OA 3 IP (CPCSCRN
OP_SPANISH) \$

TABLE CCTABLE

52 52 52

TABLE CTCODE

UCS611 528 528 RTE (PF 0) (MM 7 15) (DEST 528) \$

TABLE CTRTE

UCS611 528 (S D GWYTRK2) \$

TABLE: OFCVAR

OFC_SERVING_CC 001

TABLE: TRKGRP

GWYTRK2³¹ IMT 40 NPDGP NCIM 0 2W GIMT MIDL 16 7 16 16
 UCSGWAY NIL C N NONE 4 ALWAYS ADDR 286 0 GLOBAL N N N
 VOICE_DATA MANUAL 4 160 214 0 (**GWYTRK 52 IMT**) \$

Note: Since Terminating trunk is a Gateway trunk with the same country code as given by table CCTABLE, this is Direct Termination Outbound OA call.

Outpulse IAM:

called number = 8775221234+F

Called number NOA = National³² (3).

Calling Party Number = 1+2146112211 (Country Code from table OFCVAR is prefixed)

Calling Party Number NOA = International³³ (4).

CPC = OP_SPANISH (via Table STDPRTCT CPCSCRN option)

Transit Outbound International OA call

This is an example of a transit outbound international OA call where a international OA call destined for Panama (country code '507') originated from US national network and is routed to the CS2000 in WZ-1. The CS2000 calltypes the call as an international OA call and routes the call to a gateway trunk which connects to a foreign exchange in Mexico as a transit outbound international OA call.

Originating Trunk: Any Supported UCS Agency. (FGB for this example)

Called Party Number = 011+507+7242212345

Calling Party Number = 2146112211

CPC = SUBSCRIBER1 (Default value)

TABLE: TRKGRP

31. It is an ISUP92 gateway trunk

32. NOA is set to national significant number since the call is direct termination outbound call.

33. NOA is set to international significant number due to the calltype of direct terminating outbound call and the originator is a UCS national agent

ONTTRK1 ONAT 50 NPDGP NCOF 0 2W ONT MIDL 16 7 16 16 7 7 OT 7
0 214 S 7 FGBC 111 MANUAL 214 0 NOAUTHS NONE 0 Y 1 NONE 00
IMMEDIATE VOICE_DATA 160 \$

TABLE: PARTOSTS

00 111 611

TABLE: STDPRTCT

ONT (1) (0)

subtable STDPRT

0115077242212345 0115077242212345 NT OA 3 IP (CPCSCRN
OP_SPANISH) \$

TABLE: STS2CCDB

611 UCS611

TABLE: CTCODE

UCS611 5077 5077 RTE (PF 0) (MM 7 15) (DEST 722) \$

TABLE: CTRTE

UCS611 722 (S D GWYTRK2) \$

TABLE CCTABLE

5070 5079 507

TABLE: OFCVAR

OFC_SERVING_CC 001

TABLE: TRKGRP

GWYTRK2 IMT 40 NPDGP NCIM 0 2W GIMT MIDL 16 7 16 16
UCSGWAY NIL C N NONE 4 ALWAYS ADDR 286 0 GLOBAL N N N
VOICE_DATA MANUAL 4 160 214 0 (**GWYTRK 52 IMT**) \$

Note: Since Terminating trunk is a Gateway trunk with the different country code as given by table CCTABLE, this is Transit Outbound International call.

TABLE: TRKSGRP

GWYTRK2 0 DS1SIG C7UP 2W N Y UNEQ ACTIVEA **CCITT** THRH 0
DMSNODE Y Y **V1 ISUP92** \$ NIL CIC

TABLE: OFCVAR

OFC_SERVING_CC 001

Outpulsed IAM:

Since GWYTRK2 serving country code (SERV_CC) is not equal to the called number country code ('507'), the call is calltyped as a transit outbound international call. The call is being routed to a trunk to a foreign exchange in Mexico (country code of '52') as a transit call to Panama (country code '507').

called number = 507+7242212345+F

Called number NOA = International³⁴ (4).

Calling Party Number = 1+2146112211 (Since the originator is a UCS national agent, Country Code from table OFCVAR is prefixed)

Calling Party Number NOA = International³⁵ (4).

CPC = OP_SPANISH (via Table STDPRTCT - CPCSCRN option)

34. NOA is set to international significant number due to calltype of transit outbound international call.

35. NOA is set to international significant number due to calltype of transit outbound international call and the originator is a UCS national agent.

Transit Outbound Code 11/12 International

This is an example of a transit outbound international code 11/12 call where a international code 11/12 call destined for Panama (country code '507') originated from US national network and is routed to the CS2000 in WZ-1. The CS2000 calltypes the call as an international code 11/12 call and routes the call to a gateway trunk which connects to a foreign exchange in Mexico as a transit outbound international code 11/12 call.

Originating Trunk: Any Supported UCS Agency. (FGB for this example)

Called Party Number = 01+507+1212212345

Calling Party Number = 2146112211

CPC = SUBSCRIBER1 (Default value)

TABLE: TRKGRP

ONTTRK1 ONAT 50 NPDGP NCOF 0 2W ONT MIDL 16 7 16 16 7 7 OT 7
0 214 S 7 FGBC 111 MANUAL 214 0 NOAUTHS NONE 0 Y 1 NONE 00
IMMEDIATE VOICE_DATA 160 \$

TABLE: PARTOSTS

00 111 611

TABLE: STDPRTCT

ONT (1) (0)

subtable STDPRT

015071212212345 015071212212345 NT OA 2 IP (CPCSCRN
OP_SPANISH) \$

TABLE: STS2CCDB

611 UCS611

TABLE: CTCODE

UCS611 507 507 RTE (PF 0) (MM 7 15) (DEST 722) \$

TABLE: CTRTE

UCS611 722 (T OFRT 204) \$

TABLE: OFRT

204 (N D GWYTRK2 6 507B N) \$ \$

(Note that this is merely example datafill. There are other methods to appropriately manipulate the number to be outpulsed.)

TABLE CCTABLE

507 507 507

TABLE: OFCVAR

OFC_SERVING_CC 001

TABLE: TRKGRP

GWYTRK2 IMT 40 NPDGP NCIM 0 2W GIMT MIDL 16 7 16 16
UCSGWAY NIL C N NONE 4 ALWAYS ADDR 286 0 GLOBAL N N N
VOICE_DATA MANUAL 4 160 214 0 (**GWYTRK 52 IMT**) \$

Note: Since Terminating trunk is a Gateway trunk with the different country code as given by table CCTABLE, this is Transit Outbound International call.

TABLE: TRKSGRP

GWYTRK2 0 DS1SIG C7UP 2W N Y UNEQ ACTIVEA **CCITT** THRH 0
DMSNODE Y Y **V1 ISUP92** \$ NIL CIC

TABLE: OFCVAR

OFC_SERVING_CC 001

Outpulsed IAM:

Since GWYTRK2 serving country code (SERV_CC) is not equal to the called number country code ('507'), the call is calltyped as a transit outbound international call. The call is being routed to a trunk to a foreign exchange in Mexico (country code of '52') as a transit call to Panama (country code '507').

called number = 507+B2212345+F

Called number NOA = International³⁶ (4).

Calling Party Number = 1+2146112211 (Since the originator is a UCS national agent, Country Code from table OFCVAR is prefixed)

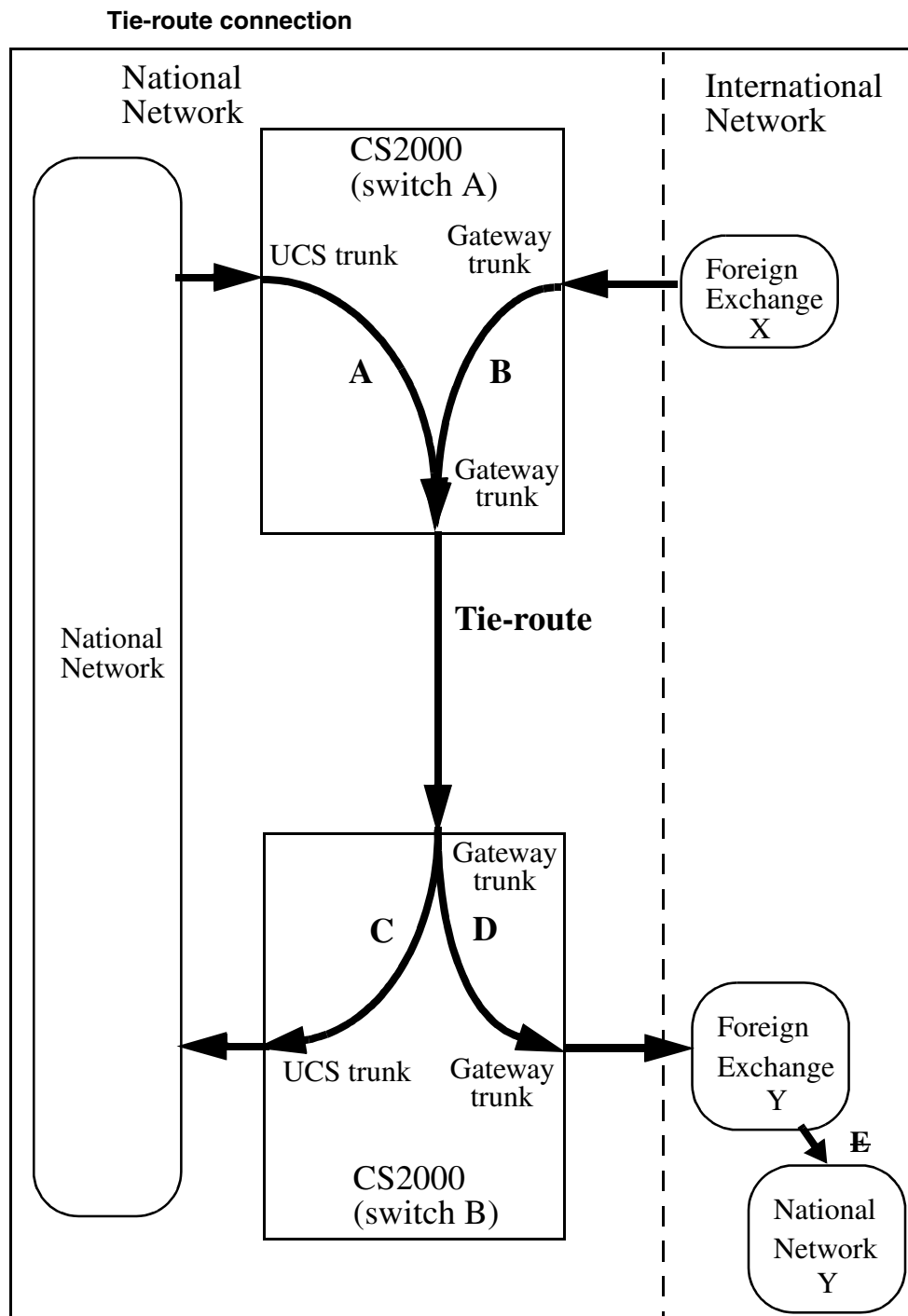
Calling Party Number NOA = International³⁷ (4).

CPC = OP_SPANISH (via Table STDPRTCT - CPCSCRN option)

36. NOA is set to international significant number due to calltype of transit outbound international call.

37. NOA is set to international significant number due to calltype of transit outbound international call and the originator is a UCS national agent.

Appendix G: Tie-route Connection Example



Direct termination inbound national calls:

In the preceding figure, connection B to connection C illustrates direct termination inbound national calls over a tie-route connection. In this case, the call is routed as a national call on switch A and switch B.

Example:

A carrier has two gateway switches (CS2000 with gateway functionality): one on the east coast of the country and one on the west coast of the country. A foreign exchange routes a direct termination inbound national call to the east coast gateway switch but the call destination is on the west coast of the country. The gateway switch on the east coast would route the call as a national call over the gateway trunk agency (tie-route connection). The gateway switch on the west coast would then route the call as a national call to the supported trunk agency which accesses the national network on the west coast.

In the preceding figure, connection A to connection C illustrates direct termination inbound national calls over a tie-route connection. In this case, the call is routed as a national call on switch A and switch B.

Example:

A carrier has two gateway switches (CS2000 with gateway functionality): one in country X in WZ-1 and another in country Y in WZ-1 where country Y requires all international traffic to go through a gateway switch. A subscriber in country X dials a 1+national number, the gateway switch translates the call as a national call and routes the call over the tie-route connection (gateway trunk agency).

The gateway switch in country Y would treat the call as a direct termination inbound national call since the call originated on a gateway trunk agency and the calltype is a national call. Based on translations, the call would be routed to a CS2000 trunk agent that accesses the national network in country Y.

Direct termination outbound international calls:

In the preceding figure, connection A to connection C illustrates direct termination outbound international call over a tie-route connection. In this case, the call is routed as an direct termination outbound international call on switch A and a direct termination inbound national call on switch B.

Example:

A carrier has two gateway switches (CS2000 with gateway functionality):

one in country X in WZ-1 and another in country Y in WZ-1 where country Y requires all international traffic to go through a gateway switch. A subscriber in country X dials a 011+country code ('1')+national number, the gateway switch translates the call as an international call and routes the call over the tie-route connection (gateway trunk agency). The gateway switch in country Y would treat the call as a direct termination inbound national call since the call originated on a gateway trunk agency and the calltype is a national call. Based on translations, the call would be routed to a CS2000 trunk agent that accesses the national network in country Y.

In the preceding figure, connection A to connection D illustrates direct termination outbound international call over a tie-route connection. In this case, the call is routed as an direct termination outbound international call on switch A and on switch B.

Example:

A carrier has two gateway switches (CS2000 with gateway functionality): one in country A in WZ-1 and another in country B in WZ-1 where country B requires all international traffic to go through a gateway switch to access the national network. A subscriber in country B dials a 011+country code for country Y+national number, the gateway switch (switch A) translates the call as an direct termination outbound international call since the country code of the called number is EQUAL to the serving country code of the gateway trunk agency and routes the call over the tie-route connection.

The gateway switch in country B would translate the call as an international call and treat the call as a direct termination outbound international call since the country code of the called number is EQUAL to the serving country code of the gateway trunk agency. The gateway trunk agency would interconnect to the gateway switch in the destination country (country Y).

Transit outbound international calls:

In the preceding figure, connection B to connection D illustrates transit outbound international call over a tie-route connection. In this case, the call is routed as an transit outbound international call on switch A and on switch B.

Example:

A carrier has two gateway switches (CS2000 with gateway functionality): one on the east coast of the country and one on the west coast of the country. A foreign exchange routes a transit inbound international call to the

east coast gateway switch but the call destination is a country that is connected to the gateway switch on the west coast of the country. The gateway switch on the east coast would route the call as an international call over the gateway trunk agency (tie-route connection).

The east coast gateway switch would treat this call as a transit outbound international call since the call is terminating to a gateway trunk agency and the destination country code prefix on called number is NOT EQUAL to the serving country code of the gateway trunk agency (country code of '1' since it resides in WZ-1).

The gateway switch on the west coast would then route the call as an international call to a gateway trunk agency that connects to the transit foreign exchange or could route the call as an international call to a gateway trunk agency that has a direct termination to the destination country (direct termination outbound international call).

In the preceding figure, connection A to connection D illustrates transit outbound international call over a tie-route connection. In this case, the call is routed as an transit outbound international call on both switch A and switch B.

Example:

A carrier has two gateway switches (CS2000 with gateway functionality): one in country A in WZ-1 and another in country B in WZ-1 where country B has the connection to a transit foreign exchange. A subscriber in country A dials a 011+country code for country X+national number, the gateway switch (switch A) translates the call as an transit outbound international call since the country code of the called number is NOT EQUAL to the serving country code of the gateway trunk agency (country code of '1' since country B is in WZ-1) and routes the call over the tie-route connection.

The gateway switch in country B would translate the call as an international call and treat the call as a transit outbound international call since the country code of the called number is NOT EQUAL to the serving country code of the gateway trunk agency. The gateway trunk agency would interconnect to a foreign exchange in country Y which has a direct connection to country X.

Appendix H: Test Call

This feature ensures that testcalls originated from any of the following test facilities:

- TTP - MAP level (Manual tests)

- ATT - MAP level (Automatic tests)

for performing tests on Q767 and ISUP92 Gateway trunks, these are terminated on the specified testlines.

Testlines that are supported by this feature are T100, T101³⁸, T102.

Origination of Testcall

This feature utilizes TST & OP commands available at MAP level and ATT for supporting origination of test calls on UCS agenda and ISUP92/Q.767.

IAM Message Generation:

The IAM message transmitted from the originating, near end switch to the terminating, far end switch is formatted as a test call IAM. The test call IAM is sent over the ISUP IMT trunks that has to be tested.

The test call IAM contains the following parameters:

- Nature of Connection Indicator
 - the Satellite Indicator field for test calls depends on TRKSGRP datafill in the same way as for non-test calls
 - the Continuity Check Indicator field for test calls contains the Continuity Check Not Required code ('00') regardless of TRKSGRP datafill
 - the Echo Suppressor Indicator field contains the Outgoing Half Echo Suppressor Not Included code ('0') regardless of TRKSGRP datafill
- Calling Party Category - contains the Test Call code ('00001101'). This value is sent in the test call IAM regardless of what facility initiates the test, line call or the number of test digits.
- Called Party Address - the Nature of Address and Numbering Plan Indicator fields of the Called Party Address parameter for test calls depend on the address signals to be transmitted. If the Called Party Address parameter contains a called party address having number of address digits greater than three; on the terminating, far end switch, then the Nature of Address field is encoded with the National (Significant) Number code ('0000011') and the Numbering Plan Indicator is encoded with the ISDN/Telephony Numbering Plan code ('001'). If the Called Party Address

38. T101 testline is supported only in a hybrid configuration.

parameter contains a test line number (i.e. a 3 digit test code) the Nature of Address field is encoded with the Test Line Test code ('1110111') and the Numbering Plan Indicator is encoded with the Unknown numbering plan code ('000'). This allows the terminating, far end switch to apply appropriate dialing plan and translation to the received digits to terminate the call to the desired test line.

- User service information - Layer 1 information field in this parameter is dependent on datafill in CARRMTC table.

Translations & Termination of test call

At the far end switch, pretranslator used for test calls is obtained from the office parameter GLOBAL_TESTCALL_PRTNM, if the Nature of address (NOA) in called party address parameter of incoming IAM for a testcall is Testline Testcode ('1110111'). If GLOBAL_TESTCALL_PRTNM is NPRT then pretranslator datafilled in PRTNM field of table TRKGRP is used. Ordinarily GLOBAL_TESTCALL_PRTNM is datafilled as 'C7PT' as pretranslator for testline numbers.

Dialplan used for a testcall depends upon the Numbering plan indicator field of incoming IAM. If numbering plan indicator is 'ISDN_TELEPHONY_NUM_PLAN', dialplan datafilled in TRKGRP is used. If dialplan datafilled in TRKGRP is NIL, dialplan from table OPT250 is taken. If the numbering plan indicator in incoming IAM is 'UNKNOWN_NUM_PLAN', dialplan is taken as ADDR.

All optional parameters (including CLI) are ignored while processing incoming Test call IAM. If CLI is received in the incoming IAM, it is not processed but it is delivered to the terminator if terminator is non-testline.

If the NOA in the Called Party Address parameter of incoming IAM indicates testline testcode, then subtable STDPRT of table STDPRTCT should be datafilled as standard route to testlines. If the route is not datafilled in table STDPRTCT then call takes universal translations. Serving Translation Scheme (STS) in such a case is derived in the following manner:

- for calls originating on INTRA IMT, STS is derived from office parameter DEFAULT_STS in table OFCVAR.
- for calls originating on GLOBAL IMT, STS is derived using OPART & TPART fields of table TRKGRP.

The selector, in table STDPRTCT, subtable STDPRT, which are supported for pretranslation of test calls are S, T, D, CT.

Once the Trunk Under Test (TUT) is connected to specified testline at the far end switch, test equipment at the near end switch starts the desired test and after the completion of the test, a log report is generated indicating the results.

TTP MAP level

TST and OP are the two commands at this level which are use for initiating a testcall on a trunk.

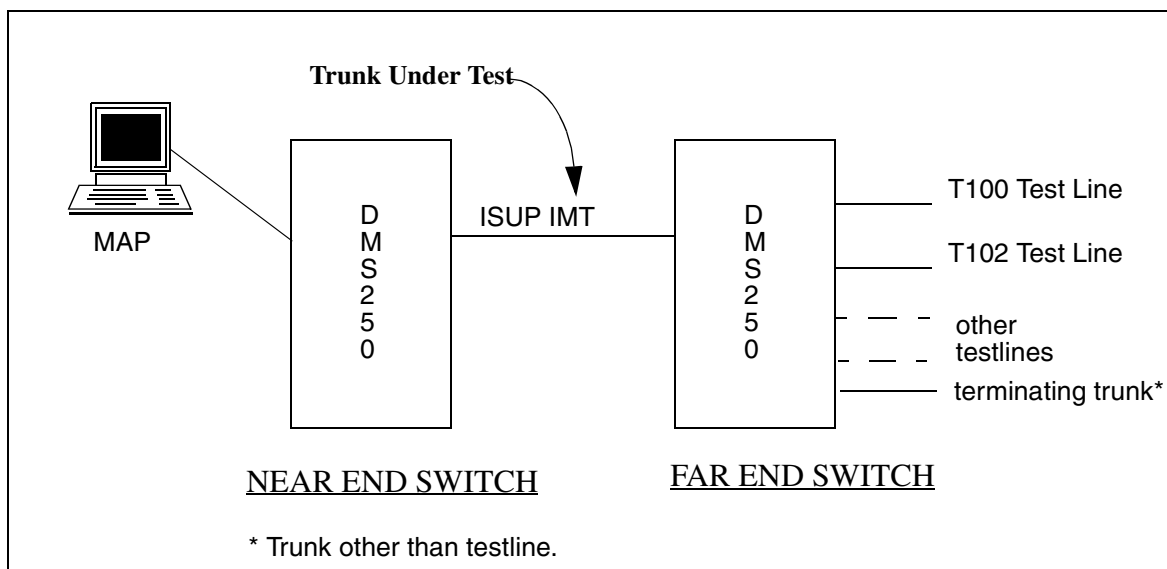
TST command

It takes a single parameter identifying the desired test and provides the ability to perform standard tests on a trunk. Following format of the command is supported.

- TST T10X, where X is in the range {0,2}

Example: Following figure depicts the configuration for manually testing the ISUP IMT, supported by this feature, from TTP MAP level:

Trunk testing from the TTP level of the MAP



For command TST T102 (Milliwatt testline) given at the TTP MAP level, the call flow till termination on the testline is as follows:

Origination at the near end switch

Table *CLLIMTCE*; pos *IMT761C7LP00*

This table gives TSTNOIND, which is used to index into table TSTLCONT and MWIDX, which is used to index into table MWDATA.

Table CLLIMTCE;

CLLI	SCLLI	MIN ALM	MAJ ALM	CRIT ALM	SYNC TYPE	TST NO IND	MW IDX	SIG TST	PRFX DIG	DIAG DATA
IMT761LP00	IMT761	5	10	15	NSS	0	0	N	N	(4)

*Table TSTLCONT; pos 0; sub TLNOS; pos T102***Table TSTLCONT;sub TLNOS**

TESTLINE	TLNUMBER	TL_MFC_ OG_SIG
T102	102	N

*Table MWDATA; pos 0***Table MWDATA**

IDXKEY	MWDATA
0	0 1004

The table TSTLCONT contains the address digits (102 in this example) to be outpulsed for the corresponding Testline. Outgoing testcall IAM, on the trunk under test, contains these address digits as address information. Since this table cannot be datafilled for more than 12 address digits, TST command can be used to outpulse at the maximum 12 address digits only.

As described in section 1.17.1, since the number of address digits are 3, Nature of Address in the IAM is set to Test line Test Code. This nature of address at the far-end-switch will indicate office parameter GLOBAL_TESTCALL_PRTNM is to be used for pretranslations.

The table MWDATA gives the frequency and the decibel level which near end switch expects from far end switch while performing the milliwatt test.

In this example the decibel level and frequency are 0 and 1004 Hz respectively.

Translation & Termination at the far end switch

Since the Nature of Address is Test Line Test Code, Office Parameter GLOBAL_TESTCALL_PRTNM is looked at to get a pretranslator name for Test Call. If the value is NPRT, then the PRTNM of TRKGRP is used.

Table OFCVAR; pos GLOBAL_TESTCALL_PRTNM

Table OFCVAR

PARMNAME	PARMVAL
GLOBAL_TESTCALL_PRTNM	C7PT

Table STDPRTCT; pos C7PT; sub STDPRT; pos 102

Table STDPRTCT

FROMDIGS	TODIGS	PRETRTE
102	102	DD 3 TERM102T 3 3 NONE

The call terminates on TERM102T Test Line and subsequent tests are performed on the Trunk Group on which the above TST command was initiated.

The above example explains termination of testcall on a testline directly through route specified in table STDPRTCT. A testcall can also be terminated on a testline using universal translation. This is explained in the example of the next section (1.17.3.2).

OP command

This command has two formats

- OP 'xxxxxxx', where xxxxxxx are valid dialed digits that may be translated at the far end office.
- OP T10X, where T10X identifies a valid trunk testline test.

Example:

For the command OP 2141001234 given at the TTP MAP level, the call flow till termination is as follows:

Origination at the near end switch

As described in section 1.17.1, since the number of address digits are 10, Nature of Address in the IAM is set to National Significant Number. This nature of address at the far-end-switch will indicate that PRTNM of Table TRKGRP is to be used for pretranslations.

Translation & Termination at the far end switch

Table TRKGRP; pos IMT761C7LP00

Table TRKGRP

GRPKEY	GRPTYP	TRAFSNO	PADGRP	NCCLS	GRPINFO
IMT761C7LP00	IMT	40	NPDGP	NCIM	UCSUST 0 2W IMT MIDL 16 7 16 UCS2UCS NIL CN NONE 4 ALWAYS ADDR 111 0 GLOBAL N N N VOICE_DATA NONE 4 160 (OHQ)(OHQTERM) \$

The OPART and TPART obtained from TRKGRP is used to derive STS from Table PARTOSTS.

Table PARTOSTS; pos 00 111

Table PARTOSTS

KEY	STS
00 111	611

The PRTNM (IMT in this example) obtained from table TRKGRP along with the incoming NOA (NATL in this example) is used to position into table TYP2PRTM.

Table TYP2PRTM; pos IMT

Table TYP2PRTM

KEY	OPRTNM
IMT NATL	IMT

Table PRETNAME; pos IMT

Table PRETNAME

PRTNM	STDPRTNM	ASTPRTNM	OCTPRTNM
IMT	IMT	NPRT	OCTR

Table STDPRTCT; pos IMT; sub STDPRT; pos 214

Table STDPRTCT;Sub STDPRT

FROMDIGS	TODIGS	PRETRTE
214	21	CT OFFNET 2 20 0 (UNIVIDX CT) \$

The STS derived previously is used to index into table STS2CTDB to get the Translator name for the call.

Table STS2CTDB; pos 611

Table STS2CTDB

STS	OFFXNAM	ONXNAM
611	IUCS611	IUCS611

Table CTCODE; pos; IUCS611 214 214

Table CTCODE

XLANAME	FROMD	TOD	XLADATA
IUCS611	214	214	RTE (PF 0) (MM 7 15) (DEST 111) \$

Table CTRTE; pos IUCS611 111

Table CTRTE

XLANAME	RTEREF	RTELIST
IUCS611	111	(S IMT762C7DR03) \$

Hence the call terminates on IMT762C7DR03.

OP T10x command takes the digits to be outputted from table TSTLCONT which cannot be datafilled for more than 12 address digits and hence this command cannot be used to output more than 12 address digits.

Please Refer to AD9016 (Open Number Plan for UCS ISUP IMT) for more details on Universal Translations.

Please refer to NTP 297-1001-595 (Trunks Maintenance Guide) for more details on the OP Command.

Parameter Interworking

This section describes the interworking of parameters which are specific to test call.

- For testcalls that originate on ISUP IMT and terminate on ISUP IMT following table shows the interworking of parameters:

Parameter Interworking (ISUP to ISUP)

IAM (Incoming)	IAM (Outgoing)
Calling Party Category: ISUP_CPC_TEST_CALL	Calling Party Category: ISUP_CPC_TEST_CALL

- For a test call originating on ISUP92/Q.767 with 3.1KHz audio as TMR, and terminating on any of the supported ISUP IMTs, bearer capability in the outgoing IAM will be speech.
- When a test call terminates on any of the supported IMTs then following table shows the mapping of Nature Of Address (NOA) and Numbering Plan Indicator of the Called Party Address (CPA) parameter in the outgoing IAM:

Outgoing IAM Parameters

Outgoing IAM parameter	CPA length > 3	CPA length < = 3
Called Party Nature of Address	NATIONAL ('0000011')	ISUP_TESTLINE('1110111')
Called Party Numbering Plan Indicator	ISDN/Telephony Numbering Plan('001')	Unknown('000')

Billing

Generation of CDRs for testcall can be controlled by office parameter CDR_FOR_TESTLINE in table OFCOPT. If CDR_FOR_TESTLINE is 'Y' CDR would be generated for the testcall with COMPCODE field as 7.

After successful completion of call using OP command, 'RLS R' command is used at the TTP MAP level to release the trunk. In this case, the COMPCODE field of CDR is populated with '5'.

Appendix I: Data Call

Data call Identification

UCP ISUP IMT (INTER/INTRA) Origination

- A call originating on an UCP ISUP IMT (Intra/Inter) is identified as a data call if
 - information digits in case of I3PA dialplan are '56'. In this case the call is a 56k data call.
 - the Information Transfer Capability (ITC) in User Service Information parameter of incoming IAM, indicates data (UNRESTRICTED DIGITAL³⁹, RESTRICTED DIGITAL). If ITC is RESTRICTED DIGITAL the call is 64k restricted digital call. If ITC is

39. When Information Transfer Capability in User Service Information parameter of incoming IAM is 3.1kHz or Speech and the dialplan is I3PA, information digits decide whether a call is a datacall.

UNRESTRICTED DIGITAL and User Rate in USI is 56kbps, then the call is 56k digital call else, it is 64k unrestricted digital call.

ISUP92/Q767 Origination

- A call originating on an Q.767/ISUP92 is identified as a data call if Transmission Medium Requirement parameter in the incoming IAM indicates data (UNRESTRICTED DIGITAL). The distinction between 56k data and 64k data is done depending upon the User Rate as is done in case of UCP INTRA agency. For these two protocols, TMR is mandatory parameter and USI is optional parameter. If both these parameters are received in IAM then TMR takes precedence in determining if the call is a datacall.

PRI Origination

- The Information Transfer Capability (ITC) in Bearer Capability parameter in incoming SETUP message indicates data (UNRESTRICTED DIGITAL, RESTRICTED DIGITAL). If ITC is RESTRICTED DIGITAL, the call is 64k restricted digital call. If ITC is UNRESTRICTED DIGITAL and Access Data Rate in Bearer Capability is 56kbps, then the call is 56k digital call else, it is 64k unrestricted digital call.

PTS Origination

For Data calls origination on PTS agents, the BCNAME field in Table TRKGRP for the PTS CLLI should be datafilled with 56KDATA or 64KDATA⁴⁰. Later, that particular PTS agent can be used for making data calls on DMS-250.

Bearer Capability Screening

Origination Screening:

The call's BC (CALLBC⁴¹) is compared with the BCNAME field of the originating trunk (FILEDBC). If screening fails the call is given Service Currently UNavailable treatment (SCUN). BC compatibility check is done using table BCCOMPAT.

Termination Screening:

The call's BC is compared with bearer capability of the terminating trunk using table BCCOMPAT. If terminating screening fails the call-route advances to the next route choice in the route list. If route exhaustion occurs, call is blocked. The treatment applied at this point is Generalized No Circuit

40. Note that while 64KDATA may be datafilled on the PTS (FGD) agent, the rate will be treated as 56K. 64K data rate is not supported on PTS agents.

41. CALLBC is the bearer capability of the call, and FILEDBC is value of the BCNAME field of table TRKGRP. FILEDBC is used as TERMBC while indexing in table BCCOMPAT.

Treatment (GNCT). The screening will pass or fail based on the datafill in table BCCOMPAT. The following table shows table BCCOMPAT with example datafills:

Table BCCOMPAT to check BC Compatibility

CALLBC^a	TERMBC¹
56KDATA	64KDATA
64KDATA	VOICE_DATA
56KDATA	VOICE_DATA
VOICE_DATA	64KDATA
VOICE_DATA	56KDATA

a. CALLBC and TERMBBC form the key for table BCCOMPAT.

Table BCCOMPAT defines bearer capability pairs that are compatible with one another. For Example, the fourth tuple in above table means a trunk with BC of VOICE_DATA can allow a call of BC 64KDATA.

Note:

- all the BC s used in this table must be defined in the table BCDEF.

If a data call terminates over a UCP INTRA trunk with I3PA in the dialplan field of TRKGRP then information digits are outputted as 56 only when it is a 56k data call.

In the Nature of Connection indicator parameter of the outgoing IAM, satellite indicator field is set to one satellite circuit in the connection.

Interworking

Following matrix shows the interworking supported by this feature:

Interworking for Data-calls.

	Terminating Agency							
Orig. Agency	Gateway	UCP Intra	UCP Inter	FGD SS7	FGD PTS	UCS PRI	FGB	DAL TIE
Gateway	X	X	X	X	X	X	X	X
UCP Intra	X							
UCP Inter	X							
FGD SS7	X							
FGD PTS	X							
UCS PRI	X							
FGB	X							
DAL TIE	X							

Parameter Interworking

This section describes the interworking of parameters which are specific to datacall.

ISUP92/Q.767 to UCP

The incoming USI and TMR parameters on ISUP92/Q.767 are mapped as follows to the ANSI USI on the outgoing UCP IMT:

Mapping of USI on UCP when no USI is received on ISUP92/Q.767

Q767/ISUP92 ISUP IAM		UCP ISUP IAM
TMR	OPTIONAL USI	MANDATORY USI

Q767/ISUP92 ISUP IAM		UCP ISUP IAM
64 K Unres.	NONE	Information transfer capability - 64 kbps Unrestricted
		Information transfer rate - 64 kbps
		Coding Standard - National Standard
		Transfer Mode - Circuit mode

Mapping of USI on UCP when 2 byte USI is received on ISUP92/Q.767

Q767/ISUP92 ISUP IAM		UCP ISUP IAM
TMR	OPTIONAL USI	MANDATORY USI
64kbps Unres.	Information Transfer Capability - Any value supported.	Information transfer capability - 64kbps Unres
	Information transfer rate - 64 kbps - Packet mode calls (00000) - For other values give BCNI ^a treatment.	Information transfer rate - 64 kbps - 64 kbps ***Call fails***
	Coding Standard - All Values	Coding Standard - National Standard
	Transfer Mode - Circuit mode - Packet mode ^b	Transfer Mode - Circuit mode ***Call fails***

a. BCNI is given when wideband data calls are originated on non-wideband trunks. Wideband data calls on wideband trunks are blocked with FNAL treatment.

b. Packet mode data calls are blocked with FNAL treatment.

Mapping of USI on UCP when 4byte USI is received on ISUP92/Q.767

Q767/ISUP92 ISUP IAM		UCP ISUP IAM
TMR	OPTIONAL USI	MANDATORY USI
64 kbps unrestricted.	ITC - Any value supported.	ITC - 64 Kbps Unrestricted.
	Information transfer rate ^a - 64 kbps - Packet mode calls (00000) - For other values give BCNI ^b treatment.	Information transfer rate - 64 kbps - 64 kbps ***Call fails***
	Coding Standard - All Values	Coding Standard - National Standard
	Transfer Mode - Circuit mode - Packet mode ^c	Transfer Mode - Circuit mode ***Call fails***
	Layer 1 information - Any supported value	Layer 1 Information ^d - Tandemed
	User Rate - 56 Kbps - All other Values	User Rate - 56 kbps - Not built on the UCP side.

a. Information Transfer Rate with values of 1472 Kbps with Coding Standard as National and Multirate are unrecognized USI values.

b. BCNI is given when wideband data calls are originated on non-wideband trunks. Wideband data calls on wideband trunks are blocked with FNAL treatment.

c. Packet mode data calls are blocked with FNAL treatment.

d. The layer 1 info. is built on the UCP only if the User Rate is 56 Kbps. The 4 byte incoming USI is sent out as a 4 byte USI only if the User Rate is 56 Kbps. For all other values, the 4 byte USI is sent out as a 2 byte USI.

3 byte USI is not valid for data calls.

Calling party category interworking (ISUP92/Q.767 to UCP)

ITU IAM(Incoming)	UCP (Outgoing)
Calling Party Category: ISUP_CPC_DATA_CALL	Calling Party Category: ISUP_CPC_DATA_CALL

ISUP92/Q.767 to ISUP92/Q.767

The supported values of TMR and USI are tandemed in case of an ISUP92/Q.767 - ISUP92/Q.767 call. If no USI is received, then a default 2byte USI is built on the outgoing side if the incoming TMR is 64K Unrestricted.

ISUP92/Q.767 to ISUP92/Q.767 call with TMR 64K Unres and no USI

Outgoing ISUP92/Q.767 TMR/USI	
TMR	OPTIONAL USI
- 64 kbps unrestricted	ITC - 64 kbps unrestricted. ITR - 64 Kbps unrestricted Coding Standard - National Standard Transfer Mode - Circuit mode

UCP to ISUP92/Q.767

The incoming USI parameter on UCP IMT is mapped as follows to TMR and USI on ISUP92/Q.767:

- a. When optional parameters are present in IAM or option ISDNXFER is set in table TRKGRP for originating agency then following table shows the interworking of parameters:

Calling party category interworking (UCP to Gateway ISUP)

UCP IAM (Incoming)	ITU IAM (Outgoing)
Calling Party Category: ISUP_CPC_DATA_CALL	Calling Party Category: ISUP_CPC_DATA_CALL

Mapping of incoming USI on UCP to TMR & USI on ISUP92/Q.767

UCP ISUP IAM	ITU ISUP IAM	
MANDATORY USI	TMR	OPTIONAL USI
Information transfer capability - 64 kbps unrestricted. - 64 kbps restricted.	- 64 kbps unrestricted - 64 kbps unrestricted	Information transfer capability - 64 kbps unrestricted. - 64 kbps restricted.
Information transfer rate - 64 kbps - Packet mode calls (00000) - For other values give BCNI ^a treatment.		Information transfer rate - 64 kbps - 64 kbps ***Call fails***
Coding Standard - All Values		Coding Standard - National Standard
Transfer Mode - Circuit mode - Packet mode ^b		Transfer Mode - Circuit mode ***Call fails***
Layer 1 information - Any supported value		Layer 1 information - Value is taken from table CARRMTC

a. BCNI is given when wideband data calls are originated on non-wideband trunks. Wideband data calls on wideband trunks are blocked with FNAL treatment

b. Packet mode data calls are blocked with FNAL treatment.

- a. When there are no optional parameter in IAM and option ISDNXFER is NOT set in table TRKGRP for originating agency then following table shows the interworking of parameters:

Mapping of ITU ISUP USI and TMR

Outgoing ITU ISUP IAM	
TMR	OPTIONAL USI

Outgoing ITU ISUP IAM	
- 64 kbps unrestricted	ITC - 64 kbps unrestricted.
	ITR - 64 kbit/s
	Coding Standard - National Standard
	Transfer Mode - Circuit mode
	Layer 1 information - Layer 1 rate adaptation
	User Rate - 56 Kbps

Calling party category interworking (UCP to Gateway ISUP)

UCP IAM (Incoming)	ITU IAM (Outgoing)
Calling Party Category: — DATA	Calling Party Category: — SUBSCRIBER1

Billing

DIGDATA field in the CDR indicates if a call is a datacall. It is a boolean and a value 'Y' indicates a datacall.

Appendix J: ECAN

Application of Echo Cancellers on Transit Switch

The following figure illustrates the use of echo cancellers in a general transit call situation.

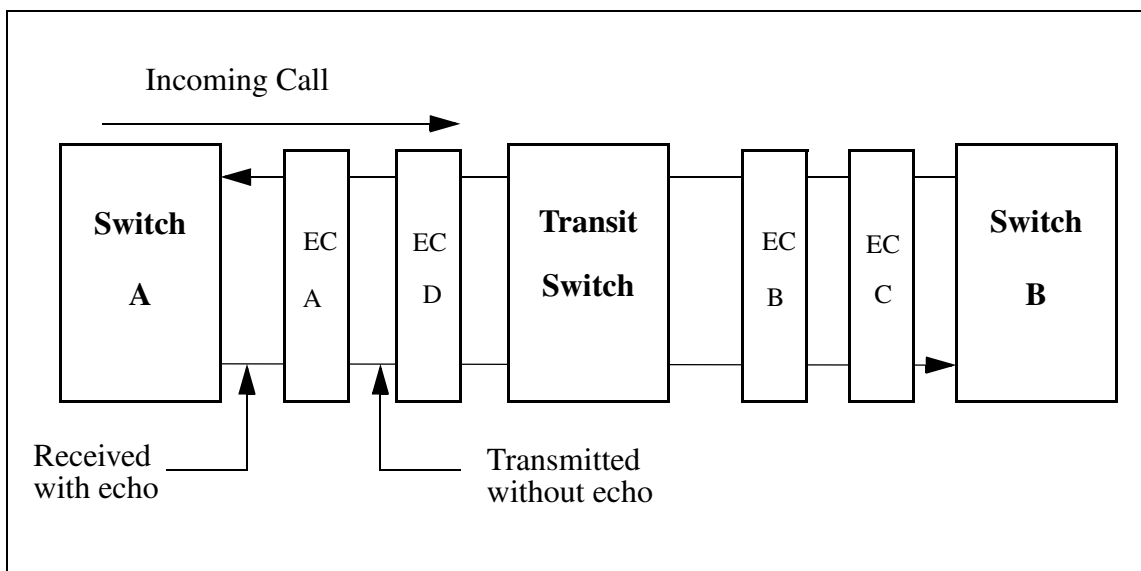
Echo canceller A is enabled as the outgoing echo canceller. At the transit switch, a forward message is received indicating that a previous switch has enabled an echo device. Therefore, the transit switch does not enable echo canceller B. At switch B, echo canceller C is enabled as the incoming device. At the transit switch, the first backward acknowledgment indicates

that a succeeding switch has already included an incoming echo device. Thus, it does not enable echo canceller D.

Typically, during call setup in the forward direction, an echo canceller is activated on the outgoing trunk if required. During the backward acknowledgment phase of the call setup, an echo canceller is activated on the incoming trunk if required. This is the conventional setup.

The echo canceller device is physically connected on a per carrier basis, but it can control echo on a per trunk basis (DMS implementation). Since there are two speakers in a call, an echo device is needed in both directions for both parties to benefit. Hence, the term 'half-echo cancellers' for one direction. Although, at most, only one incoming and one outgoing echo device should be enabled.

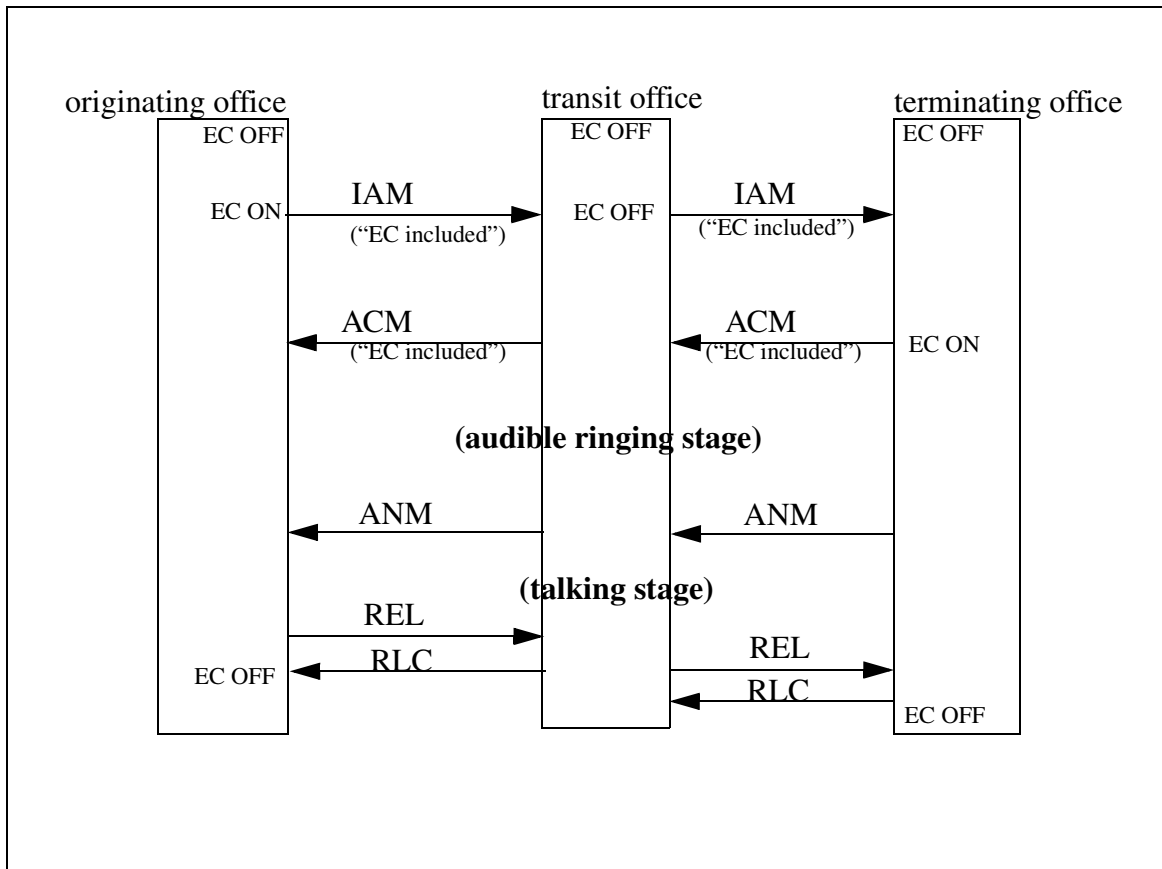
Application of Echo Cancellers on transit switch

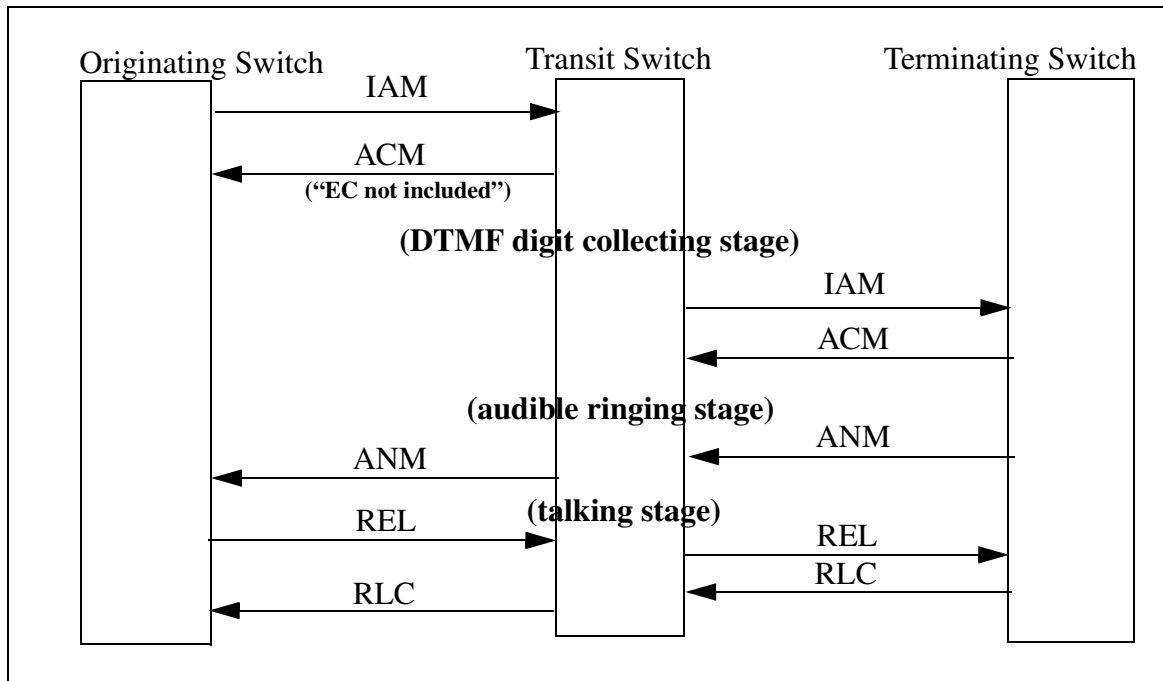


Echo Canceller Control Logic

The activation of Echo Canceller is completed at the call setup phase when echo control is required. And it is deactivated at the end of every call.

The diagram below describes how echo control is handled along with a typical ISUP call sequence.

Example of echo control in ISUP messaging

Example of echo control in DTMF digit collection call

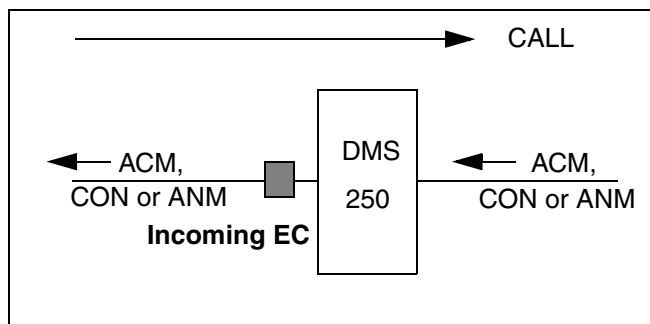
For calls which require DTMF digit collection (Figure-24), an ACM message always be send back immediately from the transit switch to the originating switch for requesting the digit collection. Therefore, the EC bit is set to “not included”, no matter the transit switch has or has not received the EC indication from the terminating switch.

Outgoing Echo Cancellers**A) Criteria for echo cancellation:**

- the incoming seizure (e.g. IAM) indicates no forward echo canceller yet; incoming CPC and TMR fields, if available, indicate voice-only call.
- echo canceller is datafilled in TRKSGRP and is available for use.

B) Signalling upon echo canceller activation:

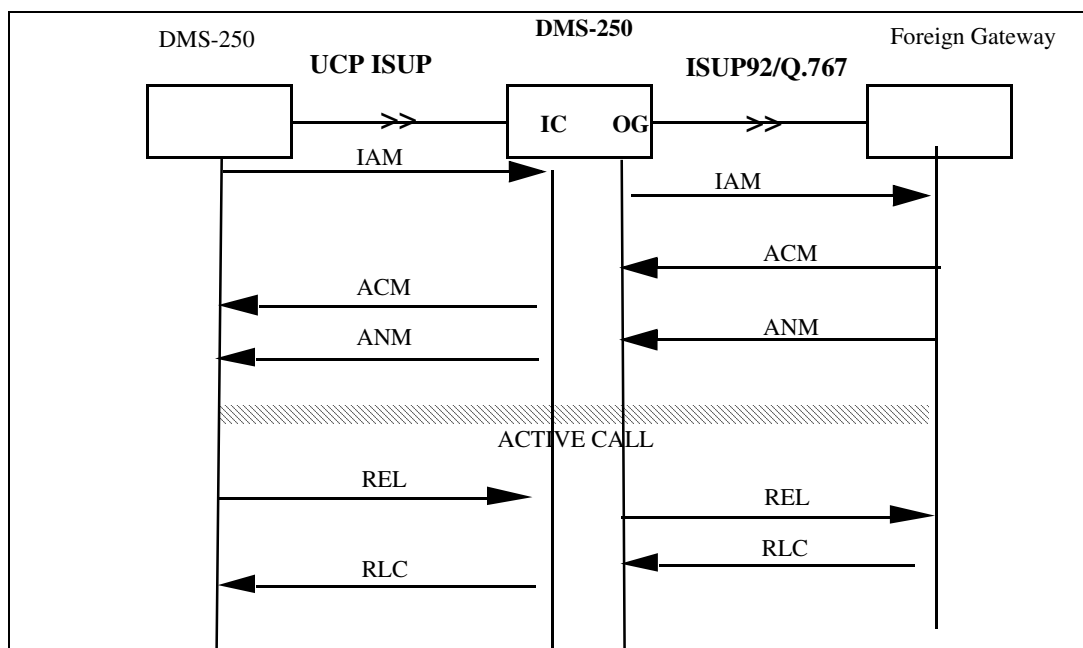
- outgoing IAM Echo Control bit is set to ‘included’.

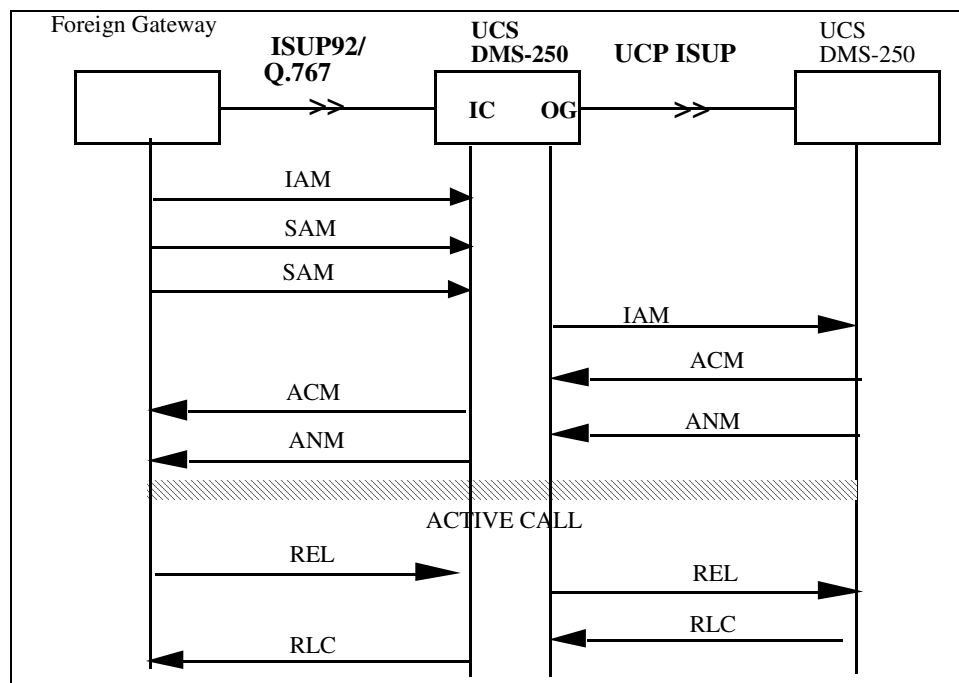
EC on the trunk in the incoming direction

For the outgoing echo cancellers, the disable/enable commands are sent to the EC module after received IAM. However, for the incoming echo cancellers (Figure - 25), the disable/enable commands are not be sent to the EC module until it receives the first backward messages (ACM, CON or ANM).

Appendix K: UCP ISUP & ISUP92/Q.767 Interworking

The following figures show the message flow diagram for UCP ISUP and ISUP92/Q.767 interworking:

UCP ISUP & ISUP92/Q.767 Interworking (Enbloc)

ISUP92/Q.767 & UCP ISUP Interworking (Overlap Sending)

Overlap method of address signaling supports the transport of called party address digits in multiple messages. If the incoming IAM message contains no digits in the Called Party Number, or incomplete digits in the Called Party Number (end-of-digit (F) is not suffixed on the called number), and the field OV LAP in table TRKSGRP is set to 'Y', the DMS-250 enters in overlap mode. Upon receipt of such an IAM message, a timer is started. The DMS-250 waits until all the information is available (via SAMs), or the timer is expired, before translations are performed. It should be noted that the DMS-250 always sends all the Called Party address digits in the Initial Address Message.

Message parameters which need to be interworked, are described in this section. Parameters are keyed as 'F' for fixed mandatory, 'V' for variable length mandatory and 'O' for optional.

IAM - UCP ISUP to ISUP92/Q.767

UCP ISUP IAM	ISUP92 IAM
Nature of Connection Indicator (F)	Nature of Connection Indicator (F)
Called Party Number (V)	Called Party Number (V)
Calling Party Number (O) ₁	Calling Party Number (O)

IAM - UCP ISUP to ISUP92/Q.767

UCP ISUP IAM	ISUP92 IAM
Charge Number (O) ₂	
Transit Network Selection Parameter (O) Carrier Identification Parameter (O)	
Forward Call Indicator (F)	Forward Call Indicator (F)
Calling Party Category (F)	Calling Party Category (F)
User Service Information (V)	Transmission Medium Requirement (F) ₃ User Service Information (O)

₁Note: The Calling Party Number is considered valid and is supported on gateway trunks only if the fields “calling party number incomplete indicator (NI)” is set to “Complete” and the “screening indicator” is “user provided, verified and passed” or “network provided” otherwise it is invalid and is discarded.

₂Note: Charge Number is not supported in ISUP92/Q.767 IAM.

₃ Note: User Service Information is a mandatory parameter in UCP while it is optional in ISUP92/Q.767. When interworking from UCP to ISUP92/Q.767, the information in the USI parameter is mapped to both the USI optional parameter and to the TMR parameter in the ISUP92/Q.767 IAM.

The formats of the TMR and USI parameters are provided below for reference.

Transmission Medium Requirement (in ISUP92/Q.767)

	8	7	6	5	4	3	2	1
Octet 1	Transmission Medium Requirement							

User Service Information (in UCP ISUP)

	8	7	6	5	4	3	2	1
Octet 1	Ext	Coding standard		Information transfer capability				
Octet 2	Ext	Transfer mode		Information Transfer rate				
Octet 3	Ext	User layer protocol id						
Octet 4	Ext	Spare		Rate				

USI, Information Transfer Rate to TMR Mapping

USI - Information Transfer Rate	TMR - Transmission Medium Requirement
speech	speech
64 Kbit/s unrestricted digital info.	64 Kbit/s unrestricted
64 Kbit/s restricted digital info.	64 Kbit/s unrestricted
3.1 kHz audio	3.1 kHz audio
7 kHz audio	3.1 kHz audio*
15 kHz Audio	3.1 kHz audio*

* Based on Table BCCOMPAT datafill. If this mapping is not datafilled, then the call is treated due to bearer incompatibility.

The following shows the interworking of the ISUP92/Q.767 IAM message to UCP ISUP IAM message:

IAM - ISUP92/Q.767 to UCP ISUP

ISUP92/Q.767 IAM	UCP ISUP IAM
Nature of Connection Indicator (F)	Nature of Connection Indicator (F)
Forward Call Indicator (F)	Forward Call Indicator (F)
Calling Party Category (F)	Calling Party Category (F)
Transmission Medium Requirement (F)	User Service Information (V) ₁
Called Party Number (V)	Called Party Number (V)
Transit Network Selection (O)	
User Service Information (O)	User Service Information (V)
Calling Party Number (O) ₂	Calling Party Number (O)

₁Note: The User Service Information in the UCP IAM message is encoded based on the

USI of the ISUP92/Q.767 IAM if received. If the USI parameter is not received in the ISUP92/Q.767 IAM, then the TMR parameter is used to encode the USI as shown in the Table below.

²Note: The Calling Party Number is considered valid and is supported on gateway trunks only if the fields “calling party number incomplete indicator (NI)” is set to “Complete” and the “screening indicator” is “user provided, verified and passed” or “network provided” otherwise it is invalid and is discarded.

ISUP92/Q.767 TMR to UCP ISUP USI Parameter Mapping

ISUP92/Q.767 Transmission Medium Requirement	UCP ISUP User Service Information
	Coding Standard - CCITT standardized coding (default)
Transmission Medium Requirement - Speech - 64 kbit/s unrestricted - 3.1 kHz audio	Information Transfer Capability - Speech - 64 kbit/s Unrestricted digital Info - 3.1 kHz audio
	Transfer mode - Circuit mode (default)
	Information Transfer Rate - 64 kbit/s (default)
	User layer1 protocol Information (default)

Parameters Mapping for messages going from Q.767 to UCP ISUP

Initial Address Message (IAM)

The following table shows the discarding and tandeming of parameter for a Q.767 to UCP IAM.

Q.767 -> UCP parameters in the IAM message

Q767 Parameter	Type	Action
Message Type	F	Tandem
Nature Of Connection Indicators	F	Process

Q.767 -> UCP parameters in the IAM message

Q767 Parameter	Type	Action
Forward Call Indicators	F	Process
Calling Party's Category	F	Process
Transmission Medium Requirement (TMR)	F	Mapped
Called Party Number	V	Process
Access Transport	O	Tandem
Calling Party Number	O	Process
Closed User Group Inter-lock Code	O	Tandem
Optional Forward Call Indicators	O	Tandem
User service information	O	Process
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

Address Complete Message (ACM)

The following table shows the discarding and tandeming of parameters for a Q.767 to UCP ACM when the SOC NSER0003 is ON and OFCVAR field ACTIVATE_INTER_INTRA_UNANS_CALL is set to 'Y'.

Q.767 -> UCP parameters in the ACM message

Q767 Parameter	Type	Action
Message type	F	Tandem
Backward call indicators	F	Process
Access transport	O	Tandem
Cause indicators	O	Tandem
Optional backward call indicators	O	Discard
User-to-user indicators	O	Tandem

Q.767 -> UCP parameters in the ACM message

Q767 Parameter	Type	Action
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

The following table shows the discarding and tandeming of parameters in Q.767 to UCP ACM when SOC NSER0003 is not ON and field ACTIVATE_INTER_INTRA_UNANS_CALL in table OFCVAR is not set to 'Y'.

Q.767 -> UCP parameters in the ACM message

Q767 Parameter	Type	Action
Message type	F	Tandem
Backward call indicators	F	Process
Access transport	O	Tandem
Cause indicators	O	Tandem
Optional backward call indicators	O	Tandem
User-to-user indicators	O	Tandem
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

Answer Message (ANM)

The following table shows the tandeming and discarding of parameters in Q.767 to UCP ANM.

Q.767 -> UCP parameters in the ANM message

Q767 Parameter	Type	Action
Message type	F	Tandem
Access transport	O	Tandem
Backward call indicators	O	Tandem
Connected number	O	Tandem
User-to-user information	O	Tandem

Q.767 -> UCP parameters in the ANM message

Q767 Parameter	Type	Action
End of optional parameters	O	Tandem

Call Progress Message (CPG)

The following table shows the tandeming and discarding of parameters from a Q.767 to UCP CPG.

Q.767 -> UCP parameters in the CPG message

Q767 Parameter	Type	Action
Message type	F	Tandem
Event information	F	Tandem
Access transport	O	Tandem
Backward call indicators	O	Tandem
Optional backward call indicators	O	Tandem
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

Connect Message (CON)

CON message is not supported in UCP protocol. The following table shows the parameters which will be tandemed and discarded while sending an ANM to the UCP trunk.

Q.767 -> UCP parameters in the CON message

Q767 Parameter	Type	Action
Message type	F	Mapped
Backward call indicators	F	Tandem
User-to-user indicators	O	Tandem
User-to-user information	O	Tandem
Access transport	O	Tandem
Connected number	O	Discard
End of optional parameters	O	Tandem

Continuity Test Message (COT)

Continuity test message is tandemmed to the UCP trunk as shown in the following table.

Q.767 -> UCP parameters in Message COT

Q767 Parameter	Type	Action
Message type	F	Tandem
Continuity indicators	F	Tandem

Forward Transfer Message (FOT)

Forward transfer message is tandemmed to the UCP trunk.

Q.767 -> UCP parameters in message FOT

Q767 Parameter	Type	Action
Message type	F	Tandem
End of optional parameters	O	Tandem

Release Message (REL)

The following table shows the tandemming and discarding of parameters in REL message when a cause value other than Normal call Clearing is received.

Q.767 ->UCP parameters in message REL

Q767 Parameter	Type	Action
Message type	F	Tandem
Cause indicators	V	Process
Automatic congestion level	O	Discard
User-to-user information	O	Discard
End of optional parameters	O	Tandem

The following table shows the tandeming and discarding of parameters in REL message when a cause value of Normal call Clearing is received

Q.767 ->UCP parameters in message REL

Q767 Parameter	Type	Action
Message type	F	Tandem
Cause indicators	V	Process
Automatic congestion level	O	Discard
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

Suspend/Resume Message (SUS/RES)

Suspend and resume messages are tandemed to UCP trunk.

Q.767 -> UCP parameters in message RES and SUS

Q767 Parameter	Type	Action
Message type	F	Tandem
Suspend/Resume indicators	F	Tandem
End of optional parameters	O	Tandem

Parameters interworking for messages from UCP to Q.767

Reference feature document AD9067 'Support for User to User Parameter' for proper requirements when mapping of the User to User parameter is required.

Initial Address Message (IAM)

The following table shows the tandeming and discarding of parameters from a UCP to Q.767 IAM.

UCP -> Q767 parameters in the IAM message

UCP Parameter	Type	Action
Message Type	F	Tandem
Nature Of Connection Indicators	F	Process
Forward Call Indicators	F	Process

UCP -> Q767 parameters in the IAM message

UCP Parameter	Type	Action
Calling Party's Category	F	Process
User service information	F	Mapped
Called Party Number	V	Process
Calling Party Number	O	Process
Carrier Identification	O	Discard
Carrier Selection	O	Discard
Charge Number	O	Discard
Channel Assignment Map	O	Discard
Generic Address	O	Discard
Generic Digits	O	Discard
Jurisdiction Information	O	Discard
Multiple Business Group (Network Information)	O	Discard
Network Specific Facilities	O	Discard
Network-Specific IAM	O	Discard
Operator Information	O	Discard
Operator Service Indicator	O	Discard
Originating Line Informa- tion	O	Discard
Remote Operations	O	Discard
Supplementary Line Infor- mation	O	Discard
Transit network selection	O	Discard
User service information (mandatory variable length parameter in UCP proto- col)	O	Process
User-to-user information	O	Tandem

UCP -> Q767 parameters in the IAM message

UCP Parameter	Type	Action
End of optional parameters	O	Tandem

Address Complete Message (ACM)

Table 92 shows the tandeming and discarding of parameters from a UCP to Q.767 ACM when the SOC NSER0003 is ON and OFCVAR field ACTIVATE_INTER_INTRA_UNANS_CALL is set to 'Y'.

UCP -> Q767 parameters in the ACM message

UCP Parameter	Type	Action
Message type	F	Tandem
Backward call indicators	F	Process
Call reference	O	discard
Cause indicators	O	Tandem
Network specific information	O	Discard
User-to-user indicators	O	Tandem
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

The following table shows the tandeming and discarding of parameters from a UCP to Q.767 ACM when SOC NSER0003 is not ON and field ACTIVATE_INTER_INTRA_UNANS_CALL in table OFCVAR is not set to 'Y'.

UCP -> Q767 parameters in the ACM message

UCP Parameter	Type	Action
Message type	F	Tandem
Backward call indicators	F	Process
Call reference	O	Discard
Cause indicators	O	Tandem

UCP -> Q767 parameters in the ACM message

UCP Parameter	Type	Action
Network specific information	O	Discard
User-to-user indicators	O	Tandem
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

Answer Message (ANM)

The following table shows the tandeming and discarding of parameters from a UCP to Q.767 ANM.

UCP -> Q767 parameters in the ANM message

UCP Parameter	Type	Action
Message type	F	Tandem
Call reference	O	Discard
Carrier Selection	O	Discard
Internetwork Specific ANM	O	Discard
Intranetwork Specific ANM	O	Discard
Network Specific Information	O	Discard
Multiple Business Group (Network Information)	O	Discard
Operator Information	O	Discard
User-to-user indicators	O	Discard
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

Call Progress Message (CPG)

The following table5 shows the tandeming and discarding of parameters from a UCP to Q.767 CPG.

UCP -> Q767 parameters in the CPG message

UCP Parameter	Type	Action
Message type	F	Tandem
Event information	F	Tandem
Cause indicators	O	Discard
User-to-user indicators	O	Discard
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

Pass Along Message (PAM)

The following table shows the tandeming and discarding of parameters from a UCP to Q.767 PAM.

UCP -> Q767 parameters in message PAM

UCP Parameter	Type	Action
Message type	F	Tandem

Release Message (REL)

The following table shows the tandeming and discarding of parameters in REL message when a cause value other than Normal call Clearing is received.

UCP -> Q767 parameters in message REL

UCP Parameter	Type	Action
Message type	F	Tandem
Cause indicators	V	Process
User-to-user information	O	Tandem
User-to-user indicators	O	Discard
End of optional parameters	O	Tandem

The following table shows the tandeming and discarding of parameters in REL message when a cause value of Normal Call Clearing is received.

UCP -> Q767 parameters in message REL

UCP Parameter	Type	Action
Message type	F	Tandem
Cause indicators	V	Process
User-to-user information	O	Tandem
User-to-user indicators	O	Discard
End of optional parameters	O	Tandem

Suspend/Resume Message (SUS/RES)

The following table shows the tandeming and discarding of parameter in the SUS and RES messages from a UCP trunk to Q.767 trunk.

UCP -> Q767 parameters in message RES and SUS

UCP Parameter	Type	Action
Message type	F	Tandem
Suspend/Resume indicators	F	Tandem
End of optional parameters	O	Tandem

Parameter interworking for messages from ISUP92 to UCP

Initial Address Message (IAM)

The following table shows the tandeming and discarding of parameters from a ISUP92 trunk to UCP trunk.

ISUP92 ->UCP parameters in the IAM message

ISUP92 Parameter	Type	Action
Message Type	F	Tandem
Nature Of Connection Indicators	F	Process
Forward Call Indicators	F	Process
Calling Party's Category	F	Process

ISUP92 ->UCP parameters in the IAM message

ISUP92 Parameter	Type	Action
Transmission Medium Requirement (TMR)	F	Mapped
Called Party Number	V	Process
Access Transport	O	Tandem
Calling Party Number	O	Process
Closed User Group Inter-lock Code	O	Tandem
Optional Forward Call Indicators	O	Tandem
User service information	O	Process
User-to-user information	O	Tandem
Original Called Number	O	Tandem
Redirecting Number	O	Tandem
Redirection Information	O	Tandem
User to User Indicators	O	Tandem
End of optional parameters	O	Tandem

Address Complete Message

The following table shows the discarding and tandeming of parameters for a ISUP92 to UCP ACM when the SOC NSER0003 is ON and OFCVAR field ACTIVATE_INTER_INTRA_UNANS_CALL is set to 'Y'.

ISUP92 ->UCP parameters in the ACM message

ISUP92 Parameter	Type	Action
Message type	F	Tandem
Backward call indicators	F	Process
Access transport	O	Tandem
Access delivery information	O	Discard

ISUP92 ->UCP parameters in the ACM message

ISUP92 Parameter	Type	Action
Call diversion information	O	Discard
Cause indicators	O	Tandem
Echo control information	O	Discard
Generic notification indicator	O	Discard
Optional backward call indicators	O	Discard
Parameter compatibility information	O	Discard
Redirection number	O	Tandem
Redirection number restriction	O	Tandem
Transmission medium used	O	Discard
User-to-user indicators	O	Tandem
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

The following table shows the discarding and tandeming of parameters in ISUP92 to UCP ACM when SOC NSER0003 is not ON and field ACTIVATE_INTER_INTRA_UNANS_CALL in table OFCVAR is not set to 'Y'.

ISUP92 ->UCP parameters in the ACM message

ISUP92 Parameter	Type	Action
Message type	F	Tandem
Backward call indicators	F	Process
Access transport	O	Tandem
Access delivery information	O	Tandem
Call diversion information	O	Tandem

ISUP92 ->UCP parameters in the ACM message

ISUP92 Parameter	Type	Action
Cause indicators	O	Tandem
Echo control information	O	Tandem
Generic notification indicator	O	Tandem
Optional backward call indicators	O	Tandem
Parameter compatibility information	O	Tandem
Redirection number	O	Tandem
Redirection number restriction	O	Tandem
Transmission medium used	O	Tandem
User-to-user indicators	O	Tandem
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

Answer Message (ANM)

The following table shows the tandeming and discarding of parameters for a ISUP92 to UCP ANM.

ISUP92 ->UCP parameters in the ANM message

ISUP92 Parameter	Type	Action
Message type	F	Tandem
Access delivery information	O	Discard
Access transport	O	Tandem
Backward call indicators	O	Tandem
Call history information	O	Discard
Connected number	O	Tandem
Echo control information	O	Discard

ISUP92 ->UCP parameters in the ANM message

ISUP92 Parameter	Type	Action
Generic notification indicator	O	Discard
Generic address	O	Discard
Optional backward call indicators	O	Discard
Parameter compatibility information	O	Discard
Redirection number	O	Tandem
Redirection number restriction	O	Tandem
Transmission medium used	O	Discard
User-to-user indicators	O	Tandem
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

Call Progress Message (CPG)

The following table shows the tandeming and discarding of parameters in the ISUP92 to UCP message.

ISUP92 -> UCP parameters in the CPG message

ISUP92 Parameter	Type	Action
Message type	F	Tandem
Event information	F	Tandem
Access delivery information	O	Tandem
Access transport	O	Tandem
Backward call indicators	O	Tandem
Call diversion information	O	Tandem
Cause indicators	O	Tandem

ISUP92 -> UCP parameters in the CPG message

ISUP92 Parameter	Type	Action
Generic notification indicator	O	Tandem
Optional backward call indicators	O	Tandem
Parameter compatibility information	O	Tandem
Redirection number	O	Tandem
Redirection number restriction	O	Tandem
Transmission medium used	O	Tandem
User-to-user indicators	O	Tandem
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

Connect Message (CON)

CON message is not supported in UCP protocol. The following table shows the parameters which will be tandemed and discarded while sending an ANM to the UCP trunk.

ISUP92 -> UCP parameters in the CON message

ISUP92 Parameter	Type	Action
Message type	F	Mapped
Backward call indicators	F	Tandem
Access delivery information	O	Discard
Access transport	O	Tandem
Call history information	O	Discard
Connected number	O	Tandem
Echo control information	O	Discard
Generic notification indicator	O	Discard

ISUP92 -> UCP parameters in the CON message

ISUP92 Parameter	Type	Action
Generic address	O	Discard
Optional backward call indicators	O	Discard
Parameter compatibility information	O	Discard
Redirection number	O	Tandem
Redirection number restriction	O	Tandem
Transmission medium used	O	Discard
User-to-user indicators	O	Tandem
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

Continuity Test Message (COT)

As shown in the following table this message is tandemed to the UCP trunk.

ISUP92 -> UCP parameters in Message COT

ISUP92 Parameter	Type	Action
Message type	F	Tandem
Continuity indicators	F	Tandem

Forward Transfer Message (FOT)

As shown in table FOT message is tandemed to the UCP trunk.

ISUP92 -> UCP parameters in message FOT

ISUP92 Parameter	Type	Action
Message type	F	Tandem
End of optional parameters	O	Tandem

Release Message (REL)

The following table shows the tandeming and discarding of parameters in REL message when a cause value other than Normal call Clearing is received.

ISUP92 -> UCP parameters in message REL

ISUP92 Parameter	Type	Action
Message type	F	Tandem
Cause indicators	V	Process
Access delivery information	O	Discard
Access transport	O	Discard
Automatic congestion level	O	Discard
Parameter compatibility information	O	Discard
Redirection number restriction	O	Discard
User-to-user information	O	Discard
User-to-user indicators	O	Discard
End of optional parameters	O	Tandem

The following table shows the tandeming and discarding of parameters in REL message when a cause value of Normal call Clearing is received.

ISUP92 -> UCP parameters in message REL

ISUP92 Parameter	Type	Action
Message type	F	Tandem
Cause indicators	V	Process
Access delivery information	O	Tandem
Access transport	O	Tandem
Automatic congestion level	O	Discard
Parameter compatibility information	O	Tandem

ISUP92 -> UCP parameters in message REL

ISUP92 Parameter	Type	Action
Redirection number restriction	O	Tandem
User-to-user information	O	Tandem
User-to-user indicators	O	Tandem
End of optional parameters	O	Tandem

Suspend/Resume Message (SUS/RES)

These messages are tandemed as shown in the following table.

ISUP92 -> UCP parameters in message RES and SUS

ISUP92 Parameter	Type	Action
Message type	F	Tandem
Suspend/Resume indicators	F	Tandem
End of optional parameters	O	Tandem

Parameter mapping for messages from UCP to ISUP92

This section shows the parameter tandeming and discarding for the messages coming on the UCP trunk and going to the ISUP92 trunk.

Reference feature document AD9067 'Support for User to User Parameter' for proper requirements when mapping of the User to User parameter is required.

Initial Address Message (IAM)

Parameter tandeming and discarding for the IAM is shown in the following table.

UCP -> ISUP92 parameters in the IAM message

UCP Parameter	Type	Action
Message Type	F	Tandem
Nature Of Connection Indicators	F	Process
Forward Call Indicators	F	Process

UCP -> ISUP92 parameters in the IAM message

UCP Parameter	Type	Action
Calling Party's Category	F	Process
User service information	F	Mapped
Called Party Number	V	Process
Calling Party Number	O	Process
Carrier Identification	O	Discard
Carrier Selection	O	Discard
Charge Number	O	Discard
Channel Assignment Map	O	Discard
Generic Address	O	Discard
Generic Digits	O	Discard
Jurisdiction Information	O	Discard
Multiple Business Group (Network Information)	O	Discard
Network Specific Facilities	O	Discard
Network-Specific IAM	O	Discard
Operator Information	O	Discard
Operator Service Indicator	O	Discard
Originating Line Information	O	Discard
Remote Operations	O	Discard
Supplementary Line Information	O	Discard
Transit network selection	O	Discard
User service information (mandatory variable length parameter in UCP protocol)	O	Process
User-to-user information	O	Tandem

UCP -> ISUP92 parameters in the IAM message

UCP Parameter	Type	Action
End of optional parameters	O	Tandem

Address Complete Message (ACM)

The following table shows the discarding and tandeming of parameters for a UCP to ISUP92ACM when the SOC NSER0003 is ON and OFCVAR field ACTIVATE_INTER_INTRA_UNANS_CALL is set to 'Y'.

UCP -> ISUP92 parameters in the ACM message

UCP Parameter	Type	Action
Message type	F	Tandem
Backward call indicators	F	Process
Call reference	O	Discard
Cause indicators	O	Tandem
Network specific facility	O	Discard
User-to-user indicators	O	Tandem
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

The following table shows the discarding and tandeming of parameters in UCP to ISUP92 ACM when SOC NSER0003 is not ON and field ACTIVATE_INTER_INTRA_UNANS_CALL in table OFCVAR is not set to 'Y'.

UCP -> ISUP92 parameters in the ACM message

UCP Parameter	Type	Action
Message type	F	Tandem
Backward call indicators	F	Process
Call reference	O	Discard
Cause indicators	O	Tandem
Network specific facility	O	Discard
User-to-user indicators	O	Tandem

UCP -> ISUP92 parameters in the ACM message

UCP Parameter	Type	Action
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

Answer Message (ANM)

Parameter tandeming and discarding for ANM message form UCP to ISUP92 are shown in the following table.

UCP -> ISUP92parameters in the ANM message

UCP Parameter	Type	Action
Message type	F	Tandem
Call reference	O	Discard
Carrier Selection	O	Discard
Internetwork Specific ANM	O	Discard
Intranetwork Specific ANM	O	Discard
Network Specific Information	O	Discard
Multiple Business Group (Network Information)	O	Discard
Operator Information	O	Discard
User-to-user indicators	O	Discard
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

Call Progress Message (CPG)

Parameter tandeming and discarding for CPG message form UCP to ISUP92 are shown in the following table.

UCP -> ISUP92 parameters in the CPG message

UCP Parameter	Type	Action
Message type	F	Tandem

UCP -> ISUP92 parameters in the CPG message

UCP Parameter	Type	Action
Event information	F	Tandem
Cause indicators	O	Discard
User-to-user indicators	O	Discard
User-to-user information	O	Tandem
End of optional parameters	O	Tandem

Continuity Test Message (COT)

Parameter tandeming and discarding for COT message form UCP to ISUP92 are shown in the following table.

UCP -> ISUP92 parameters in Message COT

UCP Parameter	Type	Action
Message type	F	Tandem
Continuity indicators	F	Tandem

Pass Along Message (PAM)

Parameter tandeming and discarding for PAM message form UCP to ISUP92 are shown in table.

UCP -> ISUP92 parameters in message PAM

UCP Parameter	Type	Action
Message type	F	Tandem

Release Message (REL)

The following table shows the tandeming and discarding of parameters in REL message when a cause value other than Normal call Clearing is received.

UCP -> ISUP92 parameters in message REL

UCP Parameter	Type	Action
Message type	F	Tandem
Cause indicators	V	Process
User-to-user information	O	Tandem
User-to-user indicators	O	Discard

UCP -> ISUP92 parameters in message REL

UCP Parameter	Type	Action
End of optional parameters	O	Tandem

The following table shows the tandeming and discarding of parameters in REL message when a cause value of Normal call Clearing is received.

UCP -> ISUP92 parameters in message REL

UCP Parameter	Type	Action
Message type	F	Tandem
Cause indicators	V	Process
User-to-user information	O	Tandem
User-to-user indicators	O	Discard
End of optional parameters	O	Tandem

Suspend/Resume Message (SUS)

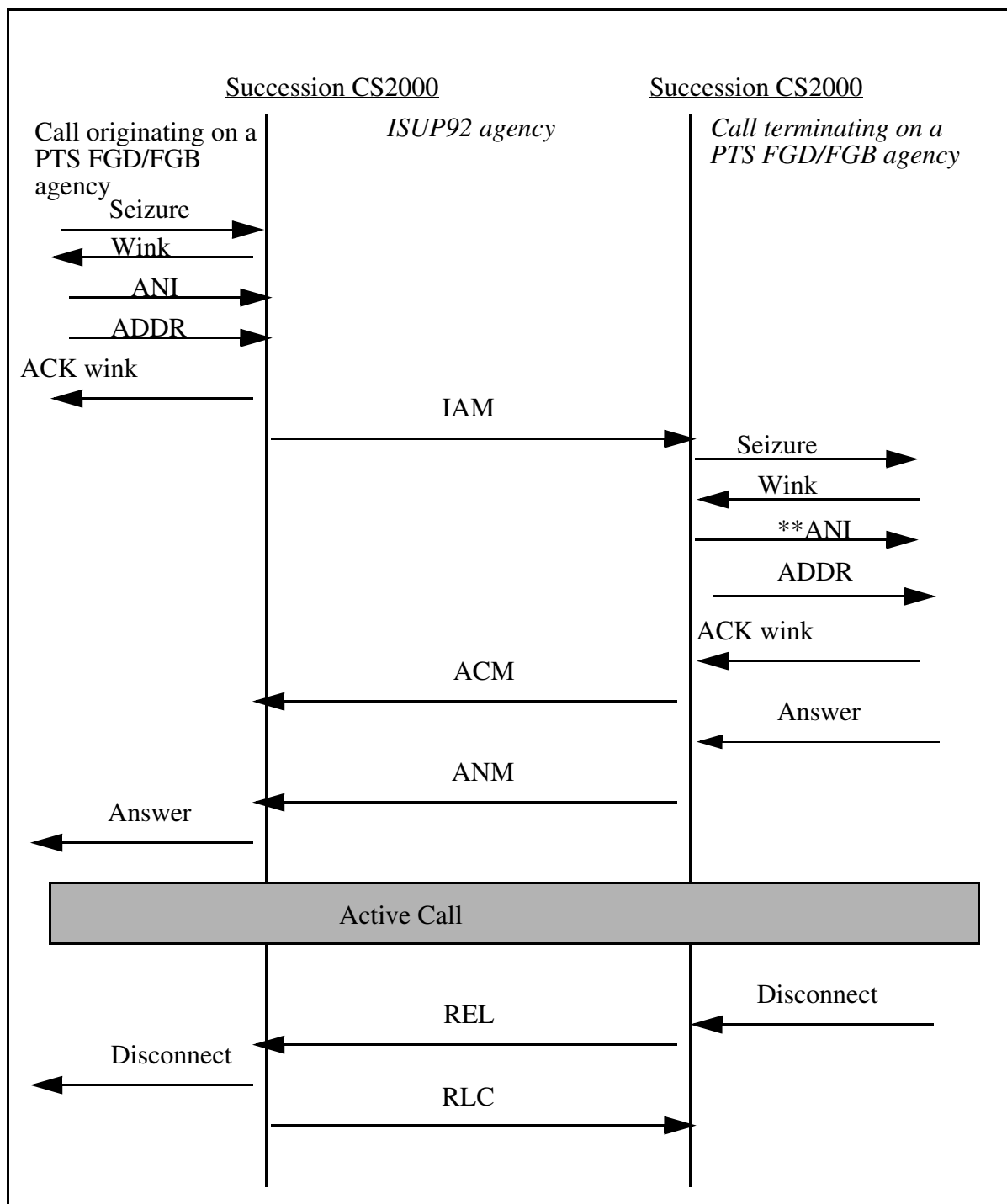
The following table shows the tandeming and discarding of parameters in SUS/RES message.

UCP -> ISUP92 parameters in message RES and SUS

UCP Parameter	Type	Action
Message type	F	Tandem
Suspend/Resume indicators	F	Tandem
End of optional parameters	O	Tandem

Appendix L: Interworking of ISUP92/Q.767 with PTS agents

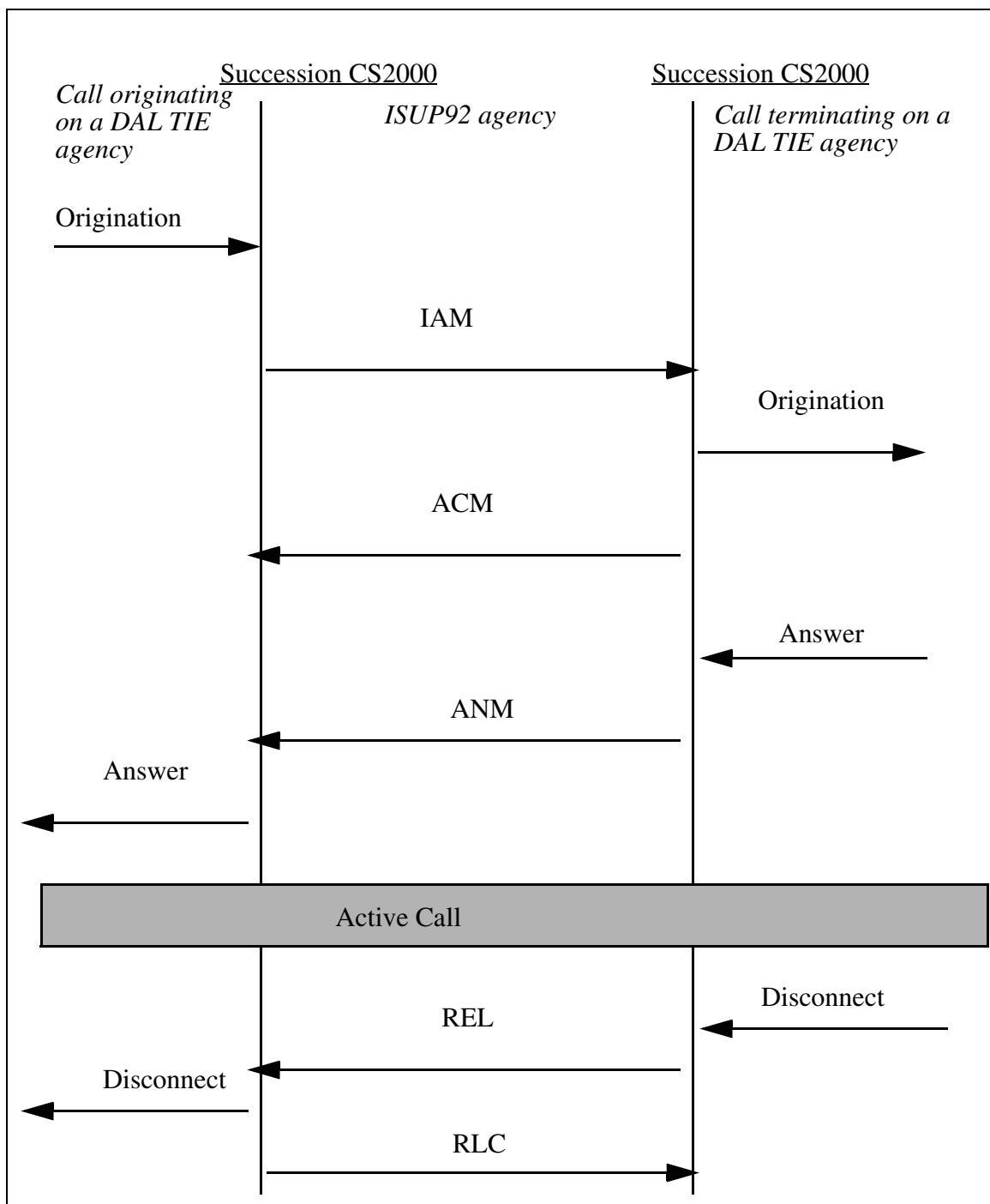
The following diagram depicts the signal flow for a call originating and terminating on an ISUP92/Q.767 agent from a PTS FGD/FGB.

Interworking between ISUP92/Q.767 and PTS FGB/FGD agent.

** In case of FGB, ANI delivery is optional.

The following diagram depicts the signal flow for a call originating and terminating on an ISUP92/Q.767 agent from a DAL TIE.

Interworking between ISUP92/Q.767 and DAL-TIE agents



The following table illustrates the message mapping between the ISUP92/Q.767 messages and the FGB/FGD messages.

ISUP92/Q.767 --> FGB/FGD messages mapping

ISUP92/Q.767 Message	FGB/FGD Message
IAM	Seized message is sent and wink is received after address digits are outpulsed
SAM	**
ACM	--
ANM	Answer message is received.
REL	On-Hook message is received
RLC	--

*** If Overlap sending is allowed, then Seized message is sent to DAL TIE only after SAM is received.*

The following table explain the mappings between the ISUP92/Q.767 messages and the corresponding DAL TIE messages.

ISUP92/Q.767 --> DAL TIE message mapping

Messages	DAL TIE messages
IAM	Seized message is sent and wink is received.
SAM	**
ACM	---
ANM	Answer message is received
REL	On-hook message is received
RLC	---

*** If Overlap sending is allowed, then Seized message is sent to DAL TIE only after SAM is received*

For PTS originations and ISUP92/Q.767 terminations, the default values of parameters in IAM are given below.

PTS-> ISUP92/Q.767, value of ISUP Parameter 'Called Party Number' in IAM

ISUP Parameter Field	ISUP value
Nature of Address	National number (0000011) ^a
Numbering Plan Indicator	ISDN (telephony) Numbering Plan (Recommendation E.164) (001)
Odd/Even Indicator	odd (1)- if odd number of digits in the called party, even (0)-if even number of digits in called party

a. The value of this parameter depends on the translation system used in the call.

PTS-> ISUP92/Q.767, value of ISUP Parameter 'Nature of Connection Indicators' in IAM

ISUP Parameter Field	ISUP value
Satellite Indicator	Datafill dependant ^a
Continuity Check Indicator	Datafill dependent ^b
Echo Control Device Indicator	Datafill dependent

a. The value of this field depends on the SAT field of table TRKSGRP

b. The value of this field depends on the CONTCHK field of table TRKSGRP

PTS-> ISUP92/Q.767, values for ISUP Parameter 'Forward Call Indicator' in IAM

ISUP Parameter Field	ISUP value
National / International Call Indicator	Call to be treated as National (0)
End to End Method Indicator	No end to end method available(00)
Interworking Indicator	Interworking encountered (1)
End to End Information Indicator	No end to end information available (0)
ISDN User Part Indicator	ISDN User part not used all the way (0)
ISDN User Part Preference Indicator	ISDN user part not required all the way (01)
ISDN Access Indicator	Originating access non-ISDN (0)

PTS-> ISUP92/Q.767, values for ISUP Parameter 'Forward Call Indicator' in IAM

ISUP Parameter Field	ISUP value
Trans_called_Num_Ind	Number_Not_Translated
Routing_attempt_Ind	No_routing_attempt(0000000)

PTS-> ISUP92/Q.767, values for ISUP Parameter 'Calling Party Category' in IAM

ISUP Parameter Field	ISUP value
Calling Party Category	ordinary subscriber (00001010)

Default values for ISUP Parameter 'Transmission Medium Requirement' in ISUP92/Q.767 IAM

ISUP Parameter Field	ISUP value
Transmission Medium Requirement	3.1 Khz audio(00000011) ^a

a. The value of this field depends upon the BCNAME field of table TRKGRP.

Default values User Service Information parameter in IAM

ISUP Parameter Field	ISUP value
Coding standards	CCITT (00)
Information transfer rate	64_KBits/S (10000)
Information transfer mode	Circuit mode (00)
Information transfer capability	3.1Khz Audio (10000)
Layer1 Identification	Layer1_G711_ALaw(00011)
User Rate	User Rate Nil(00000)
Synchronization	Synchrone(0)
Negotiation	Negot_not_inband(0)

The default values of BCI in ACM is given below for ISUP92/Q.767 to PTS interworking.

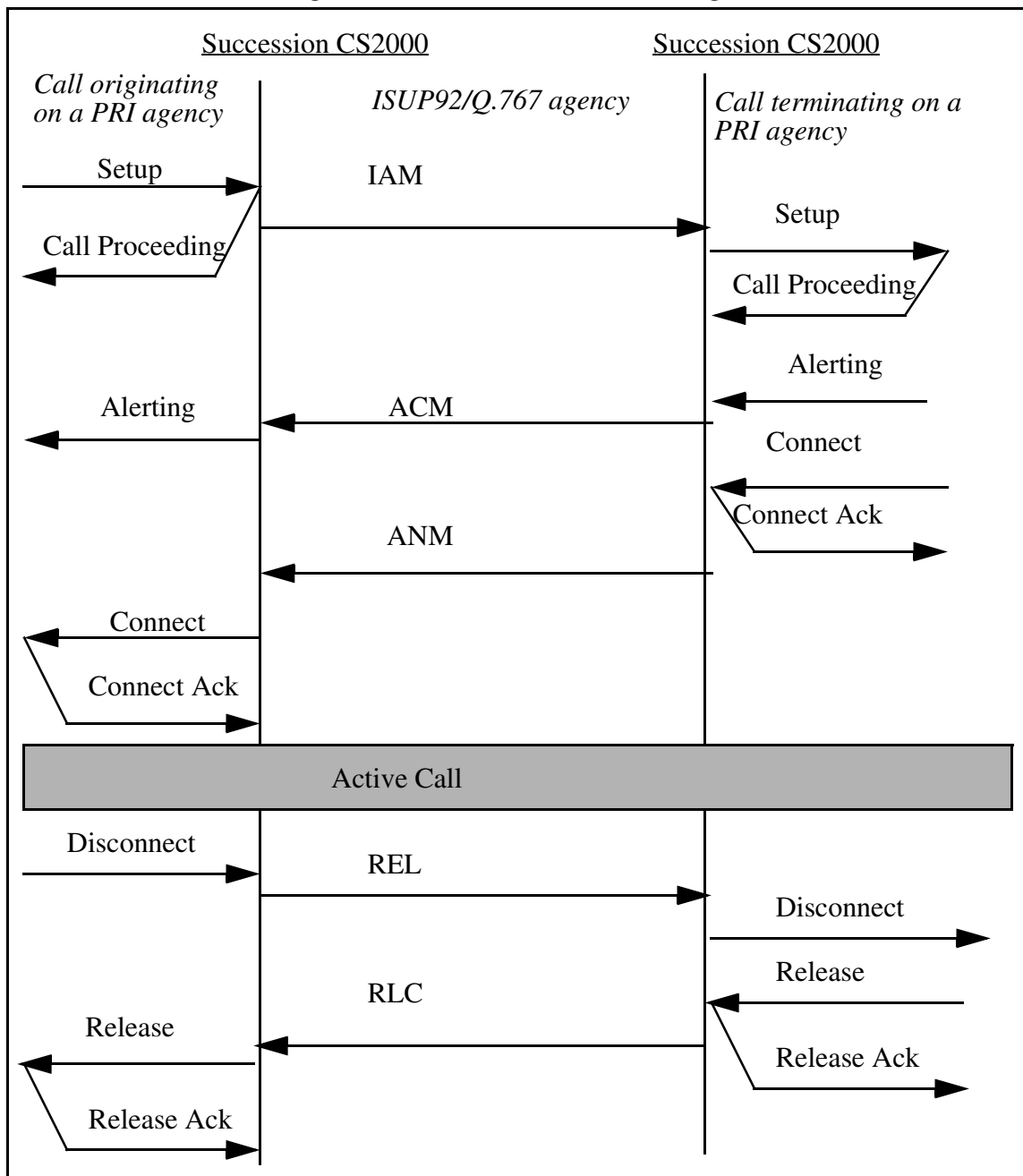
Default BCI field values in ACM for ISUP92/Q.767 origination and PTS termination.

Field name	Default value
Charge Indicator	10 "Charge"
Called party's status	No indication (00)
Called party's category	No indication (00)
End-End_Method indicator	No end-end method available (00)
Interworking indicator	Interworking encountered (1)
End-End information Indicator	No end to end information available (0)
ISUP indicator	ISUP not used all the way (0)
Holding indicator	Holding not requested (0)
ISDN access indicator	terminating access non ISDN (0)
Echo control device indicator	incoming half echo control device not included (0)
SCCP method indicator	No SCCP indication (00)

Appendix N: Interworking between ISUP92/Q.767 and UCS PRI

The following message sequence diagram depicts the signal flow for a call originating from and terminating on a ISUP92 agent from a PRI agent.

Interworking Between ISUP92/Q.767 and PRI Agents



The following table illustrates the message mapping between the isup92/q767 messages and the corresponding PRI messages:

UCS PRI to ISUP92/Q767 Message Mapping^a

UCS PRI Messages	ISUP Messages
ALERTING*	ACM
CONNECT	CON (if ACM has not been sent) ANM (if ACM has been sent)
DISCONNECT	REL
PROGRESS*	ACM
RELEASE	REL
RELEASE COMPLETE	REL
RESTART	REL
SETUP	IAM
* If ALERT is received, interworking indicator of BCI in ACM is set to 'no interworking encountered'. If PROGRESS is received, it is set to 'interworking encountered'.	

a. The ISDNXFER option of table TRKGRP for terminating ISUP agency controls the support of ISDN services, when the originating agency is a PRI trunk. It is recommended to use this option when the entire call path is predetermined to be all the way ISDN user part (all the way ISDN and SS7). If the entire call path is not ISUP all the way, then this option need not be selected. This way, we can avoid unwanted packets (ISDN options which carry services) to be sent over the network.

ISUP92/Q.767 to UCS PRI Message Mapping

ISUP Messages	UCS PRI Messages
ACM	ALERT (if Backward Call Indicator bit is set to 'no interworking encountered') PROGRESS (if Backward Call Indicator bit is set to 'interworking encountered')
ANM	CONNECT
IAM	SETUP
REL	DISCONNECT

ISUP92/Q.767 and UCS PRI Message Mapping

Mapping of SETUP message to IAM message

UCS PRI IEs	ISUP parameter
Bearer Capability (M)	User Service Info/Transmission Medium Requirement
Called Party Number (M)	Called Party Number
Called Party Subaddress (O)	Access Transport*
Calling Party Number (O)	Calling Party Number
Calling Party Subaddress (O)	Access Transport*
Low Layer Compatibility (O)	Access Transport*
High Layer Compatibility (O)	Access Transport*
Progress Indicator (O)	Forward Call Indicators
User to User (O)	User to User Info
* The IAM Message contains a maximum of one Access Transport parameter, containing UCS PRI IEs as required. The ATP mapping is subject to the datafill in Table ISDNPARM.	

Mapping of IAM -> SETUP

ISUP parameter	UCS PRI IEs
Transmission Medium Requirement (V)	Bearer Capability
User Service Information (O)	Bearer Capability
Called Party Number (V)	Called Party Number
Access Transport (O)	*
Calling Party Number (O)	Calling Party Number
Forward Call Indicators (F)	Progress Indicator
User to User Info (O)	User to User Info
* Access Transport parameter contains one or more of: HLC, LLC, Called Party Subaddress, Calling Party subaddress, Display, Facility. These are inserted in the setup message in accordance with UCS PRI encoding rules.	

Mapping of ALERT -> ACM^a

UCS PRI IEs	ISUP parameter
Progress Indicator (O)	No Mapping
User to User Info(O)	User to User Info

a. If an ALERT message is received, an ACM with BCI set to 'no interworking required' and 'ISUP all the way' is sent on the ISUP side.

Mapping of PROGRESS -> ACM^a

UCS PRI IEs	ISUP parameter
Progress Indicator (F)	No Mapping

a. If an PROGRESS message is received, an ACM with BCI set to 'interworking required' and 'Not ISUP all the way' is sent on the ISUP side.

Mapping of ACM -> ALERT / PROGRESS

ISUP parameter	UCS PRI IEs
Backward Call Indicators (F)	No Mapping
User to User Info (O)*	User to User Info
* UUI mapping happens only for the case of ACM to ALERT. This is because UUI mapping is defined only for non-interworking scenarios.	

Mapping of CONNECT -> ANM/CON

UCS PRI IEs	ISUP parameter
User to User Info(O)	User to User Info

Mapping of ANM/CON -> CONNECT

ISUP parameter	UCS PRI IEs
User to User Info (O)*	User to User Info

Mapping of DISCONNECT -> REL

UCS PRI IEs	ISUP parameter
Cause (V) * ^a	Cause Indicator
User to User Info(O)	User to User Info
*Mandatory in the first call clearing message.	

a. If the Cause Indicator Parameter has a Cause Value other than CI_NORMAL_CLEARING or if the call goes to Treatment then the tables TMTMAP and CSEMAP are used and the mappings are done as per the datafill in these Tables.

Mapping of RELEASE / RELEASE COMPLETE -> REL

UCS PRI IEs	ISUP parameter
Cause (O) * ^a	Cause Indicator
User to User Info(O)	User to User Info

Mapping of RELEASE / RELEASE COMPLETE -> REL

UCS PRI IEs	ISUP parameter
* Mandatory in the first call clearing message.	

a. If the Cause Indicator Parameter has a Cause Value other than CI_NORMAL_CLEARING or if the call goes to Treatment then the tables TMTMAP and CSEMAP are used and the mappings are done as per the datafill in these Tables.

Mapping of REL -> DISCONNECT

ISUP parameter	UCS PRI IEs
Cause Indicator (V) ^a	Cause

a. If the Cause Indicator Parameter has a Cause Value other than CI_NORMAL_CLEARING or if the call goes to Treatment then the tables TMTMAP and CSEMAP are used and the mappings are done as per the datafill in these Tables.

Note: Reference feature document AD9067 'Support for User to User Parameter' for proper datafill requirements when mapping of the User to User parameter is required.

Information Elements and Parameters Mapping**Bearer Capability <-> User Service Info**

The following mapping for Bearer Capability and User Service Information is based on different call scenarios. It is not mapped octet by octet since some octet contents may affect the other octet's existence.

56K Data⁴² Call:**ISUP92/Q.767 USI -> UCS PRI BC**

ISUP User Service Info	PRI Bearer Capability
Octet 1, Coding Standard 00 CCITT	Octet 3, Coding Standard 00 CCITT
Octet 1 Information Transfer Capability^a 01000 unrestricted digital info	Octet 3, Information Transfer Capability 01000 unrestricted digital info
Octet 2, Transfer Mode 00 Circuit Mode	Octet 4, Transfer Mode 00 Circuit Mode
Octet 2, Information Transfer Rate 10000 64 kbits/s	Octet 4, Information Transfer Rate 10000 64 kbits/s

ISUP92/Q.767 USI -> UCS PRI BC

ISUP User Service Info	PRI Bearer Capability
Octet 3, User Information layer 1 protocol 00001 Layer 1 Rate Adaption	Octet 5, Bearer Capability Multiplier 00001 CCITT Standardized rate adaption
Octet 3a, User Rate 01111 56kbts/s	Octet 5a, Access Data Rate 01111 56kbts/s

a. For all calls Bearer capability screening is done. This is to ensure that unsupported BC values are not sent on any trunk. Refer to feature AD9582 for details on Bearer capability screening.

ISUP92/Q.767 TMR -> UCS PRI BC

ISUP Transmission Medium Requirement	PRI Bearer Capability
00000010 unrestricted digital info	Information Transfer Capability: 01000 unrestricted digital info.

UCS PRI BC -> ISUP92/Q.767 USI

PRI Bearer Capability	ISUP User Service Info
Octet 3, Coding Standard 00 CCITT	Octet 1, Coding Standard 00 CCITT
Octet 3, Information Transfer Capability 01000 unrestricted digital info.	Octet 1 Information Transfer Capability 01000 unrestricted digital info
Octet 4, Transfer Mode 00 Circuit Mode	Octet 2, Transfer Mode 00 Circuit Mode
Octet 4, Information Transfer Rate 10000 64 kbts/s	Octet 2, Information Transfer Rate 10000 64 kbts/s
Octet 5, Bearer Capability Multiplier 00001 CCITT Standardized rate adaption	Octet 3, User Information layer 1 protocol 00001 Layer 1 Rate Adaption

42. A call is termed as a Data Call if the Transmission Medium Requirement is 64 Kbps Unrestricted. If the User rate is 56kbts/s then it is a 56K Data Call. If there is no user rate then it is a 64kbts/s Data Call.

UCS PRI BC -> ISUP92/Q.767 USI

PRI Bearer Capability	ISUP User Service Info
Octet 5a, Access Data Rate 01111 56kbits/s	Octet 3a, User Rate 01111 56kbits/s

UCS PRI BC -> ISUP92/Q.767 TMR

PRI Bearer Capability	ISUP92/Q.767 Transmission Medium Requirement
Octet 3, Information Transfer Capability 01000 unrestricted digital info. 01001 restricted digital info	00000010 unrestricted digital info 00000010 unrestricted digital info

64K Data Call**ISUP92/Q.767 USI -> UCS PRI BC**

ISUP User Service Info	PRI Bearer Capability
Octet 1, Coding Standard 00 CCITT	Octet 3, Coding Standard 00 CCITT
Octet 1 Information Transfer Capability 01000 unrestricted digital info	Octet 3, Information Transfer Capability 01000 unrestricted digital info.
Octet 2, Transfer Mode 00 Circuit Mode	Octet 4, Transfer Mode 00 Circuit Mode
Octet 2, Information Transfer Rate 10000 64 kbits/s	Octet 4, Information Transfer Rate 10000 64 kbits/s

ISUP92/Q.767 TMR -> UCS PRI BC

ISUP Transmission Medium Requirement	PRI Bearer Capability
00000010 unrestricted digital info	Information Transfer Capability: 01000 unrestricted digital info.

UCS PRI BC -> ISUP92/Q.767 USI

PRI Bearer Capability	ISUP User Service Info
Octet 3, Coding Standard 00 CCITT	Octet 1, Coding Standard 00 CCITT
Octet 3, Information Transfer Capability 01000 unrestricted digital info.	Octet 1 Information Transfer Capability 01000 unrestricted digital info
Octet 4, Transfer Mode 00 Circuit Mode	Octet 2, Transfer Mode 00 Circuit Mode
Octet 4, Information Transfer Rate 10000 64 kbits/s	Octet 2, Information Transfer Rate 10000 64 kbits/s

UCS PRI BC -> ISUP92/Q.767 TMR

PRI Bearer Capability	ISUP Transmission Medium Requirement
Octet 3, Information Transfer Capability 01000 unrestricted digital info.	00000010 unrestricted digital info

Voice Call⁴³**ISUP92/Q.767 USI -> UCS PRI BC**

ISUP User Service Info	PRI Bearer Capability
Octet 1, Coding Standard 00 CCITT	Octet 3, Coding Standard 00 CCITT
Octet 1 Information Transfer Capability 00000 Speech 10000 3.1Khz audio	Octet 3, Information Transfer Capability Based on the TMR Value
Octet 2, Transfer Mode 00 Circuit Mode	Octet 4, Transfer Mode 00 Circuit Mode
Octet 2, Information Transfer Rate 10000 64 kbits/s	Octet 4, Information Transfer Rate 10000 64 kbits/s

ISUP92/Q.767 USI -> UCS PRI BC

ISUP User Service Info	PRI Bearer Capability
Octet 3, User Information layer 1 protocol 00010 Recommendation G.711 A-law	Octet 5, User Information Layer 1 Protocol 00010 Recommendation G.711 Mu-law Speech

ISUP92/Q.767 TMR -> UCS PRI BC

ISUP Transmission Medium Requirement	PRI Bearer Capability
00000000 Speech 00000011 3.1KHz Audio	Octet 3, Information Transfer Capability 00000 Speech 10000 3.1Khz audio

UCS PRI BC -> ISUP92/Q.767 USI

PRI Bearer Capability	ISUP User Service Info
Octet 3, Coding Standard 00 CCITT	Octet 1, Coding Standard 00 CCITT
Octet 3, Information Transfer Capability^a 00000 Speech 10000 3.1KHz Audio	Octet 1 Information Transfer Capability 00000 Speech 10000 3.1KHz Audio
Octet 4, Transfer Mode 00 Circuit Mode	Octet 2, Transfer Mode 00 Circuit Mode
Octet 4, Information Transfer Rate 10000 64 kbits/s	Octet 2, Information Transfer Rate 10000 64 kbits/s
Octet 5, User Information Layer 1 Protocol 00010 Recommendation G.711 Mu-law Speech	Octet 3, User Information layer 1 protocol 00011 Recommendation G.711 A-law

a. In order to ensure the PRI bearer compatibility information is properly propagated to the terminating gateway IMT, the ISDNXFER option should be provisioned on the terminating ISUP trunk.

43. A Call is termed as a voice call if the TMR is either 3.1 Khz Audio or Speech.

UCS PRI BC -> ISUP92/Q.767 TMR

PRI Bearer Capability	ISUP Transmission Medium Requirement
Octet 3, Information Transfer Capability	
00000 speech	00000000 speech
10000 3.1KHz Audio	00000011 3.1KHz Audio

Default Values of ISUP Backward Call Indicator**Default Values of ISUP Backward Call Indicator**

ISUP Backward Call Indicator
Charge Indicator - Charge
Called Party Status Indicator - Subscriber Free
Called Party Category - Ordinary Subscriber
End To End Method - No End To End Method Available
Interworking Indicator- Depends on the Backward Message from PRI (See <i>Note 1</i>)
End To End Information Indicator- No End To End Information Available
ISUP Indicator - Depends on the Backward Message from PRI (See <i>Note 1</i>)
Reverse Holding Indicator -Not Required
ISDN Access Indicator - Access ISDN
Echo Control Device Indicator - Echo Control Device Not Included
SCCP Method Indicator - Connection less and Connection Oriented Methods Available
Note 1: If an ALERTING message comes from the PRI side, the Interworking Indicator in the BCI is set to 'No interworking' and the ISUP Indicator is set to 'ISUP all the way'. If an PROGRESS message comes from the PRI side, the Interworking Indicator in the BCI is set to 'Interworking encountered' the ISUP Indicator is set to 'Not ISUP all the way'.

UCS PRI Calling Party Number -> ISUP92/Q.767 Calling Party Number¹
UCS PRI Calling Party Number <-> ISUP92/Q.767 CPN

UCS PRI CPN	ISUP CPN
Type of Address, Octet 3 001 International Number 010 National Number	Nature of Address, Octet 1 0000100 International Number 0000100 International Number
Numbering Plan Identification, octet 3 0001 ISDN/Telephony numbering plan others	Numbering Plan Indicator, Octet 2 001 ISDN/Telephony Numbering Plan 001 ISDN/Telephony Numbering Plan
Presentation Indicator, Octet 3a 00 Presentation allowed 01 Presentation restricted 10 Number not available due to interworking	Address presentation, octet 2 00 presentation allowed 01 presentation restricted 00 presentation allowed
Screening Indicator, Octet 3a* 11 network provided others	Screening Indicator, Octet 2 11 network provided CPN discarded*
* If CPN is received with Screening Indicator as “User provided, not screened(00)”, “user provided, verified and passed(01)” or “user provided, verified and failed(10)”, then CPN is not mapped.	

1. The ISDNXFER option of table TRKGRP for terminating ISUP trunk is required to be present for the delivery of CPN when the originating agency is a PRI trunk. Otherwise the CPN parameter is not sent in the outgoing IAM.

ISUP92/Q767 CPN -> UCS PRI CPN**ISUP92/Q.767 CPN -> UCS PRI CPN**

ISUP CPN	UCS PRI CPN
Nature of Address, Octet 1 0000100 International Number	Type of Address, Octet 3 001 International Number
Incomplete Indicator(NI), Octet 2 0 Complete 1 Incomplete	Not mapped. CPN discarded.
Numbering Plan Indicator, Octet 2 001 ISDN/Telephony Numbering Plan	Numbering Plan Identification, octet 3 0001 ISDN/Telephony numbering plan
Address presentation, octet 2 00 presentation allowed 01 presentation restricted others	Presentation Indicator, Octet 3a 00 Presentation allowed 01 Presentation restricted 01 Presentation restricted
Screening Indicator, Octet 2 01 User provided, verified and passed 11 Network provided others	Screening Indicator, Octet 3a* 01 User provided, verified and passed 11 Network provided 00 User provided, not screened

ISUP92/Q.767 Cause Indicator -> UCS PRI Cause**ISUP92/Q.767 Cause Indicator <-> UCS PRI Cause Indicator**

ISUP Cause	UCS PRI Cause
Location, Octet 1 0111 International Network	Location, Octet 3 Based on Location field of TRKSGRP datafill.
Coding Standard, Octet 1 00 CCITT standard (Default)	Coding Standard, Octet 3 00 CCITT standard (Default)
Diagnostics, Octet 3-n Not mapped	Diagnostics, Octet 5-5b Not mapped

If the Cause Indicator Parameter has a Cause Value other than CI_NORMAL_CLEARING or if the call goes to Treatment then the tables TMTMAP (Treatment to Cause Mapping) and CSEMAP (Cause to Treatment mapping) are used and the mappings are done as per the datafill in these Tables.

UCS PRI Cause -> ISUP92/Q.767 Cause Indicator**UCS PRI Cause <-> ISUP92/Q.767 Cause Indicator**

PRI Cause	ISUP Cause Indicator
Location, Octet 1 0000 User 0001 Local Private Network 0010 Local Network 0011 Transit Network (Default) 0100 Public network serving the remote user 0101 Private Network serving the remote user 0111 International Network	Location, Octet 3 0111 International Network
Coding Standard, Octet 1 00 CCITT standard (Default) 10 National standard	Coding Standard, Octet 3 00 CCITT standard (Default)
Diagnostics, Octet 3-n Not mapped	Diagnostics, Octet 5-5b Not mapped

ISUP Forward Call Indicator <-> UCS PRI Progress Indicator

ISUP Forward Call Indicator	PRI Progress Indicator
Interworking indicator Interworking encountered	Progress Description^a Call is not end to end ISDN

a. If there is no Progress Indicator then the Interworking indicator of ISUP FCI is set to the default value of 'No Interworking Encountered'

Default values of Forward Call Indicator¹

ISUP Forward Call Indicator
National/International call indicator - Dependent on call type
End to end method indicator - No end to end method available
Interworking indicator - No Interworking encountered
End to end information indicator - No end to end information available

Default values of Forward Call Indicator¹

ISUP Forward Call Indicator
ISDN user part indicator- ISDN user part used all the way
ISDN user part preference indicator- ISDN user part preferred all the way
ISDN access indicator - Originating access ISDN
SCCP method indicator - No indication

1. The ISDNXFER option of table TRKGRP for terminating ISUP trunk is required to be present for the support of ISDN services, when the originating agency is a PRI trunk. Otherwise the PRA-ISUP call supports only the mandatory parameters and the FCI is sent as per the table below.

Default values of Forward Call Indicator

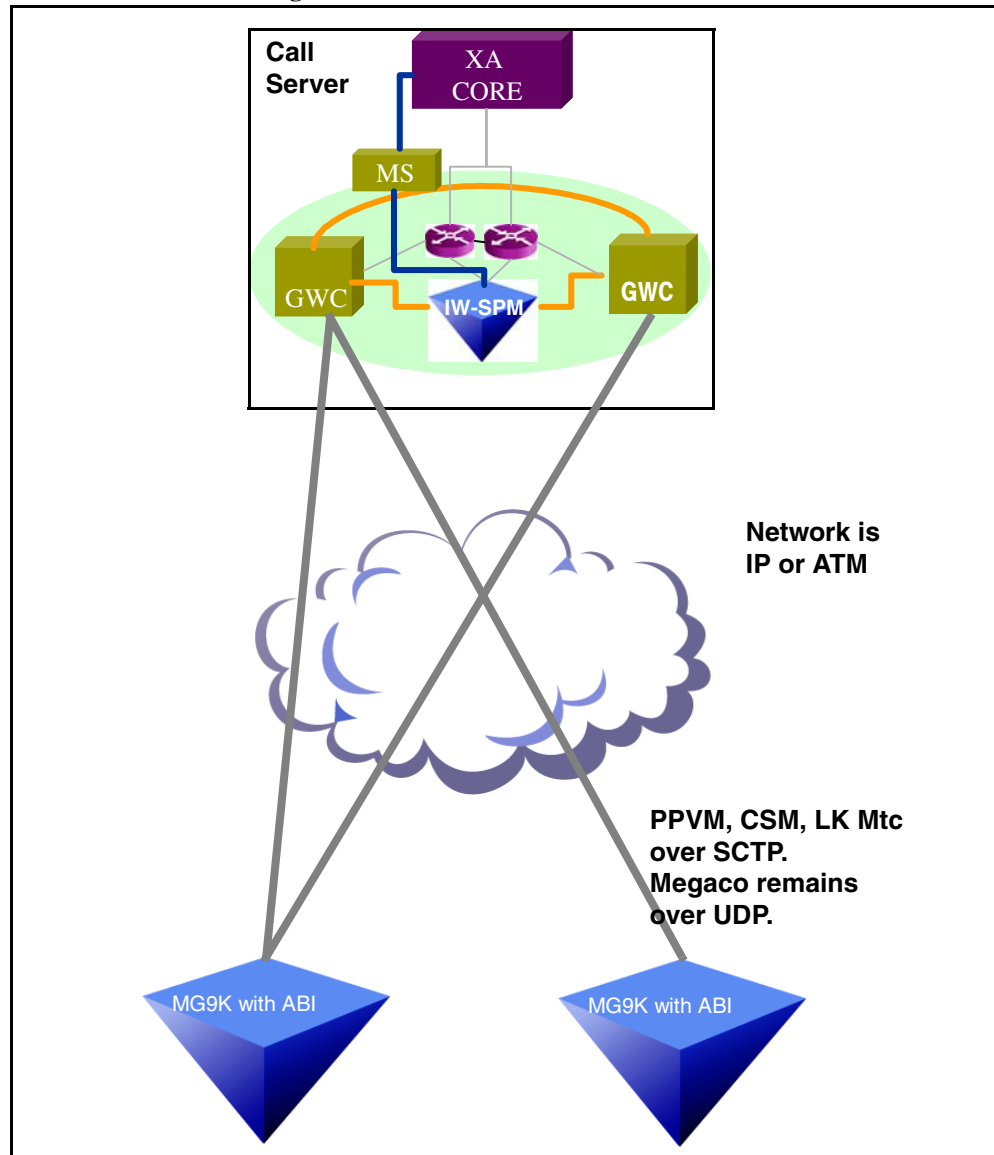
ISUP Forward Call Indicator
National/International call indicator - Dependent on call type
End to end method indicator - No end to end method available
Interworking indicator - Interworking encountered
End to end information indicator - No end to end information available
ISDN user part indicator- ISDN user part not used all the way
ISDN user part preference indicator- ISDN user part not required
ISDN access indicator - Originating access non ISDN
SCCP method indicator - No indication

Product = CS 2000**A00003767 -- IP ABI PPVM Robustness & Msg Loss Alarms (UA-IP)*****Functional Description***

This activity introduces SCTP (Stream Control Transmission Protocol) for messaging transport between a Succession GWC (gateway controller) and MG9K ABI (DS-512) cards. SCTP is used for three of the Nortel proprietary

protocols: PPVM (XPM supervision), CSM (Channel Supervision Message), and DS-512 link maintenance.

Functional Behavior Diagram



SCTP is introduced here to provide the customer with a more reliable messaging link between the GWC and ABI cards compared with the existing UDP transport. SCTP is supported on both the IP and ATM network fabrics.

SCTP provides the ability to retransmit lost messages and to ensure that the messages arrive in order. Additionally, SCTP provides alarms when message retransmits or loss get high or when a messaging link is lost. This provides the customer with the ability to find and solve network messaging problems quickly.

SCTP seamlessly and automatically upgrades and downgrades in a customer installation. The customer is not required to provide any configuration information.

When both the GWC and ABI network components are upgraded to SN07, the components will discover that they both support SCTP and will start using SCTP. If only one or neither component supports SCTP, then the existing UDP protocol will continue to be used.

Hardware Requirements or Dependencies

This activity is compatible with existing GWC and ABI hardware, including ABI hardware introduced in SN07.

Software Requirements or Dependencies

Requires gateway controller software loads of GC070 or higher.

Requires DMS-100 core loads of SNNCSH07 or higher.

Requires ABI loads of SN07 or higher.

Limitations and restrictions

None

Interactions

None

Applicable customer facing sections

Fault Management

Logs ☒

Alarms ☒

Configuration

Data Schema ☒

User Interface ☒

Element Management ☐

Security ☐

Service Order ☐

Office Parameters ☐

Accounting (includes AMA billing) ☐

Performance (includes operational measurements) ☒

Glossary

Term	Description
SCTP	Stream Control Transmission Protocol

Fault Management for A00003767

Fault management strategy

Three new alarms are introduced by this activity. These alarms are associated with ABI host XPMs and allow the customer to quickly isolate network messaging issues from other causes of XPM c-side busy.

As with other XPM faults, these alarms affect the DMS alarm banner, show up as an InService TrouBle (ISTB) reason for the applicable ABI XPM, and generate a log message.

Fault management tools and utilities

No new tools are introduced. These alarms look like other ISTB reasons on any XPM.

Logs

Explanation

Log Title: PM181

Name: PM181

Description: PM181 logs are existing DMS logs and are used extensively by the GWC in a Succession configuration. This activity extends the use of the PM181 log for Succession. When an ABI messaging alarm (described later) is set or cleared, a PM181 log is reported.

Event type: critical, major or minor depending on the alarm that is generating the log.

Format

Format of the PM181 log has not been changed beyond the formats already in used by the GWC. Information on the GWC use of PM181 can be found in NN10090-911. The following new strings are used. Strings 1, 2 & 3 are concatenated together to form the complete string:

New PM181 Log strings

String 1	String 2	String 3
ABI external messaging alarm	Links Down - Severely degraded - Degraded -	Alarm set Alarm cleared

Field descriptions

Unchanged.

Action

An associated alarm is also raised. Please refer to the alarm descriptions below for operating company actions.

Associated Operational Measurements or Performance Measurements

Not applicable

Additional information

Alarm set **Associated alarm message: ABI external messaging alarm Links Down - Alarm Set (or Alarm cleared)**

Severity: Critical; Service Outage

Cause: The messaging links between the ABI card associated with the XPM and the GWC which the XPM subtends have gone down. This causes a service outage of the XPM and all its subtending peripherals (ESA may be in effect).

The problem is somewhere between the ABI cards hosting the XPM and the GWC which the XPM subtends.

Action: Need to isolate the network component experiencing the problem. If the problem lies as a transitory problem in a network component, the messaging links may recover autonomously.

Any network component used in the messaging path could cause a messaging disruption. The GWC and XPMs are very probably fine. The following are some likely causes (but not all) of the messaging disruptions and the operator should check to ensure that components are operating normally:

- MG9K ABI card failed or was pulled and not taken out service first
- MG9K OC3 cards taken out of service
- MG9K active OC3 card failed or was pulled and not taken out service first

- Fiber links on MG9K ABI or active OC3 card pulled or failed
- Shelf controller for associated GWC failed, or taken out of service
- Network router failed or taken out of service with no alternative path for packets
- Configuration of router(s) changed so packets can't get through
- Cables to router(s) failed.
- No Single point of failure, but network message loss is so high that a messaging link can not be sustained (would probably have seen the minor and major alarms earlier).

The alarm is cleared when the message link is re-established, or by MANBSY'ing the XPM, or a DMS core reload restart.

Interfaces: DMS Core Alarm

Associated alarm message: ABI external messaging alarm Severely Degraded - Alarm Set (or Alarm cleared)

Severity: Major, service affecting

Cause: Message loss in the network has reached a point where calls may be sporadically starting to fail, loading and RTS'ing peripheral may fail.

The problem is somewhere between the ABI cards hosting the XPM and the GWC which the XPM subtends.

Action: Need to isolate the network component experiencing the problem. If the problem lies as a transitory problem in a network component, the messaging links may recover autonomously.

Any network component used in the messaging path could cause a messaging disruption. The GWC and XPMs are very probably fine. The following are some likely causes (but not all) of the messaging disruptions and the operator should check to ensure that components are operating normally:

- MG9K ABI cards in overload
- MG9K OC3 cards in overload
- Shelf controller for associated GWC in overload
- Network router(s) in overload
- Configuration of router(s) changed so there is not sufficient bandwidth

The potential for call failures is high in this state, to the network operator should recover the immediate cause. Additionally, the customer's network

operations may want to closely monitor the system and decide if further network capacity is required.

The alarm is cleared when the message link message loss decreases, the critical alarms is raised or by MANBSY'ing the XPM, or a DMS core reload restart.

Interfaces: DMS Core Alarm

Associated alarm message: ABI external messaging alarm Degraded - Alarm Set (or Alarm cleared)

Severity: Minor - potential to affect service

Cause: Message retransmission in the network has reached a point where the occasional call fails due to increased latency.

The problem is somewhere between the ABI cards hosting the XPM and the GWC which the XPM subtends. Messages are being lost, but the system is able to recover with message retransmissions. However, if this situation continues to escalate, eventually unrecoverable message loss will occur.

Action: Need to isolate the network component experiencing the problem. If the problem lies as a transitory problem in a network component, the messaging links may recover autonomously. The network engineering group should be given the collected information to determine if further network build-out or tweaking of network parameters is required.

Any network component used in the messaging path could cause a messaging disruption. The GWC and XPMs are very probably fine. The following are some likely causes (but not all) of the messaging disruptions and the operator should check to ensure that components are operating normally:

- MG9K ABI cards in overload
- MG9K OC3 cards in overload
- Shelf controller for associated GWC in overload
- Network router(s) in overload
- Configuration of router(s) changed so there is not sufficient bandwidth

The alarm is cleared when the message link message loss decreases, the critical or major alarm is raised or by MANBSY'ing the XPM, or a DMS core reload restart.

Interfaces: DMS Core Alarm

Related documentation

The MG9K ABI cards will also be generating similar alarms. The information for the new alarms at the MG9K element manager can be found in activity A0003571 documentation.

Configuration for A00003767

Hardware and Software Requirements

NA

Initial Configuration

NA

Office/Subnet parameters (OP/SP) (CM & SESM)

NA

Upgrade Impact

NA

Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
NORTEL-UEMG-RELMMSGING-MIB	NEW	

Table/MIB/Remote Database Schema information

Name: NORTEL-UEMG-RELMMSGING-MIB

Nortel-UEMG-Reliable Messaging- MIB

Functional description

The MIB has four sections

- Association general info - This contains basic information for an association, most of it will only ever be read, but it contains some thresholds for the alarms which in the future functionality could be added to change these values.

- Current OMs - Counts for the sample of OM data which is currently being collected. These OMs will give information to current health of the association and can be used to diagnose problems as they occur.
- Interval OMs - Historical samples of the OMs that have been collected. Each sample is for a 15 minute period and will retain the last 96 of these samples. These OMs can be used to help diagnose problems that occurred in the past.
- Alarms - If a threshold is crossed or the association fails/recovers an alarm will be raised or cleared. The MIB contains the data which will be contained in the alarm.

Size

One instance of the MIB will exist for each SCTP association on an ABI card.

Fields/OIDs

Refer to the following table.

MIB definitions

MIB Table	Entry	Subfield or refinement	values	Explanation and action
nnRelMsgSctpAssocTable The association information table which contains an entry for each association	NnRelMsgSctpAssocEntry An individual entry into the nnRelMsgSctpAssocTable	nnRelMsgSctpAssocId	Unsigned 32 bit	A numerical representation of an association
		nnRelMsgSctpAssocRemHostName	Octet String	The IP address of the farend of the SCTP association.
		nnRelMsgSctpAssocRemHostPort	Unsigned 32 bit	The IP port number of the farend for which the association was setup to.
		nnRelMsgSctpAssocLocalPort	Unsigned 32 bit	The IP port number on the ABI for the association
		nnRelMsgSctpAssocEntPhysIndex	Unsigned 32 bit	The numerical representation for the frame, shelf, and slot of the ABI which the association exists on
		nnRelMsgSctpAssocState	Integer closed (1), cookieWait (2), cookieEchoed (3), established (4), shutdownPending (5), shutdownSent (6), shutdownReceived (7), shutdownAckSent (8), deleteTCB (9)	The state of the association
		nnRelMsgSctpAssocMsgLoss	Unsigned32 (1..100000000)	Error rate...expressed as an integer, with 10 digits, the decimal point is in the 1st place. A value of 10**-5, 0.00001 is expressed 0000100000 or 100,000. A value of 0.05 is 0500000000 or 500,000,000 and so forth.
		nnRelMsgSctpAssocRetrans	Unsigned32 (1..100000000)	Error rate...expressed as an integer, with 10 digits, the decimal point is in the 1st place. A value of 10**-5, 0.00001 is expressed 0000100000 or 100,000. A value of 0.05 is 0500000000 or 500,000,000 and so forth.

MIB definitions

MIB Table	Entry	Subfield or refinement	values	Explanation and action
nnRelMsgSctp AssocOmCurr Table The table which contains an entry for the OMs currently being collected for each association	NnRelMsgSctp AssocEntry An individual entry into the nnRelMsgSctp AssocOmCurr Table.	nnRelMsgSctp AscCurrClosed	Unsigned 32 bit	Number of times an association has been closed
		nnRelMsgSctp AscCurrAbort	Unsigned 32 bit	Number of times an association has been aborted
		nnRelMsgSctp AscCurrOutPac ks	Unsigned 32 bit	Number of packets which have been sent using the association
		nnRelMsgSctp AscCurrInPack s	Unsigned 32 bit	Number of packets which have been received from the association
		nnRelMsgSctp AscCurrDiscPa cks	Unsigned 32 bit	Number of packets which have been discarded
		nnRelMsgSctp AscCurrRetran Packs	Unsigned 32 bit	The number of packets which have been retransmitted
		nnRelMsgSctp AscCurrT1expir es	Unsigned32	Number of times the T1 timer has expired.
		nnRelMsgSctp AscCurrT2expir es	Unsigned 32 bit	Number of times the T2 timer has expired.
		nnRelMsgSctp AscCurrT3expir es	Unsigned 32 bit	Number of times the T3 timer has expired.
		nnRelMsgSctp AscCurrCongC ount	Unsigned32	The number of times the association has become congested
		nnRelMsgSctp AscCurrCongCl eared	Unsigned32	The number of times the association has cleared up from being congested

MIB definitions

MIB Table	Entry	Subfield or refinement	values	Explanation and action
nnRelMsgSctpAssocOmInter vTable The table which contains an entry for the historical OMs that have been collected for each association	NnRelMsgSctpAssocOmInter vEntry An individual entry into the nnRelMsgSctpAssocOmInter vTable.	nnRelMsgSctpAsclInterval	Integer (1-96)	Number of times an association has been closed
		nnRelMsgSctpAsclIntervClosed	Unsigned 32 bit	Number of times an association has been closed
		nnRelMsgSctpAsclIntervAbort	Unsigned 32 bit	Number of times an association has been aborted
		nnRelMsgSctpAsclIntervOutPacks	Unsigned 32 bit	Number of packets which have been sent using the association
		nnRelMsgSctpAsclIntervInPacks	Unsigned 32 bit	Number of packets which have been received from the association
		nnRelMsgSctpAsclIntervDiscPacks	Unsigned 32 bit	Number of packets which have been discarded
		nnRelMsgSctpAsclIntervRetranPacks	Unsigned 32 bit	The number of packets which have been retransmitted
		nnRelMsgSctpAsclIntervT1expires	Unsigned32	Number of times the T1 timer has expired.
		nnRelMsgSctpAsclIntervT2expires	Unsigned 32 bit	Number of times the T2 timer has expired.
		nnRelMsgSctpAsclIntervT3expires	Unsigned 32 bit	Number of times the T3 timer has expired.
		nnRelMsgSctpAsclIntervCongCount	Unsigned32	The number of times the association has become congested
		nnRelMsgSctpAsclIntervCongCleared	Unsigned32	The number of times the association has cleared up from being congested

MIB definitions

MIB Table	Entry	Subfield or refinement	values	Explanation and action
nnRelMsgNotifications Contains the data collected for each alarm as it is raised or cleared	nnRelMsgFault	nnRelMsgFaultType	INTEGER relMsgLinkFail (1), relMsgLinkSevDegraded (2), -- msgLoss Thresh exceeded relMsgLinkDegraded (3)	Gives the type of the fault being raised or cleared.
		nnUemgAlarmSeverity	INTEGER indeterminate (1), warning (2), minor (3), major (4), critical (5)	Tells how much the system will be affected when the alarm is raised.
		nnUemgAlarmDescrip	String	Brief description of the alarm being raised or cleared
		nnRelMsgSctpAssocState	Integer closed (1), cookieWait (2), cookieEchoed (3), established (4), shutdownPending (5), shutdownSent (6), shutdownReceived (7), shutdownAckSent (8), deleteTCB (9)	The state of the association when the alarm is raised
		nnUemgAlarmDefinition	INTEGER set (1), -- Alarm is Set clear (2), -- Alarm is Cleared notAlarmed(3) -- Fault is NOT Alarmed (event only)	If the alarm is raised or cleared
		nnUemgAlarmEventTime	DateAndTime,	The time when the alarm is raised or cleared.

Datafill example

This MIB currently can not be set or changed.

Service Orders (SO) (CM & SESM)

NA

Software optionality control (SOC)

NA

Element Management

NA

Command interface changes**Directory: mapci;mtc;pm;<pm name & number>;querypm flts**

Three new messaging faults may appear for HOST ABI XPMs. The following new text strings are added to QUERYPM FLTS:

- External Pkt Ntwk Msg Link(s) Problems - CRITICAL links down
- External Pkt Ntwk Msg Link(s) Problems - Major severe message loss
- External Pkt Ntwk Msg Link(s) Problems - Minor degraded

Dshell command changes**Directory: SctpAppIf****Directory description**

This Dshell directory on the ABI contains commands to obtain information about any SCTP associations that exist on that ABI card. The information that can be obtained will be OM data and basic data on the health of the association.

Accessing directory: SctpAppI**Access to directory or MAP level and return to CI**

To access the /SctpAppl command, first telnet to the desired ABI. This will take the user to the root directory of the Dshell which will look like: ABI[0 1 15] dSH>

Now type the following command to enter the SctpAppI directory: cd /SctpAppl

To return to the root directory the user can enter either of the following commands: cd. or cd

Command: ListAssociations

Command type: ABI Dshell Command

Command target: MG9K ABI card

Command availability: Other

In house tool

Command description

The listAssociations command will list the SCTP associations on the ABI card and provide a status of each association. The command will provide the SCTP association number which will be used to view the OM data in the other commands in the SctpAppIf directory.

Command syntax

listAssociations command parameters and variables

Command	Parameters and variables
ListAssociations	[-h]
Parameters and variables	Description
-h	Prints a basic help statement for the command

Qualifications and warnings

None

Responses

None

Example

Usage examples for listAssociations command

Description of task	Prints out an Association number, a text description of the association and the state of the association.
Command:	ABI[0 1 15] dSH>listAssociations
Dshell response:	Number: Association : State 01 : ABI CARD 1 Assoc : Connected

Command: activeOMs**Command type: ABI Dshell Command****Command target: MG9K ABI card****Command availability: Other**

In house tool

Command description

The activeOMs command will print out the set of OMs that are currently being collect of the requested association number.

Command syntax**activeOMs command parameters and variables**

Command	Parameters and variables
activeOMs	[-h] <association #>
Parameters and variables	Description
-h	Prints a basic help statement for the command
association #	The number of the SCTP association that the OM data is being requested for. This can be obtained from the listAssociations command.

Qualifications and warnings

None

Responses

Bad parameter entered for the command

Outputs with associated meanings and actions

Command	
	Association not defined
or	Usage: activeOMs [association#]) Will print the OM data that is currently being collected Will print the OM data for the specific association that corresponds to the number supplied. The association numbers can be obtained using the listAssociation command
Meaning: Either a valid association number was entered but that association was not created or a invalid number was entered for the association number.	
System or user actions: Use the command listAssociations to determine a valid association number to use as the parameter for this command	

Example

Usage examples for activeOMs command

Description of task:	Prints out a table of the currently collected OM values for the specified association number

Usage examples for activeOMs command

Command:	activeOMs 0
MAP response:	Active SCTP OMs ABI CARD 1 Assoc Closd Abort OutPack InPack Discrd Retrns T1exp T2exp T3exp Cong CngCl 0001 0003 0123543 0323453 00094 00163 00021 00034 00054 00011 00011 The above table the fields have the following meanings Closd - The number of times the association was closed Abort - The number of times the association was aborted OutPack - Number of packets sent out the association InPack - Number of packets received by the association Discrd - Number of packets discarded by the association Retrns - Number of packets retransmitted by the association T1exp - Number of T1 timer expiries on the association T2exp - Number of T2 timer expiries on the association T3exp - Number of T3 timer expiries on the association Cong - Number of times the association entered congestion CngCl - Number of times the congestion was cleared

Command: HistoryOMs**Command type: ABI Dshell Command****Command target: MG9K ABI card****Command availability: Other**

In house tool

Command description

The historyOMs command will print one or more sets of OMs that had been previously collected. The users will be able to specify which set 1-96 with 1 being the latest set collected and 96 being the oldest set collected. If a range is specified it will print out the sets in the range from latest to oldest.

Command syntax

historyOMs command parameters and variables

Command	Parameters and variables
historyOMs	[-h] <Association#> [lower bound (1-96)] [upper bound (1-96)]
Parameters and variables	Description
-h	Prints a basic help statement for the command
Association #	The number of the SCTP association that the OM data is being requested for. This can be obtained from the listAssociations command.
lower bound	This parameter has a range from 1 to 96, with 1 being the latest and 96 being the oldest set of OMs collected. If this is not supplied it will default to 1, which will cause the latest set of OMs to be printed out.
upper bound	This parameter has a range of 1 to 96, with one being the newest and 96 being the oldest set of OMs being collected. If the parameter is supplied it has to be equal or greater than the lower bound parameter. This parameter will cause multiple sets of OMs to be printed out between the range of the lower and upper bound. If this parameter is not supplied it will be defaulted to the lower bound parameter and cause only one set of OMs to be printed.

Qualifications and warnings

None

Responses

Bad parameter entered for the command

Outputs with associated meanings and actions

Command
Association not defined
or
Usage: historyOMs <Association#> [lower bound (1-96)] [upper bound (1-96)]
Will print the OM history for the specific association requested.
The association numbers can be obtained using the listAssociation command
If no lower bound is entered it will print out the last saved interval of OMs for the specified one association number. If one bound parameter is supplied it will print that OM set. If both bound parameters are supplied it will print the sets between the two numbers. The upper bound has to be larger or equal to the lower bound.
Meaning: Either a valid association number was entered but that association was not create or a bad association number was entered, or the upper or lower bounds were out of range [1 - 96] or the upper bound was smaller than the lower bound
System or user actions: Use the command listAssociations to determine a valid association number to use as the parameter for this command. Also check to make sure the upper bound (if one was entered) is not smaller than the lower bound and that both lower and upper bounds (if supplied) are in the range of 1 through 96.

Example

Usage examples for historyOMs command

Description of task:	Prints out a table of the currently collected OM values for the specified association number

Usage examples for historyOMs command

Command:	historyOMs 0 5 7
MAP response:	History SCTP OMs ABI CARD 1 Assoc # Cldsd Abort OutPack InPack Discrd Retrns T1exp T2exp T3exp Cong CngCl 05 0001 0003 0123543 0323453 00094 00163 00021 00034 00054 00011 00011 06 0000 0001 0223345 0245672 00067 0099 00012 00015 00023 00007 00007 07 0001 0002 0321456 0212345 00153 00173 00041 00014 00034 00004 00004 The above table the fields have the following meanings # - number of the set of OMs being displayed cldsd - The number of times the association was closed Abort - The number of times the association was aborted OutPack - Number of packets sent out by the association InPack - Number of packets received by the association Discrd - Number of packets discarded by the association Retrns - Number of packets retransmitted by the association T1exp - Number of T1 timer expiries on the association T2exp - Number of T2 timer expiries on the association T3exp - Number of T3 timer expiries on the association Cong - Number of times the association entered congestion CngCl - Number of times the congestion was cleared

Security

NA

Configuration Walkthrough

NA

Product = CS 2000**A00003789 -- INTRA IMT CAUSE Enhancements (Succession on DMS, AAL2)*****Functional Description***

This feature introduces the capability for originating INTRA IMT trunks to route advance on four specific CAUSE values:

- CAUSE 42 - Switch Equipment Congestion (SWEQCONG)
- CAUSE 47 - Resources Unavailable (RESUNAV)
- CAUSE 51 - This is a non standardized “Service” related CAUSE (CSE_51) utilized by the customer in their own network.
- CAUSE 34 - No Circuits Available (NOCIRCAV)

This feature introduces a new office parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT in table OFCVAR which controls the optionality to route advance on CAUSE 34 - No Circuit Available (NOCIRCAV). Cause values 42, 47 and 51 are not affected by the office parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT.

PTS and SS7 INTRA IMT originators are supported and must terminate to an SS7 EANT or IMT terminator for the described CAUSE enhancements to take place.

Specifically for SS7 INTRA IMT originators this feature enables CAUSE handling in the CM with existing optional table CSEMAP for all CAUSE values in addition to the specified functionary for CAUSE 34, 42, 47 and 51.

The INTRA IMT CAUSE enhancement capability is controlled on a per trunk group basis using a new option in table TRKOPTS called INTRACSE. **NOTE: Patch SBB41 introduced the TRKOPTS option as INTRA_CSE (w/ underscore) and this activity removes the underscore for TRKOPTS option consistency and ease of use.** The INTRACSE TRKOPTS option can only be assigned to originating (IC, 2W) IMT Trunks with TRKGRP field NETWKSPC set to INTRA. The INTRACSE option contains a “route advance choice” field that can be set to Y or N.

This capability interacts with optional table CSEMAP but does not have a dependency on table CSEMAP. For more information see “Office Parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT” on page 1371.

This capability is under Software Optionality Control (SOC). The SOC order code is NSER0005.

Please refer to the following sections for detailed information on this capability:

- Background Information
- Software Optionality Control NSER0005
- Table TRKOPTS option INTRACSE

- Table OFCVAR Office Parameter
RTE_ADVANCE_FOR_INTRA_IMT_NCRT
- Call Processing CAUSE Handling

Background Information

It is important to understand the default or existing CAUSE handling behavior for both PTS and SS7 INTRA IMT originators prior to this activity.

PTS INTRA IMT originators that terminate to SS7 EANT and IMT trunks always perform CAUSE handling in the CM as the CAUSE value cannot be passed to the adjacent office due to interworking (PTS to SS7). Therefore “default” CAUSE handling for PTS INTRA IMT originators already exists. The specific CAUSE values impacted by this feature have a default functionality for PTS INTRA IMT originators as follows:

- CAUSE 34, 42 and 47 all route advance by default and can be overridden by associated CSEMAP entries to not route advance or to go to a different treatment. Refer to the following table.
- CAUSE 51 is an undefined CAUSE value and by default goes to (RODR) treatment. CSE_51 can be overridden by a CSEMAP entry to route advance or go to a different treatment. Reference for details.

Default PTS INTRA IMT CAUSE Handling Behavior

CSEMAP	CAUSE ~~34, 42, 47~~ Default Result	CAUSE ~~51~~ Default Result
No Entry	Route Advance (Default)	TRTMT (Default - RODR)
RTE ADV - N	CSEMAP TRTMT	CSEMAP TRTMT
RTE ADV - Y	Route Advance (CSEMAP)	Route Advance (CSEMAP)

SS7 INTRA IMT originators that terminate to SS7 EANT and IMT trunks do not perform CAUSE handling in the CM prior to this feature. The CAUSE values are passed (bounced) to the adjacent office without any CM interaction.

This activity, when active, will impact both SS7 and PTS INTRA IMT originators in the same way as described in section “ Office Parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT” on page 1371. When inactive, the default behavior will be as described in the section [“Background Information”](#) .

Software Optionality Control (SOC) NSER0005

The new SOC order code NSER0005 - Intra IMT Cause Enhancements is introduced by this feature. When the NSER0005 SOC state is IDLE, CAUSE

handling behavior is unchanged for calls with INTRA IMT originators. The new TRKOPTS option INTRACSE can be data filled when the SOC state is IDLE or ON. The new office parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT can also be changed when the SOC state is set to IDLE or ON.

The new SOC NSER0005 - Intra IMT Cause Enhancements is dependant upon SOC NSER0003 - Inter/Intra IMT for the described functionality to be active.

Changing the NSER0005 SOC state to ON does not in itself enable any new functionality. NSER0005 SOC in conjunction with the INTRACSE TRKOPTS option, enables the CAUSE Enhancements capability described in this document. For more information see “Office Parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT” on page 1371.

Table TRKOPTS option INTRACSE

A new TRKOPTS option called INTRACSE is introduced by this feature. The INTRACSE option contains a field called RTE_ADV_CHOICE that must be data filled to Y or N to select the route advance capabilities described in section “Office Parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT” on page 1371.

The following figure shows an example entry of the INTRACSE option data filled on a trunk CLLI in table TRKOPTS.

TRKOPTS option INTRACSE Example Entry

TABLE: TRKOPTS ----- TRKCLLI INTRACSE INTRACSE RTE_ADV_CHOICE Y

The CAUSE Enhancement capability is dependant on the originating trunk and therefore The INTRACSE option can only be assigned to IC or 2W INTRA IMT trunks. The option can be assigned to both SS7 and PTS INTRA IMT signaling trunks. The option allows the customer to activate the CAUSE enhancements capability on a per trunk group basis. INTRA IMT originators with this option assigned must terminate to an SS7 terminating trunk to enable the CAUSE Enhancement capability.

Various error messages occur during datafill if the INTRACSE option is assigned to something other than the specified trunk data. The following figure illustrates the error messages associated with the INTRACSE option.

TRKOPTS INTRACSE Datafill Error Messages

Attempts to datafill the INTRACSE option on a trunk type other than IMT, results in the following error message:

'INTRACSE option is supported only for IMT trunk types'

Attempts to datafill the INTRACSE option on an IMT trunk with a NETWKSPC value other than INTRA, results in following error message

'INTRACSE option requires NETWKSPC to be INTRA'

Attempts to datafill the INTRACSE option on an outgoing (OG) trunk, result in the following error message:

'INTRACSE option supports IC and 2W direction only.'

Office Parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT

A new office parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT is added to table OFCVAR to control the route advance behavior of CAUSE 34 in conjunction with the INTRACSE TRKOPTS option. The functionality of this parameter does not affect the route advance capability of cause values 42, 47 and 51. The values for the parm are {N,Y} and are immediately activated when changed.

The functionality of this office parameter is further explained in the section “CAUSE Processing CAUSE Handling”.

The following figure shows an example entry of the office parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT in table OFCVAR.

OFVCVAR Office Parameter Example Entry

TABLE: OFCVAR

RTE_ADVANCE_FOR_INTRA_IMT_NCRT Y

Call Processing CAUSE Handling

The CAUSE enhancements capability for this activity is described in “INTRA IMT CAUSE Handling Matrix” on page 1373. There are several variables that determine the CAUSE handling behavior for INTRA IMT originators. The variables are summarized as follows:

- SOC NSER0003 - Inter/Intra IMT must be ON. For “INTRA IMT CAUSE Handling Matrix” on page 1373 this variable is not listed and the SOC is assumed to be ON.
- SOC NSER0005 - Intra IMT Cause enhancements - IDLE / ON status indicates optionality status. IDLE implies default or existing behavior prior to this activity.
- TRKOPTS option INTRACSE. The presence of the option for a particular trunk allows two things to occur:
 - Enables CAUSE handling in the CM for INTRA IMT SS7 originators for all CAUSE values in addition to the functionality described in this document for CAUSE values 34, 42, 47 and 51.
 - Checks the status of office parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT and determines whether to enable or disable CAUSE 34 from route advancing for SS7 and PTS INTRA IMT trunks. However a CSEMAP entry for CAUSE 34 can be used to provide route advance capabilities or change the treatment handling.
- INTRACSE RTE_ADV_CHOICE Y/N - this field impacts CAUSE values 34, 42, 47 and 51 only and when set to Y enables route advance with or without CSEMAP interaction. When set to N default treatment is used or CSEMAP entries can allow route advance or change the treatment.
- CSEMAP entries for CAUSE values 42, 47 and 51. With INTRACSE RTE_ADV_CHOICE = N, the CSEMAP entries determine route advance or treatment CAUSE handling. With INTRACSE RTE_ADV_CHOICE = Y, the call always route advances regardless of CSEMAP entry.
- CSEMAP entry for CAUSE 34. If the office parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT = Y and INTRACSE RTE_ADV_CHOICE = N, the CSEMAP entry determines route advance or treatment CAUSE handling. With INTRACSE RTE_ADV_CHOICE = Y, the call always route advances regardless of CSEMAP entry. If the office parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT = N, INTRACSE RTE_ADV_CHOICE subfield has no impact on CAUSE handling for CAUSE 34. The presence of the INTRACSE option forces the call to go to treatment (NCRT). However a CSEMAP entry for CAUSE 34 can change the treatment or set the route advance bool and the call routes accordingly.

The following table describes the CAUSE Enhancement behavior provided by this activity.

INTRA IMT CAUSE Handling Matrix

SOC NSER0005	TRKOPTS INTRACSE	CSEMAP	CAUSE 42,47 and 51 Result	CAUSE 34 Result when RTE_ADVANCE_FOR_INTRA_IMT_NCRT=N	CAUSE 34 Result when RTE_ADVANCE_FOR_INTRA_IMT_NCRT=Y
IDLE	N/A	N/A	Default CAUSE Behavior ^a	Default CAUSE Behavior	Default CAUSE Behavior
ON	No Entry	No Entry	Default CAUSE Behavior	Default CAUSE Behavior	Default CAUSE Behavior
ON	No Entry	RTE ADV - N	Default CAUSE Behavior	Default CAUSE Behavior	Default CAUSE Behavior
ON	No Entry	RTE ADV - Y	Default CAUSE Behavior	Default CAUSE Behavior	Default CAUSE Behavior
ON	RTE ADV - N	No Entry	Default TRTMT ^b	Default TRTMT	Default TRTMT
ON	RTE ADV - N	RTE ADV - N	CSEMAP TRTMT	CSEMAP TRTMT	CSEMAP TRTMT
ON	RTE ADV - N	RTE ADV - Y	Route Advance (CSEMAP)	Route Advance (CSEMAP)	Route Advance (CSEMAP)
ON	RTE ADV - Y	No Entry	Route Advance (INTRACSE)	Default TRTMT (NCRT)	Route Advance (INTRACSE)
ON	RTE ADV - Y	RTE ADV - N	Route Advance (INTRACSE)	CSEMAP TRTMT	Route Advance (INTRACSE)
ON	RTE ADV - Y	RTE ADV - Y	Route Advance (INTRACSE)	Route Advance (CSEMAP)	Route Advance (INTRACSE)

a. Default CAUSE Behavior is different for SS7 and PTS See "Background Information" on page 1369, for specific details

b. Default TRTMT for CAUSE 34 is NCRT, CAUSE 42 is NBLH, CAUSE 47 is GNCT, and CAUSE 51 is RODR

Hardware Requirements or Dependencies

None

Software Requirements or Dependencies

SOC NSER0005 is dependant on SOC NSER0003 - Inter/Intra IMT. SOC NSER0003 must be ON before SOC NSER0005 call processing capabilities become active.

Limitations and restrictions

From a Table Control perspective the TRKOPTS option INTRA_CSE can only be assigned to:

- INTRA IMT (IC or 2W) PTS Trunks
- INTRA IMT (IC or 2W) SS7 Trunks

From a Call processing perspective CAUSE handling requires terminations from INTRA IMT trunk originators to EANT or IMT (INTRA or INTER) SS7 trunk terminators.

Interactions

This capability interacts with optional Table CSEMAP but is not dependant nor does it change the behavior of the CSEMAP table. For details refer to table “INTRA IMT CAUSE Handling Matrix” on page 1373.

Applicable customer facing sections

Fault Management

Logs ___N/A___

Alarms ___N/A___

Configuration

Data Schema ___X___

User Interface ___N/A___

Element Management ___N/A___

Security ___N/A___

Service Order ___N/A___

Office Parameters ___N/A___

Accounting (includes AMA billing) ___N/A___

Performance (includes operational measurements) ___N/A___

Glossary

Term	Description
AMA	Automatic Message Accounting
EANT	Equal Access Network Trunk
IMT	Inter Machine Trunk
PTS	Per Trunk Signaling
SOC	Software Optionality Control
SS7	Signaling System #7

Configuration for A00003789

Hardware and Software Requirements

N/A

Initial Configuration

N/A

Office/Subnet parameters (OP/SP) (CM & SESM)

New/modified office/subnet parameters

New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management)
OFCVAR	RTE_ADVANCE_FOR_INTRA_IMT_NCRT	New	CM

Parameter information

RTE_ADVANCE_FOR_INTRA_IMT_NCRT

Route Advance For INTRA IMT Release Cause (34) “No Circuit Available”

Functional description

This parm enables the optionality to route advance for release cause “No Circuit Available.” The SOC NSER0005 must be set to ON and the INTRACSE option in table TRKOPTS must be datafilled in order for the functionality of this parm to be enabled. The following table shows the behavior of Release Cause “No Circuit Available” when the office parm is enabled.

Option INTRACSE.RTEADV_CHOICE	RTE_ADVANCE_FOR_INTRA_IMT_NCRT	Action
Yes	Yes	Route Advance from option INTRACSE
Yes	No	Do not route advance from option INTRACSE however table CSEMAP may override and route advance
No	Yes	Do not route advance from option INTRACSE however table CSEMAP may override and route advance
No	No	Do not route advance from option INTRACSE however table CSEMAP may override and route advance

Provisioning rules

The values for this parm are boolean {N,Y}.

Range information**Range Information**

Minimum	Maximum	Default
{N,Y}	{N,Y}	N

Activation

Immediate.

Dependencies

SOC NSER0005 must be set to ON and the INTRACSE option in table TRKOPTS must be present in order to enable the functionality of this parameter.

Consequences

None

Verification

None

Memory requirements

No memory impact.

Parameter release history update

Office parm RTE_ADVANCE_FOR_INTRA_IMT_NCRT is a new parm added in table OFCVAR.

Upgrade Impact**Dump and Restore**

No customer interaction is required.

- Patch SBB41 status is checked during ONP and if patch is active the SOC status for NSER0005 is set to ON.
- Patch SBB59 status is checked during ONP and if the patch is active the office parm RTE_ADVANCE_FOR_INTRA_IMT_NCRT is set to “Y”. Otherwise the parm is set to “N”.

Element Management Upgrade

N/A

Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

New option is added to existing table TRKOPTS

New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
TRKOPTS	Changed	Unchanged

Table/MIB/Remote Database Schema information

Name: TRKOPTS

TRunK OPTionS

Functional description

A new Trunk option, INTRACSE is introduced to Table TRKOPTS. The INTRACSE option contains a subfield called RTE_ADV_CHOICE that must be datafilled to Y or N to determine route advance behavior for specific CAUSE values. The CAUSE Enhancement capability is dependant on the originating trunk and therefore The INTRACSE option can only be assigned to IC or 2W INTRA IMT trunks. The option can be assigned to both SS7 and PTS INTRA IMT signaling trunks. The option allows the customer to activate the CAUSE enhancements capability on a per trunk group basis. INTRA IMT originators with this option assigned must terminate to an SS7 terminating trunk to enable the CAUSE Enhancement capability.

Only CAUSE values 34 (NOCIRCAV), 42 (SWEQCONG), 47 (RESUNAV) and 51 (CSE_51) are impacted by this option. CAUSE values 42, 47 and 51 will always route advance if the RTE_ADV_CHOICE field is set to Y.

If the office parameter RTE_ADVANCE_FOR_INTRA_IMT_NCRT is set to Y, CAUSE value 34 will route advance according to the RTE_ADV_CHOICE and table CSEMAP. If the office parameter is set to N, CAUSE value 34 will NOT route advancing regardless of the Y/N value of the RTE_ADV_CHOICE field.

Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

Current datafill order unchanged.

Size**Table size**

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TRKOPTS	0	131072	Dynamically Allocated

Fields/OIDs

The following table lists fields/OIDs for TRKOPTS.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTION	Changed	refinement	Option: INTRACSE subfield: RTE_ADV_CHOICE - Y/N	INTRA IMT CAUSE Enhancements Enables route advance capabilities for CAUSE values 34, 42, 47 and 51. Subfield RTE_ADV_CHOICE is a Y/N prompt. When datafilled to Y CAUSE 34, 42, 47 and 51 will route advance. When datafilled to N CAUSE values 34, 42, 47 and 51 will go to their respective default treatments.

Datafill example

The following example shows sample datafill for table TRKOPTS.

```
TABLE: TRKOPTS
-----
TRKCLLI INTRACSE INTRACSE RTE_ADV_CHOICE Y
```

INTRACSE data fill incompatibilities result in the following Error Messages

Attempts to datafill the INTRACSE option on a trunk type other than IMT results in the following error message:

'INTRACSE option is supported only for IMT trunk types'

Attempts to datafill the INTRACSE option on an IMT trunk with a NETWKSPC value other than INTRA, results in following error message

'INTRACSE option requires NETWKSPC to be INTRA'

Attempts to datafill the INTRACSE option on an outgoing (OG) trunk result in the following error message:

'INTRACSE option supports IC and 2W direction only.'

Table release history update

INTRACSE with subfield RTE_ADV_CHOICE is added as an additional OPTION in table TRKOPTS.

Supplementary information

N/A

Translation verification other tools

N/A - Table TRKPOTS references are not displayed in TRAVER

Service Orders (SO) (CM & SESM)

N/A

Software optionality control (SOC)

SOC

SOC option name:	Intra IMT Cause Enhancements
SOC option title:	Yes
SOC option control type:	Usage
New SOC option?	Yes
SOC option order code	NSER0005

SOC

Option defined in DRU:	UCS
Affected products:	SN07

Element Management

N/A

Command interface changes

N/A

Security

N/A

Configuration Walkthrough

N/A

Product = CS 2000**A00003905 -- DIRP Enhancements for Billing (Succession on DMS)*****Functional Description***

Feature A00003905 increases the number of DIRP volumes in table DIRPPool from 24 to 72.

The feature uses SOC to restrict provisioning more than 24 volumes per DIRP pool if the SOC state is IDLE. Rejection messages indicate that this feature is inactive.

The SOC name for this functionality is BASE DIRP enh to 72 vol, and the ORDCODE is BASE0014.

Hardware Requirements or Dependencies

Feature A00003905 works in conjunction with feature A00002186 to realize 4G of storage capacity for a DIRP subsystem. Feature A00002186 increase DDU storage capacity from 1G to 4G. However, for any feature functionality to be active, 4G DDUs must be present in the switch with the appropriate IOM load.

Software Requirements or Dependencies

To achieve 4G of DIRP DDU storage capacity, both features A00003905 and A00002186 must be present and active. Both features are enabled and disabled via SOC. IOM load XXXYYYZZZ is required.

Limitations and restrictions

None.

Interactions

Feature A00003905 impacts table control for table DIRPPOOL. Expanding the number of volumes per pool necessitated a change in how table DIRPPOOL is manually provisioned. Volumes are no longer provisioned as individual fields but are provisioned in groups of three. Using DIRP MNT to provision volumes is unaffected.

Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema _____X_____

User Interface _____X_____

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

Glossary

Term	Description
New term	Definition
DIRP MNT	MAPCI; MTC; IOD; DIRP; MNT

Configuration for A00003905

Hardware and Software Requirements

Feature A00003905 allows 72 disk volumes to be provisioned per DIRP pool in table DIRPPool. Previously, only 24 volumes could be allocated per pool.

Feature A00002186 expands DDU capacity from 1G to 4G. IOM load XXXYYYYZZZ is required by feature A00002186.

In order for full 4G DDU capacity to be available for DIRP, feature A00002186 must be at SOC state ON. IOM load XXXYYYYZZZ must be used. Feature A00003905 must also be at SOC state ON.

The SOC name for this functionality is BASE DIRP enh to 72 vol, and the ORDCODE is BASE0014.

Initial Configuration

Feature A00003905 SOC state defaults to IDLE.

72 possible volumes are displayed in table DIRPPool. Access to provisioning more than 24 volumes is SOC controlled.

Upgrade Impact

Dump and Restore

Feature A00003905 sources the functionalities provided by software bridge SBB28. SBB28 created a new table DIRPOOL2 which linked together three 24 volume pools in table DIRPPool in order to achieve 72 volumes of storage per DIRP subsystem.

Over an ONP when bridge SBB28 is active and table DIRPOOL2 contains linked pools, feature A00003905 will consolidate all of the pools' volumes under the main pool that is provisioned against the subsystem in table DIRPSSYS. The emptied unused pools will be deleted from table DIRPPool.

Any files present in table DIRPHOLD from the volumes being consolidated will be deleted as part of the consolidation process. Files in table DIRPHOLD should be processed prior to an ONP. The following warning is displayed during POSTSWACT:

```
WARNING - ALL DIRPHOLD FILES FOR VOLUME <volume name> DELETED  
FROM TABLE DIRPHOLD, AND ARE THE USERS' RESPONSIBILITY
```

Table DIRPOOL2 is present on the new load only during the ONP and is only used for consolidation. The table is deleted from the system at the end of the ONP.

SOC state is not considered during an ONP. Feature A00003905 will always transfer and consolidate if needed. SOC state IDLE will prevent any future provisioning of volumes in a pool that has more than 24 volumes.

Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

Table	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
DIRPPPOOL	CHANGED	UNCHANGED
DIRPOOL2	NEW	NEW

Table/MIB/Remote Database Schema information

Name: DIRPPPOOL

Functional description

Table DIRPPPOOL contains information regarding the pool of available devices to be used by a DIRP subsystem for recording.

Usage sequence and implications (CM Only)

Current datafill order unchanged.

Size

Increasing the number of volumes per pool to 72 from 24 increases the memory requirements of table DIRPPPOOL. Essentially, volume related store now requires 3x as much memory ($72/24=3$). Modules DIRPGI and DIRPDSON carry the bulk of the increase in storage. The following information shows the increase:

```
BEFORE:
>store ds scan module dirpgi
Storetype      Ttl      Ttl      Min      Max
                Blks      Size      Blk      Blk
                Owned     Owned     Owned     Owned
DSTEMP_B        1 #00000A00 #00000A00 #00000A00
DSPROT_W       10 #0000C200 #000000C0 #00006300
DSPERM_B       28 #00047F40 #00006000 #00006000
DSSOS_B         1 #00000A00 #00000A00 #00000A00
DSSOS_W         1 #00000A00 #00000A00 #00000A00
Totals:        41 #00055F40
>store ds scan module dirpdson
Storetype      Ttl      Ttl      Min      Max
                Blks      Size      Blk      Blk
                Owned     Owned     Owned     Owned
DSPROT_W        1 #00001D00 #00001D00 #00001D00
DSPERM_B        1 #00001440 #00001440 #00001440
Totals:         2 #00003140
AFTER:
```

```
>store ds scan module dirpgi
```

Storetype	Ttl Blks Owned	Ttl Size Owned	Min Blk Owned	Max Blk Owned
DSTEMP_B	1	#00000A00	#00000A00	#00000A00
DSPROT_W	67	#00018540	#000004A0	#00005900
DSPERM_B	67	#00015880	#00001420	#00001420
DSSOS_B	1	#00000A00	#00000A00	#00000A00
DSSOS_W	1	#00000A00	#00000A00	#00000A00

```
Totals: 137 #0002FBC0
```

```
>store ds scan module dirpdson
```

Storetype	Ttl Blks Owned	Ttl Size Owned	Min Blk Owned	Max Blk Owned
DSPROT_W	1	#00002300	#00002300	#00002300
DSPERM_B	1	#00001740	#00001740	#00001740

```
Totals: 2 #00003A40
```

Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
DIRPPPOOL	SAME	SAME	Volume memory requirements increase by 3x. See above.

Fields

The following table lists changed fields for DIRPPPOOL.

Every individual volume field, i.e. VOLUME12, is changed to a TABLE of three volume names.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
VOLUME0	Changed	None	eight_char_vector	New Field Name: VOL00X02 The field will be provisioned with 3 volume names for volumes 00 to 02. Default: \$ \$ \$

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
VOLUME1	Changed	None	eight_char_vector	New Field Name: VOL03X05 The field will be provisioned with 3 eight_char_vector for volumes 03 to 05. Default: \$ \$ \$
VOLUME2	Changed	None	eight_char_vector	New Field Name: VOL06X08 The field will be provisioned with 3 eight_char_vector for volumes 06 to 08. Default: \$ \$ \$
VOLUME3	Changed	None	eight_char_vector	New Field Name: VOL09X11 The field will be provisioned with 3 eight_char_vector for volumes 09 to 11. Default: \$ \$ \$
VOLUME4	Changed	None	eight_char_vector	New Field Name: VOL12X14 The field will be provisioned with 3 eight_char_vector for volumes 12 to 14. Default: \$ \$ \$
VOLUME5	Changed	None	eight_char_vector	New Field Name: VOL15X17 The field will be provisioned with 3 eight_char_vector for volumes 15 to 17. Default: \$ \$ \$

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
VOLUME6	Changed	None	eight_char_vector	New Field Name: VOL18X20 The field will be provisioned with 3 eight_char_vector for volumes 18 to 20. Default: \$ \$ \$
VOLUME7	Changed	None	eight_char_vector	New Field Name: VOL21X23 The field will be provisioned with 3 eight_char_vector for volumes 21 to 23. Default: \$ \$ \$
VOLUME8	Changed	None	eight_char_vector	New Field Name: VOL24X26 The field will be provisioned with 3 eight_char_vector for volumes 24 to 26. Default: \$ \$ \$
VOLUME9	Changed	None	eight_char_vector	New Field Name: VOL27X29 The field will be provisioned with 3 eight_char_vector for volumes 27 to 29. Default: \$ \$ \$
VOLUME10	Changed	None	eight_char_vector	New Field Name: VOL30X32 The field will be provisioned with 3 eight_char_vector for volumes 30 to 32. Default: \$ \$ \$

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
VOLUME11	Changed	None	eight_char_vector	New Field Name: VOL33X35 The field will be provisioned with 3 eight_char_vector for volumes 33 to 35. Default: \$ \$ \$
VOLUME12	Changed	None	eight_char_vector	New Field Name: VOL36X38 The field will be provisioned with 3 eight_char_vector for volumes 36 to 38. Default: \$ \$ \$
VOLUME13	Changed	None	eight_char_vector	New Field Name: VOL39X41 The field will be provisioned with 3 eight_char_vector for volumes 39 to 41. Default: \$ \$ \$
VOLUME14	Changed	None	eight_char_vector	New Field Name: VOL42X44 The field will be provisioned with 3 eight_char_vector for volumes 42 to 44. Default: \$ \$ \$
VOLUME15	Changed	None	eight_char_vector	New Field Name: VOL45X47 The field will be provisioned with 3 eight_char_vector for volumes 45 to 47. Default: \$ \$ \$

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
VOLUME16	Changed	None	eight_char_vector	New Field Name: VOL48X50 The field will be provisioned with 3 eight_char_vector for volumes 48 to 50. Default: \$ \$ \$
VOLUME17	Changed	None	eight_char_vector	New Field Name: VOL51X53 The field will be provisioned with 3 eight_char_vector for volumes 51 to 53. Default: \$ \$ \$
VOLUME18	Changed	None	eight_char_vector	New Field Name: VOL54X56 The field will be provisioned with 3 eight_char_vector for volumes 54 to 56. Default: \$ \$ \$
VOLUME19	Changed	None	eight_char_vector	New Field Name: VOL57X59 The field will be provisioned with 3 eight_char_vector for volumes 57 to 59. Default: \$ \$ \$
VOLUME20	Changed	None	eight_char_vector	New Field Name: VOL60X62 The field will be provisioned with 3 eight_char_vector for volumes 60 to 62. Default: \$ \$ \$

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
VOLUME21	Changed	None	eight_char_vector	New Field Name: VOL63X65 The field will be provisioned with 3 eight_char_vector for volumes 63 to 65. Default: \$ \$ \$
VOLUME22	Changed	None	eight_char_vector	New Field Name: VOL66X68 The field will be provisioned with 3 eight_char_vector for volumes 66 to 68. Default: \$ \$ \$
VOLUME23	Changed	None	eight_char_vector	New Field Name: VOL69X71 The field will be provisioned with 3 eight_char_vector for volumes 69 to 71. Default: \$ \$ \$

Datafill example

The following example shows sample datafill and how volumes would now be added and deleted for table DIRPPPOOL.

Changing the volumes with a one line command is not recommended. Table control does not recognize NIL volume names, and unexpected provisioning may result. Always verify table changes before confirming. Changing individual volumes is possible, but the approach taken in the example below and in the sample datafill is recommended. An example of a one line volume name change is below.

```
> CHA VOL00X02 $ $ D000VOL2
```

Preferred method:

```
> CHA VOL00X02
```



```
26 VOL63X65          THREE_VOLUME_TABLE
27 VOL66X68          THREE_VOLUME_TABLE
28 VOL69X71          THREE_VOLUME_TABLE
LOGICAL TUPLE TYPE: DIRPPool_LT
>ran 27
27 VOL66X68          THREE_VOLUME_TABLE
TYPE IS THREE_VOLUME_TABLE TABLE OF 3 VECTORS OF UP TO 8 CHAR'S
>cha
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
POOLNAME: MEGAPool
>
POOLTYPE: REGULAR
>
DEVTYPE: DISK
>
VOL00X02: D000CDR D000CDR1 D000AMA
>$ D000CDR1 D000AMA
VOL03X05: D000OCC1          $          $
>
VOL06X08: $          $          $
>
VOL09X11: $          $          $
>
VOL12X14: $          $          $
>
VOL15X17: $          $          $
>
VOL18X20: $          $          $
>
VOL21X23: $ F17LAMA F02LAMA
>
VOL24X26: $          $          $
>
VOL27X29: $          $          $
>
VOL30X32: $          $          $
>
VOL33X35: $          $          $
>
VOL36X38: $          $          $
>
VOL39X41: $          $          $
>
VOL42X44: $          $          $
>
VOL45X47: $          $          $
>
VOL48X50: $          $          $
>
VOL51X53: $          $          $
>
VOL54X56: $          $          $
>
VOL57X59: $          $          $
>
VOL60X62: $          $          $
>
VOL63X65: $          $          $
>
```

```

VOL66X68: $          $          $
>
VOL69X71: $          $          $
>
TUPLE TO BE CHANGED:
14 MEGAPOOL REGULAR DISK $ D000CDR1 D000AMA D000OCC1 $ $ $ $ $ $ $ $ $ $ $ $
$ $ $ $ $ $ F17LAMA F02LAMA $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $
$ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
WARNING - ALL DIRPHOLD FILES FOR VOLUME D000CDR DELETED
FROM TABLE DIRPHOLD, AND ARE THE USERS' RESPONSIBILITY
Regular Volume D000CDR will be taken out of DIRP as soon as possible.
TUPLE CHANGED
JOURNAL FILE INACTIVE
>lis
POOLNO POOLNAME POOLTYPE DEVTYPE VOL00X02 VOL03X05 VOL06X08 VOL09X11
VOL12X14 VOL15X17 VOL18X20 VOL21X23 VOL24X26 VOL27X29 VOL30X32 VOL33X35
VOL36X38 VOL39X41 VOL42X44 VOL45X47 VOL48X50 VOL51X53 VOL54X56 VOL57X59
VOL60X62 VOL63X65 VOL66X68 VOL69X71
-----
14 MEGAPOOL REGULAR DISK $ D000CDR1 D000AMA D000OCC1 $ $ $ $ $ $ $ $ $ $ $ $
$ $ $ $ $ $ F17LAMA F02LAMA $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $
$ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $
>cha VOL00X02
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
VOL00X02: $          $          $
>D000CDR D000CDR1 D000AMA
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
TUPLE TO BE CHANGED:
14 MEGAPOOL REGULAR DISK D000CDR D000CDR1 D000AMA D000OCC1 $ $ $ $ $ $ $ $ $
$ $ $ $ $ $ $ $ $ F17LAMA F02LAMA $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $
$ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
Regular volume D000CDR allocated.
WARNING : This POOL has a mixture of device
          types which is not recommended.
TUPLE CHANGED
JOURNAL FILE INACTIVE

```

Table release history update

Each individual volume field in table DIRPPPOOL is now replaced with a field that contains three volume names. The new field name represents the 3 volume names. For example, VOL24X26 represent volumes 24, 25, and 26. Table control will require 3 volume names be entered for each new volume range field. "\$" is still used for no volume name. Changing volume names with a one line command is not recommended. In order to change a specific range of volumes perform a change on the range and be prompted for the new volumes.

SOC is used to limit provisioning of more than 24 volumes per pool in table DIRPPPOOL. If more than 24 volumes are attempted to be provisioned in table DIRPPPOOL and the SOC state is IDLE, an error message is produced

indicating the SOC limitation, and the volumes are not provisioned. The SOC name for this functionality is BASE DIRP enh to 72 vol, and the ORDCODE is BASE0014.

Supplementary information

Volumes can be provisioned via table control or through the use of the MNT and DMNT commands at the MAPCI DIRP level. MNT and DMNT usage to provision volumes remains unchanged with this feature.

Translation verification other tools

The following example shows the output from MAPCI DIRP QUERY when it is used to verify the provisioned volumes in table DIRPPPOOL for a specific subsystem.

```
>mapci nodisp;mtc;iod;dirp;query ama all
MAPCI:
MTC:
IOD:
DIRP:
SSNAME  SSNO  SEQNO  ROTATES  POOLNO  PARLPOOL  EMERGENCY
AMA      3      1      0      14      NONE      ***YES***

REGULAR
FILE(S)  STATE  VOLUME  RECCOUNT  BLOCK  E  V  V_B  VLID  FNUM  FRN#
ACTIVE   AVAIL  F02LAMA      1      1  0  23  NO   8482  0036  3184
STANDBY1 AVAIL  F17LAMA      0      0  0  22  NO   84C2  007F  6188

PARALLEL
FILE      STATE  VOLUME  BLOCK  E  V  V_B  VLID  FNUM  FRN#
          NONE

REGULAR VOLUME(S)
VOL#  VOLNAME  STATE      IOC  CRD  PORT  VOL  FSEG  ROOM  VLID  FILES
0  D000CDR  READY      1    8  N/A    5    28    28  2805
1  D000CDR1  READY      1    8  N/A    6    29    29  2806
2  D000AMA  READY      1    8  N/A    1    19    19  2801
3  D000OCC1  READY      1    8  N/A    3    77    77  2803
22 F17LAMA  READY     N/A  N/A  N/A    2   120   120  84C2  S1
23 F02LAMA  READY     N/A  N/A  N/A    2   114   114  8482  A

REGULAR SPACE
VOL#  VOLNAME  STATE      SEGS    EXP  UNEXP  TOTAL
0  D000CDR  READY      28      0      0     28
1  D000CDR1  READY      29      0      0     29
2  D000AMA  READY      19      0      0     19
3  D000OCC1  READY      77      0      0     77
22 F17LAMA  READY     120      0      0    120
23 F02LAMA  READY     114      0      0    114
```

Name: DIRPOOL2**Functional description**

Feature Bridge SBB28 introduced table DIRPOOL2 in SNNCSH04. Table DIRPOOL2 links three DIRP pools in table DIRPPOOL for a subsystem listed in table DIRPSSYS. The three pools provide 72 volumes of storage capacity per subsystem.

Table DIRPOOL2 is created in feature A00003905 solely for the purpose of providing information needed to consolidate linked pools when moving to a load that now has 72 volumes per pool in table DIRPPOOL. The table is created at IPL. Its data is transferred during DART (if applicable). The table data is used during POSTSWACT to consolidate volumes in DIRPPOOL. At the end of POSTSWACT, table DIRPOOL2 is deleted from the switch.

Basic table functionality is provided during the duration of the ONP, but no data verification is done. Valid data is assumed from the old load (pre-SNNCSH07).

Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

DIRPPOOL

DIRPSSYS

DIRPOOL2

Size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
DIRPOOL2	0	24	Memory is allocated only during ONP and is freed afterwards.

Fields/OIDs

The following table lists fields for DIRPOOL2.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
ssysname	new	none	ssnamesr	DIRP subsystem name
poolnam1	new	none	poolname sr	DIRP pool name

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
poolnam2	new	none	poolname sr	DIRP pool name
poolnam3	new	none	poolname sr	DIRP pool name

Datafill example

The following example shows sample datafill for table DIRPOOL2 which was transferred from feature bridge SBB28 data in SNNCSH04.

```
Mate>table dirpool2
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: DIRPOOL2
Mate>lis all
TOP
SSYSNAME POOLNAM1 POOLNAM2 POOLNAM3
-----
          AMA  AMAPOOL MEGAPOL MCKYPOOL
BOTTOM
```

Table release history update

Table DIRPOOL2 is introduced by feature A00003905 solely for consolidating pool volumes linked via feature bridge SBB28. SBB28 introduced table DIRPOOL2 to link up to three DIRP pools to one DIRP subsystem allowing for a maximum of 72 recording volumes. Table DIRPOOL2 is used during ONP to consolidate the linked pool volumes under the main pool that is datafilled against the subsystem in table DIRPSSYS. Post-ONP, table DIRPOOL2 is deleted from the system, and SOC for feature A00003905 is used to provision more than 24 and up to 72 volumes per pool in table DIRPPOOL.

Supplementary information

None.

Translation verification other tools

Table DIRPOOL2 data can be verified post-RESTORE by listing the table on the inactive side during an ONP.

Consolidation can be verified by checking table DIRPPOOL after POSTSWACT to ensure that all linked pool volumes were moved under the main pool provisioned against the subsystem in table DIRPSSYS.

Software optionality control (SOC)

SOC

SOC option name:	BASE DIRP enh to 72 vol
SOC option title:	Yes
SOC option control type:	State
New SOC option?	Yes
SOC option order code	BASE0014
Option defined in DRU:	BASE
Affected products:	DIRP

SOC state IDLE limits the number of provisionable volumes per pool in table DIRPPool to 24. SOC state ON increases the total number of volumes per pool to 72.

Command interface changes

Directory: MAPCI;MTC;IOD;DIRP

Directory description

DIRP provides the ability to perform a variety of commands against DIRP subsystems.

Accessing directory: DIRP

Access to directory or MAP level and return to CI
MAPCI;MTC;IOD;DIRP

QUIT ALL

Command: MNT

Command type: MENU

Command target: All

Command availability: RES

Command description

MNT mounts a specific volume to a specific DIRP subsystem.

Command syntax

MNT <DIRP subsystem> <volume name>

Qualifications and warnings

Feature A00003905 SOC limits the number of volumes provisionable per DIRP subsystem if the SOC state is IDLE. If the state is IDLE, only 24 volumes can be provisioned per DIRP pool in table DIRPPPOOL. If more than 24 volumes are attempted to be provisioned with SOC state IDLE, an error message is produced, and the volume is not mounted against the subsystem.

The SOC name for this functionality is BASE DIRP enh to 72 vol, and the ORDCODE is BASE0014.

Responses

DIRP Volume Expansion SOC is not ON. Cannot mount more than 24 VOLUMES per POOL.

The user is trying to allocate more than 24 volumes per pool with the SOC state for feature A00003905 IDLE.

MAP outputs with associated meanings and actions

Command: DIRP MNT
DIRP Volume Expansion SOC is not ON. Cannot mount more than 24 VOLUMES per POOL.
Meaning: Cannot mount more than 24 volumes per pool in table DIRPPPOOL
System or user actions:
The user needs to purchase functionality under feature A00003905 if they want to provision more than 24 volumes per pool in table DIRPPPOOL.



SN07 Feature Deltas

Product = CS 2000

A00003933 -- Succession Communication Server (SCS) 2000 - Session Server Manager: SCS 2000 - SIP Gateway application (PT-IP)

Functional Description

This activity delivers an RFC 3261 Compliant Interface for the CS 2000 enabling open interoperability with call servers, application servers, and proxy servers using the Session Initiation Protocol (SIP).

The Session Server Manager and SIP Gateway application are part of the SN07 release.

Feature Synopsis

Activity List

Activity A00003933 is the repository for all the FN information associated with the Session Server Manager - SIP Gateway application. The list of activities addressed by this FN includes:

- A00003270 SIP Open Interop Call Processing
- A00003271 Session Server Web Server Interface
- A00003272 Session Server Provisioning Framework
- A00003273 SIP Gateway Application Maintenance
- A00003279 SIP on Session Server Link Maintenance and Load Balancing
- A00003281 SIP on Session Server Call Audit
- A00003933 SIP on Session Server ICAF
- A00003277 Session Server OM Subsystem
- A00003280 SIP on Session Server Tracing/Debug Framework
- A00003282 SIP on Session Server Datasync

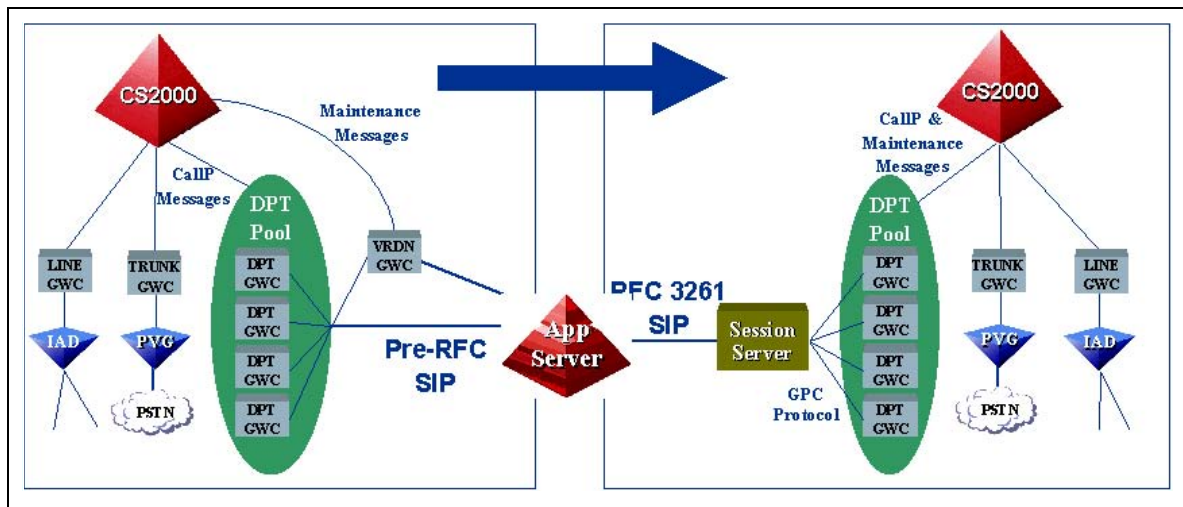
- A00003934 Session Server Project ICAF
- A00004271 SIP App Server SOC
- A00004414 SIP Call Server SOC

Project Background

SIP is a protocol designed for multimedia communication. The current SCS 2000 SIP offering is a proprietary implementation of SIP for Telephones (SIPT) based on earlier drafts of the SIP specifications. The SCS 2000 SIP implementation was developed to communicate between two CS 2000s and to the Multi-Media Communication Server (MCS). This implementation was available in SN04.

Market drivers are pushing the implementation of SIP to an open interoperability (interop) standard. To meet this requirement, the Session Server Manager is being developed to convert open interop SIP messaging into messages understandable by the CS 2000.

SIP on CS 2000 Evolution



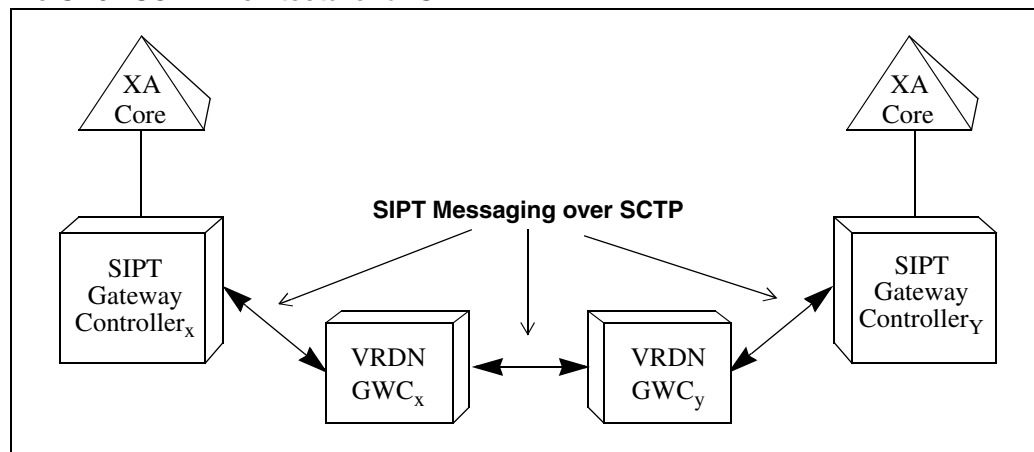
Pre-SN04 VRDN SCTP architecture

In the initial implementation of SIPT for GWC, signaling path established calls from the VRDN to the remote node. The nodes included SIPT and VRDN gateway controllers. The SIPT gateway controller's function is to process the call while the VRDN is responsible for routing the call. A signaling path exists between the SIPT Gateway Controllers and the VRDN, and between the VRDN and the remote Call Server. Call State is maintained in the VRDN.

The VRDN architecture dynamic packet trunking (DPT) call traverses the following four node types. A visual representation of this architecture is shown in the following figure.

- local SIPT and VRDN gateway controller
- remote VRDN and SIPT gateway controller

Pre-SN04 SCTP Architecture for SIPT



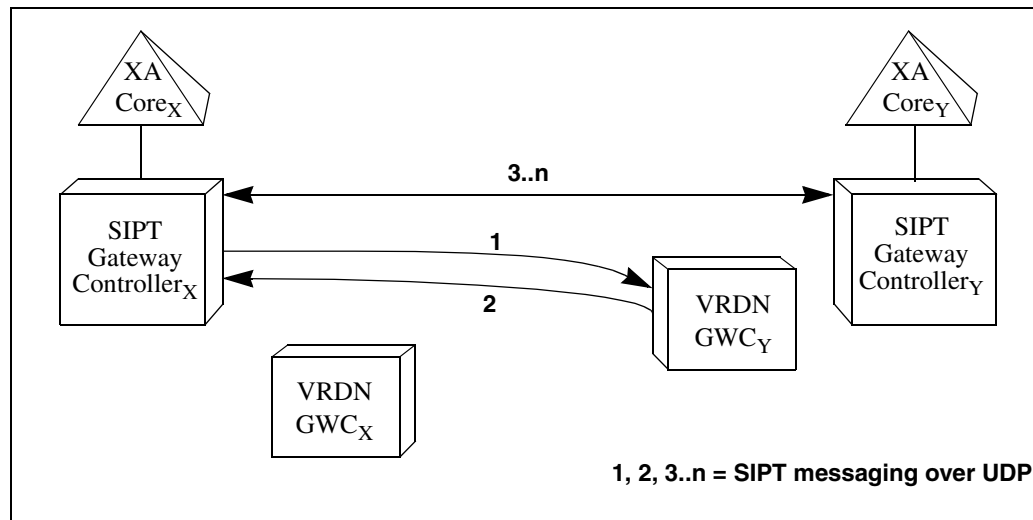
A quick summary of the steps in this figure are as follows:

- GWC_x composes an INVITE message and sends it to a local VRDN.
- Local VRDN_x determines which remote VRDN is applicable and then forwards the INVITE.
- Remote VRDN_y receives the INVITE and determines which of its SIPT gateway controllers should receive the INVITE message. The INVITE message is then sent to that SIPT gateway controller (GWC_y).

Post-SN03 VRDN architecture

In order to overcome limitations when using the previous architecture, a new SIPT architecture was introduced in SN04 (i.e. GWC07). Activity A59034776: “VRDN Capacity Enhancements” provides the majority of the functionality. The purpose of the new architecture was to decrease dependency on the local and remote VRDN.

In the previous architecture, a call from an originating SIPT GWC traverses local and remote VRDN before reaching the destination SIPT gateway controller. With the new architecture, the originating SIPT GWC sends its INVITE directly to the remote VRDN. The remote VRDN replies to the originating SIPT GWC with a 302-Temporarily Moved instead of forwarding the INVITE to the remote SIPT GWC. The 302 message contains the necessary information to contact the remote SIPT GWC. After receiving the 302, the local SIPT GWC sends the INVITE directly to the remote SIPT GWC. A diagram of the new architecture is shown below.

Post-SN03 VRDN Architecture for SIPT

A quick summary of the steps shown in this figure are as follows. Note the local VRDN for $XA-Core_X$ is still utilized when call originates from the remote $XA-Core$.

- Based on MGCINV datafill, a remote VRDN is selected. An INVITE message is sent to that MGC.
- The VRDN on the remote replies with a 302-Temporary Moved message indicating a SIPT GWC for the remote $XA-Core$. The contact header in the 302 contains the necessary information to reach GWC_Y .
- After receiving the 302 message, $SIPT\ GWC_X$ sends an INVITE to GWC_Y , which decides it will accept the call. Standard SIP messaging for call setup is performed. Once the call is complete, it is taken down via the standard SIP mechanisms.

VRDN Architecture Limitations

In the VRDN architectures, the SIP stack resides in the gateway controllers and is not compliant to RFC 3261.

In order to move forward in terms of supporting SIP compliancy and greater call volume, a new SIP architecture needs to be created. Hence, the origination of the Session Server Manager platform.

Pre-Session Server Manager OAMP Relationships

Before discussing the Session Server Manager platform, the current OAMP component relationship is presented so an understanding of the current scenario exists.

Component Relationships

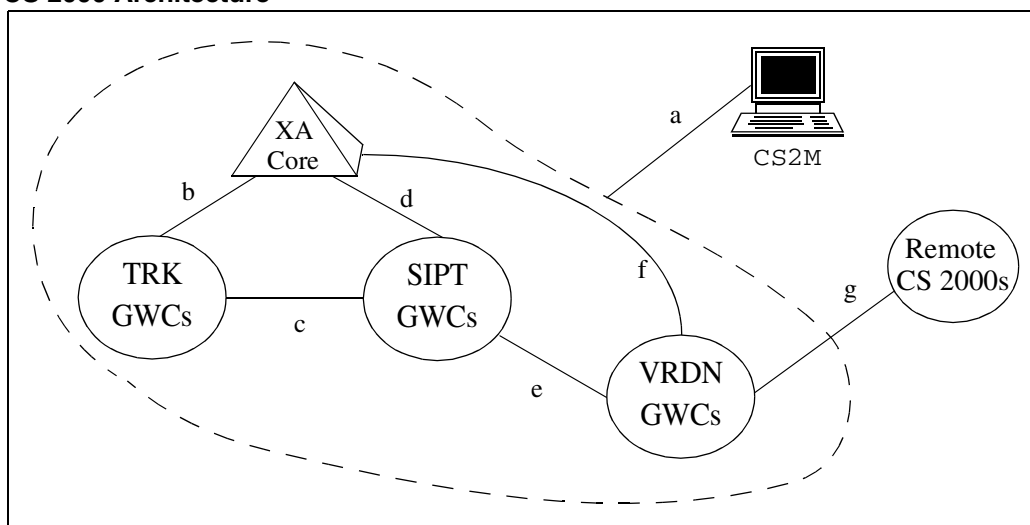
The main components with respect to SIPT call processing are shown and described briefly.

SIPT call processing components

Node	Function
XA-Core	General call processing engine of the CS 2000. The XA-Core connects to the IP network via the HIOP and the SDM. SDM is used by CS2M (formerly known as SESM) and the HIOP is used for GWC communications.
TRK GWCs	Functions as the interface between the XA-Core and gateways such as the PVG.
SIPT GWCs	Functions as interface between TRK GWC and the VRDN. Contains SIP call processing functions.
VRDN GWCs	Functions as the “router” to direct incoming/outgoing calls to the appropriate local or remote GWC.
CS2M	General OAM&P platform for most CS 2000 peripherals. Formerly known as SESM.

The figure and follow-on explanation shows and explains at a high level the relationships between each CS 2000 node.

CS 2000 Architecture



- CS2M provides OAM&P functions for the GWC and Core in the CS 2000 network. CS2M's interaction with the core consists of provisioning datafill such as certain pieces of gateway controller data (e.g. table SERVINV). CS2M is the main OAM&P component for gateway controllers. OAM&P functions include node and unit provisioning, maintenance, and reporting of performance metrics, logs, and alarms.
- While CS2M provides most of the OAM&P functions for the trunking GWC, core tables are also utilized for call processing. These tables include SERVINV, TRKMEM, and TRKSGRP.
- Only a CallP relationship exists here. This interaction consists of peer messaging in support of outgoing DPT call being routed to, or coming from, a SIPT gateway controller.

- d. The local call server uses the SIPT gateway controller to handle DPT calls. Outgoing calls destined for a remote call server are routed through a SIPT gateway controller. For the outgoing call, the core sends the trunk profile index with the IAM which maps to a destination MGC and Telephony Profile in the SIPT GWC. This information determines the remote destination MGC.

The SIPT gateway controller performs SIP processing and sends out a SIP Invite to the remote MGC. If SCPT is the transport protocol, a local VRDN is utilized. Incoming calls to the SIPT GWC originate from the local VRDN or remote MGC depending on the transport protocol used.

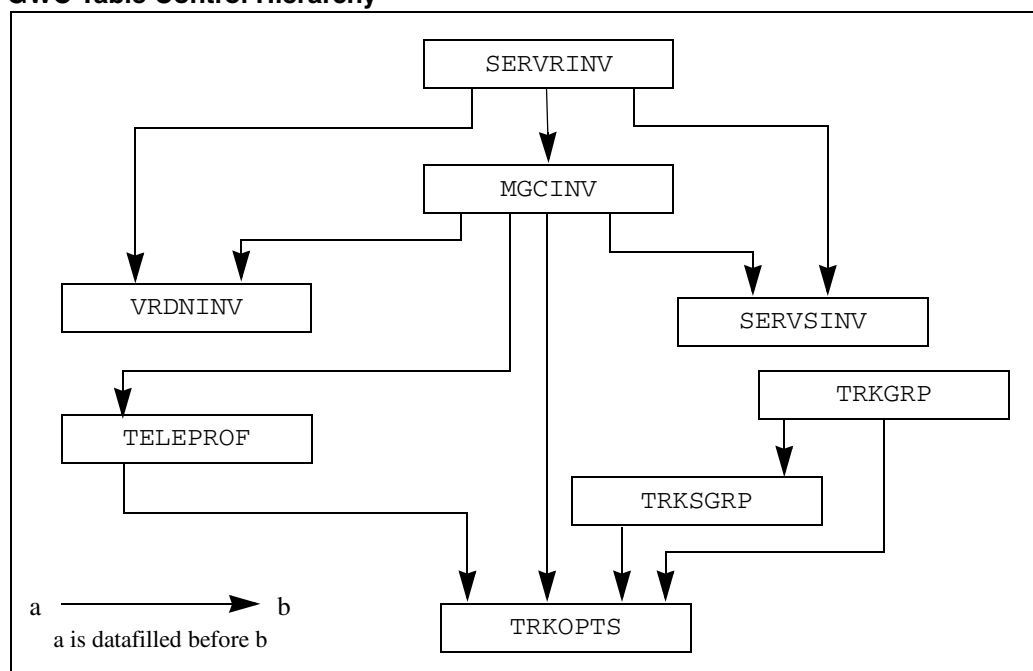
Datafill from tables SERVINV, SERVSINV, MGCINV, TELEPROF, TRKSGRP, DPTRKMEM, and TRKOPTS are utilized to perform call processing for the incoming and outgoing call.

- e. From an OAM&P perspective, datafill in MGCINV and VRDNINV indicate the MGC for a remote call server. The local call server utilizes the VRDN to route the outgoing call to the remote call server. For an incoming call, the VRDN picks a local SIPT gateway controller to handle the incoming call.
- f. Represents maintenance interactions.
- g. Represents an outgoing call to remote SIP node or an incoming call.

Provisioning

On the core, the below figure illustrates the table control relationships for gateway controllers followed by a brief description of each table. Not every possible table is shown and described.

GWC Table Control Hierarchy



Pre-Session Server Manager GWC table descriptions

Table	Description
SERVRINV	Stores provisioned data for gateway controllers including IP addresses, exec information, etc. Gateway controllers are provisioned in CS2M, and then the system automatically enters required datafill in SERVRINV.
MGCINV	Defines remote media gateway controllers for other Call Servers and their associated IP addresses, related virtual router distribution nodes, and connection protocols.
VRDNINV	Defines the locations of the VRDNs and the remote MGCs, which they serve. A VRDN is a dual-purpose device that handles outgoing routing and incoming distribution.
SERVSINV	Contains the names of the server subtending nodes and their associated gateways. The subtending nodes are the Audio Controller and the Dynamic Packet Trunk (DPT).
TELEPROF	Defines the link between a telephony profile and a destination media gateway controller (MGC).
TRKGRP	Contains customer-defined data for each trunk group that exists in the switch.
TRKSGRP	Lists the supplementary information for each subgroup that is assigned to one of the trunk groups listed in table TRKGRP.
TRKOPTS	Provisions special options on trunk groups. For our case, that option is <code>dynamic</code> and the signaling type is <code>SIPT</code>

When utilizing a Session Server Manager-only architecture, many of the above tables may be obsolete. Refer to upcoming sections for complete details.

Session Server Manager Description and Overview

The Session Server Manager is a platform for delivery of multiple applications. The Session Server Manager consists of a NEBS Level 3 compliant hardware platform plus a software framework and architecture for developing Carrier Grade applications and services. The SIP Gateway application is the initial application for the Session Server Manager platform.

Hardware

The hardware platform for the Session Server Manager is the Hewlett Packard HP-CC3310. Components include:

- Dual Intel 2.4 GHz P4 Xeon Processors
- Up to 12 GB RAM (Session Server is 4 GB)
- Memory Speed – 266 MHz DDR
- Local Disk – Dual 73GB or 146GB disk drives (Session Server is 73 GB)
- Multiple GigE copper interfaces (2 on-board plus 2 per NIC)
- 2U Form Factor

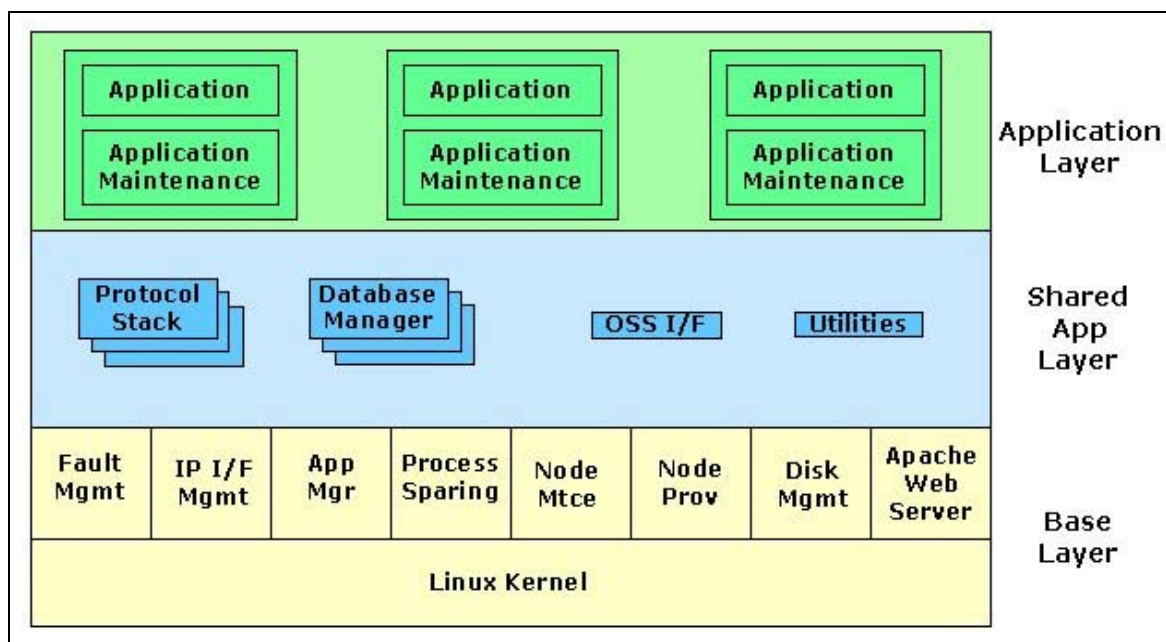
The HP-CC3310 provides processing, memory, and disk capacity for Storage Management (STORM), SIP, and planned SIP applications

Software

The Session Server Manager Software has a layered architecture, which consists of the following:

- **The base layer**, which includes the Linux kernel along with a carrier-grade platform for fault management, sparing, and application initialization
- **A shared application layer**, which contains re-usable components that can be integrated as needed into higher level applications
- **An application layer** that includes a maintenance process for each application, which manages the associated processes.

Session Server Manager Software Architecture



Session Server Manager Base Layer

The base layer uses Linux version 2.4.22. This base layer provides Carrier Grade capabilities.

Note: This section represents an SN07 view.

Fault/SWACT Management

- Detects hardware faults on the platform
- Monitors for conditions that should prompt an activity switch
- Arbitrates failure requests from applications that need to initiate a SWACT.

IP Interface Management

- Maintains Gigabit Ethernet interfaces on the platform
- Allocates bandwidth to maintenance and application tasks
- Participates in the IP address takeover during an activity switch.

Application Manager

- Provides an interface for applications to bind their maintenance processes into the system
- Monitors and re-initiates application maintenance process as needed
- Provides a possible re-use of SDM application manager software platform.

Node Maintenance

- Provides interfaces for bringing the node into service and initiating application start-up
- Provides a craftsperson interface via a Web Server
- Supports manual and autonomous maintenance actions
- Monitors between active and inactive nodes to that insure failover can be initiated when running in synchronization.

Node Provisioning

- Provides a provisioning interface via Web Server for platform configuration parameters.

Disk Management

- Provides interfaces for disk access
- Supports the STORM application in CS 2000-Compact configurations.

Apache Web System

- Consists of Apache, Apache Tomcat, and Java Runtime environment
- Provides web-based interface for provisioning and maintenance
- Presents an integrated view for all applications running on the platform.

Session Server Manager Share Layer

The share layer contains reusable components that are independent of the applications using them.

Note: This section represents an SN07 view.

Application Data Synchronization

- Allows applications to checkpoint data between the active and inactive units at specific points in time.
- Supports variable length buffers that can be refined and versioned by the application

SIP Stack

- Provides an RFC-3261 compliant SIP interface, which can be incorporated into any application running on the platform
- Allows APIs and callback interfaces that permit applications to implement state machines based on event notifications.

Database Manager

- Provides persistent data storage for each application
- Introduces a SQL based database, which is accessed through ODBC and JDBC interfaces, that isolates each application from the underlying database product
- Supports data replication between active and inactive units, and ultimately between multiple active units.

Downstream Interfaces to Billing and OMs/Statistics

- Provides a collection point for billing, and OM data for the system
- Stores information to local disk, which can be accessed via maintenance interfaces
- Opens downstream feeds, in CS 2000 configurations, to SDM for billing and IEMS (Integrated Element Management System) for logs, alarms, and statistics.

Application-specific processes

These applications-specific processes include:

- An application maintenance process
 - Initiates and then monitored by the base layer application manager
 - Creates all other processes associated with the application
 - Provides maintenance actions to transition the application in and out of service.

- Call/Transaction Processing process(es)
 - Initiates and then monitored by base layer application manager
 - Creates all other processes associated with the application
 - Provides maintenance actions to transition the application in and out of service.

Session Server Manager Application Layer

The Application Layer consists of a set of applications. The applications may or may not communicate with each other. Each application includes a maintenance application used for monitoring and interacting with the application. The SIP Gateway is the initial application delivered on the Session Server Manager.

CS 2000 Architecture with Session Server Manager

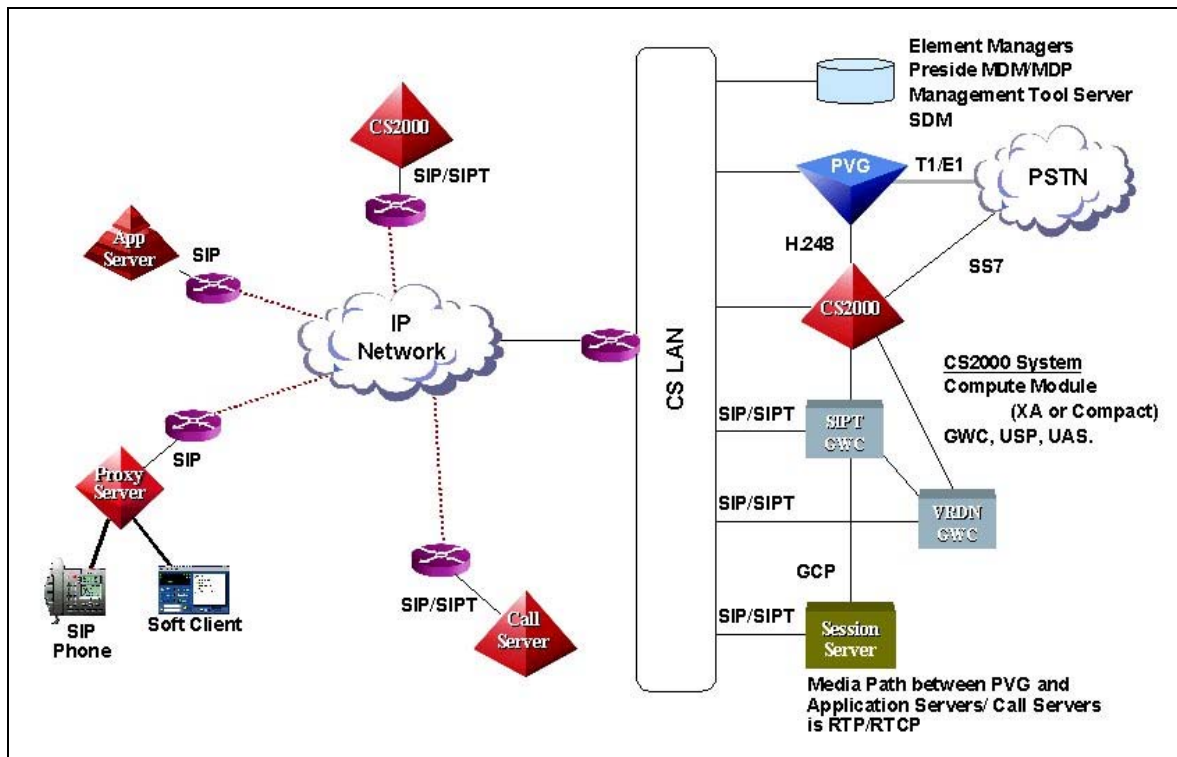
VRDN Present

With the Virtual Router Distribution Node (VRDN) present, the Session Server Manager is a peer to the VRDN. The SIPT Gateway Controller will maintain current calls through the VRDN, but will establish new calls through the Session Server Manager. Once the Session Server Manager is providing the SIP Call Processing function and no calls are left on the VRDN, the VRDN can be removed.

Note 1: Installation of the Session Server Manager at the Near End Call Server, requires actions at the Far End Call Server. These actions are addressed in the upgrade section.

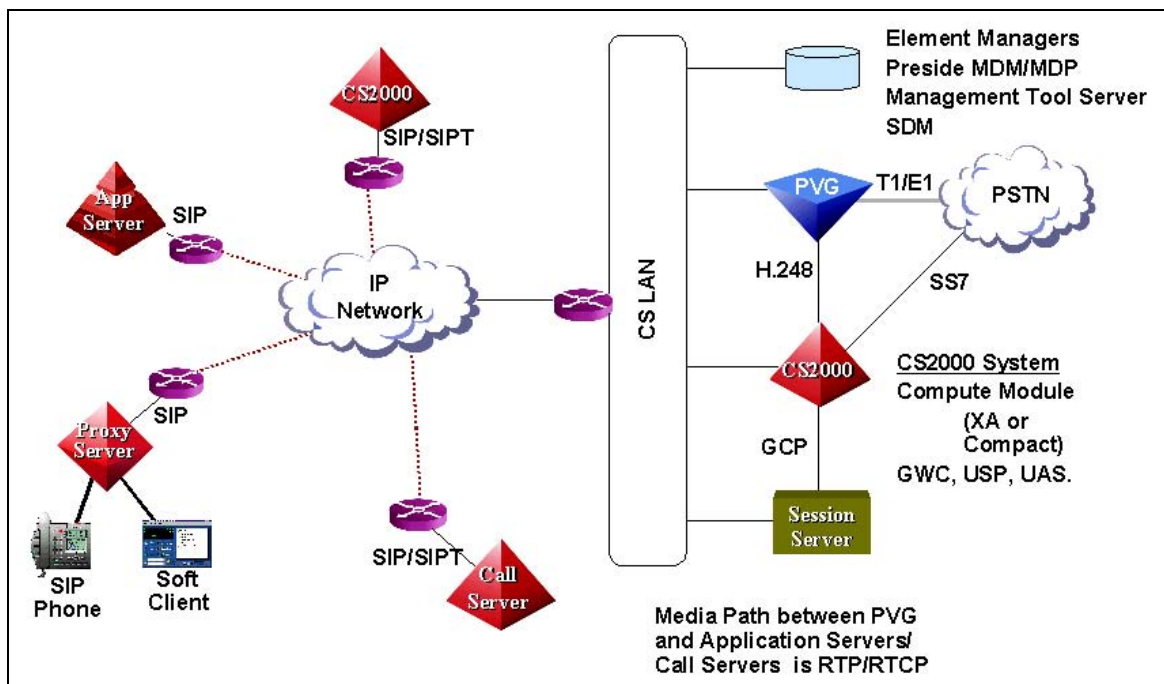
Note 2: Once the Session Server Manager is installed in a SCS 2000, the VRDN is to be removed. A configuration with Session Server Manager and VRDN in the same SCS 2000, is only supported as an upgrade path.

Session Server Manager with the VRDN present



VRDN not Present

When the VRDN is not present, the SIPT Gateway Controller establishes all calls throughout the Session Server Manager.

Session Server Manager with the VRDN not present**Services and Features**

The Session Server Manager interoperates with User Agents on the SIP Network.

- Calling Number Delivery / Blocking
- Calling Name Delivery / Blocking
- Suspend / Resume Handling

SIGNALING INTEROPERABILITY

- TDM signaling
 - ANSI ISUP
 - ANSI PRI
- Variants

SIP Signaling from the Session Server Manager is tunneled into the CS 2000 as Dynamic Packet Trunks (DPT). The DPT trunk datafill in the CS 2000 DPT Trunks are provisioned as ISUP trunks. For the SIPT implementation, any variant is allowed for the DPT trunks. SIPT allows transport of the ISUP payload in the SIP message. Transport is in accordance with the T1S1.7/2003-179R2 - T1.SIP Interworking Output Baseline Document.

SIP Gateways may not support SIPT and not provide an ISUP payload in the SIP message. When communicating with a SIP Gateway that does not provide ISUP payload in the SIP message, the CS 2000 can generate an ISUP payload; however, the payload will be based on the variant type of the DPT trunk. The SIP implementation can only generate ISUP payload for IBNT2 (for NA loads), IBN7 (for International loads), or IT.

Note: DPT trunks to SIP gateways can only be provisioned as IBNT2/IBN7 or IT.

BEARER INTEROPERABILITY

- Media
 - Fax -G3, T.38
 - DTMF- In-band G.711, Out-of-band RFC2833
 - CODEC -G.711 A/u-law, G.729a/b, codec negotiation
 - H.248

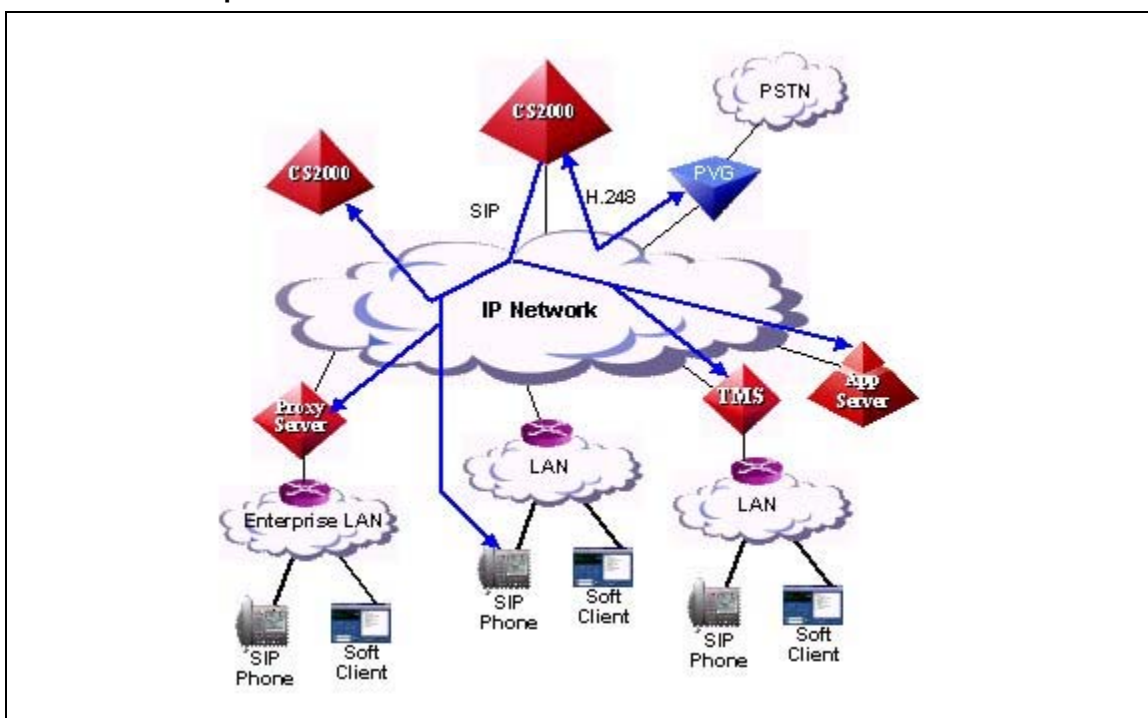
MCS & CS 2000 INTEROPERABILITY

- All SIPT supported services and functionality carried over from SN06 are supported on the Session Server Manager
- Backward SIPT compatibility with previous release
- CS 2000 with SN07 is supported with MCS 3.0.

SIP Compliancy

The initial offering is to allow interoperability with third party proxy servers and application servers. This implementation will update Nortel's compliance to the current IETF standards and drafts.

SIP Standards Compliance



The solution will provide support for (but not limited to) the following standards and drafts:

- RFC 3261¹ - SIP: Session Initiation Protocol
- RFC 3262 - Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
- RFC 3326 - SIP Reason Header

1. Session Server Manager commits to those requirements pertinent to a User Agent Client. Session Server Manager is not a User Agent Server, nor a Back to Back User Agent in SN07.

- RFC 2976 - The SIP INFO Method
- RFC 3264² - An Offer/Answer Model with the Session Description Protocol (SDP)
- RFC 3265 – Specific Event Notification (SUBSCRIBE/NOTIFY)
- RFC 3311 - The Session Initiation Protocol (SIP) UPDATE Method
- RFC 3323 - A Privacy Mechanism for the Session Initiation Protocol (SIP)
- RFC 3325 - Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
- Referred-by Mechanism – draft-ietf-sip-referredby-02
- Q.1912.5 - Interworking Between Session Initiated Protocol (SIP) and Bearer Independent Call Control Protocol or ISDN User Part
- SIP Replaces Header – draft-ietf-sip-replaces-03
- SIP Call Control Transfer – draft-ietf-sipping-cc-transfer
- T1S1.7/2003-179R2 - T1.SIP Interworking Output Baseline Document

SIP Call Processing

In the SN07 release of the Session Server Manager platform, the SIP Gateway application is the only application supported. This section discusses high-level details about this application, and the differences between the Session Server Manager- and GWC-based SIP call processing.

Also presented are example call flows for an incoming and outgoing SIP call.

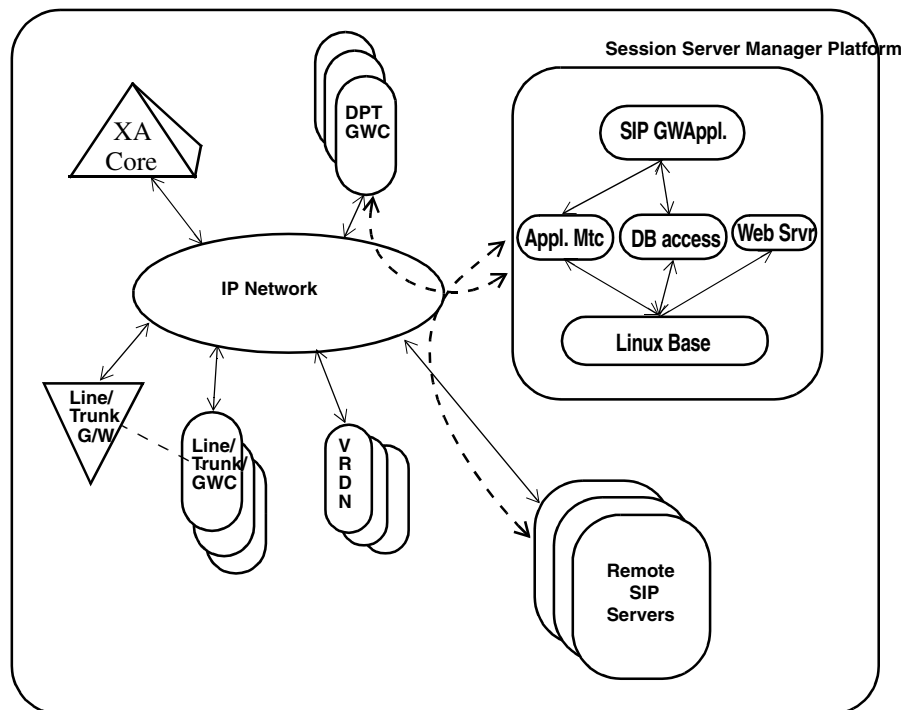
Description and Overview

The SIP Gateway application on the Session Server Manager platform is the entity primarily responsible to set-up and tear-down calls, maintain accessibility to DPT GWCs and remote SIP servers, and other functions. The SIP Gateway application provides an RFC 3261 compliant SIP interface for interworking. This application also provides the necessary support to be compliant with other RFCs including 3262 (Reliability of Provisional Responses in SIP), and 3264 (SIP Event Notification Mechanism).

The following figure illustrates a high-level view of the Session Server Manager when placed within a SCS 2000 SIP solution.

2. For SIP to SIP calls, as a B2BUA, we are compliant with RFC 3264.

For SIP to H.248 calls, as a terminating gateway, we are partially compliant due to incompatibilities between the specifications.

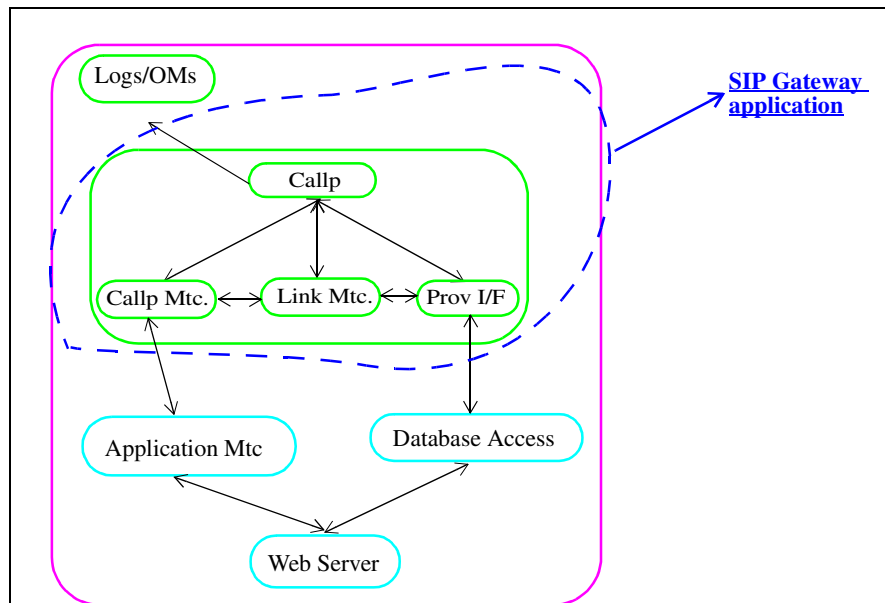
Session Server High-Level view

With the new platform, SIP call processing is done within the call processing application in the Session Server Manager. The Session Server Manager communicates with the DPT GWC in a generic call control/maintenance protocol, which will trigger the usage of Dynamic Packet Trunking (DPT) infrastructure to setup and tear-down calls.

As illustrated in Figure , "Session Server High-Level view", the Session Server Manager communicates with all the DPT GWCs as well as with remote SIP servers. In this model, all SIP-specific behavior is performed on the Session Server Manager as opposed to the GWC. CS 2000 SIP solution with a Session Server Manager does not require a VRDN, and the tasks originally performed by the VRDN are moved into the Session Server Manager.

Additionally, numerous configuration/maintenance capabilities are also provided within the Session Server Manager and are discussed in subsequent sections of this document.

The SIP Gateway application in the Session Server Manager interworks with different logical components, including call setup, maintenance, and provisioning, to satisfy different roles and responsibilities. Figure , "Session Server SIP Gateway application Logical View" illustrates the different logical components that constitute a SIP Gateway application.

Session Server SIP Gateway application Logical View

- **Call Processing Application:** This is the main component responsible for integrating different logical components to enable setup/tear-down of calls. It is responsible to send/receive incoming SIP messages, parse/analyze the message, and take appropriate action. It maintains a call state machine and generates OMs and logs whenever necessary. It also triggers a billing application to generate a billing record for calls.
- **Call Processing Maintenance:** This component provides the interface for interworking with an application maintenance entity to perform maintenance activities on the SIP Gateway application. When a craftsperson performs a maintenance action, this component is ultimately notified and performs the necessary action. Please see “SIP Gateway application maintenance” on page 1473 for additional information.
- **Link Maintenance:** This component is responsible for maintaining the availability of remote SIP servers as well as the availability of SIP GWCs. When bringing the SIP Gateway application into the server, this component discovers and maintains the list of SIPT GWCs available for call processing. In addition, this component is also responsible for maintaining a list of remote SIP servers that are available for communication.
- **Provisioning Interface:** This component provides the call processing entity access to all the provisioned data. Call processing queries this

component at various points, including startup, take-down, and call setup, to determine the course of action to be taken.

- **OMs/Logs:** Different components interact with OM/log subsystem to generate logs and OMs. Please refer to sections [“Logs” on page 1479](#) and [“Operational Measurements” on page 1480](#) for additional information.

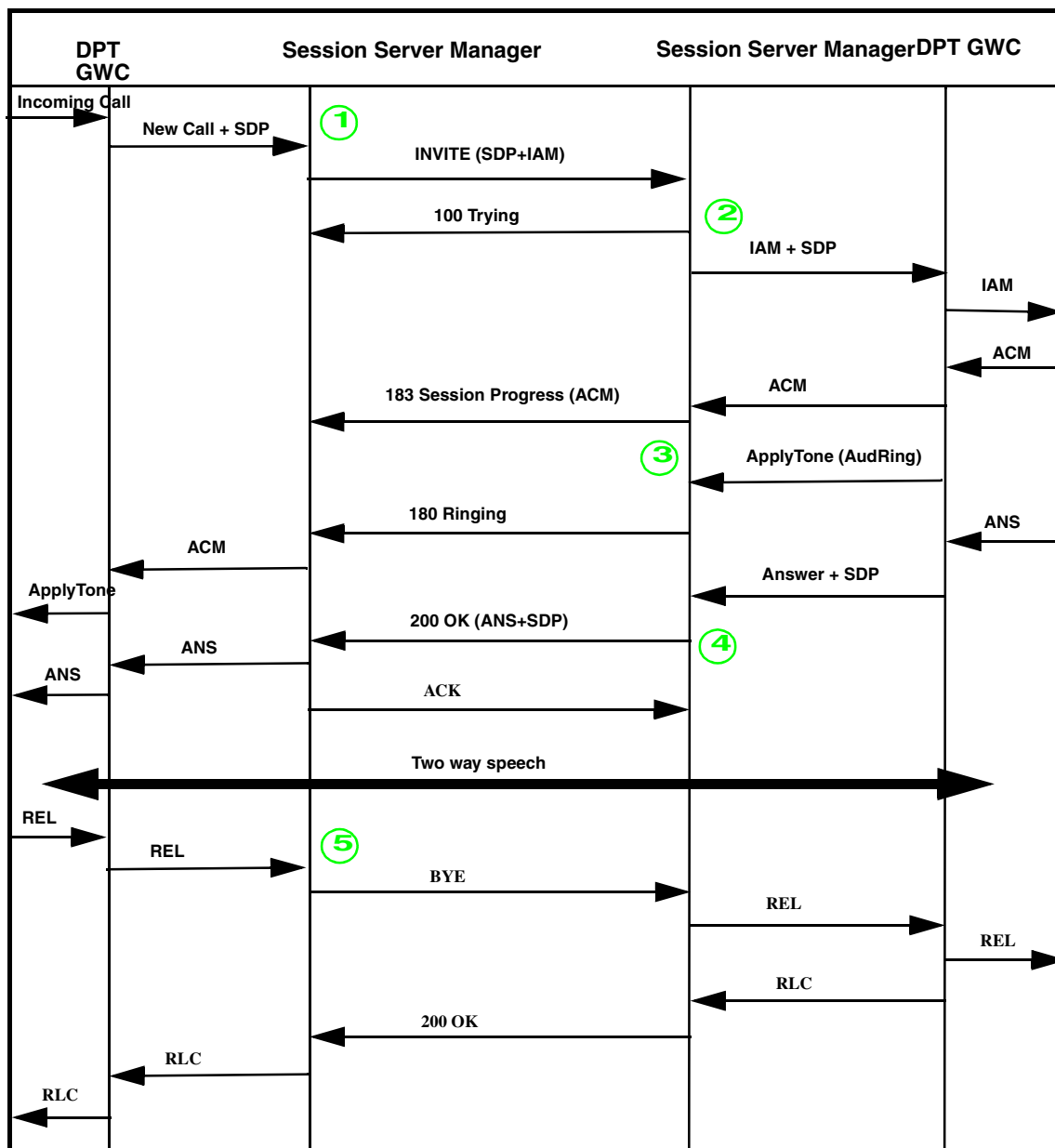
Call Flows

Both incoming and outgoing calls between SIP and the Session Server Manager make use of table SIPLINK that is datafilled in the core. SIP Access Link name information from table SIPLINK is downloaded to the Session Server Manager during the DPT GWC discovery process. In order to have successful call processing with a remote SIP server, each remote SIP server must be associated with SIP Access Link name. The SIP Access Link name is uniquely associated with a trunk group in the Core which in-turn is used for set-up of translations for various call-types.

Please refer to the configuration section of this document for more information on table SIPLINK.

Figure [“Sample Session Server Manager SIP Call Flow” on page 1418](#) captures a sample call flow for a SIP bridging scenario with Session Server Manager on both sides. Key points on the incoming and outgoing side of the call are discussed.

Sample Session Server Manager SIP Call Flow



For the purpose of this call flow, it is assumed that the core is already set up with translations to route the call over appropriate SIP trunk. A trunk is considered a SIP trunk if it is datafilled as SIPT in table TRKOPTS.

Also, it is assumed that the call flow is happening on a reliable transport protocol like TCP.

1. The core selects one DPT GWC to process the outgoing call. If there is more than one DPT GWC, then the core employs a round-robin algorithm to determine the GWC to which to present the call.

On receipt of the IAM message, the DPT GWC on receipt of the IAM message does the following:

- a. Extracts the trunk information and determines if a SIP Access Link is associated with this trunk.
- b. If a SIP Access Link is not associated with this call, the call is setup as a pre-Session Server Manager SIP call.
- c. If a SIP Access Link is associated with this call, the IP address of the Session Server Manager is retrieved and the IAM is forwarded to the Session Server Manager. (The IP address of the Session Server Manager is sent to the GWC as part of the GWC discovery process. This is discussed in the configuration section).
- d. The Session Server Manager then extracts the SIP Access information and retrieves information regarding the remote SIP server to which the call is intended.
- e. The SIP INVITE message is constructed with appropriate headers, session description, and payloads (if applicable) and is sent to the remote SIP server.

A sample INVITE message is shown below:

```
INVITE sip:2461803@47.174.73.242 SIP/2.0
From: <sip:9192461802@47.142.210.200>;tag=c8d28e2f-13c4-3f7776e3-160d-41bac49c
To: <sip:2461803@47.174.73.242>
Call-ID: 0094.4609-28-17-05-18.82@MGCA
CSeq: 1 INVITE
User-agent: CS2000/7.0
Mime-Version: 1.0
Max-Forwards: 70
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,NOTIFY,REFER
Via: SIP/2.0/TCP 47.142.210.200:5060;branch=z9hG4bK-3f7776e3-160d-11156ea5
Contact: <sip:9192461802@47.142.210.200>
Content-Type: multipart/mixed ;boundary=unique-boundary-1
Content-Length:358

--unique-boundary-1
c: application/SDP ;charset=ISO-10646
v=0
o=MGCP 0 0 IN IP4 47.174.73.241
s=MGCP Call
c=IN IP4 47.174.73.241
t=0 0
m=audio 5004 RTP/AVP 0 96
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20

--unique-boundary-1
c: application/ISUP ;version=gr394 ;base=gr394
"
```

2. On receipt of an incoming SIP call, the Session Server Manager sends back a 100 Trying message to the sending entity while the INVITE is processed. A call processing application retrieves the host or IP address information from the header information to determine the characteristics of the sending entity.

Once the remote server profile is retrieved, the SIPLINK name associated with the remote SIP server is retrieved. The ISUP IAM payload, if any, is also retrieved and forwarded to the DPT GWC along with the SIPLINK information.

The DPT GWC gets the SIP LINK information from the Session Server Manager and determines the trunk, on which the incoming call is processed.

A sample SIP 100 Trying message:

```
SIP/2.0 100 Trying
From: <sip:9192461802@47.142.210.200>;tag=c8d28e2f-13c4-3f7776e3-160d-41bac49c
To: <sip:2461803@47.174.73.242>;tag=f249ae2f-13c4-3f777333-25a1-3e96679d
Call-ID: 0094.4609-28-17-05-18.82@MGCA
CSeq: 1 INVITE
Server: CS2000/7.0
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY
Via: SIP/2.0/TCP 47.142.210.200:5060;received=47.142.210.200;branch=z9hG4bK-3f77
76e3-160d-11156ea5
Contact: <sip:2461803@47.174.73.242>
Content-Length:0
```

3. Once the incoming INVITE is processed, the remote SIP server can send any number of provisional responses (18X). ISUP payloads, such as ACM or CPG, are encapsulated in an appropriate provisional response if the remote server is capable of handling ISUP messages.

It is also possible that the provisional responses are used to apply local ringing and/or pass any media information to which the terminating side would like the originating side to hear.

A sample 183 Session Progress and 180 Ringing messages are as follows:

180 Ringing:

```
SIP/2.0 180 Ringing
From: <sip:9192461802@47.142.210.200>;tag=c8d28e2f-13c4-3f7776e3-160d-41bac49c
To: <sip:2461803@47.174.73.242>;tag=f249ae2f-13c4-3f777333-25a1-3e96679d
Call-ID: 0094.4609-28-17-05-18.82@MGCA
CSeq: 1 INVITE
Server: CS2000/7.0
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY
Via: SIP/2.0/UDP 47.142.210.200:5060;received=47.142.210.200;branch=z9hG4bK-3f77
76e3-160d-11156ea5
Contact: <sip:2461803@47.174.73.242>
Content-Length:0
```

183 Session Progress:

```
SIP/2.0 183 Session Progress
From: <sip:9192461802@47.142.210.200>;tag=c8d28e2f-13c4-3f7776e3-160d-41bac49c
To: <sip:2461803@47.174.73.242>;tag=f249ae2f-13c4-3f777333-25a1-3e96679d
Call-ID: 0094.4609-28-17-05-18.82@MGCA
```

```

CSeq: 1 INVITE
Server: CS2000/7.0
Supported: 100rel
Allow: ACK, BYE, CANCEL, INVITE, OPTIONS, INFO, SUBSCRIBE, REFER, NOTIFY
Via: SIP/2.0/UDP 47.142.210.200:5060;received=47.142.210.200;branch=z9hG4bK-3f77
76e3-160d-11156ea5
Contact: <sip:2461803@47.174.73.242>
Content-Type: application/SDP ;charset=ISO-10646
Content-Length:171

v=0
o=MGCP 0 0 IN IP4 47.174.73.241
s=MGCP Call
c=IN IP4 47.174.73.241
t=0 0
m=audio 5006 RTP/AVP 0 96
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20

```

4. When the terminating side answers the call, it forwards the ANS ISUP message (if applicable) along with its session description in a 200 OK message to the originating side.

The originating side extracts the relevant information and forwards the terminating SDP to the appropriate endpoint. It also returns a SIP ACK request to the terminating SIP server to complete the three-way hand-shake.

A sample 200 OK and ACK messages are as follows:

200 OK

```

SIP/2.0 200 OK
From: <sip:9192461802@47.142.210.200>;tag=c8d28e2f-13c4-3f7776e3-160d-41bac49c
To: <sip:2461803@47.174.73.242>;tag=f249ae2f-13c4-3f777333-25a1-3e96679d
Call-ID: 0094.4609-28-17-05-18.82@MGCA
CSeq: 1 INVITE
Server: CS2000/7.0
Content-Transfer-Encoding: binary
Supported: 100rel
Allow: ACK, BYE, CANCEL, INVITE, OPTIONS, INFO, SUBSCRIBE, REFER, NOTIFY
Via: SIP/2.0/UDP 47.142.210.200:5060;received=47.142.210.200;branch=z9hG4bK-3f77
76e3-160d-11156ea5
Contact: <sip:2461803@47.174.73.242>
Content-Type: multipart/mixed ;boundary=unique-boundary-1
Content-Length:2
--unique-boundary-1
c: application/SDP ;charset=ISO-10646
v=0
o=MGCP 0 0 IN IP4 47.174.73.241
s=MGCP Call
c=IN IP4 47.174.73.241
t=0 0
m=audio 5004 RTP/AVP 0 96
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20

--unique-boundary-1
c: application/ISUP ;version=gr394 ;base=gr394

```

ACK:

```

ACK sip:2461803@47.174.73.242 SIP/2.0
From: <sip:9192461802@47.142.210.200>;tag=c8d28e2f-13c4-3f7776e3-160d-41bac49c
To: <sip:2461803@47.174.73.242>;tag=f249ae2f-13c4-3f777333-25a1-3e96679d
Call-ID: 0094.4609-28-17-05-18.82@MGCA
CSeq: 1 ACK
User-agent: CS2000/7.0
Max-Forwards: 70
Allow: ACK, BYE, CANCEL, INVITE, OPTIONS, INFO, SUBSCRIBE, REFER, NOTIFY

```

```
Via: SIP/2.0/UDP 47.142.210.200:5060;branch=z9hG4bK-3f7776e4-1a39-4674927a
Contact: <sip:9192461802@47.142.210.200>
Content-Length:0
```

5. When either the originating or terminating sides ends the call, the ISUP REL message is forwarded to the Session Server Manager. The Session Server Manager then builds a SIP BYE message, encapsulates the ISUP message, if applicable, and sends it to the remote SIP server.

The remote SIP server on receipt of the BYE message, extracts the ISUP message, if applicable, and forwards to the DPT GWC on its way to the core. It also responds to the BYE with a 200 OK and encapsulates the ISUP RLC whenever applicable.

A sample BYE and 200 OK are as shown:

```
BYE sip:2461803@47.174.73.242 SIP/2.0
From: <sip:9192461802@47.142.210.200>;tag=c8d28e2f-13c4-3f774d15-1d8b-7effbf92
To: <sip:2461803@47.174.73.242>;tag=f249ae2f-13c4-3f774966-1453-43179ce
Call-ID: 0094.4609-28-17-05-18.82@MGCA
CSeq: 4 BYE
User-agent: CS2000/7.0
Content-Transfer-Encoding: binary
Max-Forwards: 70
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY
Via: SIP/2.0/UDP 47.142.210.200:5060;received=47.142.210.200;branch=z9hG4bK-3f77
4d31-8bca-68dc7389
Content-Type: application/ISUP ;version=gr394 ;base=gr394
Content-Length:6
```

200 OK for BYE:

```
SIP/2.0 200 OK
From: <sip:9192461802@47.142.210.200>;tag=c8d28e2f-13c4-3f774d15-1d8b-7effbf92
To: <sip:2461803@47.174.73.242>;tag=f249ae2f-13c4-3f774966-1453-43179ce
Call-ID: 0094.4609-28-17-05-18.82@MGCA
CSeq: 4 BYE
Server: CS2000/7.0
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,INFO,SUBSCRIBE,REFER,NOTIFY
Via: SIP/2.0/UDP 47.142.210.200:5060;received=47.142.210.200;branch=z9hG4bK-3f77
4d31-8bca-68dc7389
Content-Length:0
```

Carrier Grade Topics

This section describes various aspects of the Session Server Manager platform that contribute to making it a carrier grade product.

Call Audits

The Session Server Manager platform provides a secondary call auditing capability for cleaning up stranded calls and reclaiming any call processing resources on the Session Server Manager not associated with valid calls.

During normal operation, Session Server Manager calls will be cleaned up properly on call takedown or when a maintenance action results in calls being ended. The call audit assures that the calls are not left up indefinitely due to some type of lost message or other error condition.

Session Server Manager calls are audited in two directions. One audit is between the Session Server Manager and the DPT GWC associated with the call. A second audit is between the Session Server Manager and the remote SIP server associated with the call. Calls are terminated whenever any of three components (Session Server Manager, DPT GWC, or remote SIP server) do not recognize the call being audited.

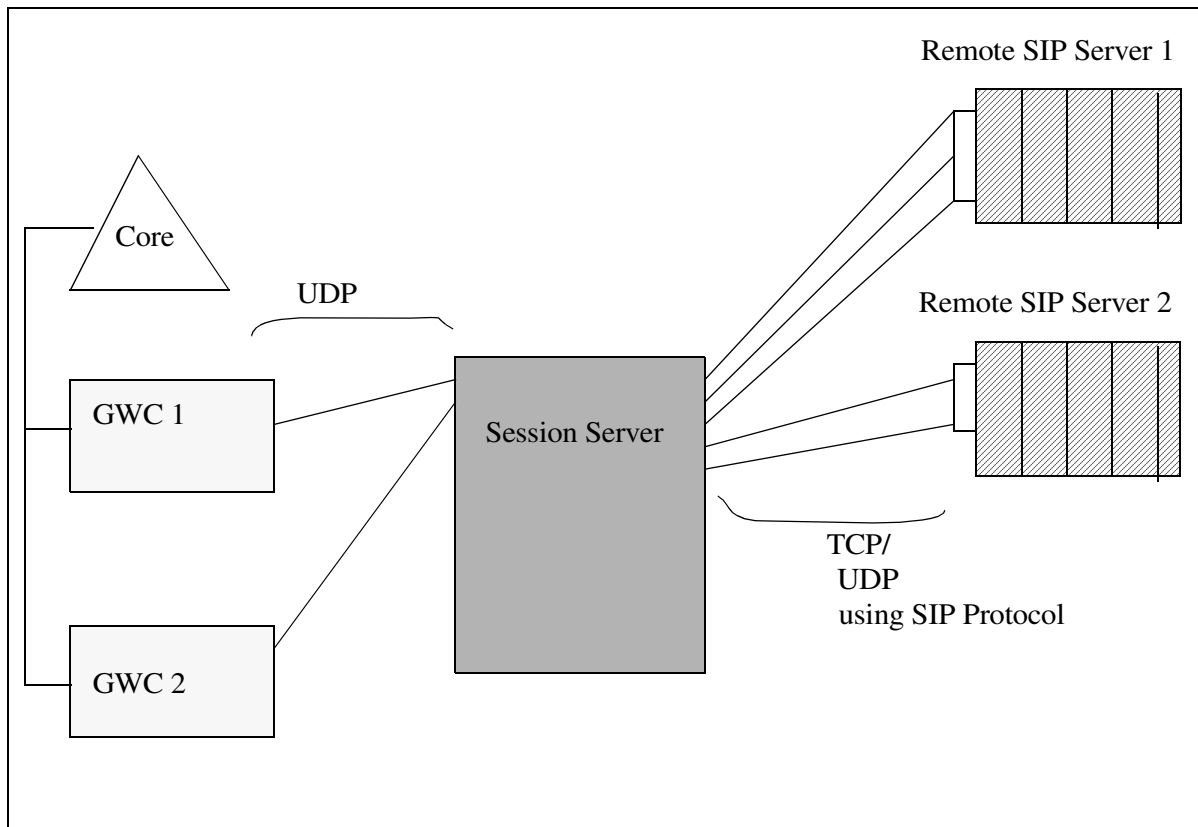
Call audits between the Session Server Manager and the remote SIP server can be configured to on a per SIP server basis, using either a SIP Info message or a SIP re-invite. When provisioning the Remote SIP Server, the “Use Info for Long Call Audit” parameter can be set to Yes or No to indicate whether to use the “SIP Info message” or not. Refer to [“Remote SIP Servers” on page 1447](#) for details on provisioning or modifying Remote SIP Server datafill.

If the SIP Info audit method is specified, the Session Server Manager will send a SIP Info message to the SIP server destination at regular intervals. If no response is received on two successive audit attempts or if an error response is received, the call will be taken down.

If the remote SIP server does not support the SIP Info message for this purpose, the SIP server must be configured to use the SIP re-invite method for auditing. If this approach is selected, a SIP Invite will be sent at regular intervals for a call once it is answered. Again, successive failures or no response results in the call being taken down. If the call is not answered after multiple audit intervals, the call will be taken down.

Link failover mechanism

The link failover mechanism involves routing calls and verifying connectivity between the Gateway Controller (GWC) and the Session Server Manager platform and between the remote Media Gateway Controller (MGC) and the Session Server Manager. The remote SIP server could be a proxy server or a final destination. Communication between the GWC and the Session Server Manager is accomplished with a normalized proprietary protocol using UDP as the transport medium. Communication between the Session Server Manager and the remote SIP server is through SIP or SIPT with a transport medium of either UDP or TCP. The diagram below illustrates the connectivity between the different entities.

Component Connectivity

To ensure that the remote SIP server is ready to receive messages from the Session Server Manager, an audit mechanism is optionally established between the Session Server Manager and its associated remote servers. The audit mechanism is accomplished by the Session Server Manager sending the SIP OPTIONS request message to the SIP servers upon a consistent interval and waiting for the response. This ability will be configurable per remote server.

When provisioning the Remote SIP Server, the “Options Supported” parameter can be set to Yes or No to indicate whether to use the “Options Supported message” or not. Refer to “Remote SIP Servers” on page 1447 for details on provisioning or modifying Remote SIP Server datafill.

When the Session Server Manager sends out a SIP OPTIONS message, if a time-out occurs or any failure causes the server using that IP address to be unreachable, the failure count is updated for that IP address. Whenever a message is received on that IP address, the failure count is reset. If the failure count reaches a specified threshold, the IP address is marked as inactive. If a new message is received on the inactive IP address, it is then reset to ACTIVE.

When all the IP addresses for a particular remote server are marked as inactive, each GWC is sent an access link status message indicating that the link is down. Additionally, an alarm will be raised on the Session Server Manager indicating the SIP-Server message path failure. When at least one IP address for that server becomes responsive, each GWC is sent an access link status message indicating that the link is up.

If a particular server does not care to support the OPTIONS message exchange capability, then its associated access links may appear to be always active. However, if repeated attempts to send SIP messages to a particular destination on a given IP corridor consistently result in failure, then once a threshold of failure has been attained, the access link will be considered out of service. As in the OPTIONS scenario, this results in the transmission of an access link status message to the GWC/Core to indicate the change in status. The access link will be returned to service upon receiving a new call from the IP address in question. In addition, the failed link will periodically be retried for call processing to determine if the link has become active again. If the link continues to fail on these retries, the link will remain out of service and any other IP routes provisioned for the destination SIP server will be used to complete the call.

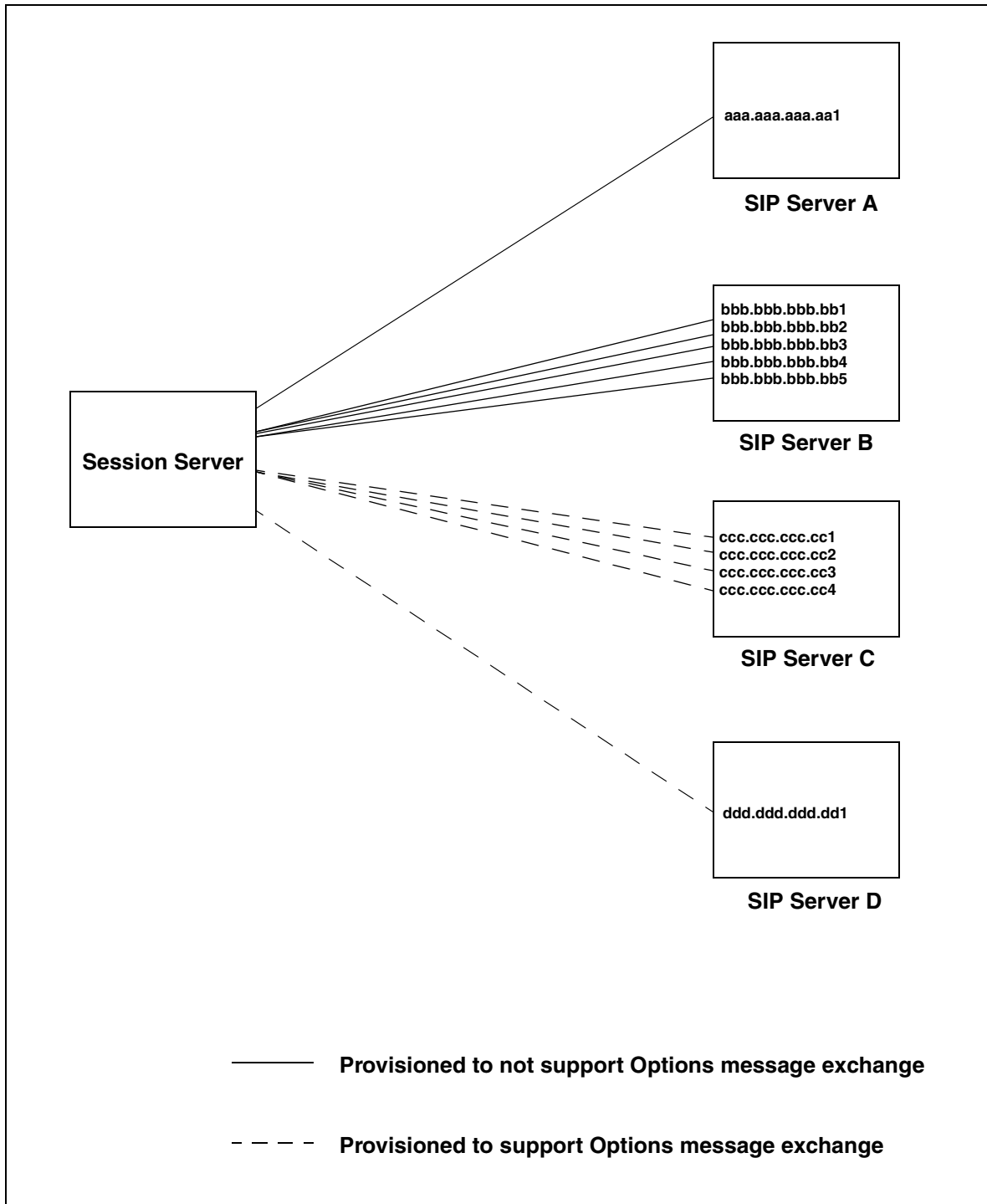
Additionally, if a particular access link has been orphaned from its server destination, i.e., provisioning has removed a particular access link's remote server association, then this will be treated in the same manner as an audit failure.

The Session Server Manager is also responsible for responding to SIP OPTIONS messages sent from remote SIP servers. Depending on the maintenance state of the Session Server Manager, it will either respond with a 200 OK (Session Server is in service) or with a 503 (Session Server is in deload or BSY state). When the Session Server Manager is in the deload or BSY state, it will not send SIP OPTIONS messages at each audit interval.

To summarize, link viability to a remote SIP server may be maintained in various different ways based on provisioning and network configuration.

1. Server A in [“Maintaining SIP Server Links from the Session Server Manager” on page 1427](#) depicts an access link with a singular IP presence may be configured to disable the OPTIONS message exchange mechanism. From the Session Server Manager viewpoint, this connection is always active regardless of the actual transport status, until it achieves a specific level of consistent failure. At this point the access link will be removed from service.

2. As shown in “[Maintaining SIP Server Links from the Session Server Manager](#)” on page 1427 by server B, an access link provisioned to not support OPTIONS messages may consist of multiple IP address destinations. These multiple IP addresses are progressively stepped through service calls bound for the remote SIP server on the given access link. In this setup, if some transport layer problem is encountered, the next IP destination in the list may be attempted until all possible routes are exhausted. Again, if all routes surpass the send failure threshold, the access link will be removed from service.
3. In the figure, the access link to server D is comprised of a single IP address configured to support OPTIONS messages. With the OPTIONS messaging ensuring a valid network connection to the server, any call that reaches the Session Server Manager bound for server D is much more likely to find its intended IP tunnel open. However, as in the server A configuration, if some transient network fault occurs that was not detected by the audit mechanism prior to an attempted message transmission on the link, there is no further fallback mechanism.
4. The final permutation of OPTIONS support and IP presence is embodied in the server C connection. This setup ensures messaging link integrity while also providing the ability to round-robin through the suite of possible destinations to the server if a transient network failure is encountered.

Maintaining SIP Server Links from the Session Server Manager

Link Status in the CM

In the CM, the status of an access link can be monitored by posting the associated SIPT trunk group³ at the MAPCI;MTC;TRKS;DPTRKS level of the MAP. Since the CM has no direct communication with the Session Server, it is dependent on receiving link status information from the SIPT gateway controllers, who receive Access Link Status messages from the Session Server and pass them on to the core.

The status of the access link on the Session Server is determined using the strategy discussed in the previous section (Link Failover Mechanisms). Any change in a link's status detected by the Session Server is immediately propagated to each SIPT gateway controller, then to the core. As long as there is stable communication between the core and at least one SIPT gateway controller and the session server, the status of a SIPT trunk in the CM should mirror that of its associated access link.

For a trunk to be INS at the DPTRKS MAP level, the following conditions must exist:

- On the Session Server, the access link associated with the trunk must be mapped to a Remote SIP Server.
- On the Session Server, the associated Remote SIP Server must have at least one active IP connection. An active connection is defined as one of the following:
 - For a Remote SIP Server configured to support SIP OPTIONS messaging for heartbeats, a connection is active if the Session Server is receiving timely 200 OK responses to its SIP OPTIONS requests on at least one of the IP connections to the remote server.
 - For a Remote SIP Server that doesn't support OPTIONS for heartbeats, a connection is active if the Session Server is successfully sending and/or receiving SIP messages at a level above the failed message threshold on at least one of the IP connections to the remote server. Note that by default the connection is considered active until proven otherwise by exceeding the failed message threshold during call processing.
- The Session Server application must be UNLOCKED.
- In the CM, at least one SIPT GWC must be in-service at the MAPCI;MTC;TRKS;DPTTRM level of the MAP.

When the last of these conditions is met, the Session Server sends an Access Link Status message indicating the link is up to each SIPT GWC. The gateway controllers then propagate the message to the CM, resulting in the state of the trunk group changing to INS.

3. The association of the trunk group to an access link is defined in CM table SIPLINK.

Once a trunk group is INS, a failure of any of the first three conditions will cause the Session Server to send an Access Link Status message indicating the link is down to each SIPT GWC. The gateway controllers then propagate the message to the CM and the CM changes the status to SYS.

If a situation occurs where there are no longer any in-service SIPT GWCs, the CM changes the state of the trunk to SYS. This is the only time the CM undertakes unsolicited action to remove a link from service; otherwise, link status in the core is totally under the control of the Session Server. In other words, when at least one SIPT GWC is in-service at the DPTTRM level, the only way the trunk group's state can be changed (other than by manual intervention) is if the Session Server sends an Access Link Status message to report the state change.

If the Session Server goes out of service due to a system failure or because of improper shutdown (which would disrupt the ability to send the Access Link Status message to the gateway controllers), all INS SIPT trunks associated with any access links on the Session Server will remain INS.

Scalability and Load Balancing

In the initial release of the Session Server Manager product, a single redundant pair of Session Server boxes will satisfy the call volume requirements. If call volume requirements increase in the future, later releases of the Session Server Manager product will address the need to expand the network to include multiple redundant pairings of Session Servers.

If additional DPT GWCs are required to handle increased call volume, they can be introduced without any impact to call processing. In addition to the normal commissioning and provisioning required to add a new DPT GWC, the IP address of the GWC(s) must be added to the list of GWCs connected to the Session Server Manager. This change is done through the web provisioning interface on the Session Server Manager and it can be made while the Session Server box is in service. The new GWC(s) will be used for call processing once they are brought in service. The Session Server Manager uses a simple round-robin scheme to distribute incoming calls across all in-service DPT GWCs.

Performance

The committed performance of the Session Server Manager, in SN07, is to meet VRDN equivalency. The VRDN currently supports a call rate of 900K Busy Hour Half Call Attempts (A half call is either the originating leg of a call, or the terminating leg).

The Session Server Manager will support up to 37,5000 simultaneous calls. Given a call model of 2 minute hold time and 30 second intercall delay, this provides a capacity of 900K BHHCA.

Upgrades

This section describes the upgrade procedures for offices that want to introduce the Session Server Manager platform into their network. Procedures vary depending on whether the office was previously running SIPT traffic using the VRDN architecture or not. The following topics are covered in this section:

- Upgrading an SCS 2000 office to include the Session Server Manager when SIPT traffic was not previously handled in the office.
- Upgrading an SCS 2000 office to include the Session Server Manager and migrating existing SIPT traffic from the VRDN architecture to the Session Server Manager platform.
- Upgrading the Session Server Manager with new software loads and/or maintenance releases (MRs).

Upgrading to Session Server Manager without VRDNs

This section is for offices that did not have SIPT traffic prior to introducing the Session Server Manager platform. Before the Session Server can be inserted in the network, the CS 2000 must first be upgraded to an SN07 or later release. Adding the Session Server Manager is a completely separate step from upgrading the office and sufficient soak time should be employed after the upgrade to SN07 or later, before the Session Server Manager platform is introduced.

The normal upgrades steps should be followed for upgrading the CS 2000, including upgrading peripherals and the DMS core. In addition to requiring an SN07 or later core release, the Session Server Manager platform also requires that all DPT GWC peripherals be at an SN07 or later release. Since the office was not previously running SIPT traffic, DPT GWCs may need to be added or existing TDM GWCs need to be converted to DPT GWCs. The normal procedures for adding or converting to DPT GWCs should be followed, there are no new commissioning or provisioning steps required for the DPT GWCs in order to have them work with the Session Server Manager platform.

Once the upgrade is complete and the DPT GWCs are in place, the following steps should be followed to add the Session Server Manager platform:

- Connect the Session Server Manager hardware platform to the CS 2000 LAN.
Please refer to feature *NCGL support for SAM-XTS and SP2000*, A00004005 for connection information.
- Commission the Session Server Manager platform.
Please refer to feature *NCGL support for SAM-XTS and SP2000*, A00004005 for commissioning information.
- Provision core tables to add DPT trunks (TRKGRP, TRKSGRP, and TRKOPTS) and to map the new DPT trunks to SIP access link names in

new table SIPLINK. For more information see “CS 2000 OAMP” on page 1435. In a later step, the SIP access links will be mapped to remote SIP server destinations through the Session Server Manager web interface.

- Provision the Session Server Manager platform using the web interface. For more information see “Session Server Manager OAMP” on page 1437.
- Bring DPT GWCs and DPT TIDs in service, if that hasn’t been done already. This is done using normal procedures for DPT GWCs.
- Bring the CSC 2000 - SIP Gateway application in service using the web interface. For more information see “SIP Gateway application maintenance” on page 1473.
- Once all components (DPT GWCs and Session Server application) are in service, access link names provisioned in core table SIPLINK are transferred to the Session Server Manager and can be seen through the web interface. Complete the Session Server Manager provisioning by mapping the access link names to remote SIP server destinations. For more information see “CS 2000 OAMP” on page 1435.
- Change DMS translations as appropriate to make use of the new DPT trunks for both incoming and outgoing calls. Once the translations changes are made, SIP traffic can begin to flow through the Session Server Manager platform. Customers may choose to route only a small set of test traffic through the Session Server Manager at first, before completing translations changes to include all the desired SIP/SIPT traffic.

Upgrading to Session Server Manager with VRDNs

This section is for offices that have existing SIPT traffic using the VRDN architecture and the Session Server Manager is being introduced as a replacement for the VRDNs. With the SN07 release of the Session Server Manager product, SCTP is not a supported transport protocol for SIPT traffic. Therefore, existing SIPT traffic through VRDNs using SCTP cannot be migrated to the Session Server Manager. If UDP is used for the SIPT traffic through the VRDN, that traffic can be migrated to the Session Server Manager using the procedures defined in this section.

Before the Session Server Manager is introduced, the office must first be upgraded to an SN07 or later release. During and immediately after the upgrade, SIPT traffic will continue to flow through the VRDNs. DPT GWCs with an SN07 or later load are capable of handling both traffic through VRDNs and traffic through the Session Server Manager at the same time.

Other than upgrading the DPT GWCs to an SN07 or later release as part of the upgrade process, no additional provisioning changes are needed to make the DPT GWCs work with the Session Server Manager.

Once the CS 2000 upgrade is complete and sufficient soak time has passed to ensure that the upgrade was successful, the Session Server Manager platform

can be introduced. The following steps should be followed to add the Session Server Manager and migrate SIPT traffic from the VRDNs to the Session Server Manager:

- Before installing the Session Server on the SN07 CS2K that is being upgraded, be sure that all SN06 CS2Ks that exchange SIP-T traffic with this office have the appropriate core and GWC patches applied. SN06 core patches ATM83P2F and ATM84P2P must be applied to allow the destination IP address of the SN07 CS2K to be changed in table MGCINV. Do not make this configuration change at this time, just make sure the patches are applied. GWC patch XZB41GZU must be applied to all DPT and VRDN GWCs at the SN06 switches to allow them to receive SIP traffic from the Session Server.
- Connect the Session Server Manager hardware platform to the CS 2000 LAN.
Please refer to feature *NCGL support for SAM-XTS and SP2000*, A00004005 for connection information.
- Commission the Session Server Manager platform.
Please refer to feature *NCGL support for SAM-XTS and SP2000*, A00004005 for commissioning information.
- Provision new core table SIPLINK with SIP access link names. SIP access links are mapped to SIP server destinations through the Session Server Manager web interface in a later step. In this step, DO NOT provision any DPT trunks against the SIP access link names in table SIPLINK. Instead, use '\$' when provisioning the DPT trunk in table SIPLINK. Table SIPLINK will be revisited at a later step to add the trunk-to-link mapping when it is time to actually swing outgoing traffic from the VRDN to the Session Server Manager.
- Provision the Session Server Manager platform using the web interface. For more information, see [“Session Server Manager OAMP” on page 1437](#).
- Bring the SCS 2000 - SIP Gateway application in service using the web interface. For more information, see [“SIP Gateway application maintenance” on page 1473](#)
- Once all components (DPT GWCs and Session Server Manager application) are in service, access link names provisioned in core table SIPLINK are transferred to the Session Server Manager and can be seen through the web interface. Complete the Session Server Manager provisioning by mapping the access link names to remote SIP server destinations. For more information see [“Session Server Manager OAMP” on page 1437](#).
- At the beginning of this step, all incoming and outgoing SIPT traffic continues to flow through the VRDNs. To swing outgoing SIPT traffic from the VRDN to the Session Server Manager, revisit core table SIPLINK

and change the tuples to include the appropriate DPT trunks against the appropriate access link names. Customers may choose to swing only one trunk at first to test the Session Server Manager, perhaps even adding a new DPT test trunk for this purpose. Note that the remote SIP server provisioning done through the web interface on the Session Server Manager should point to the VRDNs on remote CS2Ks. The remote VRDNs are capable of receiving SIPT traffic from DPT GWCs (pre-migration, if UDP transport is used), or from a Session Server Manager (once a trunk is migrated). Once table SIPLINK is changed, new outgoing calls on the affected DPT trunk will route through the Session Server Manager while existing calls finish up through the VRDN.

- To route new incoming calls through the Session Server Manager, the SN06 core and GWC patches mentioned earlier should have been applied on all CS2Ks that send SIPT traffic to the office being upgraded. Assuming the patches are applied, change the destination IP address in table MGCINV for the switch that has been upgraded. The IP address used to be the IP address of the VRDN on the upgraded switch and it must now be changed to be the IP address of the Session Server Manager. Note that the patches are only required if the remote CS 2000 is not being upgraded to SN07. With an SN07 or later load in the remote CS 2000, the IP address can be changed in table MGCINV without needing a patch. Also, the customer can skip the IP address change altogether if the remote CS 2000 is also being upgraded to include a Session Server Manager. In that case, the DPT trunks can be migrated to the Session Server Manager, which will be configured to send calls to the Session Server Manager on the other switch. Note that VRDNs are required at an office until all incoming and outgoing traffic have been migrated to the Session Server Manager. It should also be noted that the destination IP address for a SIP server configured in the Session Server Manager can be changed on the fly. This is required if the Session Server Manager was sending calls to a remote VRDN and then that remote office is upgraded to use the Session Server Manager.
- In addition to remote CS2Ks, it is possible that the upgraded CS 2000 was also receiving incoming SIP traffic from an IMS. In that case, the IMS configuration data must also be changed to send calls to the Session Server Manager instead of sending calls to the VRDN.
- Once all incoming and outgoing traffic has been migrated from the VRDN to the Session Server Manager, the VRDN GWCs can be removed or converted to another type of GWC.

Electronic Software Delivery

Session Server Manager software loads can be delivered by CD or electronically. To deliver the SIP Gateway application electronically, follow these steps:

- First, be sure that the NCGL platform software is installed on the Session Server Manager. Please refer to feature A00004005, Nortel Carrier Grade Linux (NCGL) platform “Session Server” for installation information.
- Transfer the ISO image containing the SIP Gateway application load to the /opt/swd directory on the Session Server Manager. Note that this directory has a size of 1GB and can contain no more than four SIP Gateway loads at once. Be sure to delete old loads to make room for the new load being delivered.

e.g.: scp <iso image> mtc@<Session Server IP addr>:/opt/swd

- Log into the command line on the Session Server Manager as root.
- Verify that the /cdrom device is not currently mounted by typing:

```
umount /cdrom
```

- Mount the ISO image that was transferred electronically to the /cdrom device:

```
mount -o loop /opt/swd/<ISO image> /cdrom
```

- Follow the instructions below to upgrade or install the SIP Gateway application.

Upgrading a Session Server Manager load

Upgrading a Session Server Manager with a new software release or a maintenance release is very much like upgrading any other DMS component. Session Server Managers are deployed in redundant pairs, one box acting as the active unit and another box acting as a hot standby (the inactive unit).

Use the following steps to upgrade:

- Deliver the software load to the inactive unit to be upgraded:

Note 1: The software load may be delivered by CD or electronically. For instructions on electronic deliver, please refer to section.

Note 2: For CD delivery, insert the CD in the CDROM drive and type “mount/cdrom” at the command line.

- Install the SIP Gateway application from the command line.

Note: The user must be logged in as root.

Type:

```
— cd/cdrom
```

```
— ./InstallApps (or just type cd/cdrom/InstallApps)
```

InstallApps will prompt the user to proceed with the upgrade.

- Once the InstallApps script is finished, the SIP Gateway application should come in-service automatically if it is in-service on the active unit.
- Swact the Session Server Manager using the web interface. For more information see “SIP Gateway application maintenance” on page 1473.
- Repeat the procedures for the previously active unit, which is now inactive.

OAMP

This section describes the Operations, Administration, Maintenance, and Provisioning functionality when utilizing a Session Server Manager architecture. While a majority of the OAMP functions now reside on the Session Server Manager itself, the Call Server 2000 (CS 2000) core does have OAMP changes.

This OAMP section focuses heavily on the first application to be deployed on the Session Server Manager. This application, also referred to as the SIP Gateway, should be assumed to be the main topic of discussion with respect to Session Server Manager operations, administration, maintenance, and provisioning.

CS 2000 OAMP

Call Server 2000 Core OAMP changes revolve around new table SIPLINK, which is the trigger point for calls utilizing the Session Server Manager platform as opposed to the VRDN. Also, part of the CS 2000 OAMP changes for an Session Server Manager-only environment involve the retirement of several media gateway controller related tables

The below figure illustrates the table control relationships for gateway controllers in a Session Server-only environment. This is followed by a brief description of each table. Not every possible DMS table is shown and described.

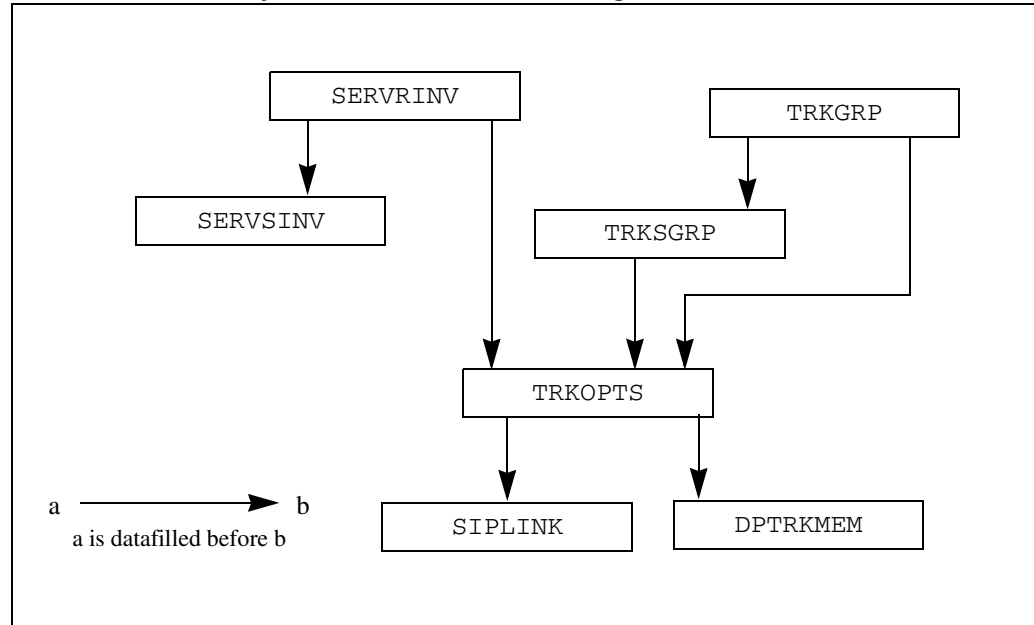
Core OAMP hierarchy with Session Server Manager**Table Descriptions**

Table	Description
SERVINV	Stores provisioned data for gateway controllers including IP addresses, exec information, etc. Gateway controllers are provisioned in CS2M and then the system automatically enters required datafilled in SERVINV
SERVSINV	Contains the names of the server subtending nodes and their associated gateways. The subtending nodes are the Audio Controller and the Dynamic Packet Trunk (DPT).
SIPLINK	Contains the access link information that is used to direct calls to the appropriate SIP server. This information is also used by Session Server devices for mapping incoming calls.
TRKGRP	Contains customer-defined data associated with each trunk group that exists in the switch.
TRKSGRP	List the supplementary information for each subgroup that is assigned to one of the trunk groups listed in table TRKGRP.
TRKOPTS	Provisions special options on trunk groups. For the Session Server Manager, that option is <code>dynamic</code> and the signaling type is <code>SIPT</code> .
DPTRKMEM	Used to provision ISDN User Part and SIP trunks dynamically for both ATM and IP networks.

The major differences between the old and new data models with respect to core provisioning are as follows:

- Retirement of tables VRDNINV, MGCINV, and TELEPROF. These three table are unnecessary when Session Server Manager functionality is utilized.
- Table SIPLINK is added to contain the access link information.
- Tables TRKGRP, TRKSGRP, TRKOPTS, DPTRKMEM, SERVSINV, and SERVINV remain unchanged.

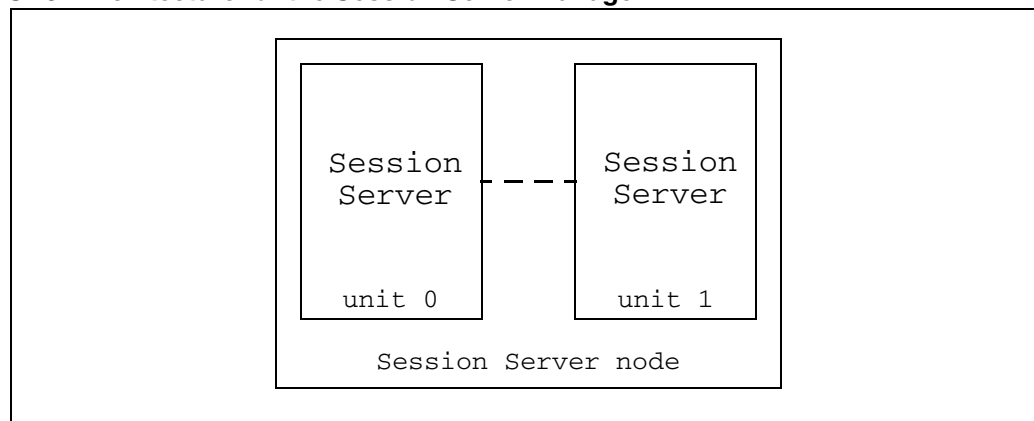
Session Server Manager OAMP

This section discusses Operations, Administration, Maintenance, and Provisioning (OAM&P) topics for the new Session Server Manager platform. Topics discussed include the following:

- OAM&P Overview
- Node Provisioning
- Node Maintenance
- SIP Gateway Provisioning
- SIP Gateway Maintenance
- Alarms
- Logs
- Operational Measurements

Before jumping into the sections mention above, a distinction should be made with respect to the Session Server Manager product release and this document. In the SN07 release, the architecture for the Session Server Manager will consist of a dual unit configuration similar to that of gateway controllers. The units consists of an active and inactive unit. Each unit is in reality a fully functional Session Server Manager that is interconnected via a gigabit ethernet LAN.

SN07 Architecture for the Session Server Manager



Overview

For the SN07 release of the Session Server Manager, there are four major OAMP areas to discuss. Those areas are as follows:

- Web Based OAM&P
- Provisioning Framework
- Application Maintenance
- Alarms, Logs, and OMs

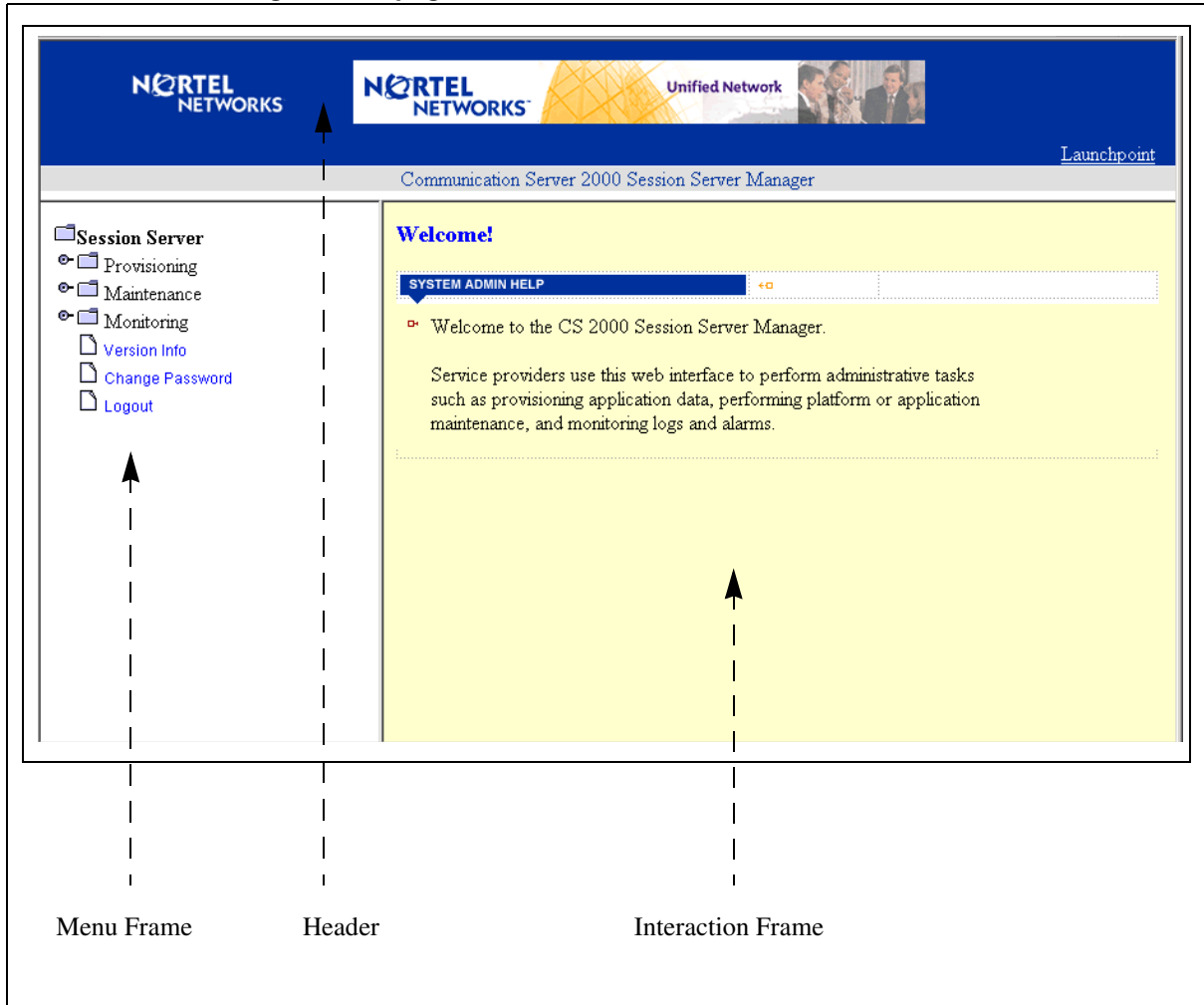
Web Based OAM&P

One paradigm shift to note is that the Session Server Manager functions as its own element manager. This means that provisioning for a Session Server Manager takes place on the Session Server itself. Additionally, maintenance type activities also take place on the Session Server Manager.

The craftsperson uses a web based interface to perform the provisioning and maintenance activities. This interface consists of a web system⁴ running on the Session Server Manager that provides provisioning web pages as well as maintenance related web pages. Please refer to activity A00004005: *NCGL Support for SAM-XTS and Session Server* for details on logging on via the web interface.

An example of the Session Server Manager home page is shown in the following figure.

4. Consists of Apache, Apache Tomcat, and Java Runtime environment.

Session Server Manager home page

All Session Server Manager web pages are divided into three areas:

- **Header**
The area with the Nortel logo and the “Home” and “Help” tags.
- **Menu Frame**
The user uses the menu bar on the left to locate the proper function in the web page hierarchy.
- **Interaction Frame**
This area is where a user fills in forms, performs maintenance actions, and obtains relevant information.

Provisioning Framework

As mentioned before, the Session Server Manager is its own element manager. That also means provisioned data is stored on the Session Server Manager itself. The storage mechanism is an on-board standard query language (SQL) database. Data in this database survives scenarios such as dead office recovery.

Application Maintenance

In the initial release, only the SIP Gateway application exists on the Session Server Manager. That application is managed via an Application Maintenance entity known as SIP Gateway Maintenance. Again, the web based interface is the craftsman's way to interact with SIP Gateway Maintenance as described in ["SIP Gateway application maintenance" on page 1473](#).

Alarms, Logs, and OMs

An application on the Session Server Manager, such as the SIP Gateway application, has the ability to generate Alarms, Logs, and Operational Measurements (OM).

Platform Commissioning

Platform provisioning for the Session Server Manager takes place during the commissioning phase when the software is installed for the first time. Initial commissioning is not done via the web based interface. Please refer to feature *NCGL support for SAM-XTS and SP2000*, A00004005 for complete commissioning information.

A quick overview of this commissioning phase is detailed below. These steps are meant as an example only.

- Power on (or reset) the Session Server Manager.
- Insert the Session Server Manager installation CD/DVD into the CDROM drive.
- Eventually the user is taken to an initial commissioning screen. Here initial commissioning prompts the user to enter the following data items for initial node provisioning:
 - Hostname - Hostname for this particular Session Server Manager unit. (e.g. "NGSS-Unit0")
 - Unit IP Address - IP Address of this particular Session Server Manager unit.
 - Subnet Mask - Subnet mask for the Session Server Manager.
 - Timezone - The timezone of the Session Server Manager (e.g. EST)
 - One or More NTP Servers - At least one Network Time Protocol server must be datafilled.

- Log Server IP Address [optional] - IP Address of a remote log server if Session Server Manager customer logs are to be reported to a far end entity. If no far end log server is being utilized, this field should remain empty.
- Network Monitor IP Address (mandatory) - Datafill with a network node that can always pinged from the Session Server. It is recommended that you specify the IP address of a highly available node on the network.
- Core IP Address [optional] - Datafilled with the IP address of the Core. This optional field is for future use.
- Web Proxy IP Address [optional] -If the Session Server Manager is to be accessed via a Web Proxy, the web proxy IP address is datafilled. For example, in the Succession environment, this would likely be the SSPFS proxy server.
If a web proxy is not going to be used, this optional field should be left blank.
- Session Server Manager Location - A text string indicating the location of the Session Server Manager.
- SNMP Trap Destination [optional] - IP Address of the far end node to receive SNMP traps from this Session Server Manager unit. If SNMP traps are not to be reported to a far end node, this optional field should remain blank.

Once the commissioning steps are complete, the Session Server Manager should fully initialize and the craftsperson has access to the on-board web system.

Node Maintenance

Please refer to A00004005: *NCGL Support for SAM-XTS and Session Server* for a complete list and description of Session Server Manager Node Maintenance type functions available. A quick summary of some of those functions include:

- Lock/Unlock Node

This provides for the ability to bring a Session Server unit into service.

- Duplex Activities

This provides for the ability for Session Server Manager to SWACT from the Active/Enabled unit to its mate unit.

- System Info

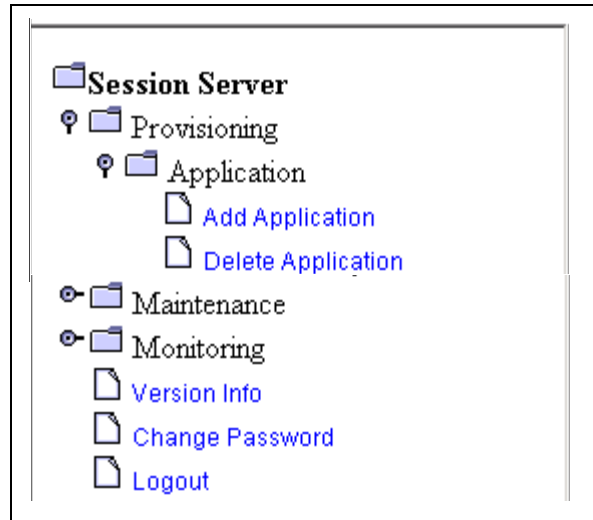
Provides information such as the date, time since last reboot, IP address of the system, and IP address of the web browser looking at the System Info page.

- System Status
Provides CPU, Process, and Memory information
- Connectivity
Allow the user to setup and monitor a remote host via pings.
- Storage
Allows a view of file system data includes partition specific data such as total space, used and available space, and the ability to set alarm thresholds based on the amount of space utilized
- Services
Displays NFS, TFTP, and active remote session status information. e.g. if two SSH sessions are in progress, the active remote session indicates “2”.
- Admin
Allows the user to perform administrative tasks related to the system. For example the user can reboot the Session Server Manager from this menu.
- Alarms
Provides the ability to view alarm information which consists of type, id, timestamp, severity, and description.
- Logs
Provides the ability to view customer related logs that are not application related.

SIP Gateway application provisioning

This section describes the provisionable data related to the SIP Gateway application. All SIP Gateway provisioning is performed via the Session Server Manager web interface.

The first provisioning step is to enable the SIP Gateway application if it is not already listed. This is a one time step, but it is required at the outset. When the Application folder in the menu frame is opened the first time, the SIP Gateway application is not listed as shown below.

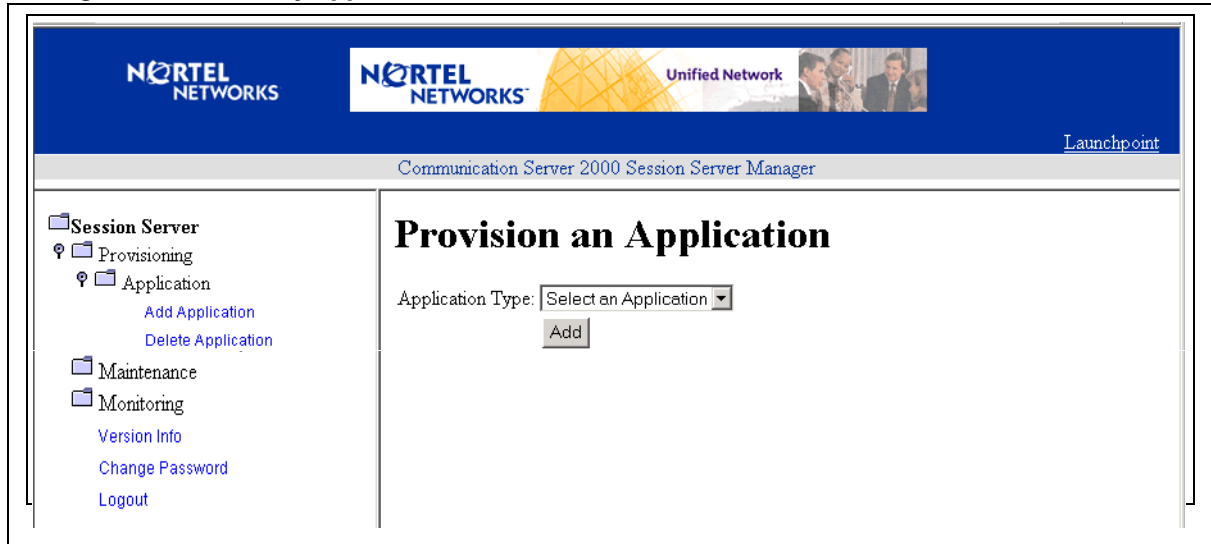
No SIP Gateway application

To add the SIP Gateway application, the craftsperson clicks on “Add Application” link and is presented with the **Provision an Application** web form as shown in [“Adding the SIP Gateway application” on page 1444](#). From this point, the craftsperson selects “SIP Gateway” and clicks on “Add” to add the application.

Note: If the SIP Gateway application is already listed, there is no need to provision it.

Note: If the SIP Gateway application is already listed and it is added again, that operation does not perform a second add. Also, it does not have a negative impact on the existing SIP Gateway application.

Adding the SIP Gateway application



After adding the application, the craftsperson should close and open the Application folder and the SIP Gateway application will be present. Next, the craftsperson uses the "SIP Gateway" level to perform provisioning.

SIP Gateway provisioning

The screenshot shows the 'Session Server' menu on the left side of the interface. The 'Provisioning' folder is expanded, showing the 'Application' folder. The 'Application' folder is also expanded, showing 'Add Application' and 'Delete Application' links. The 'SIP Gateway' folder is expanded, showing a list of sub-folders: 'Remote SIP Server', 'Access Control List', 'SIP-T GWC's', 'Access Link Map', 'NOA/NPI/PC', 'Telephony Profile', 'SIP Base', and 'ISUP and SIP Mappings'. Below these folders are 'Config Data', 'Maintenance', and 'Monitoring' links. The 'Monitoring' link is expanded, showing 'Version Info', 'Change Password', and 'Logout' links.

In the Session Server menu on the left of the page, the following is performed.

- Click on the Provisioning folder
- Click on the Application folder
- Click on the SIP Gateway folder

The provisionable items for the SIP Gateway application consist of required and optional datafill. Certain datafill is optional because either defaults exist or that datafill is not required.

Required Datafill	Optional Datafill ^a
Config Data	Access Control List
Remote SIP Servers	NOA/NPI/PC
SIP-T Gateway Controllers	SIP Base
Telephony Profile	ISUP to SIP Cause Code Map
Access Link Map	SIP to ISUP Response Code Map
ISUP Variant Map ^b	SIP Redirection Map

a. All of the optional datafill items exist in the Mappings sub-folder with the exception of “SIP Base”, which is under the “SIP Gateway” folder.

b. The SIP Base item seen in Figure relates to the ISUP Variant mapping datafill in the Mappings sub-folder.

Config Data

Before the SIP Gateway application is brought into service, four base configuration parameters should be modified to appropriate values.

LocalTcp

The IP address should be datafilled to match the IP address of the Session Server Manager. The port should be datafilled to 5060.

LocalUdp

The IP address should be datafilled to match the IP address of the Session Server Manager. The port should be datafilled to 5060.

MgcHostName

This parameter should be datafilled to match parameter HOST_MGCNAME in table OFCENG in the local CS 2000 Core.

An example of HOST_MGCNAME in the local CS 2000 core is as follows:

TABLE: OFCENG	
PARMNAME	PARMVAL
-----	-----
HOST_MGCNAME	MGCA

In the above scenario, parameter MgcHostName on the Session Server Manager should be datafilled to be MGCA.

If the Session Server Manager is being used to communicate with other CS2Ks that have VRDNs, then it is very important that the MgcHostName parameter match the HOST_MGCNAME parameter in table OFCENG. If it does not

match, DPT trunks at the far end CS 2000 will transition to a SYSB state and call processing between the CS2Ks will be halted.

Note: The string associated with the MgcHostName parm will be used to populate the Via Header of the SIP INVITE message. See section “ Call Flows” for additional information.

maxCallLegs

This parameter determines the maximum amount of simultaneous SIP transactions. The default setting is 1000.

If the SIP Gateway application is in-service when the above values are changed, it must be taken out of service and brought back in-service for the new parameter values to take effect. Details on this may be found in “ SIP Gateway application maintenance” on page 1473. Next, while many parameters exist on the “Config Data” page, **care** must be taken when changing any of them.

All the configurable parameters are found on the **Configurable Parameters** page. That page is reached from the Session Server Manager main page via:

- Click on the Provisioning folder
- Click on the Application folder
- Click on the SIP Gateway folder
- Click on **Config Data**

An example of the Config Data page can be found in [“Configurable Parameters” on page 1447](#).

Configurable Parameters

The screenshot shows the Nortel Networks web interface for the Communication Server 2000 Session Server Manager. The left sidebar contains a navigation tree with categories like Session Server, Provisioning, Application, SIP Gateway, Remote SIP Server, Access Control List, SIP-T GWC's, Access Link Map, NOA/NPI/PC, Telephony Profile, SIP Base, ISUP and SIP Mappings, Config Data, Maintenance, and Monitoring. The main content area is titled "Configurable Parameters" and contains a list of parameters with their current values and a "Modify" link for each.

Parm Name	Parm Value	Modify
generalLingerTimer	32000	Modify
inviteLingerTimer	32000	Modify
localTCPport	5065	Modify
localUDPport	5060	Modify
maxCallLegs	10	Modify
maxSipMsgSize	1536	Modify
maxSubscriptions	0	Modify
provisionalTimer	180000	Modify
retransmissionT1	500	Modify

The range of values for the configuration parameters are:

- generalLingerTimer 0 - 60000
- inviteLingerTimer 0 - 60000
- maxCallLegs 0 - 40000
- maxSubscriptions 0 - 100000
- provisionalTimer 0 - 540000
- retransmissionT1 0 - 60000
- retransmissionT2 0 - 60000
- retransmissionT4 0 - 60000

Remote SIP Servers

A remote SIP Server is a remote SIP device that the Session Server Manager communicates with via the session initiation protocol. Two examples are other Call Server 2000s or a Multimedia Communication Server (MCS).

SIP Gateway remote SIP server provisioning is performed by opening the “Remote SIP Server” folder in the left menu. Once there, the following may be performed:

- Remote SIP Server datafill may be added by clicking on the “Add Server” link. Figure shows an example of the page presented to the user after this.
- Remote SIP Servers may also be listed by clicking on “List Servers”.
- After listing the Remote SIP servers, the user may choose to delete a particular remote SIP server or modify the data for a particular SIP server.

Remote SIP Server provisioning

The screenshot displays the Nortel Networks Communication Server 2000 Session Server Manager interface. The left-hand navigation pane shows a tree structure under 'Session Server' with folders for 'Provisioning', 'Application', 'SIP Gateway', and 'Remote SIP Server'. The 'Remote SIP Server' folder is expanded, showing links for 'Add Server' and 'List Servers'. The main content area is titled 'Add a SIP Server' and contains the following fields and options:

- Server Name:** A text field containing 'NULL'.
- IP Address:** A text field containing 'NULL'.
- Port:** A text field containing '5060'.
- Protocol:** A dropdown menu set to 'UDP'.
- Opt IP Address:** A text field containing 'NULL'.
- Opt Port:** A text field containing '5060'.
- Opt Protocol:** A dropdown menu set to 'UDP'.
- Methods Supported:** A group of checkboxes including ☒ INVITE, ☒ CANCEL, ☒ BYE, ☒ OPTIONS, ☐ SUBSCRIBE, ☐ NOTIFY, ☐ REFER, ☐ PRACK, ☐ UPDATE, and ☐ INFO.
- URI Parameters Supported:** A group of checkboxes including ☐ CIC, ☐ RN, ☐ NPDI, and ☐ Phone-Context.
- SIP Headers Supported:** A group of checkboxes including ☐ Content-Disposition, ☐ Remote-Party-ID, ☐ P-Asserted-ID, ☐ P-Preferred-ID, ☐ Privacy, ☐ Reason, ☐ Replaces, ☐ Referred-By, and ☐ Originating Dial Plan ID.

Datafill for a remote SIP server consists of the following items:

Remote SIP Server Data

Title	Description	Default
Server Name	Character string name for the remote server.	N/A
Support for multiple IP Addresses, Ports, and Protocols	An IP addresses list that represents the Remote SIP Server. Up to 7 IP addresses and Ports are supported. At least one IP address must be entered.	N/A for IP, 5060 for Ports, and UDP for Protocols
Server Methods • Invite • Cancel • Bye • Prack • Subscribe • Notify • Refer • Options • Update • Info	• Click on the methods that are supported by the Remote Server	All False
URI Parameters Supported • CIC • RN • NPDI • Phone-Con-text	• Click on appropriate parameter if it is supported. • CIC parameter carries Carrier Identification Parameter from SIP to ISUP and vice-versa. • Redirect Number is used in LNP scenarios • NPDI indicates the number in Request-Uri is ported • Phone-Context indicates the context of the called party number in the Request-Uri	All False

Remote SIP Server Data

Title	Description	Default
SIP Headers Supported • Content-Disposition • Remote-Party-ID • P-Asserted-ID • P-Preferred-ID • Privacy • Reason • Replaces • Referred-By • Originating Dial Plan ID • Billing Number • Rate Plan • Terminating Dial Plan ID	• Click appropriate headers that are supported by remote server	All False
ISUP-SIP Cause Map	Contains the name of the mapping table for ISUP Release Cause to SIP response code.	N/A
SIP-ISUP Cause Map	Contains the name of the mapping table for SIP Response code to ISUP Release Cause.	N/A
SIP Redirection Map	Contains the name of the mapping table for redirection mapping.	N/A
ISUP Variant to SIP Version Mapping	Contains the name of the mapping table for ISUP Variant to SIP Version Mapping.	N/A
SIP Cause Precedence Priority	A list of precedence rules and their respective priority.	Ordered as Listed
APN Representation	Contains the choices for Action Point Number Representation	N/A
APN Prefix	Prefix that indicates if the Number in Request-URI is APN	N/A
Phone Context for APN	Phone-Context to use for APN number	N/A
APN Phone Context for Operator Requested Numbers	Phone Context to use for APN Operator Requested Numbers	N/A
SIP Header Format	Supports the compact or long form of SIP headers.	Compact
Options for Heartbeat	Indicates if SIP Options method is used to determine accessibility of the SIP server.	Yes

Remote SIP Server Data

Title	Description	Default
Telephony profile Support	An indication of whether or not the Session Server Manager will send the X-Nortel_profile header to this remote SIP Server. <i>Note:</i> Datafill with “No” when the Remote SIP Server does not support receiving the X-Nortel-Profile header in the SIP message.	Yes
Use Info for Long Call Audit	Long call audit provisioning.	No
Map Non-Screened RPI To Calling #	Whether or not to include RPI header for clg number when building outgoing INVITEs	No
Accept Early SDP	Determines if Early Session Description Protocol are allowed by the remote server	Yes
Accept Invite without SDP	Determines if incoming calls from a remote server are accepted if the INVITE does not contain SDP in it.	Yes
Accepts Encapsulated ISUP	Indicates whether to perform ISUP encapsulation or not.	Yes
Country Code Support	Indicates if country code screening is supported. If yes a country code must be datafilled.	No
Country Code	Indicates if Country Code is supported, then datafill 3 digit Country Code if Country Code Support is set to Yes.	N/A
Out of Band DTMF Payload	Indicates the Out of Band DTMF payload monitor/detection mechanism to use	N/A
Agent Representation	Indicates agent supported ISUP/PRI/Line.	ISUP
“unknown” header	Indicates the String to use when Presentation indication is Unknown	NULL
“anonymous” header	Indicates the String to use when Presentation indication is restricted	NULL
Server Name	Character string name for the remote server.	N/A
Support for multiple IP Addresses, Ports, and Protocols	An IP addresses list that represents the Remote SIP Server. Up to 7 IP addresses and Ports are supported. At least one IP address must be entered.	N/A for IP, 5060 for Ports, and UDP for Protocols

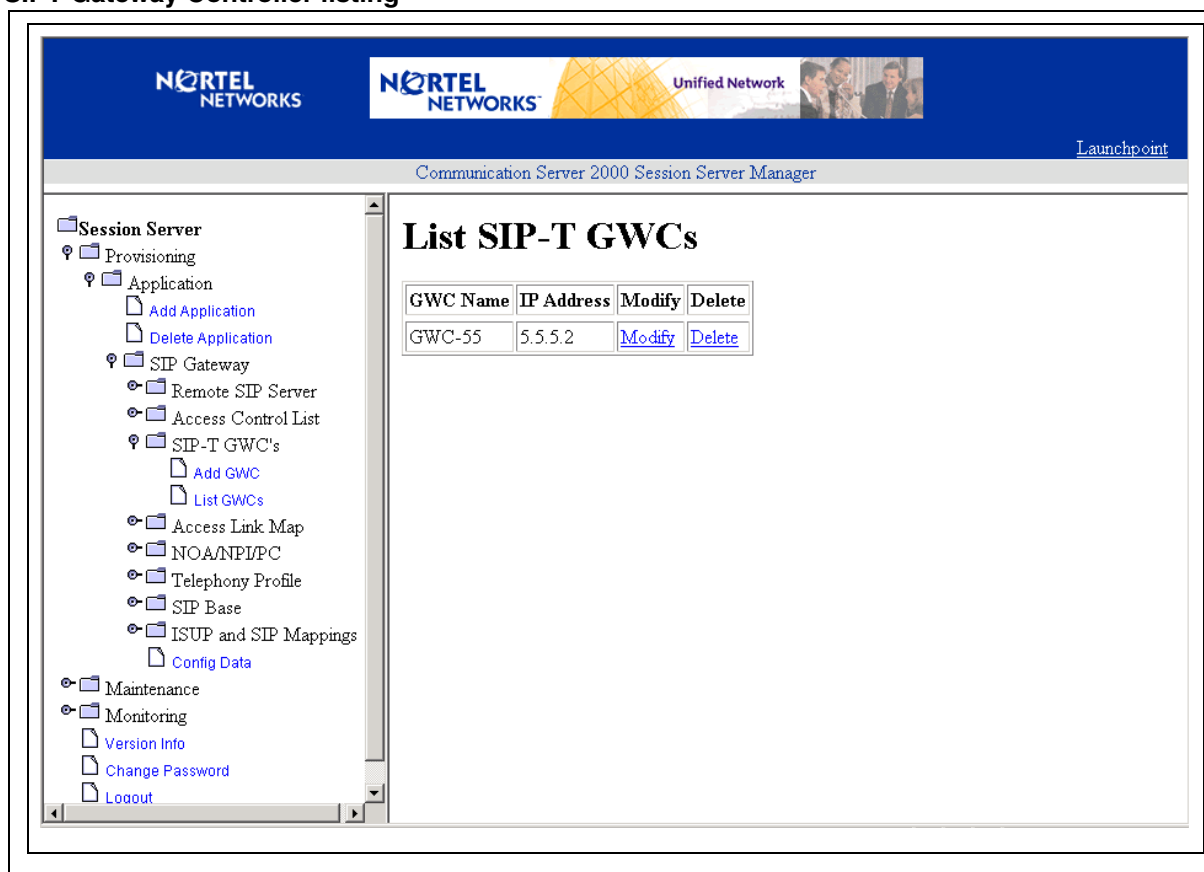
SIP-T Gateway Controllers⁵

This area of datafill consists of a list of local SIP-T⁶ gateway controllers that are used for dynamic packet trunking calls for the SIP Gateway application. SIP Gateway SIP-T GWC provisioning is performed via the following.

- In the SIP gateway provisioning menu, gateway controller datafill may be added using the “Add GWC” link in the SIP-T GWC folder
- It may also be listed by clicking on “List GWC”. Once the GWCs are listed, the user may choose to delete a GWC or modify the IP address for a particular GWC.

Datafill for a gateway controller consists of a gateway controller name and its IP address. The IP address should point to the active unit. An example of the craftsperson clicking on “List GWC” is shown in the below figure.

SIPT Gateway Controller listing



5. All GWCs are still provisioned maintained via CS2M. Datafilling a GWC in the Session Server Manager only indicates that the Session Server Manager will be communicating with that GWC.

6. SIP-T and DPT gateway controllers are one in the same with respect to the Session Server Manager.

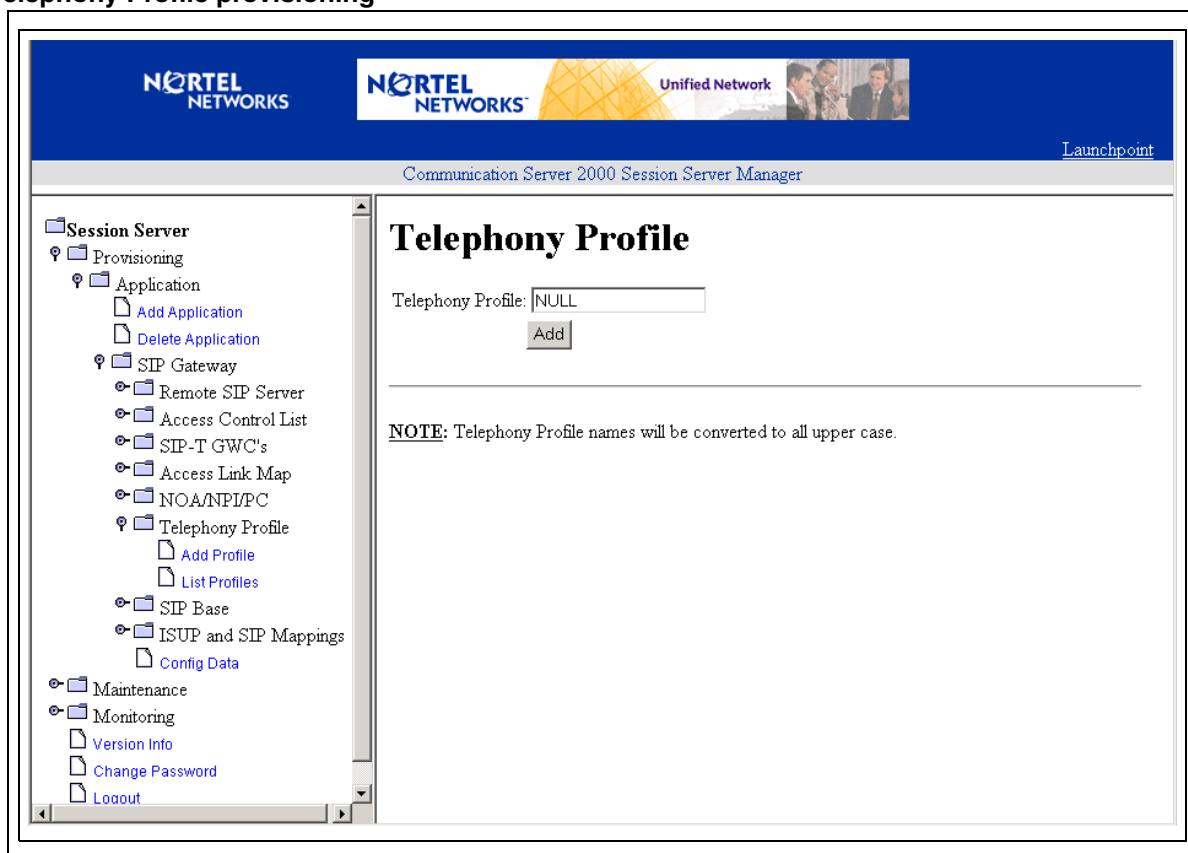
Telephony Profile

A telephony profile is a simple character string that is mapped to a SIP Access Link and Remote SIP Server pair described in section “[Access Link Map](#)” on [page 1453](#). Telephony Profile provisioning is performed via the following:

- In the SIP gateway provisioning menu, telephony profile datafill may be added using the “Add Profile” link in the Telephony Profile folder.
- It may also be listed by clicking on “List Profiles”. Once the profiles are listed, the user may choose to delete a particular one if it is not being used in any Access Link Mappings. Note that modifications on a profile are not allowed whether or not it is being used elsewhere.

An example of a user that is about add a new telephony profile is shown in the figure below.

Telephony Profile provisioning



Access Link Map

An Access Link Map provides the customer with a mechanism to determine the routing of outgoing and incoming SIP calls.

- In the SIP gateway provisioning menu, Access Link Map datafill may be added using the “Add Access Link” link in the Access Link Map folder.

- Access Link mappings can also be listed by clicking on “List Access Links”. Once the access link mappings are listed, the user may choose to delete a particular mapping. Modifications to existing mappings are not allowed.

An example of a user that is about to add a new access link mapping is shown below. An access link mapping consists of an Access Link, Telephony Profile, and a Remote SIP Server.

Access Link Map provisioning

The screenshot shows the Nortel Networks Communication Server 2000 Session Server Manager interface. The left sidebar contains a tree view with the following structure:

- Session Server
 - Provisioning
 - Application
 - Add Application
 - Delete Application
 - SIP Gateway
 - Remote SIP Server
 - Access Control List
 - SIP-T GWC's
 - Access Link Map
 - Add Access Link
 - List Access Links
 - NOA/NPL/PC
 - Telephony Profile
 - SIP Base
 - ISUP and SIP Mappings
 - Config Data
 - Maintenance
 - Monitoring
 - Version Info
 - Change Password
 - Logout

The main content area is titled "Access Link Map" and contains the following form fields:

- Link Name:
- Telephony Profile:
- Remote SIP Server:
-

ISUP Variant Map

This mapping table provides a mechanism to map ISUP Protocol, Version, and Variant to a SIP Base and Version. Example mappings are shown below.

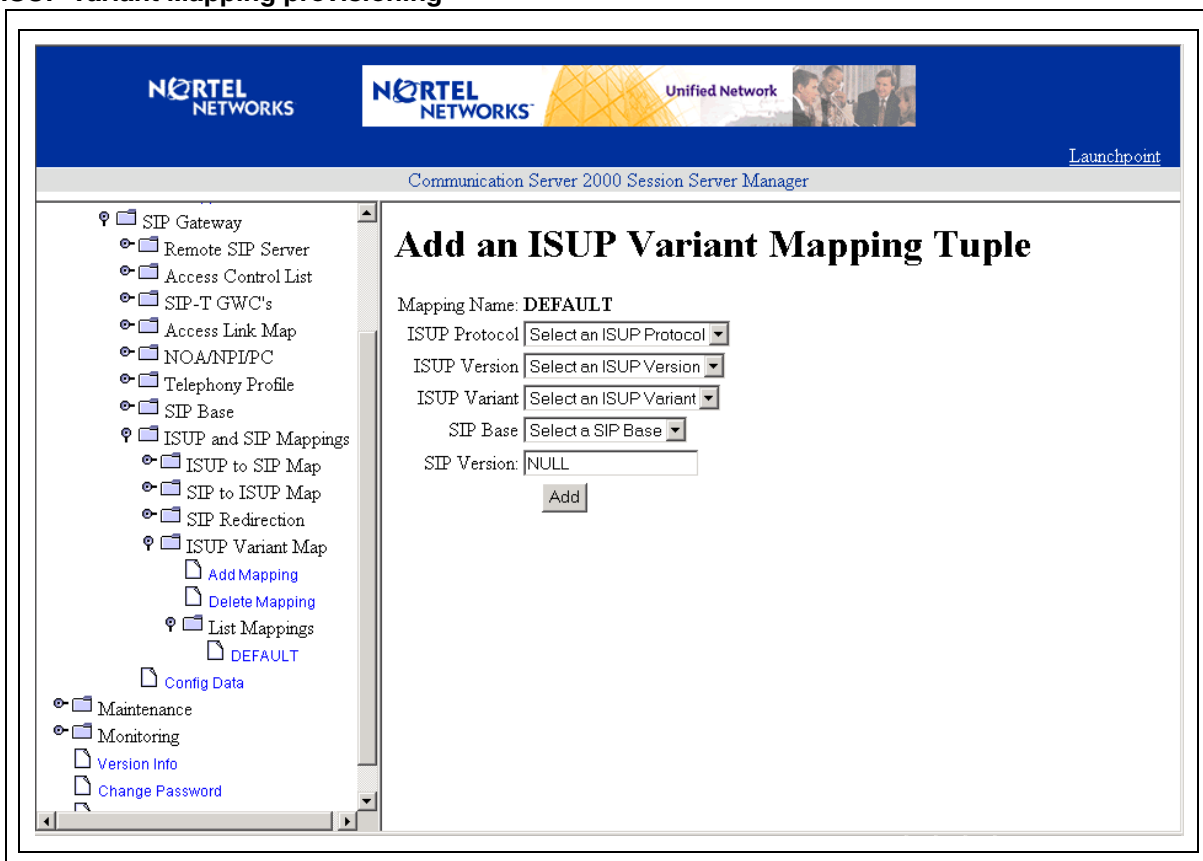
ISUP Protocol	ISUP Version	ISUP Variant	SIP Base	SIP Version
Q764			ANSI88	<user defined string>
UCP			ANSI88	<user defined string>

When adding the remote SIP servers, if you plan to select a custom mapping value for 'ISUP Variant to SIP Ver Map', then add a new variant mapping table

using the steps in Figure . If DEFAULT was selected for 'ISUP Variant to SIP Ver Map' when adding the remote SIP server, the only additional step required is to add a tuple to the DEFAULT mapping table within the ISUP Variant Map folder using the following commands:

- Click on the Provisioning folder
- Click on the Application folder
- Click on the SIP Gateway folder
- Click on the ISUP and SIP Mappings folder
- Click on the **ISUP Variant Map** sub-folder
- Click on List Mappings
- Click on DEFAULT
- In the frame on the right, click Add.
- See “ISUP Variant to SIP Version Mapping information” on page 1491 as a guide for datafill rules.

ISUP Variant Mapping provisioning



At the Add Mapping stage, the user chooses a new mapping name and the base mapping. When the new mapping is created it uses the base mapping as the one

from which to clone. The new mapping may then be modified to suit the user's call processing needs.

Once successfully added, the craftsperson may chose to add, modify, or delete tuples in their mapping or even delete their newly added mapping table. If the user were to choose to delete their new mapping, they would simply click on the "Delete Mapping" link within the "ISUP Variant Map" sub-folder. In order to modify a mapping, the craftsperson clicks on "List Mappings" and then clicks on the mapping they wish to modify.

Like other mapping tables, a default mapping table exists called DEFAULT. However this table is different in the fact that it is empty. Also this default table may have tuples added, modified or deleted.

Tuples within an ISUP to SIP Variant mapping table that are added or modified must adhere to specific datafill rules. The legal combination for the columns in a tuple are listed in the appendix in ["ISUP Variant to SIP Version Mapping information" on page 1491](#).

Access Control List [optional]

In certain scenarios it may be desirable to restrict which far-end nodes are allowed to initiate call processing with SIP Gateway application. The ability to create these restrictions exist in the form of an Access Control List (ACL)⁷.

- ACL functionality is optional and can be enabled/disabled by the users. Default value is disabled. ACL is enabled/disabled under system configuration menu of SIP gateway application.
- If ACL is disabled, all incoming SIP messages are accepted.
- Remote SIP servers are automatically included in the ACL list for screening, hence Remote SIP server IP addresses are not required to be provisioned again in the ACL list.
- With ACL enabled, SIP messages only from the list of servers provisioned in ACL list or listed in Remote SIP Server IP list are accepted.
- Please note that all the remote servers/gateways which can talk to NGSS SIP application must be datafilled in ACL, if enabled. For e.g if the remote server is a VRDN, it not sufficient to just datafill VRDN IP address, all SIPT GWCs also need to be included in the ACL, as SIPT GWCs will send SIP messages directly to NGSS.
- If ACL is enabled while both ACL list and Remote Server IP address list are empty, all incoming messages will be dropped. Hence before enabling

7. Datafill added to the access control list under SIP Gateway provisioning only affects the SIP Gateway application. Other application which exist on the Session Server Manager are not impacted by this datafill.

ACL, care should be taken to properly provision Remote SIP server and/or ACL list.

- In the SIP gateway provisioning menu, access control list datafill may be added using the “Add IP Range” link in the Access Control List folder.

When the “Add IP Range” link is clicked, the user is prompted for an IP address and a network mask. The range of IP addresses to allow is calculated based on a combination of the IP address and network mask entered.

- Provisioned servers may be listed by clicking on “List IP Ranges”. Once the IP ranges are listed, the user may choose to delete a particular IP range. Note that Remote Server IP address are not listed in this list though they are included in screening the incoming SIP messages.
- To modify an IP address range it must be deleted and re-added. It cannot be modified.
- A range of 0.0.0.0 is not supported because it is the default address if no address has been assigned yet.

A few examples of the IP/mask algorithm include:

10.1.1.1/255.255.255.255 means only one host 10.1.1.1.

10.1.1.1/255/255/255.0 means all host in the range 10.1.1.0 to 10.1.1.255

Access Control List - Adding a New IP Address

NORTEL NETWORKS **NORTEL NETWORKS** Unified Network  [Launchpoint](#)

Communication Server 2000 Session Server Manager

Session Server

- Provisioning
 - Application
 - [Add Application](#)
 - [Delete Application](#)
 - SIP Gateway
 - Remote SIP Server
 - Access Control List
 - [Add IP Range](#)
 - [List IP Ranges](#)
 - SIP-T GWC's
 - Access Link Map
 - NOA/NPI/PC
 - Telephony Profile
 - SIP Base
 - ISUP and SIP Mappings
 - [Config Data](#)
 - Maintenance
 - Monitoring
 - [Version Info](#)
 - [Change Password](#)
 - [Logout](#)

Add a new IP Address

IP Address:

Subnet Mask:

NOTE: IP addresses will be normalized into ranges as per masks.

NOTE: IP restriction for SIP addresses can be turned off and on via the Configuration Data menu.

Access Control List - List Ranges**NOA/NPI/PC Indicator mapping [optional]**

The NOA/NPI/PC Indicator mapping represents the Nature of Address/Numbering Plan to Phone Context Indicator mapping.

When selecting the NOA/NPI/PC folder, three options are available: Add NOA, List NOA, or a subfolder NOA/NPI/PC mapping.

The Add and List pages allow for the addition or deletion of “Nature of Address” values. These entries have been precluded with standard values.

Adding an NOA

The screenshot shows the 'Add an Nature of Address Name' page in the Nortel Networks Communication Server 2000 Session Server Manager. The left sidebar contains a tree view with the following structure:

- Session Server
 - Provisioning
 - Application
 - Add Application
 - Delete Application
 - SIP Gateway
 - Remote SIP Server
 - Access Control List
 - SIP-T GWC's
 - Access Link Map
 - NOA/NPI/PC
 - Add NOA
 - List NOA
 - NOA/NPI/PC Mapping
 - Add Mapping
 - Delete Mapping
 - List Mappings
 - DEFAULT
 - Telephony Profile

The main content area is titled 'Add an Nature of Address Name' and contains the following form:

NOA Name:

NOA Number:

NOTE: Nature of Address names will be displayed as-entered.

NOTE: Nature of Address numbers should be unique across interconnected systems.

Listing NOAs

The screenshot shows the 'List Nature of Addresses' page in the Nortel Networks Communication Server 2000 Session Server Manager. The left sidebar contains a tree view with the following structure:

- Session Server
 - Provisioning
 - Application
 - Add Application
 - Delete Application
 - SIP Gateway
 - Remote SIP Server
 - Access Control List
 - SIP-T GWC's
 - Access Link Map
 - NOA/NPI/PC
 - Add NOA
 - List NOA
 - NOA/NPI/PC Mapping
 - Add Mapping
 - Delete Mapping
 - List Mappings
 - DEFAULT
 - Telephony Profile
 - SIP Base
 - ISUP and SIP Mappings
 - Config Data
- Maintenance
- Monitoring
 - Version Info

The main content area is titled 'List Nature of Addresses' and contains a table with the following data:

Name	Number	Delete
Subscriber Number	1	Delete
VPN Number	2	Delete
National Significant Number	3	Delete
International Number	4	Delete
Abbreviated Number	6	Delete
Treated Call Operator Request	112	Delete
Subscriber Number Operator Request	113	Delete
National Number Operator Request	114	Delete
International Number Operator Request	115	Delete
No Number Present Operator Request	116	Delete
No Number Present Cut Thru	117	Delete
APN Number	120	Delete
International Inbound Operator Call	122	Delete

NOA/NPI/PC Mapping subfolder includes options to Add Mapping, Delete Mapping, and List Mappings.

When a call is originated this value will be added to the originating URI to indicate the context or origin of the call. For numbers like 411 and 911 this is necessary in that the number does not by itself identify the geographical origin of the call.

Either the default mapping may be changed to support such a feature or new mapping tables may be created.

Add an NOA to Phone-Context Mapping

The screenshot shows the Nortel Networks Communication Server 2000 Session Server Manager web interface. The top header includes the Nortel Networks logo, the text 'Unified Network', and a 'Launchpoint' link. Below the header, the page title is 'Add an NOA/NPI to Phone-Context Mapping'. The left sidebar contains a tree view of the system configuration, with 'NOA/NPI/PC Mapping' selected. The main content area contains the following text: 'This command will add a new Nature of Address and Numbering Plan Indicator to Phone Context mapping based on the "base" mapping selected below. The new mapping will be created as identical to the base mapping but can then be modified as needed by selecting it from the List Mappings menu.' Below this text are two input fields: 'New Mapping Name' with the value 'NULL' and 'Base Mapping Name' with a dropdown menu showing 'Select a Cause Map'. An 'Add' button is located below these fields. A note at the bottom states: 'NOTE: Mapping names will be converted to all upper case.'

New NOA to Phone-Context Mapping

The screenshot shows the Nortel Networks Communication Server 2000 Session Server Manager interface. The left sidebar contains a tree view with the following structure:

- Session Server
 - Provisioning
 - Application
 - Add Application
 - Delete Application
 - SIP Gateway
 - Remote SIP Server
 - Access Control List
 - SIP-T GWC's
 - Access Link Map
 - NOA/NPI/PC
 - Add NOA
 - List NOA
 - NOA/NPI/PC Mapping
 - Add Mapping
 - Delete Mapping
 - List Mappings
 - DEFAULT

The main content area is titled "Add an NOA/NPI to Phone Context Mapping". It contains the following form fields:

- Mapping Name: **PREFERRED**
- Nature of Address:
- Numbering Plan Indicator:
- Phone Context:
-

Delete an NOA/NPI to Phone Context Map

The screenshot shows the Nortel Networks Communication Server 2000 Session Server Manager interface. The left sidebar contains a tree view with the following structure:

- Session Server
 - Provisioning
 - Application
 - Add Application
 - Delete Application
 - SIP Gateway
 - Remote SIP Server
 - Access Control List
 - SIP-T GWC's
 - Access Link Map
 - NOA/NPI/PC
 - Add NOA
 - List NOA
 - NOA/NPI/PC Mapping
 - Add Mapping
 - Delete Mapping
 - List Mappings
 - DEFAULT
 - Telephony Profile

The main content area is titled "Delete NOA/NPI to Phone Context Map". It contains a table with the following data:

Name	Delete
DEFAULT	Can't Delete
PREFERRED	Delete

Listing of an NOA/NPI to Phone Context Map

The screenshot shows the Nortel Networks Communication Server 2000 Session Server Manager interface. The left sidebar contains a tree view with the following structure:

- Session Server
 - Provisioning
 - Application
 - Add Application
 - Delete Application
 - SIP Gateway
 - Remote SIP Server
 - Access Control List
 - SIP-T GWC's
 - Access Link Map
 - NOA/NPI/PC
 - Add NOA
 - List NOA
 - NOA/NPI/PC Mapping
 - Add Mapping
 - Delete Mapping
 - List Mappings
 - DEFAULT
 - Telephony Profile

The main content area is titled "NOA/NPI to Phone-Context Mapping: PREFERRED". It contains a table with the following columns: Nature of Address, Numbering Plan Indicator, Phone Context, Modify, and Delete. The table has one row with the values 113, 6, and 42. Below the table is an "Add" button. A note below the table states: "NOTE: To add tuples to this Mapping, click on the 'Add' button above."

ISUP Cause to SIP Response code mapping [optional]

An ISUP Cause to SIP Response code mapping table maps an ISUP Release Cause to a SIP Response code. For example, the ISUP release cause value of 17, indicating user busy, might be mapped to a SIP response code value 486 indicating busy.

A single ISUP Cause to SIP Response mapping table consists of nearly eighty ISUP Release Causes mapped to SIP response codes. Along with each mapping is a SIP Text Reason Phrase and an ISUP Text Reason Phrase. See the following table for a partial mapping.

ISUP Release Cause to SIP Response Code mapping

ISUP Release Cause	SIP Response Code	SIP Text Reason Phrase	ISUP Text Reason Phrase
...			
4	487	Request Terminated	Send Special Tone Information
5	404	Not Found	Misdialled trunk prefix
6	480	Temporarily Unavailable	Channel Unacceptable

ISUP Release Cause to SIP Response Code mapping

ISUP Release Cause	SIP Response Code	SIP Text Reason Phrase	ISUP Text Reason Phrase
7	487	Request Terminated	Call awarded and being delivered in an established channel
8	487	Request Terminated	Preemption
9	487	Request Terminated	Preemption-circuit reserved for use
16	487	Request Terminated	Normal call clearing
17	486	Busy Here	User busy
.....			

The ISUP Cause to SIP Response mapping is termed optional datafill since a pre-defined mapping table exists in the system. This mapping table is called “DEFAULT”. This predefined default mapping table may be selected when provisioning a Remote SIP Server described in “Remote SIP Servers” on page 1447. Note that this pre-defined mapping table cannot be modified.

Although a pre-defined mapping exists, users may wish to create new mapping tables for their specific processing needs. This is done through the web interface.

In order to add a new mapping table, the user goes to the “ISUP to SIP Map” sub-folder from the main Session Server Manager menu via the following commands:

- Click on the Provisioning folder
- Click on the Application folder
- Click on the SIP Gateway folder
- Click on the Mappings folder
- Click on the **ISUP to SIP Map** sub-folder
- Click on Add Mapping.

After clicking on “Add Mapping”, the following figure shows what a craftsperson sees in the web browser.

Provisioning an ISUP Cause to SIP Response code mapping

The screenshot shows the Nortel Networks Communication Server 2000 Session Server Manager interface. The top banner includes the Nortel Networks logo, the text 'Unified Network', and a 'Launchpoint' link. The main title is 'Add a ISUP to SIP Mapping'. Below the title, a descriptive text states: 'This command will add a new ISUP Release Cause to SIP Response Code Mapping based on the "base" mapping selected below. The new mapping will be created as identical to the base mapping but can then be modified as needed by selecting it from the List Mappings menu.'

The interface includes a left-hand navigation tree with the following structure:

- Application
 - Add Application
 - Delete Application
- SIP Gateway
 - Remote SIP Server
 - Access Control List
 - SIP-T GWC's
 - Access Link Map
 - NOA/NPI/PC
 - Telephony Profile
 - SIP Base
 - ISUP and SIP Mappings
 - ISUP to SIP Map
 - Add Mapping
 - Delete Mapping
 - List Mappings
 - SIP to ISUP Map
 - SIP Redirection
 - ISUP Variant Map
 - Add Mapping
 - Delete Mapping
 - List Mappings
 - Config Data

The main content area contains the following form fields:

- New Mapping Name:
- Base Mapping Name:
-

A note at the bottom states: **NOTE:** Mapping names will be converted to all upper case.

At the Add Mapping stage, the user chooses a new mapping name and the base mapping. When the new mapping is created, it uses the base mapping as the one from which to clone. The new mapping may then be modified to suit the user's call processing needs. The clone procedure exists so that a user does not have to enter the nearly eighty mappings to complete an ISUP Release Cause to SIP Response Code mapping table. A user is allowed to clone from any of the existing ISUP Release Cause to SIP Response Code mappings.

For the previous example, assume that the craftsperson entered a mapping name of MAP123. The mappings that exist in the system may be displayed by clicking on "List Mappings" within the "ISUP to SIP Map" sub-folder. In the following figure, five mappings exist including the one just created by the craftsperson. Assuming the craftsperson wants to examine or modify the new mapping table, they simply click on the "MAP123" link.

Details on a ISUP Cause to SIP Response code mapping

The screenshot shows the Nortel Networks Communication Server 2000 Session Server Manager interface. The left sidebar contains a tree view with the following structure:

- Session Server
 - Provisioning
 - Application
 - Add Application
 - Delete Application
 - SIP Gateway
 - Remote SIP Server
 - Access Control List
 - SIP-T GWC's
 - Access Link Map
 - NOA/NPI/PC
 - Telephony Profile
 - SIP Base
 - ISUP and SIP Mappings
 - ISUP to SIP Map
 - Add Mapping
 - Delete Mapping
 - List Mappings
 - DEFAULT
 - SIP to ISUP Map
 - SIP Redirection
 - ISUP Variant Map

The main content area displays the title "ISUP Cause to SIP Response Mapping: NULLVDFD" and a table with the following data:

ISUP Release Cause	SIP Response Code	SIP Text Reason	ISUP Text Reason	Modify
1	404	Not Found	Unallocated number	Modify
2	404	Not Found	No route to network	Modify
3	404	Not Found	No route to destination	Modify
4	487	Request Terminated	Send Special Tone Information	Modify
5	404	Not Found	Misdialled trunk prefix	Modify
6	480	Temporarily Unavailable	Channel Unacceptable	Modify
7	487	Request Terminated	Call awarded and being delivered in an established channel	Modify
8	487	Request Terminated	Preemption	Modify
9	487	Request Terminated	Preemption-circuit reserved for use	Modify
16	487	Request	Normal call clearing	Modify

Once clicked the mapping table is presented in the Interaction Frame. If the craftsperson then wants to modify a single tuple within that mapping table, they simply click on the “Modify” link and a tuple modify screen comes up in the Interaction Frame as shown in the following figure.

Tuple modification for an ISUP Cause to SIP Response code mapping

The screenshot displays the Nortel Networks Communication Server 2000 Session Server Manager web interface. The top banner includes the Nortel Networks logo and the text 'Unified Network'. The main title bar reads 'Communication Server 2000 Session Server Manager'. On the left, a navigation tree shows the following structure:

- Session Server
 - Provisioning
 - Application
 - Add Application
 - Delete Application
 - SIP Gateway
 - Remote SIP Server
 - Access Control List
 - SIP-T GWC's
 - Access Link Map
 - NOA/NPI/PC
 - Telephony Profile
 - SIP Base
 - ISUP and SIP Mappings
 - ISUP to SIP Map
 - Add Mapping
 - Delete Mapping
 - List Mappings
 - DEFAULT
 - SIP to ISUP Map
 - SIP Redirection
 - ISUP Variant Map

The main content area is titled 'Modify an ISUP to SIP Cause Mapping Tuple'. It contains the following fields and a button:

- Mapping Name: NULLVDFD
- ISUP Release Cause: 7
- SIP Response Code: 487
- SIP Text: Request Terminated
- ISUP Text: Call awarded and being deli
- Modify button

In this figure, the craftsperson chose to modify the tuple with the ISUP Release Cause of 5. They are then allowed to modify the SIP Response Code, SIP Text, and ISUP Text.

Existing mapping tables may be deleted by clicking on the “Delete Mapping” link within the “ISUP to SIP Map” sub-folder. When “Delete Mapping” is clicked, the user is presented with a selection of all mapping tables. Note the default mapping cannot be deleted. Finally, if the user attempts to delete a mapping that is in use by a Remote SIP Server, the request is denied.

SIP Response Code to ISUP Cause mapping [optional]

A SIP Response Code to ISUP Release Cause mapping table maps an SIP Response Codes to ISUP Release Causes. For example, the SIP Response Code of 404 may be mapped to the ISUP Release Cause of 41.

A single SIP Response to ISUP Cause mapping table consists of nearly forty SIP Response Codes mapped to ISUP Release Causes. See the following figure for an example of this mapping:

SIP Response Code to ISUP Release Cause mapping

SIP Response Code	ISUP Release Cause
400	41
401	21
402	21
403	21
404	1
.. . .	

The SIP Response Code to ISUP Release Cause mapping is termed optional datafill since a pre-defined mapping table exists in the system. This mapping table is called “DEFAULT”. This predefined default mapping table may be selected when provisioning a Remote SIP Server described in “ Remote SIP Servers” on page 1447. Note this pre-defined mapping table cannot be modified.

Although a pre-defined mapping exists, users may wish to create new mapping tables for their specific processing needs. This is done through the web interface.

In order to add a new mapping table, the user goes to the “SIP to ISUP Ma” sub-folder from the main Session Server Manager menu via the following commands:

- Click on the Provisioning folder
- Click on the Application folder
- Click on the SIP Gateway folder
- Click on the Mappings folder
- Click on the **SIP to ISUP Map** folder
- Click on Add Mapping

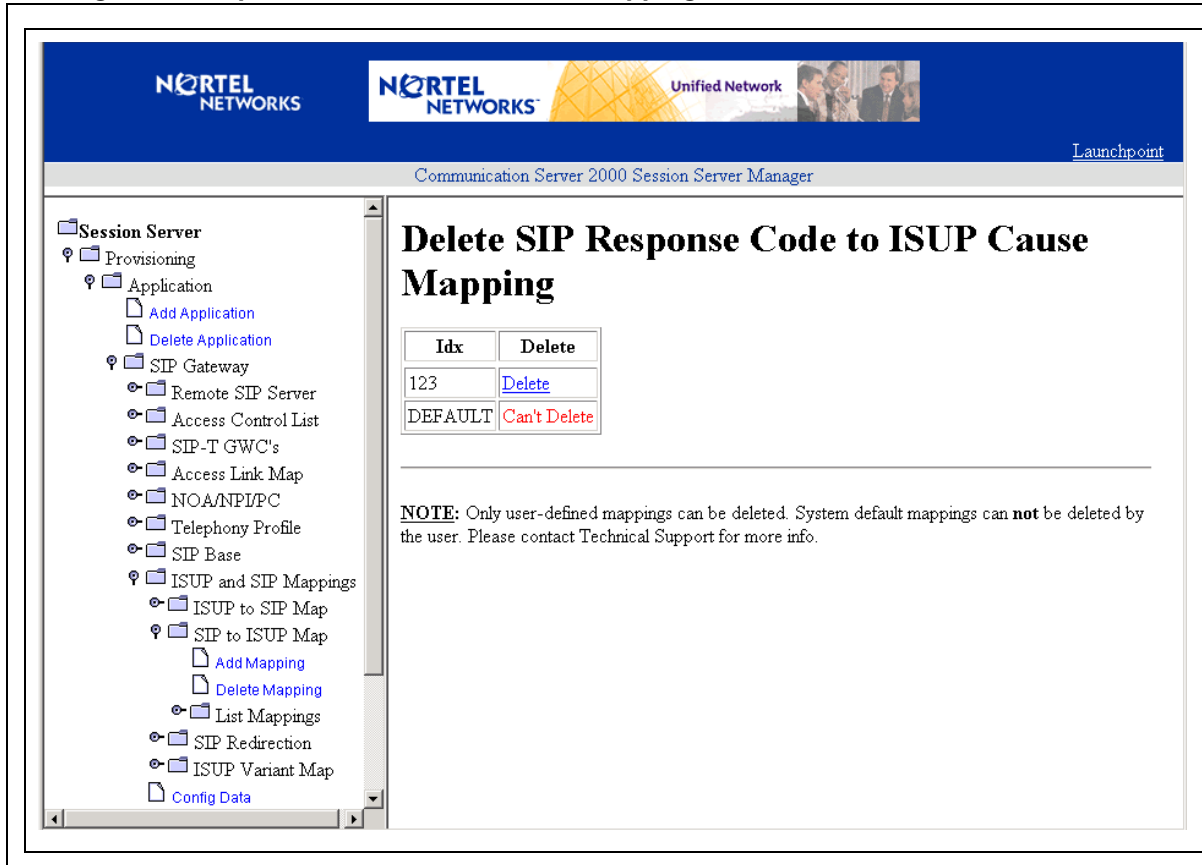
After clicking on “Add Mapping”, the following figure shows what a craftsperson sees in the web browser.

Provisioning a SIP Response Code to ISUP Cause mapping

The screenshot shows the Nortel Networks Communication Server 2000 Session Server Manager web interface. The top header features the Nortel Networks logo and the text 'Unified Network'. The main title of the page is 'Add a SIP to ISUP Mapping'. Below the title, a descriptive text states: 'This command will add a new SIP Response Code to ISUP Cause Mapping based on the "base" mapping selected below. The new mapping will be created as identical to the base mapping but can then be modified as needed by selecting it from the List Mappings menu.' The form contains two input fields: 'New Mapping Name' with the value 'NULL' and 'Base Mapping Name' with a dropdown menu showing 'Select a Cause Map'. An 'Add' button is positioned below these fields. A note at the bottom of the form reads: 'NOTE: SIP to ISUP Mapping names will be converted to all upper case.' On the left side, a navigation tree is visible, showing the hierarchy: Session Server > Provisioning > Application > Add Application, Delete Application, SIP Gateway > Remote SIP Server, Access Control List, SIP-T GWC's, Access Link Map, NOA/NPI/PC, Telephony Profile, SIP Base, ISUP and SIP Mappings > ISUP to SIP Map, SIP to ISUP Map > Add Mapping, Delete Mapping, List Mappings, SIP Redirection, ISUP Variant Map, and Config Data.

At the Add Mapping stage, the user chooses a new mapping name and the base mapping. When the new mapping is created, it uses the base mapping as the one from which to clone. The new mapping may then be modified to suit the user's call processing needs. This clone procedure exists so that a user does not have to enter the nearly forty mappings to complete a SIP Response Code to ISUP Release Cause mapping table. Note a user may clone from any of the existing SIP Response Code to ISUP Release Cause mappings.

Once successfully added, the craftsperson may choose to modify tuples in their mapping or even delete the newly added mapping table. If the user were to choose to delete their new mapping, they would simply click on the "Delete Mapping" link within the "SIP to ISUP" sub-folder. The following figure shows an example of what is presented to the craftsperson in such a scenario.

Deleting a SIP Response Code to ISUP Cause mapping**SIP Redirection Mapping [optional]**

SIP Redirection Mapping is a mapping of 3xx SIP redirection response messages to an associated 300-699 response codes. This mapping allows the customer to configure a call receiving a 3XX redirection message to be processed as a 300 or 699 related value. An example of the redirection mapping defaults are shown in the following table.

Redirection mapping defaults

SIP Redirection code	Response Code
300	300
301	301
302	302
305	305
380	380

SIP Redirection Mapping datafill is optional if the customer does not wish to change any of the above pre-defined defaults.

Although the pre-defined default mapping exists, users may wish to create new mapping tables for their specific processing needs. This is done through the web interface.

In order to add a new mapping table, the user goes to the “ISUP to SIP Map” sub-folder from the main Session Server Manager menu via the following commands:

- Click on the Provisioning folder
- Click on the Application folder
- Click on the SIP Gateway folder
- Click on the Mappings folder
- Click on the **SIP Redirection** folder
- Click on Add Mapping

After clicking on “Add Mapping”, the following figure shows what a craftsperson sees in the web browser.

SIP Redirection Mapping provisioning

The screenshot displays the Nortel Networks Session Server Manager web interface. The top header features the Nortel Networks logo and the text 'Unified Network'. Below the header, the page title is 'Communication Server 2000 Session Server Manager'. On the left side, there is a navigation tree with the following structure:

- Session Server
 - Provisioning
 - Application
 - Add Application
 - Delete Application
 - SIP Gateway
 - Remote SIP Server
 - Access Control List
 - SIP-T GWC's
 - Access Link Map
 - NOA/NPI/PC
 - Telephony Profile
 - SIP Base
 - ISUP and SIP Mappings
 - ISUP to SIP Map
 - SIP to ISUP Map
 - SIP Redirection
 - Add Mapping
 - Delete Mapping
 - List Mappings
 - ISUP Variant Map
 - Config Data

The main content area is titled 'Add SIP Redirection Mapping'. It contains the following text:

This command will add a new SIP Redirection Mapping based on the "base" mapping selected below. The new mapping will be created as identical to the base mapping but can then be modified as needed by selecting it from the List Mappings menu.

Below the text, there is a form with the following fields:

- Name:
- Base SIP Redirection Map:
-

At the bottom of the form, there is a note:

NOTE: SIP Redirection Mapping names will be converted to all upper case.

At the Add Mapping stage, the user chooses a new mapping name and the base mapping. When the new mapping is created it uses the base mapping as the one from which to clone. The new mapping may then be modified to suit the user's call processing needs.

Once successfully added, the craftsperson may chose to modify tuples in their mapping or even delete their newly added mapping. If the user were to choose to delete their new mapping, they would simply click on the "Delete Mapping" link within the "SIP Redirection" sub-folder. In order to modify a mapping, the craftsperson clicks on "List Mappings" and then clicks on the mapping they wish to modify.

SIP Base [optional]

A SIP Base is a simple character string that represents base protocols utilized when provisioning ISUP to SIP Variants described in an section . In order to provision a new SIP base, the following is done:

- In the SIP Gateway provisioning menu, SIP Base datafill may be added using the "Add SIP Base" link in the SIP Base folder.
- It may also be listed by clicking on "List SIP Base". Once the values are listed, the user may choose to delete a particular one if it is not being used in any datafilled tuples in the ISUP Variant Mapping table. Deletions on system defaults are not allowed.

Six protocol defaults exist. Those pre-defined defaults are:

ANSI88	ITU-T92-PLUS	ETSI356
ITU-T88	ETSI121	TTC93-PLUS

An example of a user listing all the SIP Base values in the system is as follows:

SIP Base listing

The screenshot shows the Nortel Networks web interface for the Communication Server 2000 Session Server Manager. The top banner includes the Nortel Networks logo and the text 'Unified Network'. The page title is 'List SIP Bases'. On the left is a navigation tree with the following structure:

- Session Server
 - Provisioning
 - Application
 - Add Application
 - Delete Application
 - SIP Gateway
 - Remote SIP Server
 - Access Control List
 - SIP-T GWC's
 - Access Link Map
 - NOA/NPI/PC
 - Telephony Profile
 - SIP Base
 - Add SIP Base
 - List SIP Bases (selected)
 - ISUP and SIP Mappings
 - Config Data
 - Maintenance
 - Monitoring
 - Version Info
 - Change Password
 - Logout

The main content area displays a table titled 'List SIP Bases' with two columns: 'SIP Base' and 'Delete'.

SIP Base	Delete
ANSI88	Can't Delete
ETSI121	Can't Delete
ETSI356	Can't Delete
ITU-T88	Can't Delete
ITU-T92-PLUS	Can't Delete
NULL	Can't Delete
TTC93-PLUS	Can't Delete

Below the table, a **NOTE** states: 'Only user-defined SIP Base names can be deleted. System default tuples can **not** be deleted by the user. Please contact Technical Support for more info.'

SIP Gateway application maintenance

In previous sections, the functionality of the SIP Gateway application, which resides on the Session Server Manager was described in detail. For the SIP Gateway application to function properly, certain actions must be performed by SIP Gateway maintenance.

Note this section is written with the assumption that the Session Server Manager's unit status is active and enabled. Refer to section "Unit Status" on page 1478 for allowed maintenance actions when the unit is either not active or not enabled.

Access the SIP Gateway maintenance section of the web page by going to:

- Click on Maintenance folder
- Click on the Application folder
- Click on SIP Gateway

SIP Gateway application maintenance

The screenshot displays the 'Communication Server 2000 Session Server Manager' web interface. On the left is a navigation tree with 'Session Server' expanded, showing 'Provisioning', 'Maintenance', 'Platform', 'Application' (with 'SIP Gateway' selected), 'Monitoring', 'Version Info', 'Change Password', and 'Logout'. The main content area shows three status tables and maintenance controls.

Session Server Status - Connected to Unit #1

Unit Number	Activity State	Operational State
0	unknown	Disabled
1	Active	Enabled

SIP Gateway Status

Administrative State	Operational State	Procedural Status	Control Status
Locked	Disabled	-	Suspended

SIP Gateway Maintenance

Administrative	Control
Lock UnLock Shut Down	Suspend UnSuspend

Below the maintenance controls are 'Refresh' and 'QueryInfo' buttons. At the bottom, a box shows 'Last Performed Operation: Refresh' and 'Result: Passed', with a 'SIP Cold SwAct' button below it.

Before performing maintenance actions, a basic outline on how to bring the SIP Gateway application into service and out of service is as follows:

Taking the application from out of service to in-service

- Unsuspend followed by Unlock

Taking the application from in-service to out of service

- Lock followed by Suspend

SIP Gateway maintenance utilizes the CCITT X.731 state and status attributes as well as X.731 commands. This is different than the standard DMS Core commands (e.g. BSY, RTS) and state (e.g. INSV), but it is consistent with recent Succession platform additions. The following table shows the four fields that comprise the CCITT X.731 state of the SIP Gateway application. The last column in the table is shown to provide a mapping to old-style DMS states to aid in understanding⁸.

8. The DMS style states are not shown on the SIP Gateway maintenance web page. It is shown above only for understanding.

SIP Gateway application states

Administrative State	Operational State	Procedural Status	Control Status	DMS Style States
Locked	Disabled	-	Suspended	OFFL
Locked	Enabled	-	-	MANB
Locked	Enabled	Terminating	-	MANBP
Unlocked	Enabled	-	-	INSV
Unlocked	Disabled	-	-	SYSB
Shutting Down	Enabled	-	-	INSVD

From the web interface, the above states may be changed via the following maintenance commands. Each of the five maintenance control items are represented by clickable buttons on the web page.

- Administrative State Control- The user can select from the following:
 - Lock
 - Unlock
 - Shut Down
- Control Status Control - The user can select from the following:
 - Suspend
 - Unsuspend

Depending on the current state, the user is not always allowed access to all of the maintenance control options.

The table below explains what controls are allowed depending on the current Admin State, Operational State, and Procedural Status. Again, DMS Style representation is shown in parenthesized italics to aid in understanding.

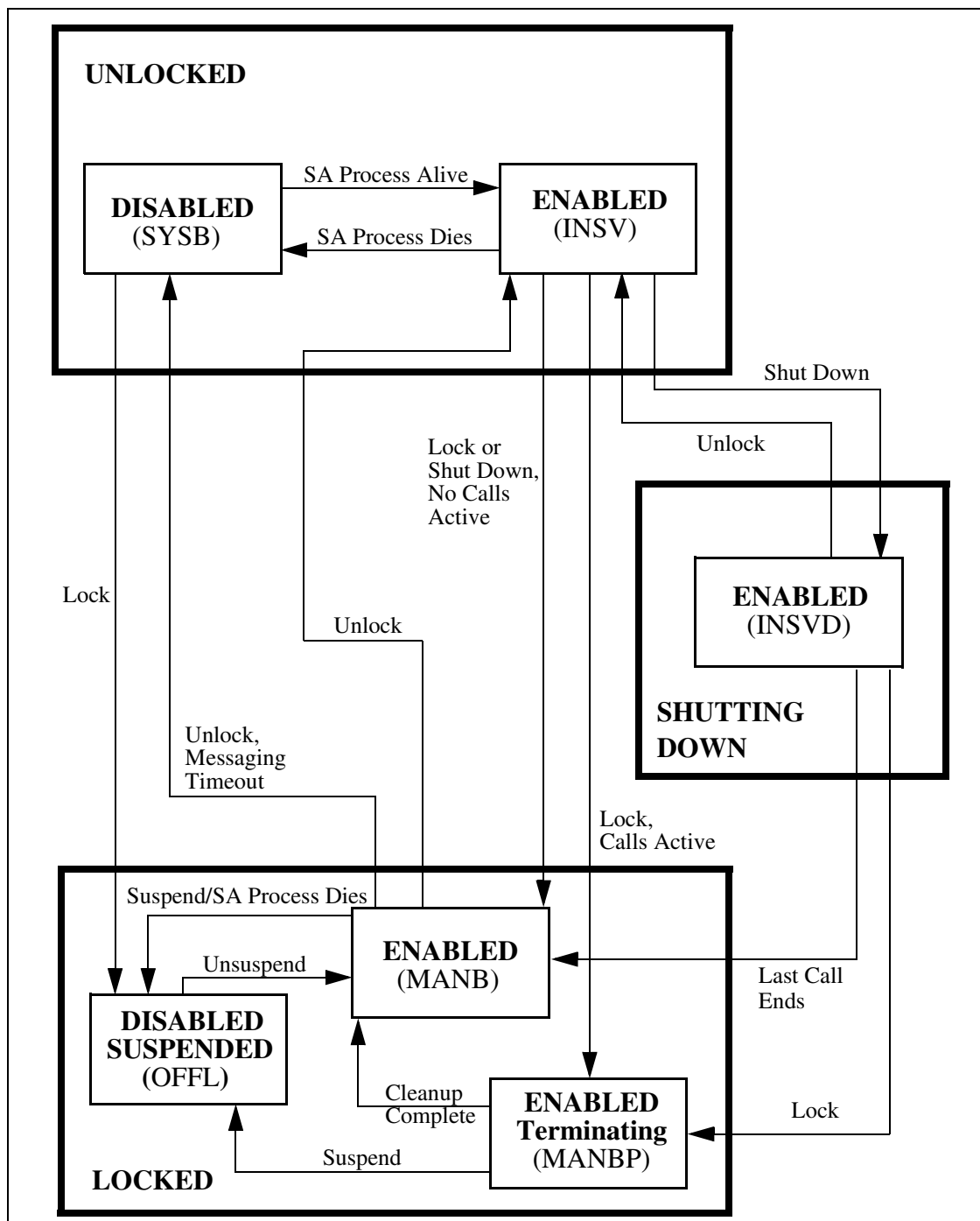
SIP Gateway Maintenance External Controls Allowed

Admin State	Operational State	Procedural Status	Control Status	Allowed Controls DMS Style Commands in ()'s
Locked	Disabled	-	Suspended	<u>Admin Control</u> None <u>Control Status</u> Unsuspend (<i>BSY</i>)

Admin State	Operational State	Procedural Status	Control Status	Allowed Controls DMS Style Commands in ()'s
Locked	Enabled	-	-	<u>Admin Control</u> Unlock (RTS) <u>Control Status</u> Suspend (OFFL)
Locked	Enabled	Terminating	-	<u>Admin Control</u> None <u>Control Status:</u> Suspend (OFFL)
Unlocked	Enabled	-	-	<u>Admin Control</u> Lock (BSYFORCE) Shut Down (BSY) <u>Control Status</u> None
Unlocked	Disabled	-	-	<u>Admin Control</u> Lock (OFFL ^a) <u>Control Status</u> None
Shutting Down	Enabled	-	-	<u>Admin Control</u> Lock (BSYFORCE) Unlock (RTS) <u>Control Status</u> None

a. From a DMS perspective, this is a non-standard command. In the DMS model you would expect to do a BSY command, and then an OFFL command to get from the SYSB to OFFL state. However, for the SIP Gateway maintenance state model, SYSB is an error condition where the SIP Gateway process has died due to some error. MANB is a state where the SIP Gateway process should be up and running. Thus, it is more applicable when manually taking the SIP Gateway out of service from the SYSB command to go directly to OFFL (as opposed to first going MANB), as both are states where the SIP Gateway process is not running.

Finally, a maintenance state is presented. DMS system commands are shown in parentheses to aid in understanding. However, DMS style commands are not shown on the web page since CCITT X.731 commands and controls are utilized.

SIP Gateway Maintenance State Diagram**Application Cold Swact**

On the SIP Gateway Application maintenance page, the SIP Cold SWACT button allows users to perform an application cold switch of activity (SWACT)

if the Session Server Manager platform is active and enabled. If the unit is not active, the button is not allowed to be pressed.

Assuming the Session Server Manager unit activity status is active and the operational state is enabled, the craftsperson can click the button to perform an application cold SWACT.

Note: From the active unit web page, the unit must be active, enabled, and the mate unit must be on standby and enabled in order to access the SIP Cold SWACT button.

If the user clicks the SIP Cold SWACT button, a dialog box appears to verify that the user wants to proceed with a SIP Gateway cold SWACT. The consequences of performing a SIP Gateway cold SWACT include the following:

- All currently active SIP Gateway calls will be taken down.
- A Session Server Manager force SWACT will then occur.

Note: This is not the normal interface to request a platform SWACT. Only proceed with the SIP Gateway cold SWACT if a platform SWACT has already taken place, and a problem has been detected with SIP Gateway call processing.

Unit Status

The previous SIP Gateway maintenance sections made the assumptions that the Session Server Manager unit's activity state was active and the operational state was enabled. If unit activity state is not active or the operation state is not enabled, maintenance actions on the SIP Gateway application are not allowed. The only buttons available for use on the SIP Gateway application maintenance page are the refresh and the QueryInfo buttons.

Alarms

The Session Server Manager has the capability for applications or the system itself to generate alarms. These alarms can be viewed on the Session Server Manager's Alarm web page. Information shown about particular alarms include the type, identifier, time-stamp, host (unit from which the alarm was raised), severity, and a description of the alarm.

The user may view alarms by going to the alarms web page. The alarm web page is located in the Monitoring menu folder.

Once the craftsperson clicks on Alarms, the alarm web page is presented in the right frame with the current alarm list. The alarm web page updates every 30 seconds and the user also has the option of invoking a re-query of alarms. This is similar to the Alarm implementation for the Storm system.

Sample Alarm page

The Alarms panel updates every 45 seconds
Datestamp of last update: Thursday May 06th 2004 03:45:52 PM EST

Type	ID	Timestamp	Host	Severity	Description
Equipment	Underlying Resource Unavailable	Thursday May 06th 2004 11:49:41 AM	znc1y0jc	Major	Array: '/dev/md1' (ntvg) Status: A physical disk has been removed from the array.
Equipment	Underlying Resource Unavailable	Thursday May 06th 2004 11:49:41 AM	znc1y0jc	Major	Array: '/dev/md0' (/boot) Status: A physical disk has been removed from the array.
Equipment	Communications Subsystem Failure	Thursday May 06th 2004 11:49:39 AM		Major	Unable to communicate with BMC to get results. cc=

Logs

The Session Server Manager has the capability for applications or the system itself to generate logs. These logs can be viewed on the Session Server Manager's log web page. Information shown about a particular log includes:

- Timestamp
- Session Server device name
- Process that generates the log
- Log ID and number
- Alarm severity
- Log type
- Log label
- Additional information

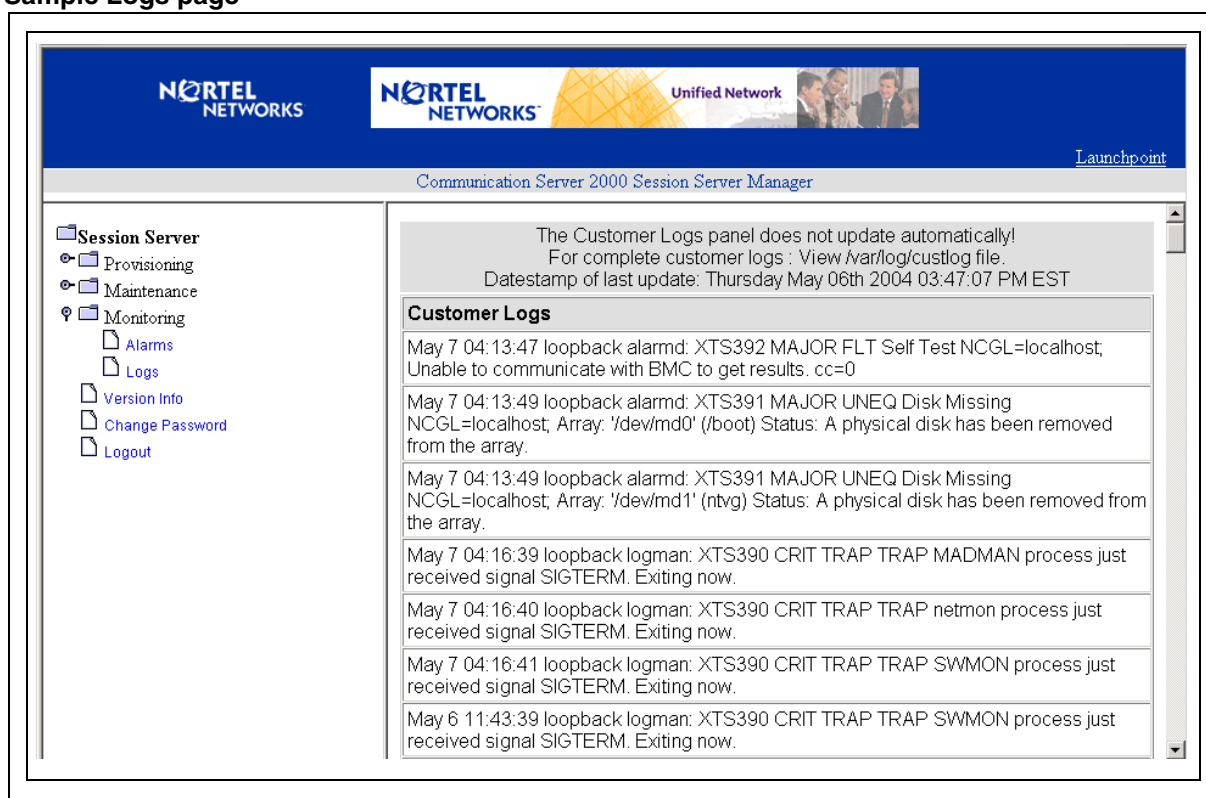
The user may view logs by going to the logs web page located in the Monitoring menu folder.

Note 1: The body of log formats shown in this document are the formats for Session Server logs if viewed from the IEMS (Integrated Element Manager System). Log formats may differ if logs are viewed from the Session Server Web Interface. However the content of the logs will not differ, only the formatting.

Note 2: When viewing logs from an IEMS, log headers may differ slightly from what is shown in this document.

Once the craftsperson click on Logs, the log web page is presented in the right frame with the current log list. A sample log web page is shown below.

Sample Logs page



Operational Measurements

Like other Call Server platforms, the Session Server Manager records operational measurements (OMs) for various performance related data items. The OM subsystem is similar to the OM subsystem but is different in some aspects. The majority of OMs pegged in SN07 are directly related to the SIP Gateway application. Also, OMs that are pegged can be viewed via a command line user interface (CLUI) after using secure shell (SSH) to login to the Session Server Manager.

After logging in to the Session Server via SSH to an account such as “mtc”, the user may issue commands such as the help command:

```
[mtc@sserv-unit0 mtc]$ omshow help

Please select from the following options.

omshow help
omshow all active
omshow all holding
omshow all lastfive
omshow <omgroup> active
omshow <omgroup> holding
omshow <omgroup> lastfive
omshow all zero
omshow <omgroup> zero
omshow holdingperiod 30
omshow holdingperiod 15
```

A brief description of the above commands are as follows:

omshow help - Print out the commands as shown above.

omshow all active - Print out all the OM groups and their associated active registers.

omshow all holding - Print out all the OM groups and their associated holding registers.

omshow all lastfive - Print out all the OM groups and their register values for the past five minutes.

omshow <omgroup> active - Print out the active registers for a particular OM group.

omshow <omgroup> holding - Print out the holding registers for a particular OM group.

omshow all zero - Zero the active registers for all OM groups.

omshow <omgroup> zero - Zero the registers for a particular OM group.

omshow holdingperiod 30 - Set the holding period to 30 minutes.

omshow holdingperiod 15 - Set the holding period to 15 minutes.

Operational Measurements are kept in two primary formats for a particular holding period. For example lets assume the holding period time is 30 minutes and the current time is 4:50 PM. The active registers represent 4:30-4:50 PM and the holding registers represent 4:00-4:30 PM. Finally at 5:00PM the active registers are copied to the holding registers. The possible holding periods for the Session Server are 15 and 30 minutes. The default holding period time is 15 minutes.

In addition to the above, the values of OM groups and registers can be output for the current five minute interval. For example, if the current time is 4:04:39 PM, the register values for the last 4 minutes and 39 seconds can be output via the “lastfive” selection.

Note OM values pegged in an application such as the SIP Gateway application may not reach the OM subsystem for a full minute. This can impact what is displayed when the omshow command is used since omshow pulls values from the OM subsystem.

Finally OM group register data pegged on one unit of a Session Server is completely independent of register data on its mate unit. Register data is not transferred from one unit to another.

Operational Measurements

This section contains a list of three OM groups and registers that are supported in SN07 on the Session Server. OMs on the Session Server are not in any related to operational measurements on the Core. Also, OMs generated on the Session Server are not sent to the CS2K Core.

OM Group: SIPGW_CALLP

Register Name	Description
IC_CALL_ATTEMPTS	Total number of incoming call attempts
OG_CALL_ATTEMPTS	Total number of outgoing call attempts
CALLS_ANSWERED	Total number of calls answered
CALLS_ABANDONED	Total number of calls abandoned
CALLS_REJECTED	Total number of calls rejected
CALLS_REDIRECTED	Total number of calls redirected

OM Group: SIPGW_SERVICES

Register Name	Description
REFER_ATTEMPTS	Total number of refer attempts ^a
REFER_SUCCESS	Total number of successful refers
IC_DTMF_SUBSCRIBES	Total number of incoming DTMF subscribes
OG_DTMF_SUBSCRIBES	Total number of outgoing DTMF subscribes
IC_DTMF_NOTIFYS	Total number of incoming DTMF notifies
OG_DTMF_NOTIFYS	Total number of outgoing DTMF notifies
IC_FAX_SUBSCRIBES	Total number of incoming fax subscribes
OG_FAX_SUBSCRIBES	Total number of outgoing fax subscribes
IC_FAX_NOTIFYS	Total number of incoming fax notifies
OG_FAX_NOTIFYS	Total number of outgoing fax notifies

a. Registers IC_FAX_SUBSCRIBES, OG_FAX_SUBSCRIBES, IC_FAX_NOTIFYS, and OG_FAX_NOTIFYS exist but are not supported in the SN07 release.

OM Group: SIPGW_MISC

Register Name	Description ^a
TCP_CALLS	Total number of TCP Calls
UDP_CALLS	Total number of UDP calls
SIP_MSG_SEND_FAILURES	Total number of SIP Msg Send Failures
INCOMING_SDP_INCOMPATIBLE	Total number of incompatible SDPs received from remote SIP servers
OUTGOING_SDP_INCOMPATIBLE	Total number of incompatible SDPs received from local gateways.

a. Register SIP_MSG_SEND_FAILURES exists but is not supported in the SN07 release.

CSV files

While the OMSHOW function provides near term information, it does not save performance info after a set period in time. In certain scenarios this historical information may prove to be valuable. Therefore OM information is also saved to comma separated value (CSV) files. Two sets of comma separated files are created.

Short Term

These six comma separated value files represents the last 30 minutes worth of information. Each file consists of a particular five minute interval within the thirty minute timeframe.

Long Term

The long term history represents the last 24 hours worth of information. If the OM collection interval is 15 minutes, then a total of 96 files are kept representing the last 24 hours. However if the collection interval is 30 minutes, 48 files are kept.

Please refer to [“Appendix D: CSV file information” on page 1500](#) for detailed information on the CSV file locations and the file format.

Software Optionality Control (SOC)

There are two new core usage SOC options that are used to limit the maximum number of simultaneous calls allowed through the Session Server Manager at any given time. Without one or both of the new SOC options, no call processing can take place using the Session Server Manager. Before discussing the new SOC options, it is important to understand the relationship between the new SOC options and the existing DPT SOC option in the core.

Existing DPT SOC option CS2B0005

Calls using the SIPT Gateway application on the Session Server Manager are considered to be DPT (Dynamic Packet Trunking) calls and are therefore limited by the base DPT SOC, CS2B0005. Before Session Server Manager calls can be made, the base DPT SOC must be purchased. This existing DPT SOC option is a usage based SOC and it specifies the maximum number of DPT ports that can be used simultaneously for processing all DPT calls.

Although DPT SOC option CS2B0005 specifies the maximum possible number of DPT ports that can be used in the office, the actual maximum for the office is governed by the office parameter DPT_MAX_PORTS in table OFCVAR. The DPT_MAX_PORTS parm can be set to any value equal to or less than the CS2B0005 SOC option and it allows fine tuning of DPT traffic limits within the bounds of the DPT SOC limit without having to obtain a new SOC limit each time.

Since dynamic packet trunking does not have fixed trunk members, it is possible that a single trunk group in the office can use all the available DPT port capacity. To prevent starvation of DPT ports for calls on other trunk groups, the maximum number of simultaneous DPT calls allowed on a particular trunk group can be limited. This adjustment is made on a trunk group basis using the MAXCALLS field in table DPTRKMEM.

Two New Session Server SOC's (CS2B0008 and CS2B0009)

The two new core usage based SOC options for the SIPT Gateway application are CS2B0008 "Call Server to Call Server SOC" and CS2B0009 "Call Server to Application Server SOC". The combined total limits of these two SOC's should not exceed the limit of the base DPT SOC option, CS2B0005. The maximum number of simultaneous DPT calls allowed for the office is still governed by the DPT_MAX_PORTS parameter in table OFCVAR, although the maximum number of simultaneous Session Server Manager calls can be further restricted by these new SOC options.

Each Session Server Manager call is designated as either a "Call Server to Call Server" call or a "Call Server to Application Server" call. This designation is made in field CONNTYPE of table SIPLINK in the core. In table SIPLINK, each SIP access communication link is marked according to whether that link is used to communicate to another call server or to an application server. If the link is used to connect to another CS 2000 or an MCS, then field CONNTYPE should be set to CS2CS, denoting a call server to call server connection. If the link is used to connect to some other type of SIP server, then field CONNTYPE should be set to CS2AS, denoting a call server to application server connection.

Current simultaneous usage for each Session Server Manager call type is tracked in the core and calls will be rejected if they cause the corresponding Session Server Manager SOC limit to be exceeded.

Hardware Requirements or Dependencies

The Session Server Manager is an integrated platform consisting of hardware and software. Please refer to section for the hardware configuration. There are no additional hardware requirements or dependencies

Software Requirements or Dependencies

Software requirements include the following:

- Nortel Carrier Grade Linux. Provided by Activity A00004005.
- Session Server Manager NGSS07
- SN07 GWC, CM
- CS2M

In order to maintain the Session Server Manager a web client is needed. The requirement for a web client is as follows:

Supported web clients on a PC:

- Windows 2000, XP, or 2003 based operating system.
- Supported web browsers on those operating systems include:
 - Internet Explorer 6.0 SP1 and above
 - Netscape 6.2.x, and Netscape 7.1 and above

Supported web clients on a Sparc:

- Solaris 8 or 9
- Supported web browsers on those operating systems include:
 - Netscape 6.2.x, and Netscape 7.1 and above

The following browser are NOT supported:

- Any browser running on Linux
- Any browser running an OS under VMware
- Any browser running under Solaris on a PC
- Any browser running on MacIntosh hardware
- Mozilla

Limitations and restrictions

The following limitations and restrictions exist for the Session Server Manager platform and the SIP Gateway application.

1. See [“Software Requirements or Dependencies” on page 1485](#) for a comprehensive list of operating systems and web browsers that are supported.
2. Javascript must be enabled in the web browser used.
3. Popup blocking should **not** be enabled within the web browser. Verify that popup blocking is not enabled prior to using the web browser to access the Session Server Manager.

4. When adding or deleting mapping tables via the web client, the craftsperson should allow the add operation to complete before performing other web actions. Aborting a web action via a “Stop” or “Back” can cause incomplete data to be added to the database.

Invalid mapping tables can always be deleted by the craftsperson via the “Delete Mapping” command in the respective mapping sub-folder.

5. When a new mapping is added to any of the mapping table folders, the folder menu at the left side of the web-browser does not automatically refresh. The user should close/open the folder to see the newly added mapping.
6. For Call scenarios, where an ISUP payload is to be generated, mandatory parameters are mapped from appropriate SIP Headers. As a result, some of the services depending on the trunk-type (IBNT2, IT, EANT) may not be available, if appropriate mapping is not defined.
7. For the List Mappings sub-folder in the “ISUP to SIP Map”, “SIP to ISUP Map”, “ISUP Variant Map”, and “SIP Redirection” mappings:

If the List Mappings sub-folder is open when a mapping table is added or deleted, the mapping names under the particular List Mappings sub-folder won't change *visually* until that sub-folder is closed and re-opened. The mapping tables will have been added or deleted per the user action. The user is **not** required to open or close the List Mappings sub-folder for the add or delete action to take effect.

8. If the optional trunk telephony profile header is not used in the SIP messages between the Session Server Manager and destination SIP servers, then only a single trunk group can be used to carry the traffic between the Session Server Manager and a single destination SIP server. If multiple trunk groups are required between the Session Server Manager and a single destination SIP server, trunk telephony profile headers are required in the SIP messages to identify which trunk to use for a particular incoming call to the Session Server Manager.
9. Multiple independent and redundant pairs of Session Servers are not supported.
10. No backup and restore functionality is available for the Session Server Manager node in SN07.
11. All currently active SIP Gateway calls will be taken down during a SIP Gateway cold SWACT.
12. The Session Server Manager Web interface utilizes and requires the use of HyperText Transport Protocol Secure (HTTPS).
13. Before HTTPS can be used on the Session Server Manager, a Secure Sockets Layer (SSL) certificate must be obtained and installed.

14. OM values pegged in an application such as the SIP Gateway application may not reach the OM subsystem for a full minute. This impact what is displayed when the omshow command is used since omshow pulls values from the OM subsystem.
15. OM group register data pegged on one unit of a Session Server is independent of register data on its mate unit. Register data is not transferred from one unit to another.
16. WARNING: To ensure data integrity, the command line interface should not be used to enter or change data in the database. Only the web interface should be used to enter or change the provisioned data.
17. Improper reboot or shutdown of the Session Server can result in data loss. Proper procedures should be followed when rebooting or shutting down a Session Server unit.
18. The Session Server 2000 GUI does not support being accessed over a NAT'd connection in SN07. Only direct (same-LAN) and SSPFS web proxied connections are supported.
19. The physical limit for table SIPLINK is 2048 tuples; however, due to the DDM limitation for table DPTRKMEM, table SIPLINK should not be datafilled to more than 400 tuples.
20. If the Session Server goes out of service due to a system failure or because of improper shutdown (thereby disrupting the ability to communicate the link status change to the gateway controllers), all in-service SIPT trunks associated with any access links on the Session Server will remain in-service.

Interactions

N/A.

Applicable customer facing sections

Fault Management

Logs ___X___

Alarms ___X___

Configuration

Data Schema ___X___

User Interface _____

Element Management _____

Security _____

Service Order ___X___

Office Parameters	_____
Accounting (includes AMA billing)	_____
Performance (includes operational measurements)_	_____

Glossary

CI	Command Interpreter
CLUI	Command Line User Interface
CM	Computing Module (aka “Core”)
CS2M	Call Server 2000 Manager
CS 2000	Call Server 2000
CS 2000 OAMP	Call Server 2000 OAMP (aka CS2M aka PTM)
DMS	Digital Multiplex Switch
DNS	Domain Name Server
DPT	Dynamic Packet Trunking
GA	General Availability
GWC	Gateway Controller
HIOP	High performance Input Output Processor
HTML	HyperText Markup Language
HTTP	HyperText Transport Protocol
HTTPS	HyperText Transport Protocol Secure
IEMS	Integrated Element Management System
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISUP	Integrated Services Digital Network User Par
JRE	Java Runtime Environment
MAPCI	Maintenance, Administration, and Provisioning Command Interpreter
MCS	Multi-Media Communication Server
MGC	Media Gateway Controller
NCGL	Nortel Carrier Grade Linux
NTP	Network Time Protocol
OAM&P	Operation, Administration, Maintenance, and Provisioning
OSS	Operations Support System
OSSGate	OSS Gateway
PAM	Pluggable Authentication Module
PI	Progress Indicator
PRI	Primary Rate Interface
PTM	Packet Telephony Manager
PVG	Packet Voice Gateway
RFC	Request For Comments
RPI	Remote Party Id
RTCP	Real-Time Control Protocol

RTP	Real-Time Protocol
RTS	Return To Service
SAM	SIP Application Maintenance
SCP	Secure Copy
SCS	Succession Communication Server/Call Server
SCTP	Stream Control Transmission Protocol
SG	SIP Gateway application
SDM	Supernode Data Manager
SDP	Session Description Protocol
SESM	Succession Element and Sub Element Manager (aka CS 2000 OAMP, aka PTM) Former name of CS2M.
SIP	Session Initiation Protocol
SIPT	Session Initiation Protocol (SPI) for Telephones
SME	Subject Matter Expert
SNMP	Simple Network Management Protocol
SNM	Session Server Node Maintenance
Session Server	Platform for the SIP Gateway application
SPM	Spectrum Peripheral Module
SQL	Standard Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
STORM	STORage Management
SWACT	Switch of Activity
TCP	Transmission Control Protocol
TPM	Telephony Profile Message
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VToIP	Voice Trunking over IP
VRDN	Virtual Router Distribution Node

References

- 1 RFC 3261: Session Initiation Protocol
- 2 RFC 2327: Session Description Protocol
- 3 RFC 3262: Reliability of Provisional Responses in the Session Initiation Protocol

- 4 RFC 3264: An Offer/Answer Model with the Session Description Protocol
- 5 RFC 3265: SIP Event Notification
- 6 RFC 3311: The SIP Update Method
- 7 RFC 3515: SIP Refer Method
- 8 A00003270: SIP Open Interop Call Processing
- 9 A00003271: Session Server Web Server Interface
- 10 A00003272: SIP on Session Server Provisioning Framework
- 11 A00003273: SIP on SIP Gateway Application Maintenance
- 12 A00003277: SIP on Session Server OM Subsystem
- 13 A00003278: SIP on Session Server OSS Interface
- 14 A00003279: SIP on Session Server Link Maintenance and Load Balancing
- 15 A00003280: SIP on Session Server Tracing/Debug Framework
- 16 A00003281: SIP on Session Server Call Audits
- 17 A00003282: SIP on Session Server Datasync
- 18 A00004005: NCGL support for SAM-XTS and SP2000

Appendix A: Miscellaneous Items

This section contains miscellaneous topics for this FN.

ISUP Variant to SIP Version Mapping information

This sub-section lists the legal permutations and combinations for tuples that may be added to an ISUP Variant to SIP Version mapping.

ISUP Variant to SIP Version mappings

ISUP Protocol	ISUP Version	ISUP Variant	SIP Base	SIP Version
Q764			ANSI88	<user defined string>
UCS			ANSI88	<user defined string>
UCP			ANSI88	<user defined string>
CCITT	100_BLUE	V1	ITU-T88	<user defined string>
	100_WHITE	V2	ITU-T92-PLUS	<user defined string>
CCITT250				<user defined string>

ISUP Variant to SIP Version mappings

ISUP Protocol	ISUP Version	ISUP Variant	SIP Base	SIP Version
Q767	100_BLUE	BASE	ETSI121	<user defined string>
		SPANISH		<user defined string>
		ITALY		<user defined string>
		FRANCE		<user defined string>
		NORWAY		<user defined string>
		NEW_ZEALAND		<user defined string>
		DENMARK		<user defined string>
		PORTUGAL		<user defined string>
		MEXICO		<user defined string>
		TURKEY		<user defined string>
		BRAZIL		<user defined string>
		CZECH		<user defined string>
		BANGLADESH		<user defined string>

ISUP Variant to SIP Version mappings

ISUP Protocol	ISUP Version	ISUP Variant	SIP Base	SIP Version
Q767	100_WHITE	BASE	ETSI356	<user defined string>
		PNG		<user defined string>
		CHILE		<user defined string>
		COSTA_RICA		<user defined string>
		GERMANY		<user defined string>
		TURKEY		<user defined string>
		SAUDI		<user defined string>
		ETHIOPIA		<user defined string>
		GEORGIA		<user defined string>
		MYANAMAR		<user defined string>
		VIETNAM		<user defined string>
		ISDEFO		<user defined string>
		ACIF_AUSTRALIA		<user defined string>
		BELGIUM		<user defined string>
		SWEDEN		<user defined string>
		JPN_INTERCONN		<user defined string>
		EGYPT		<user defined string>
		AUSTRIA		<user defined string>
		POLAND		<user defined string>
		HUNGARY		<user defined string>
		PERU		<user defined string>
		CA30_AUSTRALIA		<user defined string>
		HONG_KONG		<user defined string>
		TAIWAN		<user defined string>
		SPAIN		<user defined string>
		CHINA		<user defined string>
		SINGAPORE		<user defined string>
		ARGENTINA		<user defined string>
		BANGLADESH		<user defined string>
		RUSSIA		<user defined string>
		GISUP		<user defined string>
		TISUP		<user defined string>
		ITALY		<user defined string>

ISUP Variant to SIP Version mappings

ISUP Protocol	ISUP Version	ISUP Variant	SIP Base	SIP Version
Q767	100_EIV3	FRANCE	ETSI356	<user defined string>
		SPIROU		<user defined string>
		UK		<user defined string>
AISUP	AUST			<user defined string>
	INTRCONN			<user defined string>
	PTUP			<user defined string>
	MISUP			<user defined string>
JPNISUP			TTC93-PLUS	<user defined string>
NCCI	V1			<user defined string>
	V2			<user defined string>

Note blank areas indicate “Not Applicable” values. When adding tuples via the web form that have no applicable values for the respective columns, select “Not Applicable” to represent the blank areas listed in the table.

Appendix B: SIP on NGSS Tracing/Debug Framework

SIP on NGSS Debug and Tracing (Feature A00003280) is a stand alone tool. It controls the Radvision SIPT Toolkit log module and filters the internal NGSS traces which are written into the tracing files.

This section is primarily targeted to Customer Support groups like GNPS. While the tool will be available in the field, it should not be done on a regular basis or at high traffic levels due to the impact of running the tracing session on the capacity of the field office.

This tool can run in two modes:

1. Simple Mode - straightforward usage tracing SIP messages
2. Prompt Mode - more sophisticated usage, needs a deeper knowledge regarding what to trace and how to used this tool.

Simple Mode

The following is an overview of a typical Simple Mode tracing session.

1. user needs a telnet session to the NGSS
2. start a Simple Mode by a command `/opt/apps/bin/sp2ktrace start`
3. stop a Simple Mode by a command `/opt/apps/bin/sp2ktrace stop`

4. tracing file is located in NGSS directory **/opt/apps/logs** with the name as **siptrace.YYYYMMDD.MSG.001** (example **siptrace.20040318.MSG.00001**)
5. the siptrace file contains the SIP messages provided by Radvision Transport layer:

```
T 88b63c8 03/19/2004 14:09:13 INFO - TRANSPORT -
T 88b63c8 03/19/2004 14:09:13 DEBUG - TRANSPORT - TransportCallbackMsgToSendEv:
Application did not register to call back, default bSendMsg = 1
T 88b63c8 03/19/2004 14:09:13 INFO - TRANSPORT - SipTransportUdpSendMessage -
Sending message. local-address=192.168.192.64:5060. remote-address=1.2.3.4:5060
T 88b63c8 03/19/2004 14:09:13 INFO - TRANSPORT - SipTransportSendMessage -
About to send message with size = 335
T 88b63c8 03/19/2004 14:09:13 INFO - TRANSPORT - --> OPTIONS sip:1.2.3.4 SIP/2.0
T 88b63c8 03/19/2004 14:09:13 INFO - TRANSPORT - From:
<sip:MGCA>;tag=40c0a8c0-13c4-405afefd-49811d5-18457876
T 88b63c8 03/19/2004 14:09:13 INFO - TRANSPORT - To: <sip:CCAONE@1.2.3.4>
T 88b63c8 03/19/2004 14:09:13 INFO - TRANSPORT - Call-ID: 8909008-40c0a8c0-
13c4-405afefd-49811d5-16ba7f11@MGCA
T 88b63c8 03/19/2004 14:09:13 INFO - TRANSPORT - CSeq: 30 OPTIONS
T 88b63c8 03/19/2004 14:09:13 INFO - TRANSPORT - Via: SIP/2.0/UDP
192.168.192.64:5060;branch=z9hG4bK-405afefd-49811d5-218c6e77
T 88b63c8 03/19/2004 14:09:13 INFO - TRANSPORT - Max-Forwards: 70
T 88b63c8 03/19/2004 14:09:13 INFO - TRANSPORT - Supported: 100rel
T 88b63c8 03/19/2004 14:09:13 INFO - TRANSPORT - Content-Length: 0
T 88b63c8 03/19/2004 14:09:13 INFO - TRANSPORT -
T 88b63c8 03/19/2004 14:09:13 DEBUG - TRANSPORT - TransportCallbackMsgToSendEv:
Application did not register to call back, default bSendMsg = 1
T 88b63c8 03/19/2004 14:09:13 INFO - TRANSPORT - SipTransportUdpSendMessage -
Sending message. local-address=192.168.192.64:5060. remote-
address=192.168.192.59:5060
```

6. for continuous tracings you can type command on NGSS:

```
> tail -f /opt/apps/logs/siptrace.20040318.MSG.00001
```

to get traces onto the screen.

Prompt Mode

The following is an overview of a Prompt Mode tracing session.

1. user needs a telnet session to the NGSS
2. enter a Prompt Mode (command line interface) by a command **/opt/apps/bin/sp2ktrace** as example:

```
root@unit0 root]# /opt/apps/bin/sp2ktrace
```

3. type **help** to see which commands are available

```
SIPTRACE> help
These commands are provided:
  Help
  set (layer<1-19> filter<0-63>)
  status
  start
  stop
  Users
  display <all | Session Server Name> - for IP address status
  Quit
-----
Additional info for SET command:
Layers and their corresponding numbers are shown by
```

STATUS command.
 1 - all layers (ex. SET 1 2 sets all layers filter=INFO=2).
 There are 6 Filters as:
 DEBUG=1 INFO=2 WARN=4 ERROR=8 EXCEP=16 LOCKDBG=32.
 Filters can be logically combined - if you want to trace for ex.
 layer PARSE (7) with filters ERROR (8) and EXCEP (16)
 SET 7 24
 For cleanup use filter 0 (example SET 7 0 for above).
 Use SET 1 63 (to set tracing for everything)
 use SET 1 0 (to cleanup everything).
 Please be aware SET command only sets tracing.
 You must use START command to start tracing
 and use STOP command to end it.
 Tracing files are in the directory /opt/apps/logs/.

SIPTRACE>

4. type status command to see all available Layers and Filters:

SIPTRACE> status

```
Active Users: 1      Radvision      L o g F i l t e r s
[pid:15734] active=OFF
RV Layers          DEBUG=1 INFO=2  WARN=4  ERROR=8 EXCEP=16 LOCKDBG=32
=====
1      all          -      -      -      -      -      -
2      core         -      -      -      -      -      -
3      msg          -      -      -      -      -      -
4      transport   -      -      -      -      -      -
=====
5      transaction -      -      -      -      -      -
6      call        -      -      -      -      -      -
7      parser      -      -      -      -      -      -
8      stack       -      -      -      -      -      -
=====
9      msgBuilder  -      -      -      -      -      -
10     authenticator -      -      -      -      -      -
11     regClient   -      -      -      -      -      -
12     subscription -      -      -      -      -      -
+++++ S P 2 K      L o g F i l t e r s
13     callpAppMTC -      -      -      -      -      -
14     GCP          -      -      -      -      -      -
15     other        -      -      -      -      -      -
16     sipmsg       -      -      -      -      -      -
17     gcpmsg       -      -      -      -      -      -
18     gcpmtcmmsg  -      -      -      -      -      -
19     linkmtc      -      -      -      -      -      -
=====
SIPTRACE>
```

5. type set command to set Layers/Filters selection (in this example you chose to trace a **transport** layer (4) for **filters** DEBUG (1), INFO (2) and ERROR (8) and the another layer msgBuilder (9) for ERROR (8) only. Thus type two command: **set 4 11** (4-transport, 11= 1+2+8) and **set 9 8**

```
Active Users: 2      Radvision      L o g F i l t e r s
[pid:22958] active=OFF
RV Layers          DEBUG=1 INFO=2  WARN=4  ERROR=8 EXCEP=16 LOCKDBG=32
=====
1      all          -      -      -      -      -      -
2      core         -      -      -      -      -      -
3      msg          -      -      -      -      -      -
4      transport   x      x      -      x      -      -
=====
5      transaction -      -      -      -      -      -
6      call        -      -      -      -      -      -
7      parser      -      -      -      -      -      -
8      stack       -      -      -      -      -      -
=====
9      msgBuilder  -      -      -      x      -      -
10     authenticator -      -      -      -      -      -
11     regClient   -      -      -      -      -      -
=====
SIPTRACE>
```



```

12      subscription      -      -      -      -      -      -
+++++++ S P 2 K          L o g F i l t e r s
13      callpAppMTC      -      -      -      -      -      -
14      GCP              -      -      -      -      -      -
15      other            -      -      -      -      -      -
16      sipmsg           -      -      -      -      -      -
17      gcpmsg           -      -      -      -      -      -
18      gcpmtcmsg        -      -      -      -      -      -
19      linkmtc          -      -      -      -      -      -
=====
SIPTRACE>

```

Note: Please note “x” at the transport and msgBuilder Layer.

6. start the tracing by a **start** command

```

SIPTRACE> users

                                R a d v i s i o n S P 2 K
                                1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
Layers:
16      17      18      19      al co ms tp tr ca pa st mB au rC su MTC GCP
oth SIPMSG GCPMSG GCPMTMSG LINKMTM
User      pid      active
-----
server    15704    1      0 0 0 31 0 0 0 0 0 0 0 0 0 0 0
0          0          0
mtc        16802    0      0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0          0          0
MSG        00001    1      0 0 0 31 0 0 0 0 0 0 0 0 0 0 0
0          0          0

SIPTRACE>
SIPTRACE> stop

```

In the example above you can see three users. A server is a permanent thread with a pid (processID=15704), your session with a userID mtc and pid 16802 and one Simple Mode with userID MSG and hardcoded pid 00001. The “00001”s behind a pid column belong to the active column indicating that this session is active - it means it is collects data.

7. the siptrace file for the above tracing session (pid 22958) is located in NGSS directory /oip/apps/logs/siptrace.20040319.mtc.22958 with few first lines as:

```

=== SESSION ENTERED: [pid:22958/mtc] Fri Mar 19 14:17:19 2004
=== MONITOR UPDATED: [pid:22958/mtc] Fri Mar 19 14:38:53 2004
Filters: 0 0 0 11 0 0 0 0 0 0 0 0 0 0 0 0
=== MONITOR UPDATED: [pid:22958/mtc] Fri Mar 19 14:38:59 2004
Filters: 0 0 0 11 0 0 0 0 8 0 0 0 0 0 0 0
=== MONITOR STARTED: [pid:22958/mtc] Fri Mar 19 14:42:27 2004
T 88b63c8 03/19/2004 14:42:28 DEBUG - TRANSPORT -
TransportMultiThreadTimerEventHandler - Allocating timer expired event for timer
0x88d4fe4
T 88b63c8 03/19/2004 14:42:28 DEBUG - TRANSPORT -
TransportProcessingQueueTailEvent - TIMER_EXPIRED_EVENT 0x8906a20
T 88b63c8 03/19/2004 14:42:28 DEBUG - TRANSPORT -
TransportProcessingQueueDispatchEvents - TIMER_EXPIRED_EVENT 0x8906a20
T 88b63c8 03/19/2004 14:42:28 INFO - TRANSPORT - SipTransportUdpSendMessage -
Sending message. local-address=192.168.192.64:5060. remote-address=1.2.3.4:5060
T 88b63c8 03/19/2004 14:42:28 INFO - TRANSPORT - SipTransportSendMessage -
About to send message with size = 335
T 88b63c8 03/19/2004 14:42:28 INFO - TRANSPORT - --> OPTIONS sip:1.2.3.4 SIP/2.0
T 88b63c8 03/19/2004 14:42:28 INFO - TRANSPORT - From:
<sip:MGCA>;tag=40c0a8c0-13c4-405b06b8-4b643e6-4fdb17be
T 88b63c8 03/19/2004 14:42:28 INFO - TRANSPORT - To: <sip:CCAONE@1.2.3.4>
T 88b63c8 03/19/2004 14:42:28 INFO - TRANSPORT - Call-ID: 890bb28-40c0a8c0-
13c4-405b06b8-4b643e6-69016e79@MGCA
T 88b63c8 03/19/2004 14:42:28 INFO - TRANSPORT - CSeq: 30 OPTIONS

```

```
T 88b63c8 03/19/2004 14:42:28 INFO - TRANSPORT - Via: SIP/2.0/UDP
192.168.192.64:5060;branch=z9hG4bK-405b06b8-4b643e6-5c79301f
T 88b63c8 03/19/2004 14:42:28 INFO - TRANSPORT - Max-Forwards: 70
T 88b63c8 03/19/2004 14:42:28 INFO - TRANSPORT - Supported: 100rel
T 88b63c8 03/19/2004 14:42:28 INFO - TRANSPORT - Content-Length: 0
T 88b63c8 03/19/2004 14:42:28 INFO - TRANSPORT -
```

8. stop the session by the **stop** command.

9. exit session by a **quit** command.

Hardware Requirements or Dependencies

Customer offices without the Session Server Manager will not have the functionality delivered by this feature.

Software Requirements or Dependencies

The Session Server Manager feature must be available. Also, certain other features developed for the Session Server Manager will be required (Call Processing support, etc.) as well.

Limitations and restrictions

This tool has the following limitations:

1. Tool is currently configured for 10 concurrent Trace Clients. The Simple Mode is counted as a Client.
2. The user of this tool needs access (a telnet session) to the NGSS machine.
3. Only one Client can run in the Simple Mode at a time.
4. Every Trace Client gets its own output trace file which is being used until the Trace Client session ends (by **quit** command in the Prompt Mode or **sp2ktrace stop** in the Simple Mode). For example, if a user starts a session on Monday and runs it over 3 days, there will be only one Trace Client file with a creation date i.e. Monday date.
5. The Trace Server trace file. In contrast of the Trace Client trace file, the Trace Server trace file is created on every day. (to give a chance to get rid of old/yesterday's files). The trace file creation is not done few seconds after midnight but by the first execution (after midnight) of the print routine (which can be few hours from the midnight) depending on monitoring activities/setup.
6. If the size of any output file (siptrace) created by this tool (in the directory /opt/apps/logs) exceeds limit of 10 MBytes then this file will be overwritten from the beginning. This event is recorded together with the overwritten counter.
7. All siptrace* files in the directory /opt/apps/logs/ older than 3 days will be deleted automatically by the tracing tool.

8. Other files in the directory /opt/apps/logs need to be deleted manually.
Note: The file created by monitoring in the Simple Mode is appended every time tracing starts (by a command *siptrace start*) on the same date.
9. **WARNING:** Do not delete active/current (today) server files. Prevent the deletion of active Trace Client's files. Deleted files will not be re-created.
10. This tool provides tracing for multiple threads, which may attempt to write to the same tracing file concurrently. Non-waiting semaphores are used to prevent concurrent access into the client file. This may result in a "lost" trace record rather than to block a thread waiting on the semaphore.
11. **Configuration:** The configuration file sp2ktraceConfig is created when tool runs for very first time in the directory /opt/apps/logs. This file has currently two (default) parameters:
 - NUMBEROFINITLOGS 300
 - CLIENTFILESIZEMB 10

The first parameter configures the number of logs to be printed into the server siptrace file during the initialization (when SIP Gateway is Unsuspended). The default value is 300 logs but can be increased up to the maximum of 25000.

The second parameter allows to increase the size of the client siptrace file from the default value 10 Mbytes up to the maximum of 500 Mbytes.

These parameter must be changed prior the SIP Gateway is Unsuspended to be used.

References

- A00003698 - SIP Msg trace

Appendix C: Database Backup and Recovery

This section explains how database backups are made and how to recover the database from a backup copy.

Database Backup

Database backups are made to secure the information stored in the database. If there is a system or database failure the database can be restored from the backup files. The Solid database is automatically backed up daily based on a timed command. The automatic backup is performed at 1:00 AM each day.

There is only one backup copy of the database. It contains the last or most recently backed up copy of the database. If additional security measures are desired the customer may periodically retrieve the files saved in the backup

directory and store them on another machine. A customer could maintain a history of database changes in this manner.

Restoring database from a backup copy

The following procedure is used to restore the database from the backup copy. The database is restored to its state when the backup was made. In general this procedure should only be followed when database corruption has occurred on both units of the NGSS. The database must be restored on the active unit of the NGSS.

1. Jam the Active Unit.
2. Suspend Call Processing
3. Login in to the active unit as mtc and su to root.

```
ssh -l mtc <ipaddress>
```

```
su root
```

4. Run the restorebackup script as shown from the following directory:

```
cd /opt/apps/database/solid_install/
```

```
./restorebackup.sh
```

5. Unsuspend Call Processing
6. UnJam the Active Unit

Jamming the active unit is necessary to prevent the database from switching activity while its being restored. The database must be restored on the active unit. Call processing should be suspended since the database will not be available.

Appendix D: CSV file information

This section details the CSV file formats, its location, and shows examples.

CSV File Location

SSH Login Access

If the user desires to login to a session server unit via an account such as MTC and look at the CSV files, the main directory path is /opt/apps/ngsspm. Two subdirectories are located here:

stdhist - This directory contains the 24 hour long term values.

trafhist - This directory contains the 30 minute short term values.

FTP Access

This future section will contain the access information when FTP is utilized using the NGSSPM account to pull CSV files from a session server unit.

CSV File Format

The CSV File Format is shown below:

```
PMFile=Begin
MeasurementCategory,FileCreationTime,EarliestStartTime,LatestCaptureTime,RegisterTypeDefault,ValueTypeDefault
<string="pm">,<string>,<string>,<string>,<string="counter">,<string="integer">
System=Begin
SystemId
<string="SessionServer">
Entity=Begin
Entity
<string= Unit IPAddress>
SubEntity=Begin
SubEntity
<string=["Unit0" | "Unit1"]>
GroupVals=Begin
MeasurementKind,CaptureTime,GroupId,IntervalDuration,Reliability
<string="PeriodBased">,<string>,<string>,<integer>,<string="Valid">
Reg1Name,Reg1Value,Reg2Name,Reg2Value,Reg3Name,Reg3Value,Reg4Name,Reg4Value
<string>,<integer>,<string>,<integer>,<string>,<integer>,<string>,<integer>
Reg5Name,Reg5Value,Reg6Name,Reg6Value,Reg7Name,Reg7Value,Reg8Name,Reg8Value
<string>,<integer>,<string>,<integer>,<string>,<integer>,<string>,<integer>
Reg9Name,Reg9Value,Reg10Name,Reg10Value,Reg11Name,Reg11Value,Reg12Name,Reg12Value
<string>,<integer>,<string>,<integer>,<string>,<integer>,<string>,<integer>
Reg13Name,Reg13Value,Reg14Name,Reg14Value,Reg15Name,Reg15Value,Reg16Name,Reg16Value
<string>,<integer>,<string>,<integer>,<string>,<integer>,<string>,<integer>
Reg17Name,Reg17Value,Reg18Name,Reg18Value,Reg19Name,Reg19Value,Reg20Name,Reg20Value
<string>,<integer>,<string>,<integer>,<string>,<integer>,<string>,<integer>
Reg21Name,Reg21Value,Reg22Name,Reg22Value,Reg23Name,Reg23Value,Reg24Name,Reg24Value
<string>,<integer>,<string>,<integer>,<string>,<integer>,<string>,<integer>
Reg25Name,Reg25Value,Reg26Name,Reg26Value,Reg27Name,Reg27Value,Reg28Name,Reg28Value
<string>,<integer>,<string>,<integer>,<string>,<integer>,<string>,<integer>
Reg29Name,Reg29Value,Reg30Name,Reg30Value,Reg31Name,Reg31Value,Reg32Name,Reg32Value
<string>,<integer>,<string>,<integer>,<string>,<integer>,<string>,<integer>
GroupVals=End
GroupVals=Begin
MeasurementKind,CaptureTime,GroupId,IntervalDuration,Reliability
<string="PeriodBased">,<string>,<string>,<integer>,<string="Valid">
Reg1Name,Reg1Value,Reg2Name,Reg2Value,Reg3Name,Reg3Value,Reg4Name,Reg4Value
<string>,<integer>,<string>,<integer>,<string>,<integer>,<string>,<integer>
Reg5Name,Reg5Value,Reg6Name,Reg6Value
<string>,<integer>,<string>,<integer>
GroupVals=End
SubEntity=End
Entity=End
System=End
PMFile=End
```

Note the above example format consists of two groups. The first with 32 registers and the second with six registers.

Examples

An example CSV file is shown below:

```
# more NGSS.OMs.QoS.2004.5.5_10.15_EDT.csv
PMFile=Begin
MeasurementCategory,FileCreationTime,EarliestStartTime,LatestCaptureTime,RegisterTypeDefault,ValueTypeDefault
pm,NGSS.OMs.QoS.2004.5.5_10.15_EDT.csv,unknown,unknown,counter,integer
System=Begin
SystemId
SessionServer
Entity=Begin
Entity
47.142.123.46
SubEntity=Begin
SubEntity
Unit0
GroupVals=Begin
MeasurementKind,CaptureTime,GroupId,IntervalDuration,Reliability
PeriodBased,unknown,SIPGW_CALLP,15,Valid
Reg1Name,Reg1Value,Reg2Name,Reg2Value,Reg3Name,Reg3Value,Reg4Name,Reg4Value
IC_CALL_ATTEMPTS,0,OG_CALL_ATTEMPTS,0,CALLS_ABANDONED,0,CALLS_ANSWERED,0
Reg5Name,Reg5Value,Reg6Name,Reg6Value
CALLS_REJECTED,0,CALLS_REDIRECTED,0
GroupVals=End
GroupVals=Begin
MeasurementKind,CaptureTime,GroupId,IntervalDuration,Reliability
PeriodBased,unknown,SIPGW_SERVICES,15,Valid
Reg1Name,Reg1Value,Reg2Name,Reg2Value,Reg3Name,Reg3Value,Reg4Name,Reg4Value
REFER_ATTEMPTS,0,REFER_SUCCESS,0,IC_DTMF_SUBSCRIBES,0,OG_DTMF_SUBSCRIBES,0
Reg5Name,Reg5Value,Reg6Name,Reg6Value,Reg7Name,Reg7Value,Reg8Name,Reg8Value
IC_DTMF_NOTIFYS,0,OG_DTMF_NOTIFYS,0,IC_FAX_SUBSCRIBES,0,OG_FAX_SUBSCRIBES,0
Reg9Name,Reg9Value,Reg10Name,Reg10Value
IC_FAX_NOTIFYS,0,OG_FAX_NOTIFYS,0
GroupVals=End
GroupVals=Begin
MeasurementKind,CaptureTime,GroupId,IntervalDuration,Reliability
PeriodBased,unknown,SIPGW_MISC,15,Valid
Reg1Name,Reg1Value,Reg2Name,Reg2Value,Reg3Name,Reg3Value,Reg4Name,Reg4Value
TCP_CALLS,0,UDP_CALLS,0,SIP_MSG_SEND_FAILURES,0,SIMULTANEOUS_CALLS,0
Reg5Name,Reg5Value,Reg6Name,Reg6Value,Reg7Name,Reg7Value,Reg8Name,Reg8Value
UDP_CALLS_HIGHWATERMARK,0,TCP_CALLS_HIGHWATERMARK,0,SIMULTANEOUS_CALLS_HIGHWATERMARK,0,INCOMING_SDP_IN
COMPATIBLE,0
Reg9Name,Reg9Value
OUTGOING_SDP_INCOMPATIBLE,0
GroupVals=End
SubEntity=End
Entity=End
System=End
PMFile=End
```

Fault Management for A00003933

This section provides information on logs and alarms for the features under the SIP Gateway application umbrella. Separate sections are provided for the Call Processing, Application Maintenance, and Provisioning logs and alarms.

SIP Gateway application Call Processing Logs and Alarms

The following is a description of logs and alarms generated by the SIP Gateway application Call Processing. Note that these logs and alarms are only generated and reported on the SIP Gateway application.

They can be viewed via the SIP Gateway Maintenance web browser interface on the Session Server Manager - SIP Gateway application web page.

Note 1: The body of log formats shown in this document are the formats for Session Server logs if viewed from the IEMS (Integrated Element Manager System). Log formats may differ if logs are viewed from the Session Server

Web Interface. However the content of the logs will not differ, only the formatting.

Note 2: When viewing logs from an IEMS, log headers may differ slightly from what is shown in this document.

SIP Gateway application Call Processing Logs

The SIP Gateway application Call Processing software produces the following logs:

- SIPC310 - SIP CallP No Database Connection
- SIPC310 (related log) - SIP CallP Database Connection Established
- SIPC 650 - SIP CallP No Data Found
- SIPC301 - All SIP Incoming Msgs Blocked
- SIPC750 - Incoming SIP messages dropped
- SIPGW700 - SIP Call Processing Application Logs

SIPC310 SIP CallP No Database Connection Log

Log SIPC310 “SIP CallP No Database Connection” is associated with the generation of the Critical alarm due to a loss of connectivity between the database and the CallP application, a Critical alarm is generated.

Log Title: SIP CallP

Name: SIPC310

Description: No Database Connection

Event type: Trouble

Format

For the SIPC 310 log, the following are values/explanations of the variable values:

- alarmLevel = CRIT- Indicates it is a critical alarm
- componentID = SIPC
- category = Communications - Indicates communication failure between CallP and the database
- description = No Database Connection
- probableCause = outOfService
- specificProblem = Communication failure with Database
- correlationIdList = None
- neVendorSpecificInfo = None
- technologySpecificInfo = None
- reportName = SIPC
- reportNum = 310
- eventType = TBL
- label = SIP CallP

The following is a sample log:

```
May 19 14:02:54 ngss4 alarmd: SIPC310 CRIT TBL SIP CallP
NCGl=ngss4;Unit=0;SIPC No Database Connection
```

Action

Establish connectivity between CallP and the Database.

Associated Operational Measurements or Performance Measurements

None

SIPC310 SIP CallP Database Connection Established Log

A second associated SIPC310 log is generated “SIP CallP Database Connection Established” when the connection that caused the first SIPC310 log is re-established and the alarm is cleared.

Log Title: SIP CallP

Name: SIPC3100

Description: Database Connection Established

Event type: Trouble

Format

For the SIPC 310 alarm and related log, the following are values/explanations of the variable values:

- alarmLevel = None - Indicates that the alarm is cleared
- componentID = SIPC
- category = Communications - Indicates communication failure between CallP and the database has been established
- description = Database Connection Established
- probableCause = outOfService
- specificProblem = Communication Established with Database
- correlationIdList = None
- neVendorSpecificInfo = None
- technologySpecificInfo = None
- reportNum = 310
- eventType = TRBL
- label = SIP CallP

The following is a sample log:

```
May 19 14:03:34 ngss4 alarmd: SIPC310 NONE TBL SIP CallP
NCGL=ngss4;Unit=0;SIPC Automatically cleared due to alarm generator
process death
```

Action

None

Associated Operational Measurements or Performance Measurements

None

SIPC 650

The SIPC 650 log is an informational log that is generated when the CallP application goes to get data from the database for a particular table and no data is found.

Log Title: IP CallP

Name: SIPC 650

Description: No Data Found

Event type: Info

Format

For the SIPC 650 log, the following are values/explanations of the variable values:

- Report Name = SIPC
- Report Number = 650
- Alarm Value = NONE
- Event Type = INFO
- label = "No Data Found:" <data type>

The following is a sample log:

```
May 13 13:32:17 JOEBOB sipgwyappln: SIPC650 NONE INFO SIP CallP No  
Data Found: ACCESS LINK MAP
```

Action

None

Associated Operational Measurements or Performance Measurements

None

SIPC301

The SIPC301 log is a critical log that is generated when the SIP Gateway Call Processing Application will not receive any incoming SIP messages due to Access Control List being enabled and no valid entries in the Remote SIP server or ACL list.

Log Title: All Incoming SIP Msgs Blocked

Name: SIPC301

Description: ACL enabled without valid entries

Event type: Trouble

Format

For the SIPC301 log, the following are values/explanations of the variable values:

- Report Name = SIPC
- Report Number = 301
- Alarm Value = CRIT
- Event Type = TBL
- label = “All SIP Incoming Msgs Blocked” <data type>

The following is a sample log:

```
Nov 12 21:32:08 loopback sipgwyappln: SIPC301 CRIT TBL All SIP  
Incoming Msgs Blocked
```

Action

None

Associated Operational Measurements or Performance Measurements

None

SIPC750

The SIPC750 log is generated when the SIP Gateway Call Processing Application drops incoming SIP messages due to Access Control List restrictions.

A Minor, Major or Critical log is generated based on the number of SIP messages dropped in last 15 minutes:

- Minor Threshold: 25
- Major Threshold: 100
- Critical Threshold: 500

Log Title: SIP Access Control List

Name: SIPC750

Description: Incoming SIP messages dropped

Event type: Trouble

Format

For the SIPC301 log, the following are values/explanations of the variable values:

- Report Name = SIPC
- Report Number = 750
- Alarm Value = MIN/MAJ/CRIT
- Event Type = TBL
- label = “SIP Access Control List” <data type>

The following is a sample log:

```
Nov 12 21:32:08 loopback sipgwyappln: SIPC750 CRIT TBL Incoming 600  
SIP messaged dropped
```

Action

None

Associated Operational Measurements or Performance Measurements

None

SIPGW700 - SIP Call Processing Application Logs

The following is a description of the customer logs generated by SIP call processing application. SIP Call Processing Application Logs are INFO logs which can be viewed via the SIP Gateway Maintenance web browser interface on the Session Server.

Following is the format of the log:

```
<Date> <Time> <DeviceName> sipgwyappln: SIPGW700 NONE INFO SIPCALLP <LogMessage>
```

Following are values/explanations of variable values listed above:

- <Date>: Current date
- <Time>: Current time
- <DeviceName>: The name assigned to the Session Server
- <LogMessage>:
 - PostGainNotifyCallp Called on INACTIVE side
 - Sync call to the standby unit failed with callid *callld*
 - GCP NewCall received for Unsupported Agent : *agentType*
 - No more CallDataBlocks to process CallID: *callld*
 - Failed to add ISUP payload for call *callld*
 - Remote SIP server not mapped for SIP LINK Index *SipLinkIdx*
 - No Active Server for SIP Link *SipLinkIdx*
 - HandleNewCall::Failed to Set MDB for callid *callld*

- No GCP Nodes to process call with callid *callld*
- Unauthorized Call attempt from MGC *DestMgc*
- HandleSipUPDATERequest::MDB Parsing for UPDATE failed for callid *callld*
- HandleACK::MDB Parsing for ACK failed for callid *callld*
- Handle200OKINVITERecvd::MDB Parsing for 200 OK INVITE failed for callid *callld*
- Incompatible media format received in 200 OK response to INVITE.
- Handle200OKINVITERecvd::Failed to send ACK for callid *callld*
- Handle200OKINVITERecvd::Failed to get Outbound Message for callid *callld*
- Handle200OKINVITERecvd::Failed to add 305 warning header for callid *callld*
- HandleReINVITE::MDB Parsing for Re INVITE failed for callid *callld*
- HandleSipINFORequest::MDB Parsing for INFO failed for callid *callld*
- HandleACKReINVITE::MDB Parsing for ACK failed for callid *callld*
- new message received with bad syntax start-line. *msgDestName*
- new message received with bad syntax. *msgDestName*
- Unable to Get Received Message (ACK) for callid *callld*
- *Module:Procedure* Null App Call Context
- *Module:Procedure* Unable to Get Received Message
- Media Error: CALLID: *callld* - 488 Not Acceptable Here Received
- Media Error: CALLID: *callld* - 606 Not Acceptable Received
- Incompatible media format, call rejected.
- Media type not available, call rejected.
- GCP Socket Open Failed
- Failed to get Active IP Address
- Bind for GCP Socket Failed
- supportedExtensionList was Null defaulted to 100rel
- NGSS Profile Data Creation Failed for Server *sipServerName*

Following is a sample SIPGW700 log:

```
May 11 15:09:33 sp2k-1 sipgwyappln: SIPGW700 NONE INFO SIPCALLP  
supportedExtensionList was Null defaulted to 100rel
```

SIP Gateway application Call Processing Alarms

SIP Gateway Callp Database Access Alarm

When the CallP application tries to access the database and it fails due to a loss of connectivity between the database and the CallP application, a Critical alarm is generated. The log associated with the generation of the alarm is the SIPC 550 log “SIP CallP No Database Connection”.

When the connection is re-established, the alarm is lowered and an associated SIPC 550 log is generated “SIP CallP Database Connection Established”

SIP Gateway Callp ACL Trouble Alarm

This alarm is raised when incoming SIP messages are dropped due to Access Control List enforcements. The alarm handler polls for dropped messages every 15 minutes. The severity of the alarm is based on the number of packets dropped in last 15 minute time interval. The severities include

- Minor Threshold: A minor alarm is raised if 25 or more messages (but less than 100) are dropped.
- Major Threshold: A major alarm is raised if 100 or more messages (but less than 500) are dropped.
- Critical Threshold: A major alarm is raised if 500 or more messages are dropped.

If no messages are dropped in the next 15 minutes, the raised alarm is cleared.

SIPC 750 logs are generated for each of the alarms as described in logs section.

SIP Gateway Application Maintenance Logs and Alarms

The following is a description of logs and alarms generated by the SIP Gateway Application Maintenance software. Note that these logs and alarms are only generated and reported on the SIP Gateway application, and are not resident on the DMS core for example.

They can be viewed via the SIP Gateway Maintenance web browser interface on the Session Server Manager - SIP Gateway application web page.

The following information corresponds to the content delivered in the SN07 release, and may be updated for following releases.

SIP Gateway Application Maintenance Logs

The SIP Gateway Application Maintenance software produces the following logs:

- SIPM500 - SIP Gateway Maintenance State Change Log
- SIPM300 - SIP Gateway Maintenance Trouble Log
- SIPM301 - SIP Gateway Maintenance Trouble Alarm Log
- SIPM302 - SIP Gateway Maintenance Sync Trouble Alarm Log

SIPM500 - SIP Gateway Maintenance State Change Log

This is an INFO log which is generated any time the SIP Gateway Application maintenance state changes.

Following is the format of this log:

```
<Date> <Time> <DeviceName> sipgwymtc: SIPM500 NONE INFO SIP Gateway Maintenance State Change
[Administrative : <AdminFrom> -> <AdminTo>]
[Operational   : <OperFrom>  -> <OperTo>]
[Control       : <CtrlFrom>  -> <CtrlTo>]
[Procedural    : <ProcFrom>  -> <ProcTo>]
[User Requested : <Yes|No>]
[Reason        : <StateChangeReason>]
[Web User ID   : <webuserid>]
```

Following are values/explanations of variable values listed above:

- <Date>: Current date
- <Time>: Current time
- <DeviceName>: The name assigned to the Session Server
- <AdminFrom> and <AdminTo>:
 - Locked
 - Unlocked
 - Shutting Down
- <OperFrom> and <OperTo>:
 - Enabled
 - Disabled
- <CtrlFrom> and <CtrlTo>:
 - Suspended
 - Not Suspended
- <ProcFrom> and <ProcTo>:
 - Terminating
 - Not Terminating

- <StateChangeReason>:
 - Unsuspend command issued
 - Suspend command issued
 - Lock command issued
 - Lock command in progress
 - Lock operation complete
 - Unlock command issued
 - Shut Down command issued
 - Shut Down operation complete
 - System originated change of state
 - Timeout waiting to terminate call processing
 - Audit Failure
 - Timer Problem
 - Data corruption detected
- <webuserid>: If applicable, this is the web interface login ID of the user performing the maintenance that caused the state transition. If not applicable, this value is left blank.

Following is a sample SIPM500 log:

```
Apr 12 10:45:06 RTPF-SIP0 sipgwymtc: SIPM500 NONE INFO SIP Gateway Maintenance State Change
[Administrative : Locked      -> Unlocked]
[Operational    : Enabled     -> Enabled]
[Control        : Not Suspended -> Not Suspended]
[Procedural     : Not Terminating -> Not Terminating]
[User Requested : Yes]
[Reason         : Unlock command issued]
[Web User ID    : mtc]
```

SIPM300 - SIP Gateway Maintenance Trouble Log

This is a TBL (Trouble) log which is generated any time the SIP Gateway Application Maintenance software encounters an unexpected condition.

Following is the format of this log:

```
<Date> <Time> <DeviceName> sipgwymtc: SIPM300 NONE TBL SIP Gateway Maintenance Trouble
[Reason Text : <TroubleReason>]
[Error Code  : <ErrorCode>]
```

Following are values/explanations of variable values listed above:

- <Date>: Current date
- <Time>: Current time

- <DeviceName>: The name assigned to the Session Server
- <TroubleReason>:
 - SAM to Web Server message send failure
 - SAM to SIP CallP message send failure
 - Been Terminating too long. Timer Expired.
 - SAM Wait Timer Messaging Timeout
 - SAM/SIP CallP Audit Messaging Timeout
 - Failed to set the SIP Gateway Application state
 - SIP Gateway Application process death
 - Failed to start the SIP Gateway Application process
 - Failed to set a timer
 - SIP CallP created, but not in the requested state
 - SIP CallP created, but failed to reply to SAM
 - SIP CallP on the Inactive failed to respond to a request
 - SIP CallP on the Inactive failed to get to the requested state
 - SAM failed to send a reply to a platform swact request
 - SAM failed a Swact Request due to an invalid Swact Request
 - SAM failed a Graceful Swact Request due to being marked to do a COLD Swact
 - SAM failed a Swact Precheck Request due to option = FORCE
 - SAM failed a Swact Precheck or PreSwact request due to option = NOW
 - SAM failed a Swact Request due to an invalid option
 - SAM failed a Swact Request due to an unacceptable platform status
 - SAM failed a Swact Request due to not being In-Sync
 - Swact Precheck Failed due to failure received in SIP CallP response
 - Swact Precheck Failed due to failure to notify SIP CallP
 - Swact Precheck Failed due to timeout waiting on SIP CallP response
 - Swact PreSwact Failed due to failure received in SIP CallP response
 - Swact PreSwact Failed due to failure to notify SIP CallP
 - Swact PreSwact Failed due to timeout waiting on SIP CallP response
 - Swact AbortSwact Failed due to failure received in SIP CallP response
 - Swact AbortSwact Failed due to failure to notify SIP CallP

- Swact AbortSwact Failed due to timeout waiting on SIP CallP response
- Swact PostSwact Failed due to failure received in SIP CallP response
- Swact PostSwact Failed due to failure to notify SIP CallP
- Swact PostSwact Failed due to timeout waiting on SIP CallP response
- Disable PreCheck Failed due to failure received in SIP CallP response
- Disable PreCheck Failed due to timeout waiting on SIP CallP response
- Disable PreDisable Failed due to failure received in SIP CallP response
- Disable PreDisable Failed due to timeout waiting on SIP CallP response
- Disable AbortDisable Failed due to failure received in SIP CallP response
- Disable AbortDisable Failed due to timeout waiting on SIP CallP response
- Swact PreSwact Failed due to failure to notify SIP CallP
- Disable PreDisable Failed due to failure received from the mate SAM
- Disable PreDisable Failed due to failure to notify SIP CallP
- Disable PreDisable Failed due to timeout waiting on mate SAM response
- Disable AbortDisable Failed due to failure received from the mate SAM
- Disable AbortDisable Failed due to failure to notify SIP CallP
- Disable AbortDisable Failed due to timeout waiting on mate SAM response
- Disable Request Failed due to Callback called with existing disable request outstanding
- Disable Request Failed due to Callback called when platform not active and enabled
- Disable Inactive Failed due to Callback called when platform not in duplex
- Disable Inactive PreCheck Failed due to Callback called when SAM had a conflicting wait state
- Disable Inactive PreDisable Failed due to Callback called when SAM had a conflicting wait state
- Disable Inactive AbortDisable Failed due to Callback called when SAM had a conflicting wait state
- Disable PreCheck Failed due to failure to notify SIP CallP

- Disable PreDisable Failed due to failure to notify the Mate SAM
- Disable AbortDisable Failed due to failure to notify the Mate SAM
- Disable Active Failed due to Callback called when platform was in duplex
- Disable Active Graceful Failed due to Callback called when SIP State was not suspended
- Disable Callback called with invalid request
- SAM received a response to a Swact request that contained an invalid request
- SAM received a response to a Swact request that contained an invalid option
- SAM received a response to a Swact request that contained an invalid result
- Mate SAM failed a Prepare For COLD Swact request, reverting to a WARM swact
- Failed to notify the Mate SAM to Prepare For COLD Swact request, reverting to a WARM swact
- Timed out waiting on the Mate SAM to respond to a Prepare For COLD Swact request, reverting to a WARM swact
- SAM failed to register with DataSync
- <ErrorCode>: This is an integer code used for debugging. -1 is the default value.

Following is a sample SIPM300 log:

```
Apr  6 13:24:47 RTPF-SIP0 sipgwymtc: SIPM300 NONE TBL SIP Gateway Maintenance Trouble
[Reason Text : SIP Gateway Application process death]
[Error Code  : -1]
```

SIPM301 - SIP Gateway Maintenance Trouble Alarm Log

This is a TBL (Trouble) log which is generated any time the SIP Gateway Maintenance Trouble Alarm is raised or lowered.

Following is the format of this log:

```
<Date> <Time> <DeviceName> alarmd: SIPM301 <AlarmSeverity> TBL SIP Gateway Maintenance Trouble
Alarm : <DeviceInfo> <AlarmRaiseLowerText>
```

Following are values/explanations of variable values listed above:

- <Date>: Current date
- <Time>: Current time
- <DeviceName>: The name assigned to the Session Server

- <AlarmSeverity>: The current severity of the alarm:
 - CRIT
 - NONE
- <DeviceInfo>: Info that specifies the device to which the alarm pertains
- <AlarmRaiseLowerText>:
 - SIP Gateway Application System Busy
 - SIP Gateway Application System Busy - Alarm Cleared

Following are sample SIPM301 logs:

```
Apr 6 14:39:00 RTPF-SIP0 alarmd: SIPM301 CRIT TBL SIP Gateway Maintenance Trouble Alarm :  
NCGL=RTPF-SIP0;Unit=0; SIP Gateway Application System Busy
```

```
Apr 6 14:39:01 RTPF-SIP0 alarmd: SIPM301 NONE TBL SIP Gateway Maintenance Trouble Alarm :  
NCGL=RTPF-SIP0;Unit=0; SIP Gateway Application System Busy - Alarm Cleared
```

SIPM302 - SIP Gateway Maintenance Sync Trouble Alarm Log

This is a TBL (Trouble) log which is generated any time the SIP Gateway Maintenance Sync Trouble Alarm is raised or lowered. This occurs when the SIP Gateway application state gets out of sync, or gets back in sync in a duplex Session Server configuration.

Following is the format of this log:

```
<Date> <Time> <DeviceName> alarmd: SIPM302 <AlarmSeverity> TBL SIP Gateway Maintenance Sync  
Trouble Alarm : <DeviceInfo> <AlarmRaiseLowerText>
```

Following are values/explanations of variable values listed above:

- <Date>: Current date
- <Time>: Current time
- <DeviceName>: The name assigned to the Session Server
- <AlarmSeverity>: The current severity of the alarm:
 - MAJOR
 - NONE
- <DeviceInfo>: Info that specifies the device to which the alarm pertains
- <AlarmRaiseLowerText>:
 - SIP Gateway Application Mtc Out Of Sync
 - SIP Gateway Application Mtc Out Of Sync - Alarm Cleared

Following are sample SIPM302 logs:

```
Apr 13 09:13:15 RTPF-SIP0 alarmd: SIPM302 MAJOR TBL SIP Gateway Maintenance Sync Trouble Alarm  
: NCGL=RTPF-SIP0;Unit=0; SIP Gateway Application Mtc Out Of Sync
```

Apr 13 09:13:45 RTPF-SIP0 alarmd: SIPM302 NONE TBL SIP Gateway Maintenance Sync Trouble Alarm :
NCGL=RTPF-SIP0;Unit=0; SIP Gateway Application Mtc Out Of Sync - Alarm Cleared

SIP Gateway Application Maintenance Alarms

Following are the two alarms the SIP Gateway Application Maintenance software may produce:

- SIP Gateway Maintenance Trouble Alarm
- SIP Gateway Maintenance Sync Trouble Alarm

SIP Gateway Maintenance Trouble Alarm

This is a critical alarm that is raised when the SIP Gateway Application transitions to a state that indicates it should be in-service, but is not, and the Session Server unit the application is running on is in an enabled operational state. This “system busied” state is represented by state values as follows:

- Administrative State = Unlocked
- Operational State = Disabled
- Procedural Status = “-” or Not Terminating
- Control Status = “-” or Not Suspended

Call processing cannot occur while in this state.

When the SIP Gateway Application transitions out of this state (automatically or manually) this alarm is lowered. It is also lowered if the Session Server unit the application is running on leaves the enabled operational state.

When this alarm is raised, the system will attempt recovery immediately. If immediate recovery is not successful, reattempts are made automatically every 30 seconds.

A manual method to attempt recovery from this state would entail issuing the following commands from the SIP Gateway Maintenance web browser interface:

- Lock command
- Unsuspend command
- Unlock command

Refer to the SIPM301 logs described above which are generated when this alarm is raised or lowered.

SIP Gateway Maintenance Sync Trouble Alarm

This is a major alarm that is raised when the Session Server the SIP Gateway Application is running on is in a duplex configurations with both units in an enabled operational state, and the SIP Gateway application state becomes out of sync between the two Session Server units.

This alarm is lowered if the Session Server leaves the duplex configuration with both units in an enabled operational state, or if the SIP Gateway application state becomes synchronized between the two Session Server units.

The SIP Gateway application should attempt to sync itself automatically every 30 seconds. If there repeated failures, a manual method to attempt recovery from this condition would entail issuing the following commands from the SIP Gateway Maintenance web browser interface:

- Lock command
- Suspend command
- Unsuspend command
- Unlock command

Refer to the SIPM302 logs described above which are generated when this alarm is raised or lowered.

Session Server Provisioning Logs and Alarms

The following is a description of logs and alarms generated by the Session Server Provisioning software. The alarms and logs are generated in response to database connectivity changes of state detected by the provisioning watchdog program.

They can be viewed via the CS 2000 Session Server Manager Platform Main web browser page via the 'Alarms' and 'Customer Logs' buttons.

Session Server Provisioning Logs

The Session Server provisioning software produces the following logs:

- DBSE300 - Database Connectivity Change Log

DBSE300 - Solid Database connectivity change Log

This is a Trouble (TBL) log which is generated any time a change in database connectivity is detected. It reports '**No Solid DB Connection**' when database connectivity is lost. It reports '**Solid DB Connection Restored**' when database connectivity is reestablished.

Log Title: No Solid DB Connection

Name: DBSE300

Description: No Database Connection

Event type: Trouble

The DBSE300 “No Database Connection” log is generated in tandem with a Critical alarm due to a loss of connectivity between the Session Server provisioning watchdog program and the Solid database.

Following is the format of this log:

- reportName = DBSE
- reportNum = 300
- eventType = TBL
- alarmValue =
 - CRIT
 - None
- label = **No Solid DB Connection** ~ when database connectivity is lost.
- label = **Solid DB Connection Restored** ~ when database connectivity is restored.

Example Logs

The following is a sample log when the database connection is lost.:

```
Mar 22 21:27:48 vm0 alarmd:DBSE300 CRIT TBL No Solid DB Connection No
Database Connection
```

The following is a sample log when the database connectivity is restored:

```
Mar 22 21:27:48 vm0 alarmd:DBSE300 CRIT TBL Solid DB Connection
Restored No Database Connection
```

Action

Take corrective action to restore the unresponsive database.

Associated OMs

None.

Associated Alarms

Critical No Database Connection Alarm

Session Server Provisioning Alarms

The Session Server Provisioning software produces a critical alarm when it detects a loss of connectivity to the database. An example of this alarm follow:

```
Communications Out of Service Monday March 22nd 2004 09:34:54 AM
Critical No Database Connection
```

When this alarm is raised the provisioning watchdog software will attempt to switch activity to the mate copy of the Session Server platform only if connectivity to the mate's database can be verified.

Action

Take corrective action to restore the unresponsive database.

Associated Logs

DBSE300

Configuration for A00003933**Hardware and Software Requirements**

The Gateway Controller's (GWC's) software load must be upgraded to receive SIPLINK before CM SIPLINK is datafilled.

Initial Configuration

There is no initial configuration.

Office/Subnet parameters (OP/SP) (CM & CS2M)

Not Applicable

Upgrade Impact

SIPLINK is a new table.

Data schema (DS) (CM, MIBS, RDB)**New/modified tables, MIBs, or Database Schema****New or modified tables**

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
SIPLINK	NEW	NEW

Table/MIB/Remote Database Schema information**SIPLINK**

Session Internet Protocol Communication Link

Functional description

New table SIPLINK creates an association between CS 2000 agents (e.g., ISUP trunks) and a SIP link name.

The SIPLINK table is downloaded to GWCs datafilled as DPT SIPT in table SERVSINV.

Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

TRKOPTS with SIPT

DPTRKMEM with DPTRKKEY.CLLI and SIPT signaling

SIPLINK with SIPTTRK already datafilled in TRKOPTS:OPTKEY.CLLI and in DPTRKMEM.

Size

Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SIPLINK	0	2048	Memory allocated in increments for 64 tuples (each 6 bytes)

Fields/OIDs

The following table lists fields/OIDs for SIPLINK.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
LINKNAME	new	key	VECTOR OF UP TO 16 CHARS	alpha numerical name of the siplink
CONNTYPE	new		CS2CS or CS2AS	a connection type indicates CallServer to CallServer or CallServer to ApplicationServer
AGNTDATA	new	selector	ISUPTRK	currently only ISUPTRK is implemented
SIPTTRK	new	refinement	VECTOR OF UP TO 16 CHARS	alpha numerical name of the trunk (CLLI)

Datafill example

The following example shows a sample datafill for tables TRKOPTS, DPTRKMEM and SIPLINK.

- **TABLE TRKOPTS (after Trimodal restructuring - SN07)**

OPTKEY OPTINFO

SIP_LOOP_1 DPT DPT SIPT NET_IP Y

- **TABLE DPTRKMEM**

DPTRKKEY RANGEINF MAXCALLS

SIP_LOOP_1 SIPT 100

- **TABLE SIPLINK**

LINKNAME CONNTYPE AGNTDATA

ACCESS_LINK_2 CS2CS ISUPTRK **SIP_LOOP_1**

Table release history update

This is new table for SN07 (patchable into SN06.0)

Supplementary information

None

Translation verification other tools

None

Service Orders (SO) (CM & CS2M)

Not Applicable.

Software optionality control (SOC)

There are two new core usage SOC options that are used to limit the maximum number of simultaneous calls that are allowed through the Session Server Manager at any given time. Without one or both of the new SOC options, no call processing can take place using the Session Server Manager.

These usage SOC's do not take the place of Base DPT usage SOC CS2B0005. The latter is still needed to set the value of office parameter DPT_MAX_PORTS in table OFCVAR. DPT_MAX_PORTS limits the overall number of simultaneous DPT calls.

SOC CS2B0008

SOC CS2B0008

SOC option name:	CS to CS calls
SOC option title:	Yes/No
SOC option control type:	usage
New SOC option?	Yes
SOC option order code	CS2B0008
Option defined in DRU:	MSH
Affected products:	SN07

SOC limitations

The usage-controlled CS2B0008 SOC added by this activity applies to calls that meet the following criteria:

- the incoming or outgoing trunk group has the DYNAMIC option with SIPT SIGNALING in table TRKOPTS,
- a match of the incoming or outgoing trunk group is found in the SIPTTRK field of one of the tuples in table SIPLINK,
- the CONNTYPE field of the tuple in table SIPLINK is set to CS2CS.

A counter keeps track of the current number of calls matching the above criteria. For each new CS2AS call, the current value in the counter is checked against the limiting value in the CS2AS SOC. If the addition of a new call of this type would exceed the SOC limit, the call is sent to treatment; otherwise, the counter is incremented and the call is allowed to proceed. When the call is ended, the counter is decremented.

In the following example of table SIPLINK, incoming and outgoing SIPT calls on trunk group NGSSLOOP will increment the usage counter for the CS2AS SOC.

TABLE: SIPLINK

LINKNAME	CONNTYPE	AGNTDATA
-----	-----	-----
NGSSOUTLK	CS2AS ISUPTRK	NGSSOUT
NGSSINLINK	CS2AS ISUPTRK	NGSSINC
LOOPAROUND1	CS2CS ISUPTRK	NGSSLOOP

Here is an example of the output of the SOC SELECT command for the new SOC:

```
>select option CS2B0008
GROUP:CS2B
OPTION      NAME                RTU  STATE  USAGE  LIMIT  UNITS  LAST_CHG
-----
CS2B0008 CS to CS Calls        N    -      127    500    1VC   04/01/19
```

SOC CS2B0008 interactions:

- Calls that peg the new CS2B0008 count will always peg the CS2B0005 count as well.
- If the SOC limit set for CS2B0008 exceeds the limit of the Base DPT SOC CS2B0005, the latter is the limiting factor in determining the maximum number of simultaneous CS2AS calls.
- Feature A00004271 SIP App Server SOC introduces new OM group NGSSOM for tracking the effects of the CS2B0008 SOC limit setting on CS2CS calls.

SOC CS2B0009**SOC CS2B0009**

SOC option name:	CS to AppS calls
SOC option title:	Yes/No
SOC option control type:	usage
New SOC option?	Yes
SOC option order code	CS2B0009
Option defined in DRU:	MSH
Affected products:	SN07

SOC limiting

The usage-controlled CS2B0009 SOC added by this activity applies to calls that have the following characteristics:

- the incoming or outgoing trunk group has the DYNAMIC option with SIPT SIGNALING in table TRKOPTS,
- a match of the incoming or outgoing trunk group is found in the SIPTTRK field of one of the tuples in table SIPLINK,
- the CONNTYPE field of the tuple in table SIPLINK is set to CS2AS

A counter keeps track of the current number of calls matching the above criteria. For each new CS2AS call, the current value in the counter is checked against the limiting value in the CS2AS SOC. If the addition of a new call of this type would exceed the SOC limit, the call is sent to treatment; otherwise, the counter is incremented and the call is allowed to proceed. When the call is ended, the counter is decremented.

In the following example of table SIPLINK, incoming SIPT calls on trunk group NGSSINC and outgoing calls on trunk group NGSSOUT will increment the usage counter for the CS2AS SOC.

TABLE: SIPLINK

LINKNAME	CONNTYPE	AGNTDATA
-----	-----	-----
NGSSOUTLK	CS2AS ISUPTRK	NGSSOUT
NGSSINLINK	CS2AS ISUPTRK	NGSSINC
LOOPAROUND1	CS2CS ISUPTRK	NGSSLOOP

Here is an example of the output of the SOC SELECT command for the new SOC:

```
>select option CS2B0009
GROUP:CS2B
OPTION      NAME                RTU  STATE  USAGE  LIMIT  UNITS  LAST_CHG
-----
CS2B0009   CS to AppS Calls      N    -      127    500    1VC    04/01/19
```

SOC limitations

- Calls that peg the new CS2B0009 count will always peg the CS2B0005 count as well.
- If the SOC limit set for CS2B0009 exceeds the limit of the Base DPT SOC CS2B0005, the latter is the limiting factor in determining the maximum number of simultaneous CS2AS calls.

Element Management

Not Applicable.

Security

Not Applicable.

Configuration Information

This feature allows the craftsperson to provision a number of fields on a remote-server basis, as per customer requirements. The following section captures the provisioning information for specific configurations. The different configurations discussed include:

- NGSS - NGSS
- NGSS - SN07 VRDN
- NGSS - SN06.2 VRDN
- NGSS - SN06 VRDN
- NGSS - MCS

Please refer to the FN section for detailed information on provisionable fields.

Default Provisioning Information Various Configurations

Field	NGSS - MCS	NGSS - SN07 VRDN	NGSS-NGSS
IP Address	x.x.x.x	x.x.x.x	x.x.x.x
Port	5060	5060	5060 ^a
Protocol	UDP	UDP	UDP or TCP

Default Provisioning Information Various Configurations

Field	NGSS - MCS	NGSS - SN07 VRDN	NGSS-NGSS
Optional IP (1-6)	none	none	none
Methods:	INVITE, CANCEL, BYE, OPTIONS, INFO, PRACK	INVITE, CANCEL, BYE, OPTIONS, SUBSCRIBE, NOTIFY, PRACK, INFO	INVITE, CANCEL, BYE, OPTIONS, SUBSCRIBE, NOTIFY, PRACK, INFO, UPDATE, REFER
URI Parameters Supported	none	cic	all
SIP Headers supported	Content-Disposition, one of Remote-Party-ID or P-Asserted-ID/Privacy	Content-Disposition, one of Remote-Party-ID or P-Asserted-ID/Privacy, Diversion	Content-Disposition, one of Remote-Party-ID or P-Asserted-ID/Privacy, Reason, Replaces, Referred-By, Diversion
ISUP to SIP Cause Map ^b	Default	Default	Default
SIP to ISUP Cause Map ^c	Default	Default	Default
SIP Redirection Map ^d	Default	Default	Default
ISUP Variant to SIP Version Map ^e	Default	Default ^f	Default
NOA/NPI to Phone Context Map:	None	None	Default ^g

Default Provisioning Information Various Configurations

Field	NGSS - MCS	NGSS - SN07 VRDN	NGSS-NGSS
SIP Cause Precedence Priority	Default (OR) Encap: Third Retry: Second CauseCode: First	Default	Any
APN Information	Not Applicable	Not Applicable	Applicable ^h
Backward Call Indicator (BCI) Data	(I) Inetworking Encountered (K) ISUP Not used All the Way (M) Terminating Access is not ISDN	(I) Inetworking Encountered (K) ISUP Not used All the Way (M) Terminating Access is not ISDN	(I) Inetworking Encountered (K) ISUP Not used All the Way (M) Terminating Access is not ISDN
Forward Call Indicator (FCI) Data	Treat as National Call (D) Interworking Encountered (F) ISUP Not Used All the Way (HG) ISUP Not required (I) Originating Access nonISDN	Treat as National Call (D) Interworking Encountered (F) ISUP Not Used All the Way (HG) ISUP Not required (I) Originating Access nonISDN	Treat as National Call (D) Interworking Encountered (F) ISUP Not Used All the Way (HG) ISUP Not required (I) Originating Access nonISDN
SIP Header format	Compact or Long	Compact or Long	Compact or Long
Options for Heartbeat	yes	yes	yes
Telephony Profile	yes	yes	yes or no
Use Info for Long Call Audit	yes	yes	yes or no

Default Provisioning Information Various Configurations

Field	NGSS - MCS	NGSS - SN07 VRDN	NGSS-NGSS
Map non-screened RPI to Calling#	yes	yes	yes
Accepts Early SDP	no	yes	yes
Accept Invite without SDP	yes	yes	yes
E.164 Format Allowed ⁱ	no	no	yes ^j
Enforce Code-Compatibility ^k	no	no	yes or no ^l
Accepts Encapsulated ISUP	no	yes	yes or no
CountryCode Support ^m	no	no	yes or no
Hop-Counter	7	7	7
Out of Band DTMF	vnd.nortelnetworks.digits	telephone-event	telephone-event
Agent	ISUP	ISUP	ISUP
Unknown Header	any string	any string	anystring
Anonymous Header	any string	any string	any string

- a. The port can be configured to a number of choice. Ensure the port number is consistent across the communicating NGSSs.
- b. A custom ISUP - SIP cause map can be added by clicking on “*ISUP and SIP Mappings*” tab and adding a new mapping under “*ISUP to SIP Map*”.
- c. A custom SIP - ISUP cause map can be added by clicking on “*SIP and ISUP Mappings*” tab and adding a new mapping under “*SIP to ISUP Map*”.
- d. A custom SIP Redirection Map can be added by clicking on “*ISUP and SIP Mappings*” tab and a new mapping under “*SIP Redirection*”.

- e. This maps ISUP *Protocol/Version/Variant* <--> *SIP base and Version* fields. See FN section for instructions on how to add a new mapping. Also, See Appendix for base/version for different protocol variants that are required for communicating with VRDN configurations. For all other configurations, base/version entries are configurable.
- f. When interworking with VRDN, add an entry with base/version of gr394/gr394 for any external protocol (Q764 NULL NULL gr394 gr394)
- g. Nature Of Address/Numbering Plan Identifier <--> Phone-Context Mapping table. For incoming SIP calls, this table is used to determine the NOA/NPI values to be used in the ISUP message. Similarly, for outgoing calls, this table is used to determine the 'phone-context' parameter to be added to Request-URI. The button "**Phone-Context**" (under URI-Parameters) must be turned ON for this functionality to take effect. New mapping entries can be added by following the procedure described in FN section.
- h. This is used to setup handling of Action Point Number (APN), Private Numbering Plan type calls. There are three different types this can be configured as shown in the pull-down menu. **1. Use Prefix** ---> requires datafill of Prefix field. **2. Use Prefix and Phone Context** --> requires datafill of both Prefix and Phone-Context fields. **3. Phone Context Only** --> requires datafill of Phone Context Field.
- i. Marking this field 'Y' requires datafill of Country Code Supported to be set to 'Y' and entry of valid Country Code in the provided field.
- j. Marking this field 'Y' requires datafill of Country Code Supported to be set to 'Y' and entry of valid Country Code in the provided field.
- k. Marking this field 'Y' requires selection of at least one applicable codec in the 'Config Data' section.
- l. Marking this field 'Y' requires selection of at least one applicable codec in the 'Config Data' section
- m. Must be marked 'Y' and valid Country code datafilled, if '*e.164 supported*' is set to 'Y'

Default Provisioning Information Various Configuration

Field	NGSS - SN06.2 VRDN	NGSS - SN06 VRDN
IP Address	x.x.x.x	x.x.x.x
Port	5060	5060
Protocol	UDP	UDP
Optional IP (1-7)	none	none
Methods:	INVITE, CANCEL, BYE, OPTIONS, SUBSCRIBE, NOTIFY, PRACK, INFO	INVITE, CANCEL, BYE, OPTIONS, PRACK, INFO
URI Parameters Supported	cic	none

Field	NGSS - SN06.2 VRDN	NGSS - SN06 VRDN
SIP Headers supported	Content-Disposition, one of Remote-Party-ID or P-Asserted-ID/Privacy, Diversion	Remote-Party-ID
ISUP to SIP Cause Map ^a	Default	Default
SIP to ISUP Cause Map ^b	Default	Default
SIP Redirection Map ^c	Default	Default
ISUP Variant to SIP Version Map ^d	Default ^e	Default ^f
NOA/NPI to Phone Context Map:	None	None
SIP Cause Precedence Priority ^g	Default	Default
APN Information	Not Applicable	Not Applicable
Backward Call Indicator (BCI) Data	(I) Inetworking Encountered (K) ISUP Not used All the Way (M) Terminating Access is not ISDN	(I) Inetworking Encountered (K) ISUP Not used All the Way (M) Terminating Access is not ISDN

Field	NGSS - SN06.2 VRDN	NGSS - SN06 VRDN
Forward Call Indicator (FCI) Data	Treat as National Call (D) Interworking Encountered (F) ISUP Not Used All the Way (HG) ISUP Not required (I) Originating Access nonISDN	Treat as National Call (D) Interworking Encountered (F) ISUP Not Used All the Way (HG) ISUP Not required (I) Originating Access nonISDN
SIP Header format	Compact or Long	Compact or Long
Options for Heartbeat	yes	yes
Telephony Profile	yes	yes
Use Info for Long Call Audit	yes	yes
Map non-screened RPI to Calling#	yes	yes
Accepts Early SDP	yes	yes
Accept Invite without SDP	yes	yes
E.164 Format Allowed ^h	no	no
Enforce Code-Compatibility ⁱ	no	no
Accepts Encapsulated ISUP	yes	yes
CountryCode ^j Support	no	no
Hop-Counter	7	7

Field	NGSS - SN06.2 VRDN	NGSS - SN06 VRDN
Out of Band DTMF	telephone-event	Not Applicable
Agent	ISUP	ISUP
Unknown Header	any string	any string
Anonymous Header	any string	any string

- a. A custom ISUP - SIP cause map can be added by clicking on “*ISUP and SIP Mappings*” tab and adding a new mapping under “*ISUP to SIP Map*”.
- b. A custom SIP - ISUP cause map can be added by clicking on “*SIP and ISUP Mappings*” tab and adding a new mapping under “*SIP to ISUP Map*”.
- c. A custom SIP Redirection Map can be added by clicking on “*ISUP and SIP Mappings*” tab and a new mapping under “*SIP Redirection*”.
- d. This maps ISUP *Protocol/Version/Variant* <--> *SIP base and Version* fields. See FN section for instructions on how to add a new mapping. Also, See Appendix for base/version for different protocol variants that are required for communicating with VRDN configurations. For all other configurations, base/version entries are configurable.
- e. When interworking with VRDN, add an entry with base/version of gr394/gr394 for any external protocol (Q764 NULL NULL gr394 gr394)
- f. When interworking with VRDN, add an entry with base/version of gr394/gr394 for any external protocol (Q764 NULL NULL gr394 gr394)
- g. You can change the precedence setting for testing purposes and select different precedence for different interworkings
- h. Marking this field ‘Y’ requires datafill of Country Code Supported to be set to ‘Y’ and entry of valid Country Code in the provided field.
- i. Marking this field ‘Y’ requires selection of at least one applicable codec in the ‘Config Data’ section.
- j. Must be marked ‘Y’ and valid Country Code datafilled, if ‘e.164 Supported’ is set to ‘Y’

Default Configuration Data Settings

Field	Default Value
general Linger Timer	32000
Invite Linger Timer	32000
local TCP Port	5060 ^a
local UDP Port	5060 ^b
maxCallLegs	1000 ^c

Default Configuration Data Settings

Field	Default Value
maxSipMsgSize	1536
maxSubscriptions	1000
provisionalTimer	180000
retransmission T1	2000
retransmission T2	4000
retransmission T4	5000
retry Count	6
codec G729 Allowed	N ^d
codecPCMUAllowed	N ^e
codecPCMAAllowed	N ^f
enableOnBoardBilling	N ^g
enableAccessControl ^h List	N
mgcHostName	Must Correspond to table of ceng 'mgc_hostname' parameter in the core
susAutoRefresh	N
supportedExtensionList	100rel

- a. This can be configured for NGSS-NGSS calls
- b. This can be configured for NGSS-NGSS calls
- c. Max value of 40000
- d. Must be set if 'codec-enforcement' is turned on for the server
- e. Must be set if 'codec-enforcement' is turned on for the server
- f. Must be set if 'codec-enforcement' is turned on for the server
- g. Billing is MCI specific
- h. If this turned ON, please ensure ALL the IP Addresses the NGSS box communicates with are part of the Access Control List. (IP Addresses that are datafilled in Remote Server Page area automatically part of the list.) For example, when communicating with VRDN implementation, ensure the IP Addresses of all the communicating SIP GWCs are part of the list. Otherwise, call processing will not work.

Appendix

The following mapping will be used for NGSS to communicate with VRDN configuration.

NGSS to VRDN mapping

Protocol	Version	Variant	Base	Version
Q764	NUL	NULL	gr394	gr394
UCP	NULL	NULL	ansi88	gr394
ccitt	V1	base	etsi121	etsi121
ccitt	v2	base	etsi356	etsi356
btup	null	null	gb_iup	gb_iup



SN07 Feature Deltas

Product = CS 2000

A00003971 -- SPM Log Robustness (Succession on DMS)

Functional Description

SPM Log robustness initiative is intended to enhance the logs generated for SPMs.

During an analysis of the CSR responsiveness, it was found that SPM logs did not provide sufficient data for analysis. To provide a faster resolution of SPM issues, a need was felt to enhance the logs generated for SPMs. In conjunction, MAP responses for various commands have been enhanced to provide greater details about the failure/refusal of MAP commands.

Hardware Requirements or Dependencies

None

Software Requirements or Dependencies

MAP response modification

When a manual or force swact is issued on the CEM protection level MAP, if the command fails, a reason is displayed along with the existing response. When a RTS is issued on a RM, if the command fails because of the RM not having a valid load in flash, a message appears. This message has been corrected to include a 'have a' in the existing message 'RM does not valid load in Flash'.

More details can be found in the Configuration section of this book.

LOGS

The following existing logs are impacted by this activity

Activity status of the unit/device will be displayed along with the other fields for the following logs

- SPM300 - Device Fault report log
- SPM500 - Device state change log
- SPM650 - Boot loader pass log
- SPM651 - Boot loader fail log
- SPM684 - Erase Flash log
- SPM301 - Patch failed log
- NODE302 - Software Alarm log
- NODE303 - Wrong Application Data
- NODE326 - Hardware Fault
- NODE600 - System Recovery Action
- NODE601 - System Status Notification

TaskName will be displayed along with the taskID for the following logs.

- SPM311 - SW Exception Report
- SPM312 - Trap

New field 'Reason' will be added to the following log to provide a reason for protection switch failure.

- SPM331 - Failed Device Protection Switch

The following new logs have been introduced

- SPM 682 - indicates CEM manual reset.
- SPM 683 - indicates reason for CEM swact.
- NODE 602 - indicates reason for CEM state transition

For more details about the enhancement to the above logs, please refer to the Fault Management chapter of this book.

Limitations and restrictions

None

Interactions

None

Applicable customer facing sections

Fault Management

Logs

__X__

Alarms

Configuration

Data Schema	_____
User Interface	___X___
Element Management	_____
Security	_____
Service Order	_____
Office Parameters	_____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

Glossary

Term	Description
CEM	Common Equipment Module
CSR	Customer Service Request
MAP	Maintenance and Administration Position
SPM	Spectrum Peripheral Module
SWACT	Switch Activity

Fault Management for A00003971**Fault management strategy**

As a part of this activity the following enhancements are done.

- Some of the existing logs generated for SPMs shall be modified to provide additional data.
- Two new SPM logs, SPM 682 and SPM 683 shall be implemented to report on conditions related to manual reset of CEM/RM and CEM swact trigger respectively.
- A new NODE log, NODE602 shall be implemented to report on the CEM state transition reasons. This log is generated only when the CEM state transitions from Insv to Istb or Insv to Sysb. This log provides the reason for the state transition.

Fault management tools and utilities

Logutil

Logs

This section gives details of each log modified/added.

SPM300

Explanation

Log Title: Device Fault report

Name: SPM 300

Description:

This log is generated when a fault occurs on a SPM device.

Event type: TBL

Format

The following figure shows the format and an example of the SPM 300 log after the completion of this activity.

Format and example of SPM 300 log

Format of SPM 300 log

```
<office_id> <alarm> SPM300 <mmdd hh:mm:ss ssdd> TBL Device Fault Report
Location   : SPM : <spm_number> <cpk_type> : <cpk_number> Activity:<A or I>
Status     : <one of the 3 strings given below>
Problem Description: <text up to 16 chars>
<text up to 64 chars>
Action: Replace the following cards in the ordered list.
Cardlist:
<device_cardlist>
Location: <SPM node_no> Type: <spm_type> Fabric: <fabric_type>
```

Example of SPM 300 log

```
STEC207AT *** SPM300 JUL28 07:02:21 6701 TBL Device Fault Report
Location   : SPM : 25 VSP : 7 Activity: A
Status     : Fault Raised
Problem Description: Critical
8I: RM reset reason: Last Gasp
Action     : Replace the following cards in the order listed.
Cardlist   :
  Site    Flr   Row FrPos ShfPos ShfPec   Slot
  HOST    3     A   0    59     NTLX66AA  4
  HOST    3     A   0    43     NTLX82AA  8
```

Field descriptions

The newly added field 'Activity' indicates the activity status of the device. The status field indicates 'Fault Raised' instead of 'Alarm Raised'. The following table describes the modified fields.

SPM 300 field details

Field	Modified/ Added	Value	Description
Activity	Added	A or I	This indicates activity status of the device. A - Active; I - Inactive;
Status	Modified	Fault Raised Fault Cleared Info Only	This indicates whether fault was raised/ cleared or whether the log is meant just for information only.

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

None.

Additional information

None.

SPM500**Explanation**

Log Title: Device State change report

Name: SPM 500

Description:

This log is generated when a state change occurs on a SPM RM.

Event type: INFO

Format

The following figure shows the format and an example of the SPM 500 log after completion of this activity.

Format and example of SPM 500 log

Format of SPM 500 log

```
<office_id> <alarm> SPM500 <mmdd hh:mm:ss ssdd> INFO Device State Change
Location   : SPM : <spm_number> <cpk_type> : <cpk_number>
From       : <state> <activity status>
To         : <state> <activity status>
Location   : <SPM node_no> Type: <spm_type> Fabric: <fabric_type>
```

Example of SPM 500 log

```
RTPY07AW *** SPM500 AUG28 03:06:11 7700 INFO Device State Change
Location: SPM : 10   DLC : 0
From      : InSv (Active )
To        : SysB (Inactive)
```

Field descriptions

The newly added string along with the state ‘Active/Inactive’ indicates the activity status of the device on which state change is being reported.

SPM 500 field details

Field	Modified/Added	Value	Description
From	Modified	Active/Inactive	In addition to the state of the device, the activity before transition is also indicated.
To	Modified	Active/Inactive	In addition to the state of the device, the activity after transition is also indicated.

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

None.

Additional information

None.

SPM650**Explanation**

Log Title: SPM Bootloader log (loading passed)

Name: SPM 650

Description:

This log is generated when a SPM bootloader completes load transfer successfully.

Event type: Not applicable

Format

The following figure shows a format and example of the SPM 650 log after completion of this activity.

Format and example of SPM 650 log**Format of SPM 650 log**

```
RTPY07AW      SPM650 <mmmmdd hh:mm:ss ssdd> PASS
               SPM Device Loader Success
Report:        <report seq. num> OF <total num. of report>
Device:        SPM <spm num> <device type> <device unit no> Activity : <A or I>
Result:        Passed
Load File:     <load file name>
Elapsed Time:  <elapsed hour>:<elapsed min>:<elapsed sec>
KiloByte Loaded: <kiloByte downloaded>
```

Example of SPM 650 log

```
RTPY07AW      SPM650 AUG28 02:46:52 8400 PASS
               SPM Device Loader Success
Report:        1 OF 1
Device:        SPM 10 VSP 2 Activity : I
Result:        Passed
Load File:     DSP20AM_010012
Elapsed Time:  00:03:49
KiloByte Loaded: 2926
```


Field descriptions

The newly added field 'Activity' indicates the activity status of the device. The following table gives details of the newly added field.

SPM 650 field details

Field	Modified/ Added	Value	Description
Activity	Added	A or I	This indicates activity status of the device. A - Active I - Inactive

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

None.

Additional information

None.

SPM651**Explanation**

Log Title: SPM Bootloader log (loading Failed)

Name: SPM 651

Description:

This log is generated when a SPM bootloader fails to transfer load.

Event type: Not applicable

Format

The following figure shows the format and an example of the SPM 651 log after completion of this activity.

Format and example of SPM 651 log

Format of SPM 651 log

```
RTPY07AW * SPM651 <mmmmdd hh:mm:ss ssdd> FAIL
          SPM Device Loader Failure
Report:   <report seq. num> OF <total num. of report>
Device:   SPM <spm num> <device type> <device unit no> Activity : <A or I>
Result:   Failed
Load File: <load file name>
Elapsed Time: <elapsed hour>:<elapsed min>:<elapsed sec>
Failure Reason: <kiloByte downloaded>
```

Example of SPM 651 log

```
RTPY07AW * SPM651 AUG28 02:11:03 3800 FAIL
          SPM Device Loader Failure
Report:   1 OF 1
Device:   SPM 10 VSP 2 Activity : I
Result:   Failed
Load File: DSP20AM_010012
Elapsed Time: 00:00:46
Failure Reason: Loading Aborted
```

Field descriptions

The newly added field 'Activity' indicates the activity status of the device. The following table gives details of the new field added.

SPM 651 new field details

Field	Modified/Added	Value	Description
Activity	Added	A I	This indicates activity status of the device. A - Active I - Inactive

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

None.

Additional information

None.

SPM684

Explanation

Log Title: Erase Flash log

Name: SPM 684

Description:

This log is generated when a EraseFl command is executed on a CEM MAP.

Event type: INFO

Format

The following figure shows the format and an example of the SPM 684 log after completion of this activity.

Format and example of SPM 684 log

Format of SPM684 log

```
<Office id> SPM684 <mmdd hh:mm:ss ssdd>INFO ERASE FLASH
Location: SPM : <spm no> CEM : <unit no> Activity : <A or I>
Userid : <userid>
Description:<one of the 4 strings given below>
Location   : <SPM node_no> Type: <spm_type> Fabric: <fabric_type>
```

```
string1 : ERASE FLASH INITIATED
string2 : ERASE FLASH COMPLETED
string3 : ERASE FLASH FAILED
string4 : ERASE FLASH REJECTED
```

Example of SPM log

```
RTPY07AW      SPM684 AUG28 03:04:25 4800 INFO ERASE FLASH
Location      : SPM : 10 CEM : 0 Activity : I
Userid        : USER1
Description    : ERASE FLASH COMPLETED
```

Field descriptions

The newly added field 'Activity' indicates the activity status of the device. The following table gives details about the new field.

SPM 651 new field details

Field	Modified/Added	Value	Description
Activity	Added	A I	This indicates activity status of the device. A -Active I -Inactive

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

None.

Additional information

None.

SPM301**Explanation**

Log Title: Device Patching Report

Name: SPM 301

Description:

This log is generated when patching fails on a SPM device.

Event type: TBL

Format

The following figure shows the format and an example of the SPM 301 log after completion of this activity.

Format and example of SPM 301 log

Format of SPM301 log

```
<office_id> <alarm> SPM301 <mmdd hh:mm:ss: ssdd> TBL Device Patching Report
Location : SPM : <spm_number> <cpk_type> : <cpk_number> Activity:<A or I>
Status : <one of the 2 strings given below>
Location: <SPM node_no> Type: <spm_type> Fabric: <fabric_type>
```

string 1 : Patching operation failure set

string 2 : Patching operation failure cleared

Example of SPM301 log

```
INTL7006CD ** SPM301 JAN01 09:50:33 1600 TBL Device Patching Report
Location : SPM : 2 CEM : 1 Activity: I
Status : Patching operation failure set
```

Field descriptions

The newly added field 'Activity' indicates the activity status of the device. The following table gives details about the new field.

SPM 301 new field details

Field	Modified/Added	Value	Description
Activity	Added	A I	This indicates activity status of the device. A -Active I -Inactive

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

None.

Additional information

None.

SPM311

Explanation

Log Title: SW exception Report

Name: SPM 311

Description:

This log is generated when software error (SWERR) occurs on a SPM device.

Event type: TBL

Format

The following figure shows the format and an example of the SPM 311 log after completion of this activity.

Format and example of SPM 311 log

Format of SPM311 log

```
<office_id> <alarm> SPM311 <mmmmdd hh:mm:ss ssdd> TBL SW Exception Report
SPM <node number> <circuit pack> <circuitpackno> : <activity>           Time: <timestamp>
  Filename: <filename>                               LineNumber: <linenumber>
  TaskID: <task id>      Index: <index number>          Reason: <reason>
  TaskName: <taskname string>
  ErrStr: <error string>
  ErrData: <error data>
  Traceback: <traceback>
```

Example of SPM311 log

```
MSH306BB      SPM311 FEB24 03:10:47 5519 TBL  SW Exception Report
SPM 12 CEM 1 : I                               Time: 03:10:47.145
Filename: isupSgrpDDMData.cpp                 LineNumber: 489
TaskID: 000000DF      Index:                   Reason:
TaskName: processMipArbitrati
ErrStr:
ErrData: 00376230 026B6D24 026B6D1C 026B6D40 00D1FA58
Traceback: 00D1FD14 00CEA1A4 00D2D044 00D2F598 00D2F894 00D2E87C
```

Field descriptions

The newly added field 'TaskName' gives the task name for the task Id. The following table gives details about the new field.

SPM 311 field details

Field	Modified/ Added	Value	Description
TaskName	Added	String	This indicates taskname corresponding to the taskID field.

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

None.

Additional information

None.

SPM312**Explanation**

Log Title: Trap log

Name: SPM 312

Description:

This log is generated when a trap occurs in a SPM device.

Event type: TBL

Format

The following figure shows the format and an example of the SPM 312 log after completion of this activity.

Format and example of SPM 312 log

Format of SPM312 log

```
<office_id> <alarm> SPM312 <mmdd hh:mm:ss ssdd> TBL Trap
SPM <node number> <circuit pack> <circuitpackno> : <activity>           Time: <timestamp>
TaskID: <task id>  TrapNo: <trap number>
TaskName: <taskname string>
Instr: <instruction>          Flt: <fault>          Vector: <vector>
Traceback: <traceback>
```

Example of SPM312 log

```
MG4K106BG *** SPM312 MAR03 03:37:59 8963 TBL Trap
SPM 64 CEM 0 : A                               Time: 03:37:59.155
TaskID: 000000D3 TrapNo: 00000001
TaskName: OmSubsystemStart
Instr: 009CFB00 Flt: 00000000 Vector: 00000300
Traceback: 009CF44C 00774B44 01608508 FDFDFDFD FDFDFDFD FDFDFDFD
           FDFDFDFD FDFDFDFD FDFDFDFD FDFDFDFD
```

Field descriptions

The newly added field ‘TaskName’ gives the task name corresponding to the task Id displayed in the log. The new field is described in the following table.

SPM 312 field details

Field	Modified/Added	Value	Description
TaskName	Added	String	This indicates taskname corresponding to the taskID field.

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

None.

Additional information

None.

SPM331

Explanation

Log Title: Failed Device Protection Switch

Name: SPM 331

Description:

This log is generated when sparing fails/is rejected or when PROTFAIL alarm is cleared on a SPM device.

Event type: TBL

Format

The following figure shows the format and an example of the SPM 331 log after completion of this activity.

Format of SPM 331 log

Format of SPM 331 log

```
<office_id> <alarm> SPM331 <mmdd hh:mm:ss ssdd> TBL Failed Device Protection Switch
Location: SPM : <spm_number> <cpk_type> : <cpk_number>
Status : <one of the strings given below>
Description: <Description string>
Reason : <Failure Reason string>
Location : <SPM node_no> Type: <spm_type> Fabric: <fabric_type>
```

Example of SPM 331 log

```
MSH207BL *** SPM331 NOV27 02:32:27 1100 TBL Failed Device Protection Switch
Location: SPM : 25 VSP : 0
Status : Alarm Raised
Description: Manual spare from VSP 1 to VSP 0 failed.
Reason : dest Config failed!
```

Field descriptions

The newly added field 'Reason' indicates the Reason for the protection switch failure/refusal. The following table gives details of the new and modified fields.

SPM 331 field details

Field	Modified/ Added	Value	Description
Reason	Added	string	This indicates reason for failure/rejection of protection switching for the device.

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

None.

Additional information

None.

SPM682**Explanation**

Log Title: Resetmod

Name: SPM 682

Description:

This log is generated when CEM/RM is manually reset on the MAP. This log is generated in the following conditions

- 1> When resetmod command is initiated from the MAP
- 2> When resetmod command is completed
- 3> When resetmod command fails
- 4> When resetmod command is aborted
- 5> When reset via mate is initiated (on CEM) from the MAP
- 6> When reset firmware is initiated from the MAP

Event type: INFO

Format

The following figure shows the format and examples of the SPM 682 log.

Format of SPM 682 log

Format of SPM682 log

```
<Office id> SPM682 <mmdd hh:mm:ss ssdd> INFO RESETMOD
Location: SPM : <spm no> <cpk_type> : <cpk_number>
Userid : <userid>
Description:<one of the 7 strings given below>
Location : <SPM node_no> Type: <spm_type> Fabric: <fabric_type>
```

Description strings:

```
Resetmod Initiated
Resetmod Completed
Resetmod Firmware Initiated
Resetmod ViaMate Initiated
Resetmod Rejected
Resetmod Failed
Resetmod Aborted
```

Example of SPM 682 log

```
STEC207AS      SPM682 JUL16 07:31:58 7311 INFO RESETMOD
                Location   : SPM : 25   CEM : 0
                Userid     : USER1
                Description  : Resetmod initiated
```

```
STEC207AS      SPM682 JUL16 07:31:58 7311 INFO RESETMOD
                Location   : SPM : 25   DSP : 1
                Userid     : USER1
                Description  : Resetmod initiated
```

When the resetmod command is issued with the option nowait, the logs are as follows

```
RSN07AOINDY1    SPM682 OCT18 14:59:57 4700 INFO RESETMOD
                Location   : SPM : 1   CEM: 1
                Userid     : ADMIN
                Description  : Resetmod initiated
```

```
RSN07AOINDY1    SPM682 OCT18 15:04:17 4500 INFO RESETMOD
                Location   : SPM : 1   CEM: 1
                Userid     :
                Description  : Resetmod Completed
```

Field descriptions

The following table describes each field in detail.

SPM 682 field details

Field	Value	Description
INFO RESETMOD	Constant	Indicates that the log is a info log and related to resetmod
spm number	Numeric	Indicates the spm number on which resetmod was initiated
cpk_type	String	This is the circuitpack type on which the manual reset was issued.
cpk_number	Numeric	This is the circuit pack number on which manual reset was issued.
UserId	string	Gives the login ID of the user who issued the reset command.
Description	Resetmod Initiated Resetmod Completed Resetmod Aborted Resetmod Failed Resetmod Firmware Initiated Resetmod ViaMate Initiated Resetmod Rejected	This is a description of the resetmod status.

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

None.

Additional information

None.

SPM683**Explanation**

Log Title: CEM swact trigger

Name: SPM 683

Description:

This log is generated when CEM swact occurs.

Event type: INFO

Format

The following figure shows the format of the SPM 683 log.

Format of SPM 683 log

Format of SPM 683 log

```
<office_id> <alarm> SPM683 <mmdd hh:mm:ss ssdd> INFO CEM Swact Trigger
Location: SPM : <spm_number>
Swact Reason: <Description string>
Location : <SPM node_no> Type: <spm_type> Fabric: <fabric_type>
```

Example of SPM 683 log

```
MSH207BL      SPM683 NOV27 00:45:30 3300 INFO CEM Swact
Location      : SPM : 25   CEM : 0
Swact Reason: System Cold switch from CEM 0 to CEM 1.
              CEM SWACT due to Critical Fault. See NODE logs.
Location: SPM 25 Type: DMSCP

MSH207BL      SPM683 NOV27 00:45:05 1900 INFO CEM Swact
Location      : SPM : 25   CEM : 0
Swact Reason: Manual switch from CEM 0 to CEM 1.
              No other details.
Location: SPM 25 Type: DMSCP
```

Field descriptions

The following table describes each field in detail.

SPM 683 field details

Field	Value	Description
INFO CEM Swact trigger	Constant	This indicates that the log is a information log related to CEM swact trigger.
spm number	Numeric	Indicates the SPM number on which CEM swact occurred.
Status	No Alarm	Gives the status of the alarm.
Description	String	This gives the description of what triggered the CEM swact.

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

None.

Additional information

None.

NODE 600**Explanation**

Log Title: System Recovery Action

Name: NODE 600

Description:

This log is generated when a system recovery is happening on a node/unit

Event type: INFO

Format

The following figure shows an example and format of the NODE 600 log. The activity status is displayed in the log only if the architecture type is not load shared.

Format and example of NODE600 log**Format of NODE600 log**

```
NODE600 mmmdd hh:mm:ss ssdd INFO TBL System Recovery Action
Location= <node>
Trouble= <trouble_code>
Action= <user_action>
Activity=<Activity status A or I>
Integrated Node Maintenance Detailed Information
Trouble Reason= <INM trouble condition reason>
```

Example of NODE600 log

```
RTPY07AW      NODE600 AUG28 01:04:40 8300 INFO System Recovery Action
Location: SPM 12 Unit 1
System recovery is in progress
Activity: I
Integrated Node Maintenance Detailed Information
INM retry audit trigger received
Information for analysis, no immediate action required
```

Field descriptions

The newly added field 'Activity' indicates the activity status of the unit.

NODE 600 field details

Field	Modified/ Added	Value	Description
Activity	Added	A I	This indicates activity status of the unit. A -Active I - Inactive

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

None.

Additional information**NODE601****Explanation**

Log Title: System Status Notification

Name: NODE 601

Description:

This log is generated indicating a status notification.

Event type: INFO

Format

The following figure shows the format of the NODE 601 log.

Format of NODE 601 log

```
NODE601 <mmdd hh:mm:ss ssdd> INFO System Status Notification
Location: <node> <Unit number>
Activity: <activity status A or I>
Integrated Node Maintenance Detailed Information
<Detailed information>
```

Example of NODE 601 log

```
RTP5      NODE601 JUL01 12:23:05 4627 INFO System Status Notification
Location: SPM 1 Unit 1
Activity : I
Integrated Node Maintenance Detailed Information
Data not synchronized
Loadname mismatch
Check datafill and correct if necessary
Datafill Loadname does not match Loadname in PM
```

Field descriptions

The newly added field 'Activity' indicates the activity status of the unit.

SPM 601 field details

Field	Modified/Added	Value	Description
Activity	Added	A I	This indicates activity status of the unit. A - Active I - Inactive

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

None.

Additional information

None.

NODE302**Explanation**

Log Title: Software Alarm

Name: NODE 302

Description:

This log is generated when a software fault or alarm occurs.

Event type: TBL

Format

The following figure shows the format of the NODE 302 log.

Format of NODE 302 log

NODE 302 <mmdd hh:mm:ss> <ssdd> TBL Software Alarm
Location: <NODE>
Activity:<Activity status A or I>
Integrated Node Maintenance Detailed Information
Trouble Reason: <Trouble_Reason>
Trouble Detail: Details of trouble

Example of NODE302 log

NODE 302 <mmdd hh:mm:ss> <ssdd> TBL Software Alarm
Location: SPM 1 Unit 1
Activity: I
Integrated Node Maintenance Detailed Information
Trouble Reason: <Trouble_Reason>
Trouble Detail: <Details of trouble>

Field descriptions

The newly added field 'Activity' indicates the activity status of the unit.

NODE 302 field details

Field	Added/Modified	Value	Description
Activity	Added	A I	This indicates activity status of the unit. A - Active I - Inactive

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

None.

Additional information

None.

NODE303**Explanation**

Log Title: Wrong Application Data

Name: NODE 303

Description:

This log is generated when Wrong Application Data due to manual or system initiated activities is detected.

Event type: TBL

Format

The following figure shows the format of the NODE 303 log.

Format of NODE 303 log**Format and example of NODE log**

NODE 303 <mmdd hh:mm:ss> <ssdd> TBL Wrong Application Data
Location: <NODE>
Trouble: <Trouble_Type>
Action: <User_Action>
Activity:<Activity status A or I>
Integrated Node Maintenance Detailed Information
Trouble Reason: <Trouble_Reason>
Trouble Detail: CEM in Slot <slot_number(7or 8)> has Application Data of CEM <cem_number(0 or 1)>

NODE303 FEB15 01:57:54 2112 TBL Wrong Application Data
Location: SPM 0 Unit 1
Trouble: CEM has Application Data of Mate CEM
Action: Check LINK300 Logs & reconnect DS512 Links correctly
Activity: I
Integrated Node Maintenance Detailed Information
Trouble Reason: DS-512 Link/Links may be misconnected.
Trouble Detail: CEM in Slot 8 has Application Data of CEM 0.

Field descriptions

The newly added field 'Activity' indicates the activity status of the unit.

NODE 303 field details

Field	Added/Modified	Value	Description
Activity	Added	A I	This indicates activity status of the unit. A- Active I-Inactive

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

None.

Additional information

None.

NODE326**Explanation**

Log Title: Hardware Fault

Name: NODE 326

Description:

This log is generated when a hardware fault occurs.

Event type: TBL

Format

The following figure shows the format of the NODE 326 log.

Format of NODE 326 log

```
NODE326 <mmdd hh:mm:ss ssdd> TBL Hardware Fault
Location: <node> <unit number>
Status: <Alarm status>
Trouble: <trouble_code>
Action: <user_action>
Activity: <activity status A or I>
Integrated Node Maintenance Detailed Information
Trouble Reason: <INM trouble condition reason>
Trouble Detail: <trouble detail>
```

Example of NODE326 log

```
RSN07AOINDY1 ** NODE326 OCT02 14:55:30 3300 TBL Hardware Fault
Location: SPM 3 Unit 0
Status: Alarm raised
Trouble: Card fault
Action: Restore communication with the Resource Processor
Activity: I
Integrated Node Maintenance Detailed Information
Trouble Reason: Link isolation condition
Trouble Detail: Link/Messaging hardware
```

Field descriptions

The newly added field 'Activity' indicates the activity status of the unit.

NODE 326 field details

Field	Added/ Modified	Value	Description
Activity	Added	A I	This indicates activity status of the unit. A-Active I-Inactive

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

None.

Additional information

None.

NODE602

Explanation

Log Title: CEM State Change Reason Report

Name: NODE 602

Description:

This log is generated when a CEM unit of an SPM transitions from Insv to Sysb or Insv to Istb.

Event type: INFO

Format

The following figure shows the format of the NODE 602 log.

Format of NODE 602 log

```
<office_id> <alarm> NODE602 <mmdd hh:mm:ss ssdd> INFO CEM State Change Reason Report
Location: SPM : <spm_number> CEM : <Unit number>
Reason : <Description string>
Location : <SPM node_no> Type: <spm_type> Fabric: <fabric_type>
```

Example of NODE602 log

```
MSH207BL      NODE602 DEC01 00:38:58 1500 TBL  CEM State Change Reason Report
Location: SPM: 10  CEM : 0
Reason : /RmmMgr/CfltSet
Location: SPM 10  Type: SMG4      Fabric: ATM
```

Field descriptions

The fields in the NODE 602 log are explained below in Table , “NODE 602 field details,” on page 1565.

NODE 602 field details

Field	Value	Description
INFO CEM State Change Reason Report	Constant	This indicates that the log is a information log related to CEM state change reason.
spm number	Numeric	Indicates the SPM number on which CEM state transition occurred.

Field	Value	Description
CEM unit number	Numeric	This gives the unit number of the CEM which underwent a state transition.
Reason	String	This gives the description of the reason for CEM state transition.

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

None.

Additional information

None.

Related documentation

None.

Configuration for A00003971**Hardware and Software Requirements**

When a manual or force swact is issued on the CEM protection level MAP, if the command fails, a reason should be displayed along with the existing response.

When the RTS of a RM fails due to invalid load in the flash, a message is displayed. This existing message needs to be corrected to include a 'have a' to make it grammatically correct.

Command interface changes**Directory: <directory name/MAP level>**

CEM PROT level (protection level)

Directory description

This level is used to perform a manual/forced sparing on a CEM.

Accessing directory: <directory name>**Access to directory or MAP level and return to CI**

To access the protection level for a CEM unit, the following is used on the command interface.

```
mapci;mtc;pm;post spm <spm_number>;select cem <cem number>;prot
```

To quit and return to the CI level, the following command is used

quit mapci

Command: <Manual/Force>

Command description

Manual command performs a manual sparing action on the selected CEM unit.

Responses

In case of failure or refusal of the manual/force sparing command, a response is output indicating the reason for failure/refusal. The list of reason strings in the response is as shown below

No swact comment
Node not inservice
Will disrupt service
Maintenance in progress
No response from unit(s)
Data-sync blocked swact.
Clock-sync blocked swact.
Carriers not up.
Hardware failure.
Unit not active. Hence cannot switch activity.
Mate CEM blocking swact.
Mate not present. Node is in simplex mode
Mate not available. Check the state of mate unit
Unable to contact mate. Mate isolated
Mate unit's state is worse off
Mate unit has already assumed activity.
Swact in progress.

The following figure shows the format of the response on the MAP.

MAP command response for CEM swact failure/refusal

CM	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
CM Flt	SysB	5 CkEr	2CSLk	2 SPM	.	.	.CS	1Crit	.
M	M			*C*				*C*	
Protectn				SysB	ManB	OffL	CBsy	ISTb	InSv
0 Quit		PM		0	0	1	0	10	9
2		SPM		0	0	0	0	4	0
3		CEM		0	0	0	0	2	0
4									
5		SPM	4 ISTb						
6		Prot Grp: CEM			Mode: N/A			Schema: N/A	
7 Force		Sh0 U R A Stat		Sh0 U R A Stat		Sh1 U R A Stat		Sh1 U R A Stat	
8 Manual		1 -- - - ----		8 1 S A ISTb		1 -- - - ----		8 -- - - ----	
9		2 -- - - ----		9 -- - - ----		2 -- - - ----		9 -- - - ----	
10		3 -- - - ----		10 -- - - ----		3 -- - - ----		10 -- - - ----	
11		4 -- - - ----		11 -- - - ----		4 -- - - ----		11 -- - - ----	
12		5 -- - - ----		12 -- - - ----		5 -- - - ----		12 -- - - ----	
13 Select_		6 -- - - ----		13 -- - - ----		6 -- - - ----		13 -- - - ----	
14		7 0 W I ISTb		14 -- - - ----		7 -- - - ----		14 -- - - ----	
15		Y							
16		SPM 4 CEM	1 Manual: Request has been submitted.						
17		SPM 4 CEM	1 SwAct: Command failed.<Failure reason string>						
18									
CMap3									
Time	19:51								

Directory: <directory name/MAP level>

RM circuit pack level

Directory description

This level is used to perform maintenance commands on a RM.

Accessing directory: <directory name>**Access to directory or MAP level and return to CI**

To access the RM level for the circuit pack, the following is used on the command interface.

mapci;mtc;pm;post spm <spm_number>;select <RM circuitpack><RM unit number>

To quit and return to the CI level, the following command is used

quit mapci

Command: <RTS>**Command description**

RTS command returns the circuit pack(s) to service.

Responses

In case of failure a message is displayed on the MAP.

If the failure is due to an invalid load in the flash, the following message is displayed on the MAP.

RM does not valid load in Flash.

This message has been changed to

RM does not have a valid load in Flash.

The following figure shows the format of the response on the MAP.

MAP response for RTS failure due to invalid load in flash

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
AMDI	Istb	1IOCOS	.	7 SPM	4 RS	.	52CC.	1 Maj	ATM_21
C		M		*C*	*C*		*C*	M	*C*
DLC				SysB	ManB	OffL	CBsy	ISTb	InSv
0 Quit		PM		4	0	0	0	20	5
2		SPM		0	0	0	0	8	1
3 ListSet		DLC		1	0	0	0	1	0
4									
5		SPM	5 DLC	0 InAct	SysB				
6 Tst									
7 Bsy		Loc : Row B	FrPos 0	ShPos 59	ShId 1	Slot 1	Prot Grp : 1		
8 RTS		Default Load: DLC71AZ					Prot Role: Working		
9 OffL		rts							
10 LoadMod		SPM 5 DLC	0 RTS: Request has been submitted.						
11		Severity: Critical							
12 Next		Problem : Restart failed, no load in Flash, please reload.							
13 Select_									
14 QueryMod		Action : No Cardlist Available.							
15 ListAlm		SPM 5 DLC	0 RTS: Command failed. RM does not have a valid load						
16 Prot		in Flash.							
17 SPERFORM									
18									
MALINI									
Time 04:31		>							

Product = CS 2000

A00003995 -- SESM: H323 GW Change Capability (UA-IP)

Functional Description

This document details the Succession CS2K H.323 provisioning functionality being delivered in SN07. It describes the changes being made to the CS2K Management Tools (CMT) GUI (manual) and XML (machine-driven) provisioning components of the CS2K Configuration Management System.

This feature is introduced as an ongoing effort for provisioning H.323 Gateways (GW) and Endpoint Groups (EPG) within the Succession software suite. Software that was included in the 6.0 release gave users the ability to provision H.323 gateways of fixed capacity and attributes. A desirable amendment to existing functionality is the ability to change the initial provisioning without affecting already provisioned GWs and EPGs.

This feature provides the following new or amended functionality:

- Change the capacity of a H.323 GW after initial provisioning
- Change the IP address of a H.323 GW after initial provisioning
- Change the Port of a H.323 GW after initial provisioning
- Allow users to specify the TID location of EPGs
- Provide modified GUI display capabilities for H.323 EPGs

An important change to point out as a consequence of this feature is that EPGs are no longer automatically added when a H.323 GW is added. This change was implemented so that greater flexibility could be realized when adding EPGs. It gives the users the ability to specify the location of the EPs in the system so that Terminal Space can be controlled, and therefore fragmentation can be better managed.

This document will describe in detail how the new functionality is used and modifications to existing H.323 provisioning features. For a comprehensive discussion concerning H.323 provisioning, please refer to FN SN06.1 CS2K H.323 Provisioning Application - Actid A00001913.

Hardware Requirements or Dependencies

N/A

Software Requirements or Dependencies

N/A

Limitations and restrictions

Introduction of support for H.323 GWs in the SN06.1 release created EPGs of size 32 for International customers. Because of the desire to be consistent with trunk provisioning capacities and the potential for interactions in hybrid offices, EPGs are updated to be of size 31 in the SN06.0 release and beyond. Already provisioned EPGs of size 32 will continue to work with post SN06.1 releases, but, Nortel strongly recommends that these EPGs are deleted and re-added so that they are provisioned as size 31 EPGs.

Interactions

N/A

Applicable customer facing sections

Fault Management

Logs

Alarms

Configuration

Upgrade

__X__

Data Schema

Service Order

Element Management

__X__

User Interface

__X__

Accounting (includes AMA billing)

Performance (includes operational measurements)

Glossary

Acronym	Definition
ASPEN	Nortel proprietary GW control protocol (not an acronym).
BLM	Business Line Management
CLLI	Common Language Location Identifier
CM	Computing Module
CMT	Call Server 2000 Management Tools

CORBA	Common Object Request Broker Architecture
CPE	Customer Premises Equipment
CS	Call Server
CS2K	Call Server 2000
DDMS	DMS Data Management System
DMS	Digital Multiplex System
DTC	Digital Trunk Controller
DTCI	ISDN Digital Trunk Controller
DTD	Document Type Definition
EP	Endpoint
EPG	Endpoint Group
EPID	End Point Identifier
ETSI	European Telecommunications Standards Institute
GPS	Global Product Support
GUI	Graphical User Interface
GW	Gateway
GWC	Gateway Controller
GWCEM	Gateway Controller Element Manager
H.323	Industry protocol for GW/GK<->GW/GK communication (not an acronym).
HLD	High Level Design
HTML	HyperText Markup Language
IDL	Interface Definition Language
IP	Internet Protocol
ITA	Internet Transparency Agent
JAR	Java Archive
JDBC	Java Database Connectivity
JNLP	Java Network Launching Protocol

JWS	Java Web Start
LAN	Local Area Network
LTC	Line/Trunk Controller
MEGACO	H.248. Industry protocol for MG/MGC <->MG/MGC communication.
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIB	Management Information Block
MI2	Manatee Iteration II
MOP	Method of Procedure
MTC	Maintenance
NA	North American
NAT	Network Address Translator
NN	Node Number
NPM	Network Patch Manager
NTNA	Northern Telecom North American (proprietary PRI variant)
NV	Network View
OAM&P	Operations, Administration, Maintenance and Provisioning
OSS	Operation Support System
OSSDI	OSS Data Interface
PRI	Primary Rate Interface
PLM	Product Line Management
PSTN	Public Switched Telephone Network
PTM	Packet Telephony Manager
RMGC	Redirecting Media Gateway Controller
SDM	SuperNode Data Manager
SESM	Succession Element and Sub-Element Manager [system]

SNMP	Simple Network Management Protocol
SQL	Structured Query Language (for DBs)
SSPFS	Succession Solaris Platform Foundation Software
SS7	Signaling System 7
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TID	Terminal Identifier
TMM	Trunk Maintenance Manager
TN	Terminal Number

Configuration for A00003995

Upgrade Impact

Element Management Upgrade

This activity is responsible for handling modifications from the SN06.0 release to the SN07 release. No user interaction is required; the updates are automatically applied when the system is upgraded from SN06.0 to SN07.

The introduction of H.323 support in the SN06.1 and SN06.0 releases implemented automatic addition of EPGs when a GW is added. Naming conventions for these auto-generated EPGs are “AUTOGEN_EPG_XXX” where XXX is a number between 0 and 999. With the updated philosophy of manually adding EPGs, the current names of the EPGs provisioned no longer is appropriate. Therefore, EPGs that have the “AUTOGEN_EPG” nomenclature will be converted to the new naming convention of “EPG_XXX”. Note that the numerical value (XXX) will not be changed between releases. For example, a SN06.0 EPG named AUTOGEN_EPG_123 will be converted to a SN07 naming convention of EPG_123.

Data schema (DS) (CM, MIBS, RDB)

N/A

Service Orders (SO) (CM & SESM)

N/A

Element Management

New/modified GUIs and Functionality

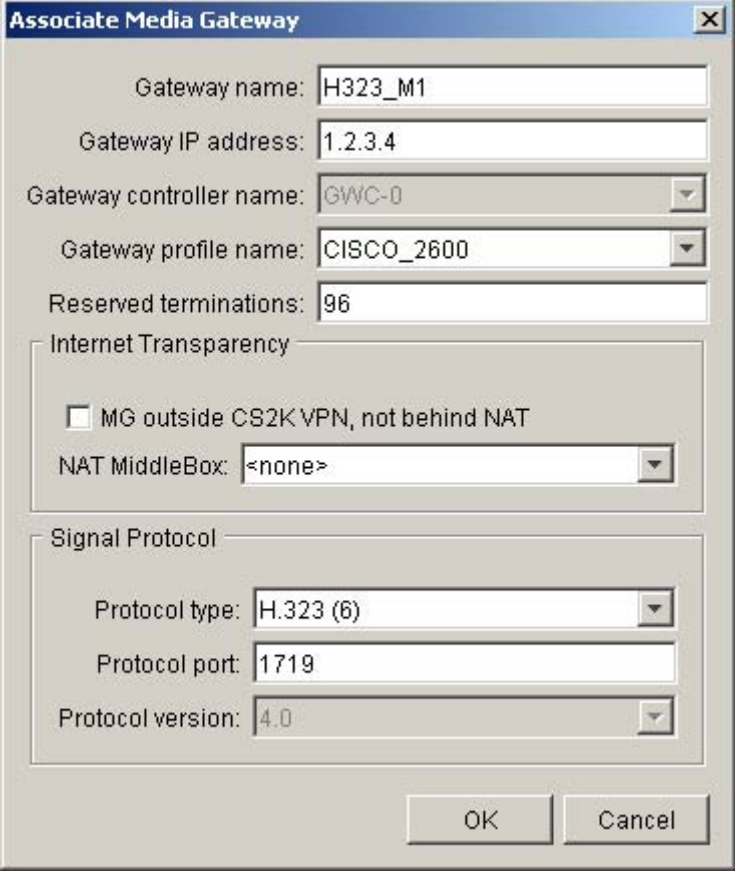
This section describes the Updates to GUIs affected by H.323 provisioning as a result of this activity. It lists dialogs that have cosmetic changes and the new functionality associated with them. For some cases, existing dialogs have not been changed but new functionality has been modified to accommodate updated H.323 provisioning. These dialogs are listed in this section too as a means to describe the new functionality.

New or modified GUIs

GUI name	NEW, CHANGED, DELETED
Associate Media Gateway	Changed functionality in SN07
GWC Provisioning Panel Endpoint Group Component	Deleted in SN07
Add Carrier	New for H.323 in SN07
GWC Provisioning Panel Carrier Component	New for H.323 in SN07
Trunks Associated with EPG Dialog	New for H.323 in SN07
Change Gateway	Changed in SN06.0, propped into SN07
Change Gateway IP and Port Dialog	New in SN06.0, propped into SN07
Change Gateway Capacity Dialog	New for H.323 in SN07
Disassociate Gateway	Changed functionality in SN07
Delete Carrier	New for H.323 in SN07

GUI information

GUI name: Associate Media Gateway



The image shows a Windows-style dialog box titled "Associate Media Gateway". It contains several input fields and dropdown menus for configuring a media gateway. The fields are: Gateway name (H323_M1), Gateway IP address (1.2.3.4), Gateway controller name (GWC-0), Gateway profile name (CISCO_2600), and Reserved terminations (96). There is a section for Internet Transparency with a checkbox for "MG outside CS2K VPN, not behind NAT" (unchecked) and a NAT MiddleBox dropdown (set to <none>). Another section for Signal Protocol contains fields for Protocol type (H.323 (6)), Protocol port (1719), and Protocol version (4.0). At the bottom are OK and Cancel buttons.

Gateway name:	H323_M1
Gateway IP address:	1.2.3.4
Gateway controller name:	GWC-0
Gateway profile name:	CISCO_2600
Reserved terminations:	96
Internet Transparency	
☐ MG outside CS2K VPN, not behind NAT	
NAT MiddleBox:	<none>
Signal Protocol	
Protocol type:	H.323 (6)
Protocol port:	1719
Protocol version:	4.0

Functional description

The Associate Media GW dialog is displayed by using the configuration menu from the main CMT GUI or by selecting the "Associate" button from the GW panel of a GWC. This dialog is used to add H.323 GWs to the CMT which in turn populates the GWC device. The fields that are available with this dialog have not been updated in the SN07 release, however, functionality has been updated.

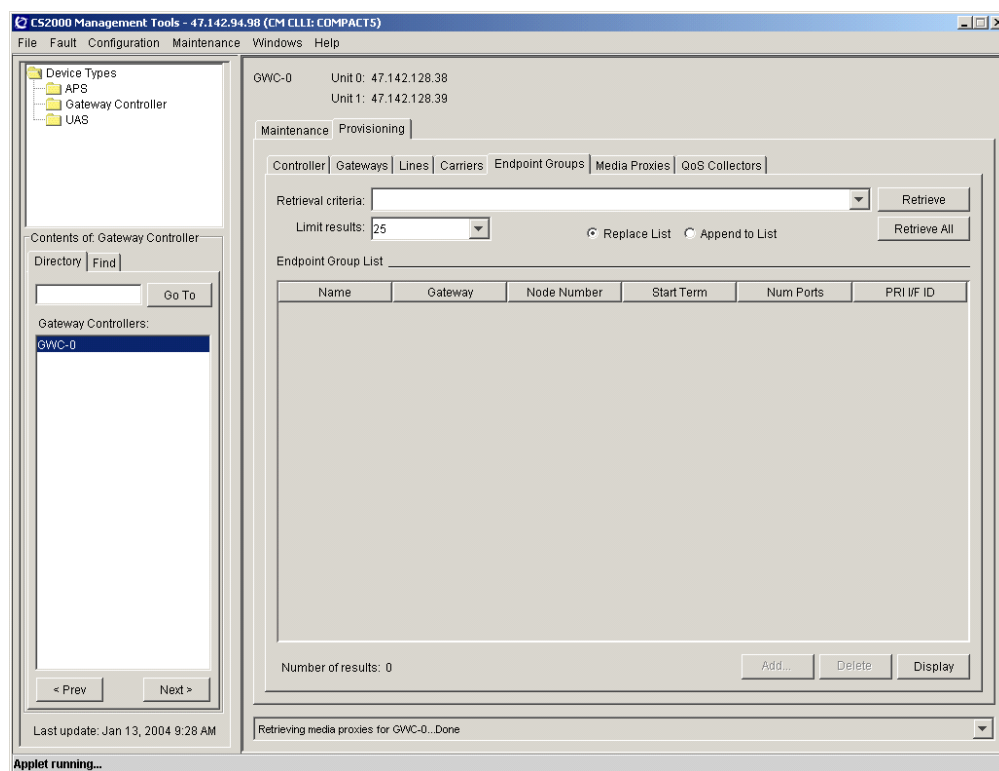
GUI usage and implications

Prior to the SN07 release, adding a H.323 GW to the system had unique functionality for H.323 GWs in that EPGs were automatically created and added to the system. The size of the EPGs (24 or 31) is dependent upon configuration options selected when the CMT product is initially installed. For North American systems, 24 is used, International systems, 31. As well, the number of EPGs provisioned was automatically calculated by the system so

that the appropriate number of groups were added as dictated by the mandatory “Reserved terminations” field. With pre-SN07 functionality, the location of the TIDs allocated was under system control.

In SN07, this behavior has been altered. EPGs are no longer automatically added. Because of this, a separate and additional step of adding the EPGs is required using the “Add carrier” operation. Details concerning the add carrier operation are described in a later section of this document. In other words, adding a GW does not give the system terminations capability, it is only used as a means of adding a GW which must then be filled with terminations. Profiles for H.323 gateways have not been altered by this activity and the maximum capacities implemented in pre-SN07 releases are still applicable.

GUI name: EndpointGroup Panel



Functional description

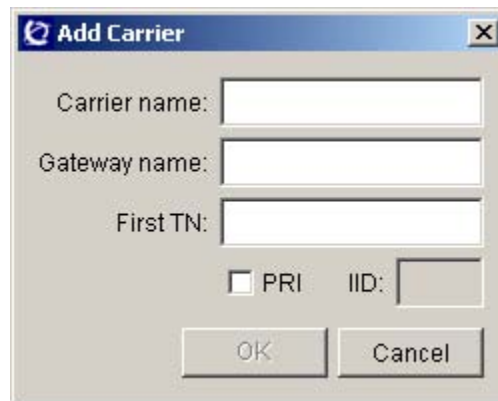
In pre-SN07 releases the Endpoint Groups panel was used to display the Endpoint Groups and attributes for H.323 GWs. Because of the updated philosophy of adding the EPGs using the carrier dialogs and logic, this panel is removed in the SN07 release and replaced by the Carriers Panel.

GUI usage and implications

Deleted in SN07.

Note: The GUI listed in this document shows the Endpoint Groups tab. This is a temporarily GUI depiction used for discussion purposes only. For the released version of the SN07 product the GWC tabs will not include this panel.

GUI name: Add Carrier



Functional description

The Add Carrier dialog is an existing dialog that is now available for provisioning H.323 EPGs. This dialog is displayed when the user selects the “add” button from the “Carriers Panel” and is used to add EPGs to H.323 GWs. As in previous releases, the size for the EPG is dependent upon the configuration set when installing the CMT. For North American systems, 24 is used, for International systems, 31 is used.

GUI usage and implications

H.323 EPGs are added to the system as PRI groups and mimic the provisioning behavior of PRI carriers. However, the PRI checkbox and IID values are auto generated by the system for H.323 and are not required to be input by users. The final version of this GUI is still under development and will be updated as it becomes available.

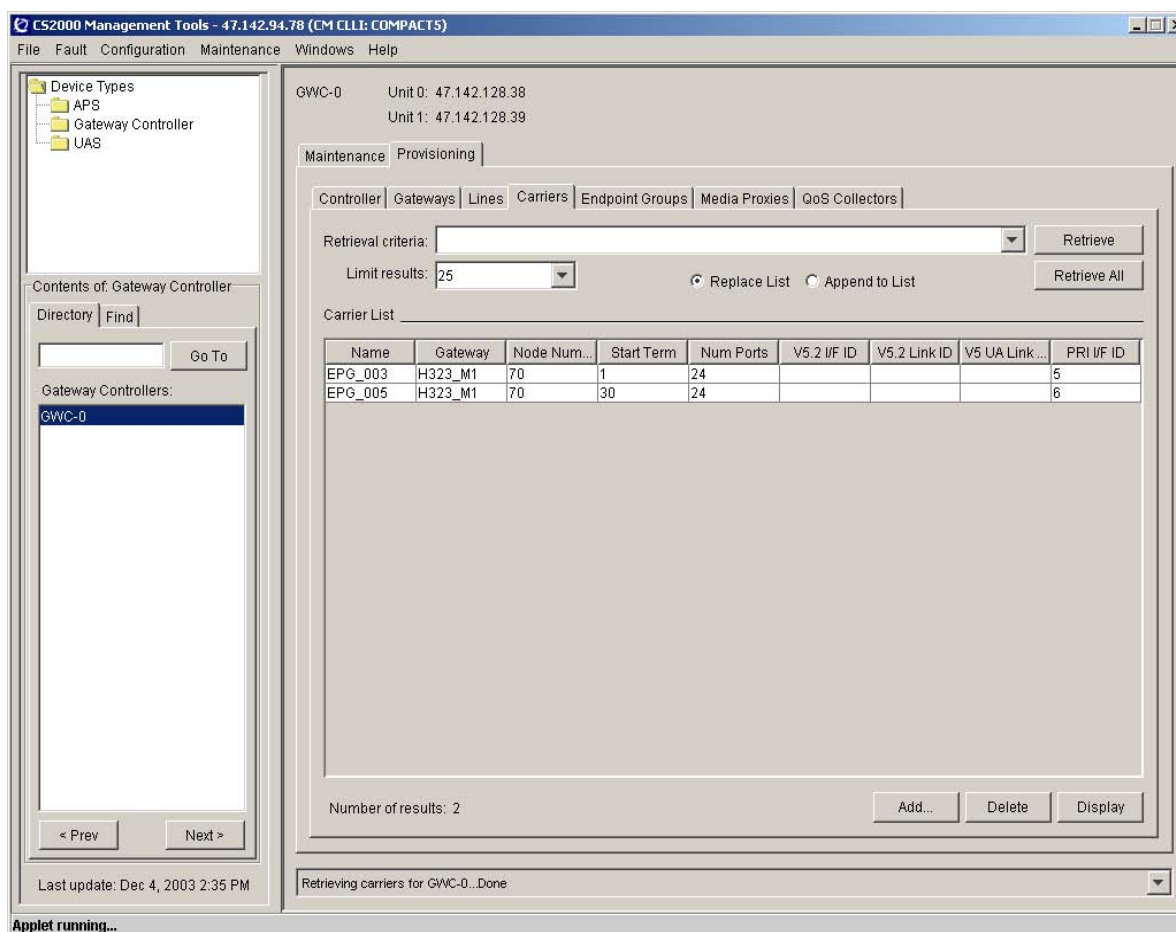
The Carrier name field is used to input the name of the EPG and this name must be unique within the GW. Naming conventions for these EPGs are fairly simple and should be input as follows; EPG_XXX where XXX represents an integer value between 000 and 999. The integer part must be zero padded. As well, the character part is case sensitive and must be input using upper case “EPG” followed by the “_” character. Example datafill might be: EPG_000. Having duplicate EPGs on different GWs is allowed.

The “Gateway name” field is used to indicate which GW the EPG is added to. In order for the operation to succeed, the GW specified must already exist within the system. Multiple EPGs can be added to a GW up to the maximum

capacity as dictated by the reserved capacity that is provisioned for the GW. For example, a GW on a North American system that has a reserved capacity of 240 can have up to 10 EPGs added to it (10 EPGs x 24 EPs = 240 EPs).

The “FirstTN” field is a new optional field made available in the SN07 release. If this field is left blank the system will automatically pick which TIDs are used and how they map to the EPs. These values and mappings can be displayed using the Carrier Panel and Trunks Associated Dialog described later in this document. As well, the listAllCarriers XML interface (described later in this document) can be used to view these values. If the user puts a value in for the “FirstTN” field, a contiguous block of 24 or 31 endpoints are created at the specified starting location. The contiguous TID locations must be available or the operation will fail.

GUI name: Carrier Panel



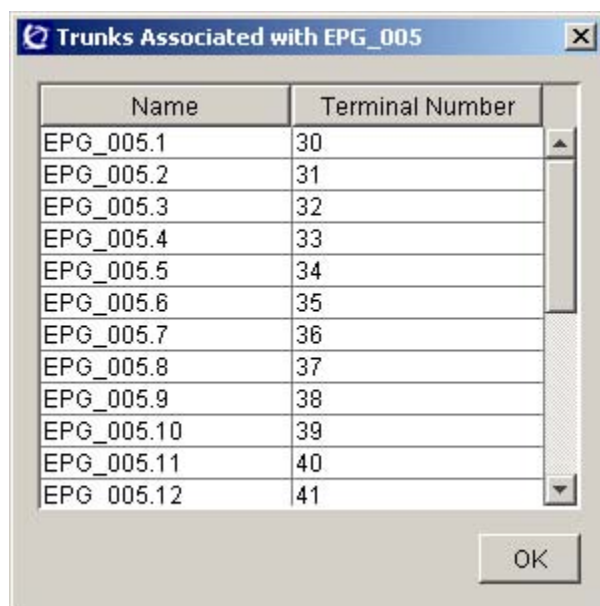
Functional description

The Carrier Panel is an existing panel that is now used for display of H.323 EPGs. This panel is made available by selecting the Carrier tab from the GWC Provisioning panel. In order to display H.323 EPGs provisioned, the “Retrieve” and “Retrieve All” buttons should be selected. Information such as the EPG name, associated GW, Node number and Starting TN, number of ports are pertinent to H.323 EPGs listed.

GUI usage and implication

This panel should be used to view attributes of EPGs associated with H.323 GWs. It replaces the Endpoint Group panel that was used to display this information prior to the SN07 release. In order to expand a EPG and see EP/TID mappings a EPG should be selected and the “Display” button should be selected. Details concerning this functionality are listed below.

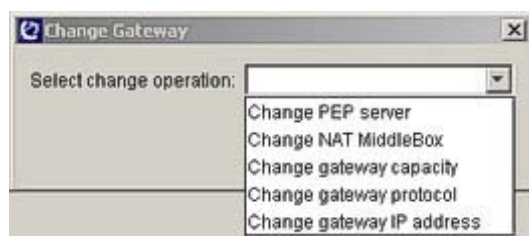
Note: The GUI listed in this document shows the EndpointGroups tab. This is temporarily GUI representation used for discussion purposes only. In the final SN07 version of this product the GWC tabs will not include the panel.

GUI name: Trunks associated with EPG Expansion Dialog**Functional description**

The Trunks Associated dialog is an existing dialog that is now available for viewing H.323 EPG mappings in the SN07 release. This dialog is generated by selecting a EPG within the carriers panel and selecting the “display” button.

GUI usage and implications

This dialog is used to view EP/TN mappings for a H.323 EPG. It can be used to view system or user defined starting TN mappings. The naming conventions for individual EPs is EPG_XXX.xx where xx is an integer between 1 and 31.

GUI name: Change GW**Functional description**

The Change GW dialog is used as a starting point to change attributes of an existing GW. A user picks the attribute they want to change from the combo box and the dialog is expanded to display appropriate fields. The Change GW dialog is an existing dialog that has been amended to include the “Change gateway IP address” pick. This update was introduced in SN06.0 release and this activity is responsible for moving this functionality into the SN07 product.

In addition to the IP pick update, new functionality of supporting “Change gateway capacity” is now supported for H.323 GWs.

This dialog is rendered by selecting a GW from the GWs panel and selecting the “change” button. Once the dialog is displayed the combo box arrow is selected to display the pick.

GUI usage and implications

The change IP and Port ability is restricted to updating H.323 GWs. If an attempt is made to change the IP by a GW type other than H.323, the operation will fail. In addition, only 1 GWs IP or Port can be updated at a time using this operation. If multiple GWs are selected in the GWs panel the “Change gateway IP address” pick is not rendered.

Note: The Change GW protocol operation is another operation that can be used to change the port value associated with a GW. This operation has not been affected by this activity.

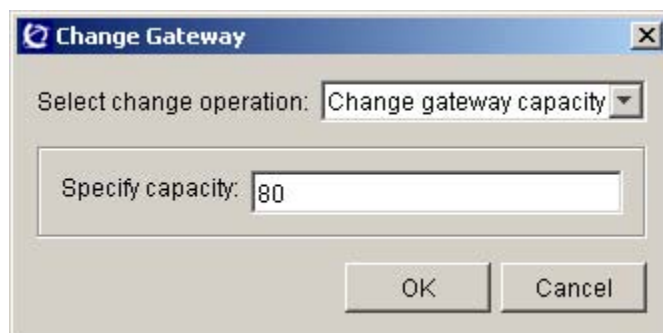
Note: The ability to change a small line GWs IP to discovery is available by going to the gateways panel and selecting the “change” button with no GW rows selected. For this case, a unique change dialog is rendered that allows this operation. Changing a H.323 GWs IP to discovery is not supported and has not been affected by this activity.

GUI name: Change GW IP and Port**Functional description**

The Change GW IP and Port dialog was newly added in the SN06.0 release and propped to SN07 by this activity. This dialog allows users to change the IP and/or Port associated with a H.323 GW. Either the IP, Port or both can be changed with a single transaction. However, in order to change only one of the values the other value must be input with the previously provisioned value. For example, if a user wanted to change the port from 4721 to 4800 but leave the IP alone they would put 4800 in the port field and the already provisioned IP in the IP field.

GUI usage and implications

This dialog allows users to change IP and/or Ports associated with H.323 GWs. If a non-H.323 GW attempts to change the IP to a value other than discovery, this action will fail. If a H.323 GW attempts to change the IP to discovery, the operation will fail.

GUI name: Change GW Capacity

Functional description

The Change gateway capacity dialog is an existing dialog that is now available for changing the capacity of H.323 GWs in the SN07 release. This dialog is generated by selecting a GW or range of GWs within the GWs panel and selecting the “change” button. Once the dialog is rendered, select the “change gateway capacity” pick for the list made available by selecting the combo box arrow.

GUI usage and implications

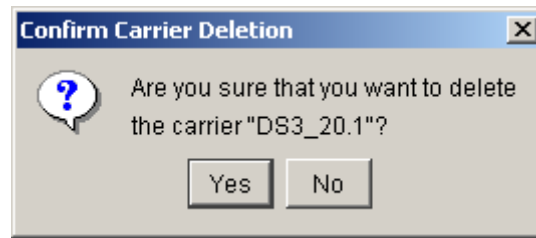
Changing the H.323 GWs capacity in the SN07 release mirrors changing the capacity for other GW types. The capacity can be increased or decreased with the following constraints. A GWs capacity can be increased to the maximum allowed capacity for the GW type as dictated by the profile. A GWs capacity can be decreased to a smaller value as long as it is changed to a value greater than or equal to the number of EPs already allocated. If the user wants to change the capacity to a number smaller than the number of EPs provisioned, then the delete carriers operation should be used to remove EPG capacity and then the change capacity operation should be performed. Note that changing the capacity does not add or delete EPGs from the gateway. Changing the capacity only affects the potential number of EPs that can be provisioned. In order to add or remove EPGs, the “add carrier” or “delete carrier” operations should be used.

GUI name: Disassociate GW**Functional description**

The Disassociate Media Gateway is the dialog used to remove a GW from the CMT and subtending elements. It is displayed when the user selects a GW and pushes the Disassociate button on the GWs panel. The GUI for this operation has not been updated in the SN07 release, however, functionality associated with this action has.

GUI usage and implications

Disassociating a H.323 GW in a pre-SN07 release performed automatic deletions of EPGs and individual EPs dependent upon the EP state. In SN07, this behavior is modified so that H.323 GW deletions mirror behavior of other GW deletions in that if EPs exist for the GW, the transaction will fail. In other words, deletion of a H.323 GW requires the user to remove all EPGs from the GW prior to attempting the disassociate GW operation.

GUI name: Delete Carrier**Functional description**

The Delete Carrier dialog is an existing dialog this is now available to remove H.323 EPGs from the system. This dialog is generated by going to the carriers panel, selecting a carrier, then pushing the “delete” button.

GUI usage and implications

This operation should be used to remove EPGs from a H.323 GW. In order to remove the EPG, the EPs within the group must be in an Out Of Service condition.

User Interface changes**OSSGate User Interface**

This activity modifies support for the operations listed below:

- **changeMG capacity (updated functionality for H.323)**
- **changeMG IP and port (new parameters)**
- **associateMG (updated functionality for H.323)**
- **addCarrier (updated functionality for H.323)**
- **queryEndpointGroup (deleted in SN07)**
- **listAllCarriers (updated functionality for H.323)**
- **disassociateMG (updated functionality for H.323)**
- **deleteCarrier (updated functionality for H.323)**

Terminology & Description of New Method Parameters**changeMG Capacity**

This feature introduces the ability to change the EPG provisioning capacity of a previously provisioned GW. Although this capability currently exists for GWs using other protocols, it is now supported for GWs using the H.323 protocol.

changeMG IP and Port

This feature introduces the ability to change the IP and/or Port address associated with an existing GW. This capability is only supported for H.323 gateways and will be rejected if a GW with a protocol other than H.323 attempts the change IP/Port operation. Support for this operation allows a user to change the IP, Port, or both with a single transaction.

assocMG

Associate MG is the OSSGate XML interface used to datafill new Media Gateways. The interface to associate a GW using XML was available with the introduction of H.323 functionality in the SN06.1 release. This interface has not been modified from the previous release. However, it is important to realize that functionality provided for this action is changed in SN07 in that EPGs are no longer automatically provisioned. In order to add EPGs to a GW, an additional step of adding a carrier group or groups is required.

addCarrier

The addCarrier interface is an existing interface that is now used to provision H.323 EPGs. This command will add a EPG of size 24 or 31 endpoints to a GW dependent upon market configuration. CMT systems that were configured as “North America” will provision EPGs of size 24, and systems configured as “International” will provision EPGs of size 31. In order to provision a GW with multiple EPGs, this command should be called repeatedly with a unique EPG.

This command will automatically grab the first available block of contiguous TID space TNs available on the GWC if the optional “firstTN” tag is not used. The user can also specify the starting TID location if this field is included. This option gives users the ability to assign EPs to specific TID locations if they desire. If a firstTN tag is included, the system will assign a contiguous group of 24 or 31 EPs (system specific depending upon North American or International configuration) starting at the given location. If any of the TNs in the range are already allocated the command will fail.

queryEndpointGroup

This interface is removed in the SN07 release. In order to retrieve EP/TID mappings for H.323 GWs, the listAllCarriers interface should be used.

listAllCarriers

The list all carriers XML command is an existing command that should be used starting in SN07 to retrieve EP/TID mappings for H.323 GWCs. This command replaces the queryEndpointGroup command. Several filters (FILTER_ALL, FILTER_GWC, FILTER_MG, and FILTER_CARRIER) are available to limit the range of mappings to return. For details concerning use of these filter please refer to the XML examples and schema listings below.

XML - Example Commands and Responses

Listed below are syntax examples of the XML commands affected by the H.323 work in this activity. For some cases, new functionality is introduced. For others, new optional tags in reference to H.323 are highlighted. The XML in these examples are formatted for ease of understanding.

XML command examples for Change MG command

The following are examples of the enhanced change MG XML commands and the corresponding response messages for each operation supported by this activity. This activity introduces three new attributes that can be changed on an existing H.323 GW, the capacity, the IP, and the Port. The capacity change is a stand alone operation while the IP and Port changes can be combined.

Example format of changeMG IP and/or Port

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList >
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      < changeMG usn="1" version="1.0" >
        <Parameters>
          <mgUIName>H323_M1</mgUIName>
          <mgIpAddr>22.44.66.88</mgIpAddr>
          <mgProtocolPort>88</mgProtocolPort>
        </Parameters>
      </assocMG>
    </Methods>
  </Command>
</CommandList>
```

Example format of successful **changeMG** response to change IP and Port:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Response>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <changeMG usn="1" version="1.0">
        <RC>0</RC>
        <mgUIName>H323_M1</mgUIName>
        <MsgTxt>H323_M1 Change MG Successful.
          All Change MG requests have been processed.</MsgTxt>
      </changeMG>
    </Methods>
  </Response>
</CommandList>
```

Example format of failed **changeMG** response to change IP and Port:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Response>
    <Interface>cs2KCfgMgrIf</Interface>
    <Methods>
      <changeMG usn="1" version="1.0">
        <RC>43</RC>
        <MsgTxt>* H323_M1 Change MG Failed - Invalid MG Name
          All Change MG requests have been processed.</MsgTxt>
      </changeMG>
    </Methods>
  </Response>
</CommandList>
```

Example format of **changeMG** Capacity

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList >
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      < changeMG usn="1" version="1.0" >
        <Parameters>
          <mgUIName>H323_M1</mgUIName>
          <reservedTerminations>500</reservedTerminations>
        </Parameters>
      </assocMG>
    </Methods>
  </Command>
</CommandList>
```

Example format of successful **changeMG** response to change Capacity:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Response>
    <Interface>cs2KCfgMgrIf</Interface>
    <Methods>
      <changeMG usn="1" version="1.0">
        <RC>0</RC>
        <mgUIName>H323_M1</mgUIName>
        <MsgTxt>H323_M1 Change MG Successful.
          All Change MG requests have been processed.</MsgTxt>
      </changeMG>
    </Methods>
  </Response>
</CommandList>
```

Example format of failed **changeMG** response to change Capacity

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Response>
    <Interface>cs2KCfgMgrIf</Interface>
    <Methods>
      <changeMG usn="1" version="1.0">
        <RC>43</RC>
        <MsgTxt>* H323_M1 Change MG Failed - Invalid MG Name
          All Change MG requests have been processed.</MsgTxt>
      </changeMG>
    </Methods>
  </Response>
</CommandList>
```

Command Examples for Associate MG command

The command syntax for assocMG command has not changed from prior releases in reference to adding H.323 GWs. The syntax is listed here as a convenience and to highlight that the reserved terminations tag is now optional for H.323 GWs.

Example format of an **assocMG** command

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <assocMG usn="1" version="1.0">
        <Parameters>
          <mgUIName>H323_M1</mgUIName>
          <mgProfileName>CISCO_2600</mgProfileName>
          <mgIpAddr>47.49.23.43</mgIpAddr>
          <mgProtocolType>6</mgProtocolType>
          <mgProtocolVersion>4.0</mgProtocolVersion>
          <mgProtocolPort>2427</mgProtocolPort>
          <gwcUIName>GWC-0</gwcUIName>
          <reservedTerminations>200</reservedTerminations>
        </Parameters>
      </assocMG>
    </Methods>
  </Command>
</CommandList>
```

Command Examples for Add Carrier command

The addCarrier command is an existing XML interface that is now used to provision H.323 EPGs. After adding a H.323 GW this command should be used to populate the terminations. The firstTN tag is optional and is used to dictate the starting location of a contiguous block of 24 or 31 EPs.

Example format of an **addCarrier** command **with optional firstTN** tag:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList >
  <Command>
    <Interface>EndptGrpProvIf</Interface>
    <Methods>
      <addCarrier usn="1" version="1.0" >
        <Parameters>
          <mgName>H323_M1</mgName>
          <carrierName>EPG_001</carrierName>
          <firstTN>649</firstTN>
        </Parameters>
      </addCarrier>
    </Methods>
  </Command>
</CommandList>
```

Example format of an **addCarrier** command **without optional firstTN** tag

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList >
  <Command>
    <Interface>EndptGrpProvIf</Interface>
    <Methods>
      <addCarrier usn="1" version="1.0" >
        <Parameters>
          <mgName>H323_M1</mgName>
          <carrierName>EPG_001</carrierName>
        </Parameters>
      </addCarrier>
    </Methods>
  </Command>
</CommandList>
```

Example format of successful **addCarrier** response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Response>
    <Interface>EndptGrpProvIf</Interface>
    <Methods><addCarrier usn="1" version="1.0">
      <ReturnData>
        <Row><firstTID>649</firstTID>
          <numberOfTids>24</numberOfTids></Row>
        <RC>0</RC>
        <MsgTxt>Add CARRIER operation was successful</MsgTxt>
      </ReturnData>
    </Methods>
  </Response>
</CommandList>
```

Example format of failed **addCarrier** response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Response>
    <Interface>EndptGrpProvIf</Interface>
    <Methods><addCarrier usn="1" version="1.0">
      <MethodName>queryMG</MethodName>
      <RC>4</RC>
      <MsgTxt>EGP> The mgName does not have corresponding MG UI
    name <MsgTxt>
    </Methods>
  </Response>
</CommandList>
```

Command Examples for List All Carriers command

The list all carriers command is an existing command that is now used to view mappings for H.323 EPGs. This command replaces the queryEndpointGroup command that was used in pre-SN07 releases. Several different tag filters are available to determine the scope of listings. For more details concerning other filters, refer to the schema later in this document.

Example format of **listAllCarriers** command with GWC filter:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList >
  <Command>
    <Interface>EndptGrpProvIf</Interface>
    <Methods>
      <listAllCarriers usn="1" version="1.0">
        <Parameters>
          <FILTER_GWC>
            <gwcName>GWC-6</gwcName>
          </FILTER_GWC>
        </Parameters>
      </listAllCarriers>
    </Methods>
  </Command>
</CommandList>
```

Example format of successful **listAllCarriers** response

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
<Response>
<Interface>EndptGrpProvIf</Interface>
<Methods>
<listAllCarriers usn="1" version="1.0">
<ReturnData>
<gwc name="GWC-6">
  <mg name="H323_M1">
<carrier name="EPG_001">
<svcData>
<service>PRI</service>
<IID>7</IID>
</svcData>
<endptList>
<endPt name="EPG_001.1"><tid>36 1</tid></endPt>
<endPt name="EPG_001.2"><tid>36 2</tid></endPt>
:
:
<endPt name="EPG_001.22"><tid>36 22</tid></endPt>
<endPt name="EPG_001.23"><tid>36 23</tid></endPt>
<endPt name="EPG_001.24"><tid>36 24</tid></endPt>
</endptList>
</carrier>
<carrier name="EPG_002">
<svcData>
<service>ISUP</service>
</svcData>
<endptList>
<endPt name="EPG_002.1"><tid>36 1401</tid></endPt>
<endPt name="EPG_002.2"><tid>36 1402</tid></endPt>
<endPt name="EPG_002.3"><tid>36 1403</tid></endPt>
:
:
<endPt name="EPG_002.22"><tid>36 1422</tid></endPt>
<endPt name="EPG_002.23"><tid>36 1423</tid></endPt>
<endPt name="EPG_002.24"><tid>36 1424</tid></endPt>
</endptList>
</carrier>
</mg>
</gwc>
<RC>0</RC>
<MsgTxt>
Retrieval of Carriers Successfully Completed. </MsgTxt>
</ReturnData>
</listAllCarriers>
</Methods>
</Response>
</CommandList>
```

Failed response to **listAllCarriers** command

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Response>
    <Interface>EndptGrpProvIf</Interface>
    <Methods>
      <listAllCarriers usn="1" version="1.0">
        <MethodName>listAllCarriers</MethodName>
        <RC>4</RC>
        <MsgTxt> The gwcName does not have corresponding Gateway
Controller</MsgTxt>
      </listAllCarriers>
    </Methods>
  </Response>
</CommandList>
```

Command examples of Disassociate MG

Tags values for the disAssocMG XML command are not changed in the SN07 release. Functionality for issuing this command has changed, however. Command syntax is listed here as a convenience to the reader.

Example format of **disAssocMG** command

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList >
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <disAssocMG usn="1" version="1.0">
        <Parameters>
          <mgUIName>H323_M1</mgUIName>
        </Parameters>
      </disAssocMG>
    </Methods>
  </Command>
</CommandList>
```

Command examples of Delete Carrier

Tags values for the delete carrier XML command are not changed in the SN07 release. Functionality for issuing this command has changed, however. Command syntax is listed here as a convenience to the reader.

Example format of **Delete Carrier**

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList >
  <Command>
    <Interface>EndptGrpProvIf</Interface>
    <Methods>
      <deleteCarrier usn="1" version="1.0">
        <Parameters>
          <mgName>H323_M1</mgName>
          <carrierName>EPG_000</carrierName>
        </Parameters>
      </deleteCarrier>
    </Methods>
  </Command>
</CommandList>
```


XML Schema Listings for affected H.323 commands

Change MG

The XML tags for the changeMG have been changed in the SN07 release. In SN06.0 and prior releases, the choice of “profile” or “capacity” was listed. Underlying server code did not support “profile” changes using this command so this tag has been removed. New tags “mgIpAddr” and “mgProtocolPort” have been added as optional parameters. With the new schema, the user has the ability to include the reserved termination choice or the IP and/or Port choice, but, cannot list both choices within a single transaction. Since the IP and Port tags have been made optional, the user can include either or both within a single transaction. Note that failure to include any of the choice tags will result in a failed operation.

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  version="1.0"
  xml:lang="en" >
  <!--
  ****
  ****
  **** -->
  <!-- * Define changeMG Method Parameters -->
  <!--
  ****
  ****
  **** -->
  <xsd:complexType name="changeMGMethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="changeMGParamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="changeMGParamsType">
    <xsd:sequence>
      <xsd:sequence>
        <xsd:element name="mgUIName" type="NoSpaceNameType" />
      </xsd:sequence>
    </xsd:choice>
    <xsd:element name="reservedTerminations" type="ReservedTerminationsType" />
    <xsd:sequence>
      <xsd:element name="mgIpAddr" type="IPAddressType" minOccurs="0" />
      <xsd:element name="mgProtocolPort" type="xsd:unsignedShort" minOccurs="0" />
    </xsd:sequence>
  </xsd:choice>
  </xsd:sequence>
  </xsd:complexType>
</xsd:schema>
```

Tag value definitions listed in cs2kcfbase:

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  version="1.0"
  xml:lang="en" >
  <!--
  ****
  ****
  **** -->
  <!-- ** Global Attribute Groups Used by all schemas -->
```

```
<!--
*****
***** -->

<!-- ***** -->
<!-- * Define Common Usn_Version Attribute Group-->
<!-- ***** -->
<xsd:attributeGroup name="Usn_VersionAttrbGroup" >
  <xsd:attribute name="usn" type="xsd:integer" use="required" />
  <xsd:attribute name="version" type="xsd:decimal" default="1.0" use="optional" />
</xsd:attributeGroup>
<!--
*****
***** -->
<!-- ** Global Complex Types Used by all schemas -->
<!--
*****
***** -->
<!--
*****
***** -->
<!-- * Global Simple Types Used or Useable by all schemas follows: -->
<!--
*****
***** -->
<!--
*****
***** -->
<!-- * Define No Space Name Type -->
<!--
*****
***** -->
<xsd:simpleType name="NoSpaceNameType">
  <xsd:restriction base="xsd:token">
    <xsd:minLength value="1" />
    <xsd:pattern value="\S{1,32}" />
  </xsd:restriction>
</xsd:simpleType>
<!--
*****
***** -->
<!-- * Define IPAddressType-->
<!--
*****
***** -->
<xsd:simpleType name="IPAddressType">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}" />
  </xsd:restriction>
</xsd:simpleType>
<!--
*****
***** -->
<!-- * Define MGProtocolType-->
<!--
*****
***** -->
<xsd:simpleType name="MGProtocolType">
  <xsd:restriction base="xsd:integer">
    <xsd:minInclusive value="1" />
    <xsd:maxInclusive value="6" />
    <xsd:pattern value="\d{1}" />
  </xsd:restriction>
</xsd:simpleType>
<!--
*****
***** -->
<!-- * Define GWCNameType-->
```

```

<!--
*****
***** -->
<xsd:simpleType name="GWCNameType">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="GWC-\d\d?\d?" />
  </xsd:restriction>
</xsd:simpleType>
<!--
*****
***** -->
<!-- * Define ReservedTerminationsType -->
<!--
*****
***** -->
<xsd:simpleType name="ReservedTerminationsType">
  <xsd:restriction base="xsd:integer">
    <xsd:minInclusive value="0" />
    <xsd:maxInclusive value="6400" />
  </xsd:restriction>
</xsd:simpleType>
<!--
*****
***** -->
<!-- * Define IpPortType -->
<!--
*****
***** -->
<xsd:simpleType name="IpPortType">
  <xsd:restriction base="xsd:integer">
    <xsd:minInclusive value="0" />
    <xsd:maxInclusive value="65535" />
  </xsd:restriction>
</xsd:simpleType>
<!--
*****
***** -->
<!-- * Define MGSiteNameType -->
<!--
*****
***** -->
<xsd:simpleType name="MGSiteNameType">
  <xsd:restriction base="NoSpaceNameType">
    <xsd:maxLength value="4" />
  </xsd:restriction>
</xsd:simpleType>
</xsd:schema>

```

Assoc MG

No changes have been made to this schema. This interface should be used in a similar manner as it was in prior releases, however, automatic addition of EPGs will not be realized.

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  version="1.0"
  xml:lang="en" >
  <!--
  *****
  ***** -->
  <!-- * Define AssocMG Method Parameters -->

```

```

<!--
*****
***** -->
<xsd:complexType name="assocMGMethodType">
  <xsd:all>
    <xsd:element name="Parameters" type="assocMGParamsType" />
  </xsd:all>
  <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
</xsd:complexType>
<xsd:complexType name="assocMGParamsType">
  <xsd:sequence>
    <xsd:element name="mgUIName" type="NoSpaceNameType" />
    <xsd:element name="mgProfileName" type="NoSpaceNameType" />
    <xsd:element name="mgIpAddr" type="IPAddressType" />
    <xsd:element name="mgProtocolType" type="MGProtocolType" />
    <xsd:element name="mgProtocolVersion" type="xsd:decimal" />
    <xsd:element name="mgProtocolPort" type="xsd:unsignedShort" />
    <xsd:element name="mgSiteName" type="MGSiteNameType" minOccurs="0" />
    <xsd:element name="gwcUIName" type="GWCNameType" minOccurs="0" />
    <xsd:element name="reservedTerminations" type="ReservedTerminationsType" minOccurs="0" />
    <xsd:choice minOccurs="0">
      <xsd:element name="pepServerName" type="xsd:token" />
      <xsd:element name="NATname" type="xsd:token" />
    </xsd:choice>
  </xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

Add Carrier

The add carrier has not been changed from previous releases but is listed here for convenience since this interface is now required to add a EPG to a H.323 GW. It should be pointed out that although internally, H.323 GWs are provisioned as PRI trunk types, this tag and the subsequent IID value should not be input as a tag because these values are auto calculated and provisioned by the system. Input of these values is ignored if the user mistakenly inputs them.

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  version="1.0"
  xml:lang="en" >
  <!-- ***** -->
  <!-- * Define AddCarrier Method Parameters -->
  <!-- ***** -->
  <xsd:complexType name="addCarrierMethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="addCarrierParamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="addCarrierParamsType">
    <xsd:sequence>
      <xsd:element name="mgName" type="CarMGNameType" />
      <xsd:element name="carrierName" type="CarrierNameType" />
      <xsd:element name="svcData" type="svcDataType" minOccurs="0" maxOccurs="1"/>
      <xsd:element name="firstTN" type="firstTNType" minOccurs="0" maxOccurs="1" />
    </xsd:sequence>
  </xsd:complexType>
  <!-- ***** -->
  <!-- * Define svcDataType -->
  <!-- ***** -->
  <xsd:complexType name="svcDataType">
    <xsd:choice>

```

```

    <xsd:element name="PRI" type="PRISvcType" />
    <xsd:element name="V5.2" type="V5.2SvcType" />
    <xsd:element name="ISUP" type="xsd:string" fixed="" />
    <xsd:element name="H.323" type="xsd:string" fixed="" />
  </xsd:choice>
</xsd:complexType>
<!-- ***** -->
<!-- * Define PRISvcType -->
<!-- ***** -->
<xsd:complexType name="PRISvcType">
  <xsd:sequence>
    <xsd:element name="IID" type="firstTNType" />
  </xsd:sequence>
</xsd:complexType>
<!-- ***** -->
<!-- * Define V5.2SvcType -->
<!-- ***** -->
<xsd:complexType name="V5.2SvcType">
  <xsd:sequence>
    <xsd:element name="v5.2IId" type="firstTNType" />
    <xsd:element name="v5.2LinkId" type="firstTNType" />
    <xsd:element name="v5.2UALinkId" type="firstTNType" />
  </xsd:sequence>
</xsd:complexType>

<!-- ***** -->
<!-- * Define firstTNType -->
<!-- ***** -->
<xsd:simpleType name="firstTNType">
  <xsd:restriction base="xsd:integer">
    <xsd:minInclusive value="1" />
    <xsd:maxInclusive value="4094" />
  </xsd:restriction>
</xsd:simpleType>

</xsd:schema>

```

List All Carriers

The list all carriers schema is an existing interface that should be used to view Endpoint/TID mappings. This interface replaces the SN06.0 queryEndpointGroup interface. No changes have been made to this interface for SN07, but, since it is now a required interface to list mappings for H.323 GWs it is listed here as a convenience.

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  version="1.0"
  xml:lang="en" >
  <!-- ***** -->
  <!-- * Define listAllCarriers Method Parameters -->
  <!-- ***** -->
  <xsd:complexType name="listAllCarriersMethodType">
    <xsd:sequence>
      <xsd:element name="Parameters" type="listAllCarParamsType" />
    </xsd:sequence>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="listAllCarParamsType">
    <xsd:choice>
      <xsd:element name="FILTER_ALL" type="xsd:string" fixed="" />
      <xsd:element name="FILTER_GWC" type="filterGWCType" />
      <xsd:element name="FILTER_MG" type="filterMGType" />
      <xsd:element name="FILTER_CARRIER" type="filterCarType" />
    </xsd:choice>
  </xsd:complexType>

```

```

    </xsd:choice>
  </xsd:complexType>
  <xsd:complexType name="filterMGType">
    <xsd:sequence>
      <xsd:element name="mgName" type="CarMGNameType" />
    </xsd:sequence>
  </xsd:complexType>
  <xsd:complexType name="filterCarType">
    <xsd:sequence>
      <xsd:element name="mgName" type="CarMGNameType" />
      <xsd:element name="carrierName" type="CarrierNameType" />
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>

```

Disassociate MG

Tags values for the disAssocMG XML command are not changed in the SN07 release. Schema's is listed here as a convenience to the reader.

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  version="1.0"
  xml:lang="en" >
  <!--
  *****
  ***** -->
  <!-- * Define disAssocMG Method Parameters -->
  <!--
  *****
  ***** -->
  <xsd:complexType name="disAssocMGMethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="disAssocMGParamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="disAssocMGParamsType">
    <xsd:sequence>
      <xsd:element name="mgUIName" type="NoSpaceNameType" />
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>

```

Delete Carrier

Tags values for the Delete Carrier XML command are not changed in the SN07 release. Schema's are listed here as a convenience to the reader.

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  version="1.0"
  xml:lang="en" >
  <!--
  *****
  ***** -->
  <!-- * Define deleteCarrier Method Parameters -->
  <!--
  *****
  ***** -->
  <xsd:complexType name="deleteCarrierMethodType">
    <xsd:all>

```

```
<xsd:element name="Parameters" type="delCarrierParamsType"/>
</xsd:all>
<xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
</xsd:complexType>
<xsd:complexType name="delCarrierParamsType">
  <xsd:sequence>
    <xsd:element name="mgName" type="CarMGNameType" />
    <xsd:element name="carrierName" type="CarrierNameType" />
  </xsd:sequence>
</xsd:complexType>
</xsd:schema>
```

Configuration Walkthrough

As previously mentioned, H.323 provisioning rules have changed from the 6.0 to the SN07 release. The following sections give a quick overview of operations used for provisioning and highlight the differences in the 2 releases. The operations are supported using either the CMT GUI or the XML interfaces except where indicated.

Adding a H.323 EPG

- SN06.0
 - Add a H.323 GWC to the system
 - Associate GW with the GWC
 - Adds GW to GWC
 - Adds EPG to GW
 - Picks starting TID automatically
 - Requires query to identify TID information for table TRKMEM
- SN07
 - Add a H.323 GWC to the system
 - Associate GW with the GWC
 - Adds a GW to GWC
 - Reserves TID space for EPGs
 - Add EPGs to GW using Add Carrier command
 - Allows users to specify starting TID
 - Consistent with PVG trunking
 - Repeat this step for the desired number of EPs and EPGs
 - Query can be used to identify TID information if desired

Deleting a H.323 GW

- SN06.0
 - Ensure EPs on the GW are in an Out Of Service state

- Select the GW to delete and issue disassociate MG command
 - Deletes EPGs from the GW
 - Deletes GW
- SN07
 - Ensure EPs on the GW are in an Out Of Service state
 - Delete EPGs from GW using Delete Carriers command
 - Repeat this step until all EPGs are removed
 - Delete GW using Disassociate MG command

Increasing the Reserved Capacity for a H.323 GW

- SN06.0
 - Not available
- SN07
 - Select the GW from the GW GUI and issue change operation
 - Change value must be less than or equal to maximum value as dictated by GWs profile
 - GWC must have enough TID locations unreserved to accommodate change as dictated by the GWCs profile
 - Add additional EPGs to GW using Add Carrier command
 - Allows users to specify starting TID
 - Consistent with PVG trunking
 - Repeat this step for the desired number of EPs and EPGs
 - Query can be used to identify TID information if desired

Decreasing the Reserved Capacity for a H.323 GW

- SN06.0
 - Not available
- SN07
 - Select and remove EPGs that are over the new lower limit if necessary using the Delete Carrier operation
 - Select the GW from the GW GUI and issue change operation

- Decreases TID reserve capacity allocated for GWC
- Does not remove any EPs

SN07 Feature Deltas

Product = CS 2000

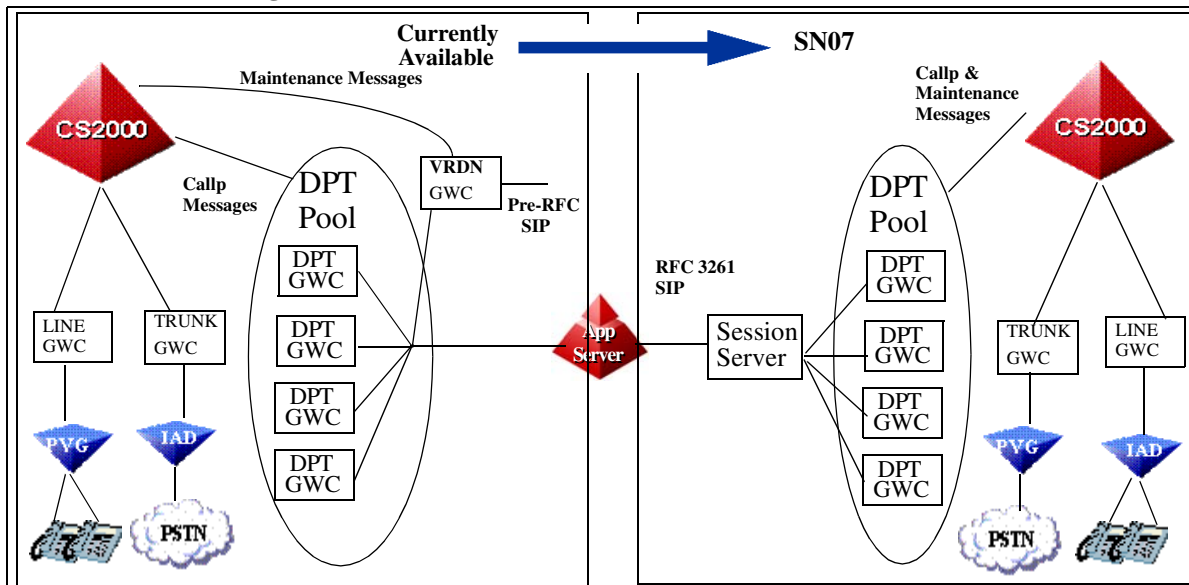
A00004005 -- NCGL Support for SAM XTS and SP2000 (PT-IP)

Functional Description (FN)

Overview

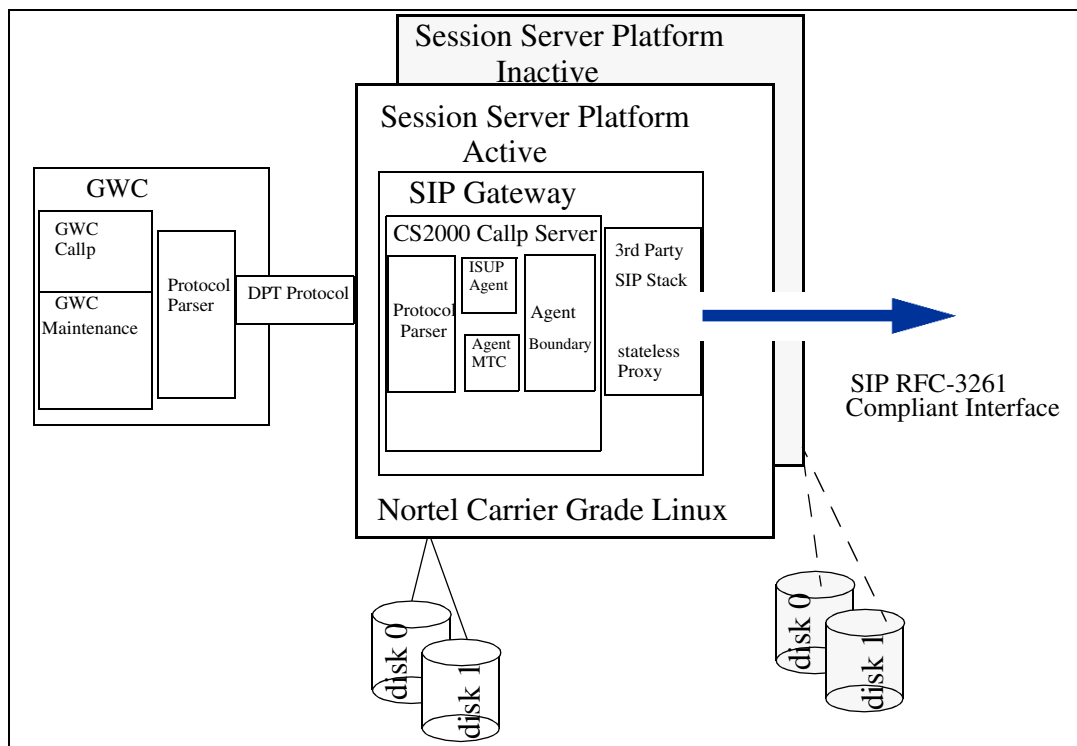
The purpose of this design is to create a highly available base platform for delivery of multiple applications. The Session Server consists of a Network Equipment-Building System (NEBS) Level 3 compliant hardware platform plus a software framework and architecture for developing Carrier Grade applications and services.

Design Intent of Session Server Platform



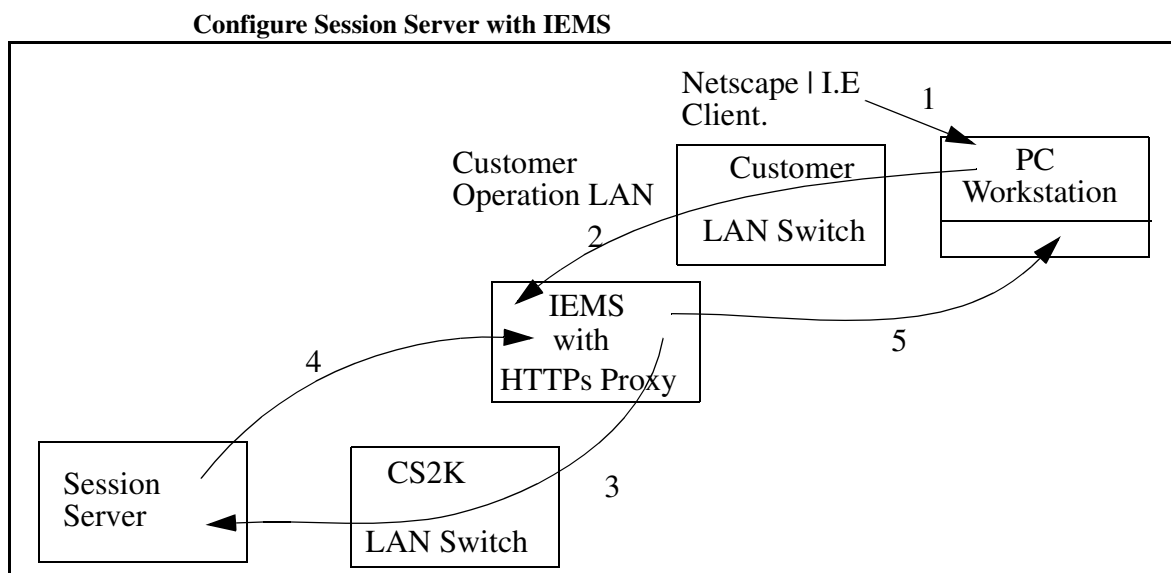
In the SN07 release, the architecture for the Session Server will consist of a mated pair of Services Application Module- eXtreme Thin Server (SAM-XTS) with a configuration similar to that of gateway controller. The units consists of an active and inactive unit. Each unit is in reality a fully functional Session Server that is interconnected via a gigabit ethernet LAN as shown in the following figure. Each server provides processor capacity, local disk storage, and high-bandwidth network connectivity.

Mated Pair Session Server



The Session Server can be configured to use the Integrated Element Manager System (IEMS) between the customer operation LAN and the Call Server 2000(CS2K) LAN or it can be configured without the IEMS.

The following figure shows a proposed configuration with IEMS, where an Hypertext Transfer Protocol (HTTP) proxy is configured on the IEMS to redirect the Netscape/Internet Explorer browser to the Session Server.



The configuration steps include:

1. user point the browser to web link on the IEMS
2. IEMS invoke the HTTPs proxy
3. the HTTPs proxy on the IEMS will redirect the link to the Session Server
4. Session Server will reply back to IEMS
5. IEMS will in turn respond to user request

The SIP Gateway application is the initial application for the Session Server platform, with the intention to provide a reusable infrastructure that can support additional applications. For complete details on the SIP Gateway Application, please refer to the latest version of the functional description section for feature A00003933.

Hardware Requirements or Dependencies

The Session Server technology is based on the SAM-XTS a second generation 2U NEBS compliant server from Intel. It is the same chassis as the currently shipping SAM-XTS for STORM, but adds additional CPUs and more RAM.

Each server will be equipped with:

- Dual Intel 2.4 GHz P4 Xeon Processors
- 4 GB RAM is the Standard - could have up to 12 GB RAM
- Memory Speed - 266 MHz DDR
- Local Disk - Dual hot swap 73GB
- Multiple GigE copper interfaces(2 on board + 2 Port NIC)

- NEBS Level 3 compliant
- 2U Form Factor

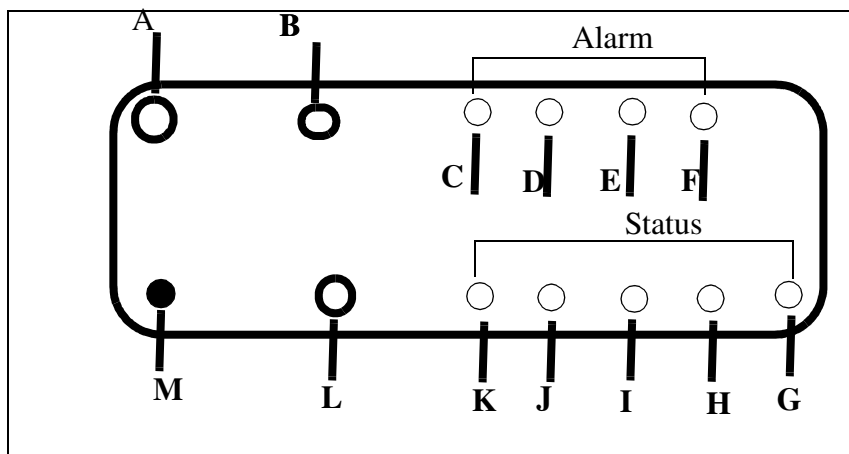
The field replaceable components on the Session Server are:

- Hard disk
- Power supply
- CD drive

Front/Back Panel Features and LEDs

The Session Server front panel features and LEDs are shown in Figure , "Front Panel LEDs on The Session Server".

Front Panel LEDs on The Session Server



Something worth noting here is only the most critical alarm LED is illuminated. For example, if a minor alarm is present and a major alarm occurs, the minor alarm data will be retained; only the major alarm LED will be illuminated. If the condition that set the minor alarm previously still exists when the major alarm is cleared, the minor alarm will once again become illuminated.

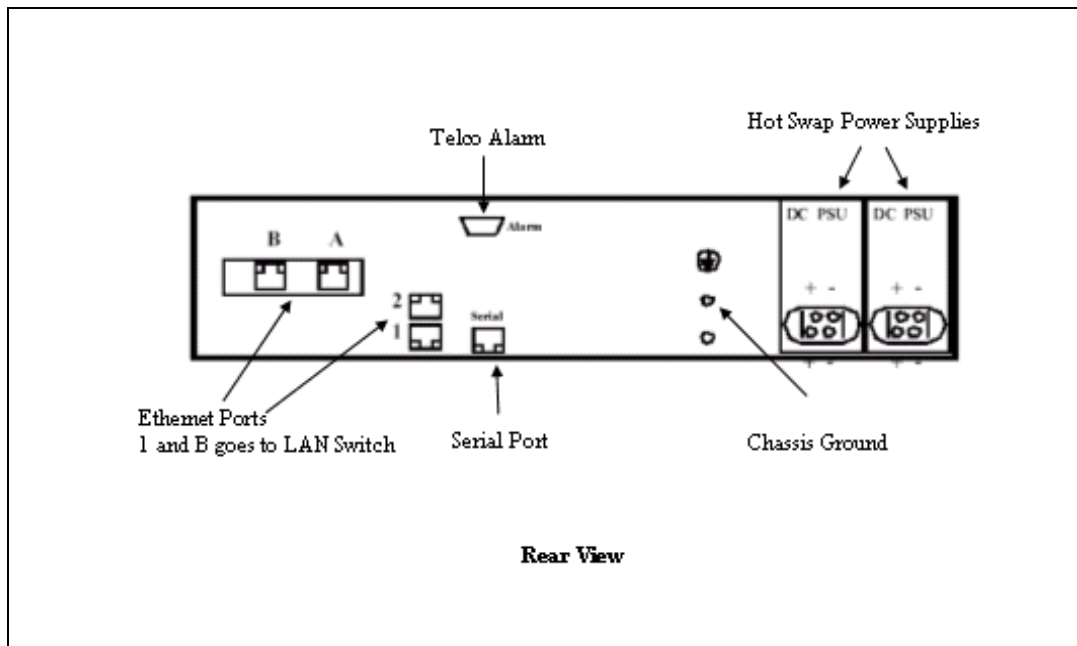
Front Panel Features

Item	Feature	Description
Front Panel Switches		
A	Power switch	Toggle the server power
B	Reset switch	Reset the server
L	ID switch	Toggles server ID LED
Front Panel Alarm LEDs and		
C	Critical CRT (red)	When continuously lit, indicates the presence of a critical system fault.

Item	Feature	Description
D	Major MJR (red)	When continuously lit, indicates the presence of a major system fault.
E	Minor MNR (red)	When continuously lit, indicates the presence of a minor system fault.
F	Power (amber)	When continuously lit, indicates the presence of a power system fault. The front panel power alarm relay will be engaged.
Front Panel Status LEDs		
G	Disk 0 Activity/Fault LED (green or red)	Indicates disk 0 SCSI hard drive activity when green, or a disk 0 SCSI hard drive fault when red. When flashing green/red indicates that disk 0 is rebuilding disk array.
H	Disk 1 Activity/Fault LED (green or red)	Indicates disk 1 SCSI hard drive activity when green, or a disk 1 SCSI hard drive fault when red. When flashing green/red indicates that disk 1 is rebuilding disk array.
I	Main power LED (green)	When continuously lit, indicates the presence of DC power in the server. The LED goes out when the power is turned off or the power source is disrupted.
J	NIC0/NIC1 activity LED (green)	Indicates activity on either NIC0 or NIC1.
K	System ID LED (green)	Indicates any system SCSI hard drive activity.

The connection ports on the rear view of the Session Server is shown in the following figure.

Connection Ports



Software Requirements or Dependencies

The Session Server software has a layered architecture, which consists of the following:

- The base NCGL layer, running on Linux version 2.4 kernel.
- An application layer that includes a maintenance process for each application, which manages the associated processes.

The software running on this server has the following features:

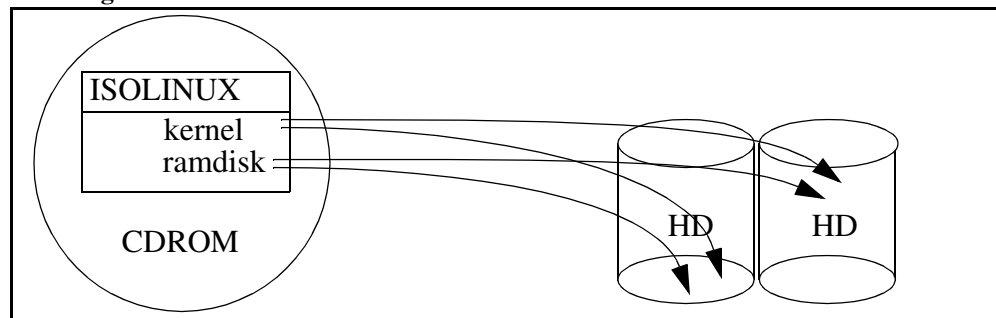
- Linux operating system
- Maintenance applications for node maintenance, fault detection, and failover
- Apache Web server for provisioning and maintenance

The Session Server has its own requirements in terms of software delivery and upgrade.

Software Delivery

The Session Server software load packages the kernel and ramdisk images using CDROM as the software delivery mechanism. The CDROM will be bootable, so that software installation and upgrades are as simple as inserting the CD into the drive and rebooting. The software installation procedure is done separately on a per Session Server unit.

CD Image Installation to Hard Disks



Software Upgrade

The Session Server web interface contains a section under the admin panel to allow for upgrade to new load, as shown in Figure , on page 1634 . The customer can select a default boot load as well as remove any older loads, which may no longer be needed. Space will be reserved on the hard drive to maintain approximately 3 or 4 Session Server loads in case fallback to a previous load is required. Further, it will allow for an upgrade of the Session Server load from either a CD inserted in the CDROM drive, from an ISO image located on the network, or from a Session Server CD mounted

elsewhere in the network (via FTP). In summary the supported upgrade methods are:

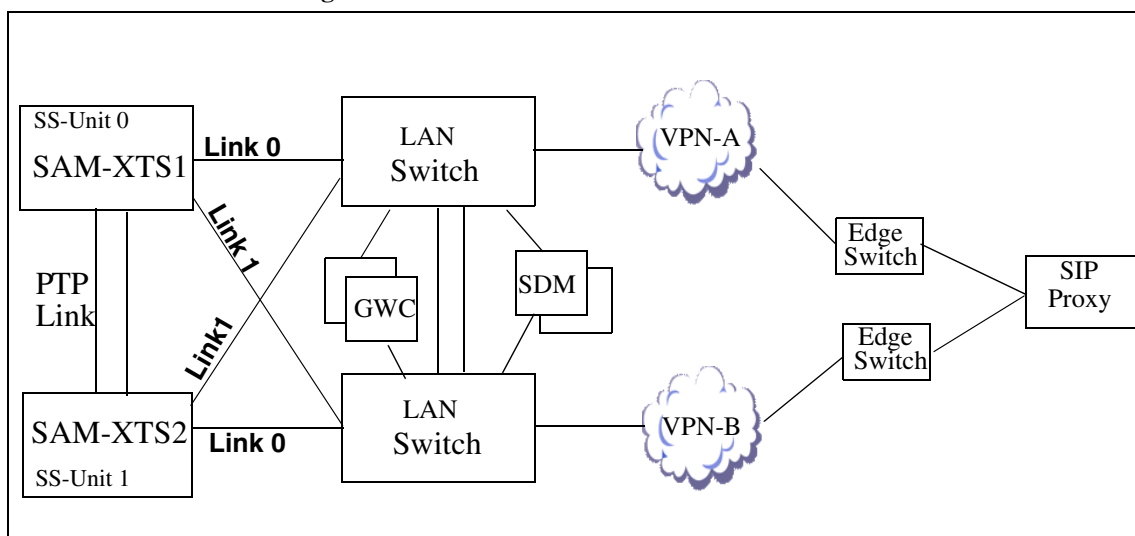
- local cdrom
- local file (iso image, or load.tgz from CDROM)
- remote file via ftp (iso image, or load.tgz from CDROM)
- remote file via http (iso image, or load.tgz from CDROM)
- remote file via https (iso image, or load.tgz from CDROM)

Note: This section addresses the upgrade of a simplex Session Server. More details will be added to this section to support the upgrade of a duplex Session Server.

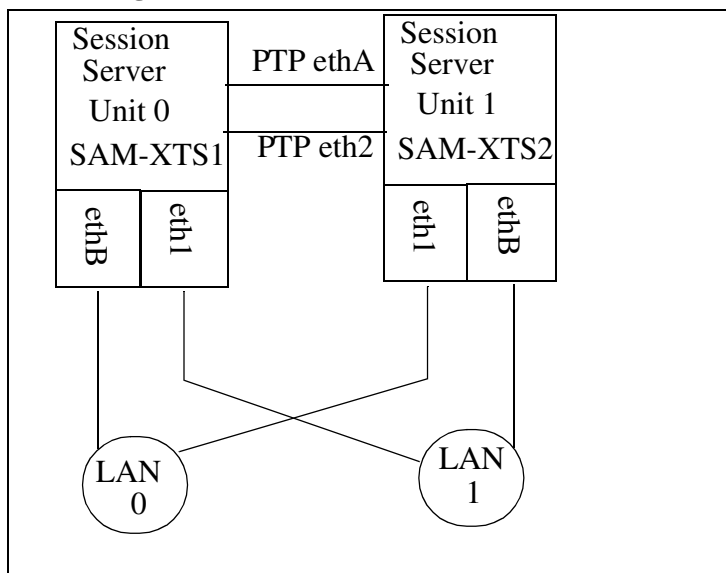
Network Connectivity

Each Session Server (SS) is configured with two GigE interfaces directed to the LAN switch, as represented by link 0 and link 1 in the following figure. In addition, two interfaces connect unit 0 to unit 1, shown as the Point To Point (PTP) link.

Link Configuration of the Session Server



The following figure shows an example of the link configuration on the Session Server where “ethB” of each server is connected directly to the LAN switch, and “eth1” is connected to the alternative LAN switch.

Link Configuration for Session Server**Session Server IP addresses**

The Session Server requires a block of eight consecutive IP addresses that have to be on the same subnet as the Call Server (CS) LAN. The customer determines the IP addresses. The last octet of the IP address must be divisible by 8. Refer to the following figure. It is worth indicating that the PTP IP addresses are internally set by the system to 192.168.1.1 and 192.168.1.2.

Example of Session Server Configuration

Session Server IP addresses	Example Unit 0	Example Unit 1	Datafilled By user	Description
Active Node ^a	172.16.16.72	172.16.16.72	no	Logical application
Inactive Node	172.16.16.71	172.16.16.71	no	Logical application
Local unit	172.16.16.67	172.16.16.70	yes	Logical unit link
Local unit, Link 0	172.16.16.65	172.16.16.68	no	Physical unit link
Local unit, Link 1	172.16.16.66	172.16.16.69	no	Physical unit link
Mate unit	172.16.16.70	172.16.16.67	yes	Logical unit link
Mate unit, Link 0	172.16.16.68	172.16.16.65	no	Physical unit link
Mate unit, Link 1	172.16.16.69	172.16.16.66	no	Physical unit link
Local PTP link 0	192.168.1.1	192.168.1.2	no	Local point to point link ^b
Mate PTP link 1	192.168.1.2	192.168.1.1	no	Mate point to point link

a. Active node last set of digits must be divisible by 8

b. The IP addresses **192.168.1.1/192.168.1.2** are assigned to the local/mate Point to Point (PTP) links. To avoid conflict, make sure **not** to assign the same IP addresses for the Session Server.

Session Server OA&M

This section discusses Operations, Administration, and Maintenance (OA&M) topics for the new Session Server platform.

As mentioned earlier, the architecture for the Session Server will consist of a dual unit configuration similar to that of gateway controllers. The units consists of an active and inactive unit. Both units have the ability to raise alarms and generate logs. The alarms raised on the active and inactive units can be viewed from either unit. However, the logs can be viewed on the same unit that generated the log.

Web Based OAM

The Session Server runs its own Element Manager (EM). This means that the web server runs locally on the Session Server. Which in turn means that maintenance type activities for the Session Server also take place on the Session Server.

The craftsperson uses a web based interface to perform the maintenance activities. This interface consists of a web server running on the Session Server that provides maintenance and monitoring related web pages.

The web agent is the browsing application which will be used to display the Session Server EM. The supported browsers are:

- Internet Explorer 5.5+
- Netscape Navigator 6.0+

Netscape is supported on both PC (Windows) and Solaris clients, but not on Linux clients. It is worth mentioning here that the browser will redirect the IP of the web client so it always refers to the local unit IP address. Refer to the following table for an example.

Apache IP address redirect configuration

Incoming IP	Redirect IP
active IP	Local unit (0/1) IP
Inactive IP	Local unit (0/1) IP
Local unit (0/1) IP	no

All Session Server web pages are divided into three areas:

- **Header**

The area with the Nortel logo and the “Platform”, “Application”, and “Help” tags. All functions will be performed under the “Platform Tag”.

- **Menu Frame**

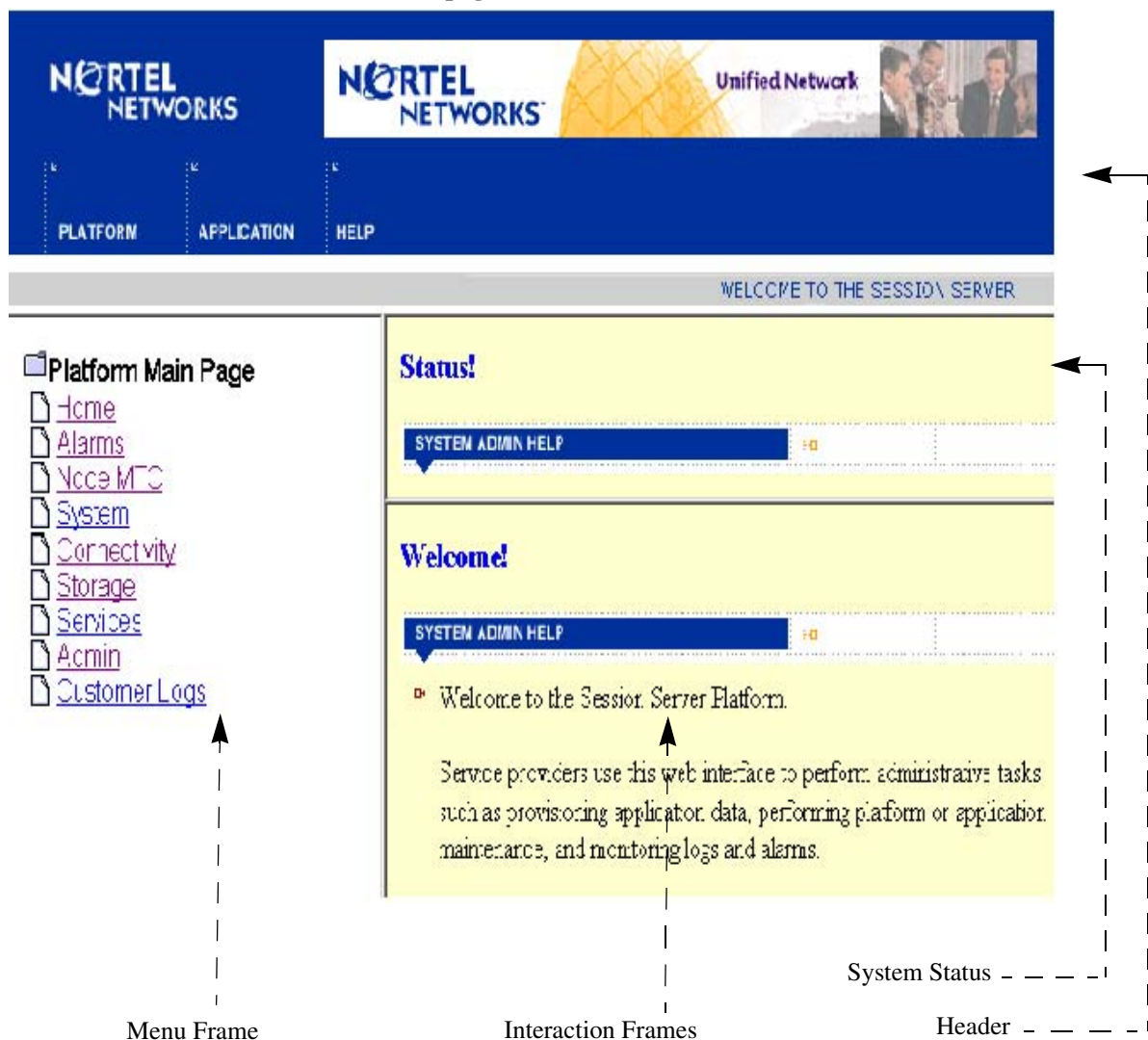
The user uses the menu bar on the left to locate the proper function in the web page hierarchy.

- **Interaction Frame**

This area is where a user fills in forms, performs maintenance actions, and obtains relevant information.

An example of the home page of the Session Server is shown in the following figure.

Session Server home page



Platform Main Page Links Description

Function	Description
Home	Displays basic system information in an introductory screen.
Alarms	Provides the ability to view alarm information which consists of type, id, timestamp, severity, and description.
Node MTC	Provides the ability to perform the node maintenance actions including swact and jam/unjam.
System	Provides the ability to view chassis data, CPU information, Process Information, and Memory Information.
Connectivity	Provides the connectivity status of local ethernet ports and network connectivity to the mate server and the ability to perform link maintenance actions such as lock/unlock, and swact.
Storage	Allows a view of file system data including partition specific data such as total space, used and available space.
Services	Provides the ability to view network active remote sessions and NTP information.
Admin	Allows the user to perform administrative tasks related to the system such as setting the timezone, bootload management to setup the default load, and software upgrade.
Customer Logs	Provides the ability to view customer related logs that are not application related.

System Status

The intention is to have the ability to view the status of both SS units at the same time when the user logs in. The status will be displayed as a frame on top of the interaction frame. Within the status frame the following information will be shown:

- unit activity status (Act/Inact)
- unit jam status (yes/no)
- ethernet link 0 status (“.”, “M”, “S”, “-”, “NA” Act/Inact)
- ethernet link 1 status (“.”, “M”, “S”, “-”, “NA” Act/Inact)
- point to point links status (“.”, “M”, “S”, “-”, “NA”)
- session server host name
- location

In order to display the system status, a PHP script will be used to pool the required information to display within the frame. The status frame will be refreshed every 30 seconds. The valid link states mapping is captured in the following table.

Mapping of link States

Link State	Description
.	INSV - In SerVice
M	MANB - MAN Busy
S	SYSB - SYStem Busy
-	UNEQUIP -UNEQUIpPed IP
NA	UNKNOWN

System Status Frame Layout

		Jam:	Link0:	Link1:	PTP Link	Hostname	Location
Unit 0	Act	no	. Act	. Inact	.	SS-1	RTPG
Unit 1	Inact	no	. Act	. Inact	.	SS-2	RTPG

Home

The home panel will display platform information for both Session Server units, which includes the following:

- Current date
- Time since last reboot
- System booted from
- Last restart cause
- Last power event cause
- Current version
- Platform IP Address
- Platform EM Client IP Address
- Server Location

Alarms

The Session Server has the capability to generate Alarms to report faults due to:

- network connectivity
- maintenance action failure

- mate communication
- disk usage
- memory usage
- disk mirroring failures

The alarms that are raised at this panel are the ones that are currently active on the system.

In addition, an application on the Session Server, such as the SIP Gateway application, has the ability to generate Alarms, Logs, and Operational Measurements (OM). The alarms that are raised on the Session Server are reported to the SNMP Trap destination server, if one is provisioned.

Alarms are formatted and displayed as defined in ITU-T Recommendation X.733 (Systems management: Alarm reporting function), as follows:

<Component id> <Type> <ID> <Timestamp> <Severity> <Description>

Component ID

The component ID was not part of the alarm table in Drop 1. It is going to be added to help identify the unit that reported the alarm. The component id will consist of at least the hostname, unit number, and location.

Type

The alarm type specifies the alarm category for the given alarm. Valid alarm types are:

Alarm Type (CCITT X.733)

1	Communications alarm
2	Quality of service alarm
3	Processing error alarm
4	Equipment alarm
5	Environmental alarm

ID

The alarm ID specifies, in general terms, why the given alarm was raised.

Examples of alarm IDs seen on Session Server are:

- Threshold Crossed
- Communications subsystem failure
- Loss of Signal

Please refer to section “ Appendix B - Alarms” on page 1636 for a complete list of alarm IDs.

Timestamp

The alarm timestamp specifies when the alarm was raised. The date and time given were current on the Session Server system when the given alarm was raised.

Severity

The alarm severity specifies the seriousness of the given alarm.

Alarm severity can be one of the following:

— Warning

Indicates the detection of a potential or impending service affecting fault.

— Minor

Indicates the detection of a non-service affecting fault condition and that corrective action should be taken in order to prevent a more serious fault.

— Major

Indicates that a service affecting condition has developed and an urgent corrective action is required.

— Critical

Indicates that a service affecting condition has developed and immediate corrective action is required.

Note: 'cleared' is also a valid alarm severity, but will not be seen on the Alarms Panel, since the Alarms Panel only shows alarms that are currently raised.

Description

The alarm description provides specific details about the given alarm.

Alarms Panel Limitations

- The Alarms Panel sort order cannot be modified (it defaults to sorting by severity then by time), nor does the Alarms Panel support filtering of alarms.
- The Alarms Panel header will scroll out of sight if the browser client is not large enough to view all alarms and the user scrolls to the bottom of the window.

- If the SS system date/time are changed after an alarm is raised, the Alarms Panel does not update its timestamps. The timestamps shown at the Alarms Panel were those current at the time that the alarms were raised.
- The Alarms Panel refreshes automatically every 45 seconds. The refresh period is set by the system and is not configured
- If the system threshold values are changed after an alarm is raised, the Alarms Panel does not update its values in the *description* field. The threshold values shown at the Alarms Panel are still the values that were current at the time that the alarms were raised. In general, any of the text in an alarm is valid from the time the alarm was raised and is never updated.
- A critical alarm will not necessarily cause the system to SWACT. For a complete list of conditions that could cause the system to reset please refer to section “Fault Handling” on page 1623.

Node Maintenance Actions

From the Session Server EM the user can perform node maintenance actions such as SWACT and JAM/UNJAM. The following figure shows the proposed layout for the node maintenance frame.

Node MTC Frame Layout

Title Session Server -Unit-0			
Operation State	Enabled	Stand by State	Providing Service
Activity State	Active	Jam State	no
Alarm State	Major (2)	Node Name	SS-2-UNIT-0
Loadname	1.0.0.0311262225	Unit IP Address	172.16.16.67

Title Session Server -Unit-1			
Operation State	Enabled	Stand by State	HotStandby
Activity State	Standby	Jam State	no
Alarm State	00 00 00	Node Name	SS-2-UNIT-1
Loadname	1.0.0.0311262225	Unit IP address	172.16.16.70

☐ Force

Swact

Jam

Unjam

This frame is accessible from the menu list, namely “Node MTC”. The unit that the user is logged into will be highlighted. If that unit reboots, then the

connectivity to that session will be lost. On the other hand, if the connection to the mate unit is lost, then all the fields for that unit will show unavailable status until the unit recovers.

System

The system panel is used to view system parameters for both Session Server units. However, modification actions to set system thresholds can be performed on the unit the user logged in to. From the system panel the following parameters are available:

- view Chassis Information (system self test, chassis subsystem).
- view CPU usage (shows 1 min, 5 mins, and 15 mins load average/threshold).
- view the number of zombie processes on (shows minor, major, and critical alarm thresholds).
- view memory usage.

Connectivity / Link Maintenance

This section discusses the connectivity panel where link maintenance can be performed. When selecting this tab, the user can view both unit's Ethernet connectivity status as well as perform link maintenance actions to lock/unlock and switch link activity. The following figure shows the connectivity frame layout. The list of IP addresses will be shown when selecting the QueryIP button. For a complete list of valid link status please refer to [Table "Mapping of link States" on page 1614](#).

Link MTC Frame Layout

Title Session Server -Unit-0				
	Status	Link Maintenance		
Local Link 0	• Act	Lock	Unlock	SwLnk
Local Link 1	• Inact	Lock	Unlock	SwLnk
PTP Link 0	• Act	Lock	Unlock	
PTP Link 1	• Act	Lock	Unlock	

Title Session Server -Unit-0				
	Status	Link Maintenance		
Local Link 0	• Act	<i>Lock</i>	<i>Unlock</i>	<i>SwLnk</i>
Local Link 1	• Inact	<i>Lock</i>	<i>Unlock</i>	<i>SwLnk</i>
PTP Link 0	• Act	<i>Lock</i>	<i>Unlock</i>	
PTP Link 1	• Act	<i>Lock</i>	<i>Unlock</i>	

Note: In SN07 actions on mate links is not supported.
Hence the gray color for lock/unlock/SwLnk.

Query IP

The query IP data is captured in a pop up window. The content of the query IP is shown in the following table.

Example of Query IP command output for unit 0

Description	IP Address
Local Point To Point	192.168.1.1
Local Link 0	172.16.16.65
Local Link 1	172.16.16.66
Local Unit	172.16.16.67
Active Unit	172.16.16.72
Inactive Unit	172.16.16.71
Mate Point To Point	192.168.1.1
Mate Link 0	172.16.16.68
Mate Link 1	172.16.16.69
Mate Unit	172.16.16.70

Disk Management

The Session Server EM has a storage panel which provides the following disk management functionality:

- view RAID array status
- disk maintenance
 - remove disk
 - insert disk
- view volume group information
- view filesystem information
- create a new filesystem
- remove a filesystem
- modify a filesystem

This panel displays information that is relevant to the local unit to which the browser is pointing.

Network Services

This panel is used to display the network active remote session status connected to the server and to view the NTP servers status.

This panel will display information specific to the Session Server unit the user is logged into. If the server local time gets out of sync with the NTP server, then the only way to resync the time is to reboot the inactive server, perform a swact, and reboot the newly inactive unit.

Admin

The admin panel is used to perform administrative tasks related to the Session Server unit. The actions supported from this panel are:

- Change Timezone Setting
- Bootload Management (to set default bootloader, or remove bootloader)
- Software Upgrade, the user has the following options to upgrade the bootloader:
 - Anonymous FTP
 - FTP
 - HTTP
 - HTTPS
 - Local File
 - Local CDROM

- Server Maintenance (reboot or halt)

Customer Logs

The Session Server provides the capability for the system or the application running to generate logs. The logs can be viewed on the Session Server's log view web page. Information shown about a particular log includes the fields shown in the following table. The Session Server generates different types of logs. This section, however, addresses the customer logs.

```
<time stamp> <hostname> <process name> <Name> <Number> <Severity> <Event Type> <Label>  
<Description>
```

```
* Nov 12 15:54:56 loopback alarmd: NXTS802 MINOR INIT Array: '/dev/md0'
```

*										
*									+---	description
*								+-----		label
*							+-----			event type
*						+-----				Severity
*					+-----					log number
*				+-----						log name
*			+-----							process name
*		+-----								hostname
*	+-----									time stamp

```
Nov 11 16:20:43 loopback alarmd: XTS301 MINOR INIT Array: '/dev/md0' (/boot) Status:  
The array is currently being rebuilt.
```

Example of Customer Logs Format

Name	Number	Severity	Event Type	Label	Description
NXTS	301	CLEARED , MINOR, MAJOR, CRITICAL	Fault (FLT)	Array	Hard disk related alarm
NXTS	802	CLEARED , MINOR, MAJOR, CRITICAL ,NONE	Fault (FLT) Trouble (TBL)	Error Status Threshold exceeded	Filesystem- related alarms

For screen shots of each panel on the platform main page, please refer to “Appendix A - Platform Main Web Page Interface” on page 1628.

Commissioning

The Session Server is a standalone system. It is equipped with a commissioning tool called “commish” to allow the customer to configure the system as part of the initial setup of the server. This tool can be used at the vt100 console port of the Session Server. The following values can be configured using the commish:

- hostname
- IP address
- Subnet Mask
- Gateway (default CS LAN router)
- Timezone
- One or more NTP servers
- Log server IP address
- Network Nodes IP (SDM, HTTPs proxy, and Core IP addresses)
- Server Location
- SNMP Trap destination

The user interface of the commish tool is broken up into the following sections as depicted in the following diagram.

Commish user Interface Areas

Title	
Stages	Status
	Prompt Text Entry
	Back Next
	Help

The general philosophy is that for each screen:

- The title remains constant and indicates that this is the system setup
- The Stage bar along the left will highlight the stage on which the user is currently
- The Status will indicate in a longer form with what stage the user is interacting
- The help along the bottom indicates some useful piece of advice about what the user is being asked
- The prompt requests a piece of information from the user
- The text entry area is where the user types the requested information

- The back and next buttons are used to navigate between the screens
- The interface is navigated by using the 'tab' key to cycle between the text entry area and the 'next' and 'back' buttons. The 'enter' key is used to make a selection.

For some screenshots and details about the interface, please See “Appendix C - Commish Human Machine Interface” on page 1638.

SNMP Support

The Session Server supports SNMP V3 with “No Privacy” and “No Authentication” options. The user can use the commish tool, described in “Commissioning” on page 1622, to configure two TRAP destinations and SNMPv3 user name. As part of SNMP support, the Session Server can raise the following traps to report alarms severity:

- nortelNMIalarmClearNotification
- nortelNMIwarningAlarmNotification
- nortelNMIminorAlarmNotification
- nortelNMImajorAlarmNotification
- nortelNMICriticalAlarmNotification

Fault Handling

This section provides a summary of the fault handling behavior of the SAM-XTS node maintenance in reaction to various faults. The fault handling behavior is based upon the compact Call Agent behavior for all but the disk cases.

SAM-XTS Fault Handling

Fault Event	Simplex/ Duplex, Affected Unit	Action
Total Loss of LAN Connectivity	Duplex, Active	Failover to the inactive. Reset former active recovers and comes back into sync.
Total Loss of LAN Connectivity	Simplex, Active	Wait about two minutes and reset active unit if persistent. (The wait handles SDM and router upgrade outage.)
Total Loss of LAN Connectivity	Duplex, Both	Wait about two minutes and reset if persistent; wait 20 seconds and reset inactive if persistent.
Single Ethernet Outage	Any, Any	Switch active ethernet if necessary. Monitor for ETH recovery.
Loss of Point to Point Connectivity	Duplex, Both	Alarm and log continue mate communication via LAN.

SAM-XTS Fault Handling

Fault Event	Simplex/ Duplex, Affected Unit	Action
Sanity Time Out or Power Cycle	Duplex, Active	Inactive immediately takes over; former active resets.
Sanity Time Out or Power Cycle	Duplex, Inactive	Inactive resets
Sanity Time Out or Power Cycle	Simplex, Active	Active resets and determines mastership.
Total Disk Outage.	Duplex, Active	Failover to inactive. Former active waits 15 minutes and resets if persistent.
Total Disk Outage	Simplex, Active	Alarm and log but wait for manual action.
Total Disk Outage	Duplex, Inactive	Inactive waits 15 minutes and resets if persistent.

Users Categories

The following is a list of groups that will be used on SAM-XTS platform. This list comes from Succession Element and Sub Element Manager (SESM), and is consistent with the existing Succession users.

Authorization Groups

Group Name	Group Number	Description
mgcadm	1011	Can do anything. This is equivalent to being the root user
mgcmte	1014	Can do any non-service impacting platform maintenance activities. Cannot change provisioning data.
mgcsprov	1013	Application provisioning user. Can modify provisioning data, but cannot take any platform maintenance actions
mgcrw/mgcro	1012/1015	Can view base or provisioning information but cannot initiate any changes.
succssn	104	required for login access to the Session Server

The following table describes the list of default users on the system, and their associated groups. At commissioning time, the customer will be able to remove any unneeded users, and will be forced to change the passwords on any of those which remain.

Default Users

User Name	Groups	Removable	Description
root	mgcadm root system	no	System root user. Direct login will not be allowed - must login as another user, and can then su to the root user.
admin	mgcadm	no	Management root user. Not able to remove this user since at least one must exist in order to become root.
mtc	mgcmte	yes	NCGL-XTS maintenance user.
prov	mgcsprov	yes	Application provisioning user.
provmtc	mgcmte, mgcsprov	yes	Able to take most actions - can do most maintenance activities as well as make provisioning changes
guest	mgcro	yes	Guest user. Can view but not make any changes.

Limitations and restrictions

The Session Server does not support software alarming of the following failure situations:

- Over temperature
- CPU failure
- RAM failure
- Fan Failure
- Power supply failure (the power LED and relay contact will be raised)

There is no support for backup and restore in SN07 release.

In this release, to halt the Session Server from the admin panel is equivalent to the administrative state to lock the server.

The Session Server software does not support/include the STORM (STOrage Management) functionality.

Interactions

The following external interfaces are supported on the Session Server to provide access to the server:

- SFTP or SCP (for secure file transfer)
- SSH (for secure login), which supports the following encryption algorithms:
 - 3DES 168 bits

- Blowfish 128 bits
- Twofish 128 bits
- AES 128 bits

The SSL encryption algorithms supported are:

- RC4 - 128-bit keys
- RC2 - 40 bit key
- DES - 40 bit key
- DES - 56 bit key
- 3DES - 168 bit key
- HTTP (Session Server Web Interface)
- HTTPS (Secure HTTP)

All of the existing interfaces will be maintained, and since they are all standards based protocols, no compatibility issues are expected.

Note: The user will not be able to access the Session Server using the “telnet” command because it is not supported due to security issues.

Applicable customer facing sections

Fault Management

Logs	___X___
Alarms	___X___

Configuration

Data Schema	___N/A___
User Interface	___X___
Element Management	___X___
Security	___N/A___
Service Order	___N/A___
Office Parameters	___N/A___

Accounting (includes AMA billing)	___N/A___

Performance (includes operational measurements)	___N/A___

Glossary

Term	Description
CI	Command Interpreter
CM	Computing Module (aka "Core")
CS2K	Call Server 2000
CS2K OAMP	Call Server 2000 OAMP (aka SESM aka PTM)
DMS	Digital Multiplex Switch
GWC	Gateway Controller
HTTP	HyperText Transport Protocol
IEMS	Integrated Element Management System
IMS	Interactive Multimedia Services
IP	Internet Protocol
MAPCI	Maintenance, Administration, and Provisioning Command Interpreter
MGC	Media Gateway Controller
NCGL	Nortel Carrier Grade Linux
NEBS	Network Equipment-Building System
NTP	Network Time Protocol
OAM&P	Operation, Administration, Maintenance, and Provisioning
OSS	Operations Support System
OSSGate	OSS Gateway
PAM	Pluggable Authentication Module
PTM	Packet Telephony Manager
PVG	Packet Voice Gateway
RFC	Request For Comments
RTS	Return To Service
SAM-XTS	Services Application Module- eXtreme Thin Server
SG	SIP Gateway application
SDM	Supernode Data Manager

Term	Description
SDP	Session Description Protocol
SESM	Succession Element and Sub Element Manager (aka CS2K OAMP, aka PTM)
SIP	Session Initiation Protocol
SIPT	Session Initiation Protocol (SPI) for Telephones
SME	Subject Matter Expert
SNMP	Simple Network Management Protocol
SNM	Session Server Node Maintenance
Session Server	Platform for the SIP Gateway application
SPM	Spectrum Peripheral Module
STORM	STORage Management
SWACT	Switch of Activity
TCP	Transmission Control Protocol
VRDN	Virtual Router Distribution Node

References

- 1 A00003933: Session Server SIP Gateway Application

Appendix A - Platform Main Web Page Interface

This appendix contains the web page screenshots. Please note that screenshots captured here are for the Drop 1 deliverable, where the session server only supports simplex mode. This section will be updated when SN07session server full duplex functionality is completed.

Platform Home Panel

This panel will contain data for both Session Server units.

[Home](#)

Platform Home

Platform Information

Date:	Wednesday November 19th 2003 10:22:59 AM CST
Time since last reboot:	7 days, 19 hours, 2 minutes, 38 seconds
System Power-On Time:	0 years 216 days 15 hours
System booted from:	Hard disk drive
Last restart cause:	Last restart due to push button reset
Last power event cause:	Last power down caused by loss of power feed.
Current version:	1.0.0.0311071944
Platform IP Address:	47.174.73.243
Platform EM Client IP Address:	47.129.118.118
Server Location:	rtpg

Alarms Panel

Like other Session Server EM panels, the Alarms panel will display the alarms on both the active and inactive units. The alarms are refreshed every 45 seconds.

Note: This screen shot is Drop1 functionality.

Alarms

Alarms

Type	ID	Timestamp	Severity	Description
Equipment	Underlying Resource Unavailable	Fricay November 14th 2003 07:09:07 PM	Major	Array: '/dev/md1' (ntvg) Status: A physical disk has been removed from the array.
Equipment	Underlying Resource Unavailable	Fricay November 14th 2003 07:09:07 PM	Major	Array: '/dev/md0' (/boot) Status: A physical disk has been removed from the array.
Equipment	Communications Subsystem Failure	Fricay November 14th 2003 07:09:05 PM	Major	Unable to communicate with BMC to get results. cc=

System Panel

This panel contains data for the user's Session Server unit.

System Information

System Information

Chassis Information

Self Test	Chassis Subsystems
Unable to communicate with BMC to get results. cc=%x	Undetermined

CPU Information

1 min. load average	5 mins. load average	15 mins. load average	1 min. load average threshold value	5 min. load average threshold value	15 min. load average threshold value
0.02	0.04	0.01	14.00	14.00	14.00

Process Information

Number of processes	Number of zombie process (es)	Minor alarm threshold value	Major alarm threshold value	Critical alarm threshold value
41	0	5	7	10

Memory Information

Total	Total memory	Total memory	Total memory	Total memory	Minor alarm	Major alarm	Critical alarm

Disk Storage Panel

This panel contains data for the user's Session Server unit.

Storage Panel

Disk Storage

RAID Array Status

Name	Size (GB)	State	Disk 0	Disk 1	Status
/boot	0.10	Disk Missing	.	Missing	Array is faulty
rtvg	3.90	Disk Missing	.	Missing	Array is faulty

Disk Maintenance

Disk Number	Disk Size (GB)	Disk State	Disk Action
0	0.00	.	None
1	Unknown	Missing	Insert

Filesystem Information

Monitor	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	Total Space Available (MB)	Total Space Available (%)	Min Alar Thresh (%)
Start	/		61.47	32.26	52.49	29.20	47.51	96.00
Start	/boot		98.65	41.37	42.24	56.98	57.76	85.00

Services Panel

This panel is used to display the active remote session status connected to the server, and to view the NTP servers status. This panel contains data for the user's Session Server unit.

Services

Platform Services			
Network Services			
Active Remote Sessions			
2			
NTP Information			
Server 1	Server 2	Server 3	Service Status
172.16.136.1 establishing sync	undefined	undefined	Running

Admin Panel

The admin panel is used to perform administrative tasks related to the Session Server unit. The actions supported from this panel are:

- Change Timezone Setting
- Bootload Management (to set default bootloader, or remove bootloader)
- S/W upgrade
- Server Maintenance (reboot or halt)

This panel contains data for the user's Session Server unit.

Admin

Platform Admin

Timezone Setting		
	Canada/Eastern	Set Timezone

Bootload Management		
Bootload	Maintenance	
1.0.0.031118:543	Default Bootload	
1.0.0.031118:443	Set default	Delete
1.0.0.031118:435	Set default	Delete

Customer Logs Panel

The customer logs panel displays a historical view of customer logs that have been generated on the Session Server unit. The most recent logs are displayed at the bottom of the log file.

Limitation of this panel is that the user can only view the logs that pertain to the user's specific unit.

Customer Logs

Logs

Customer Logs

Nov 11 16:20:43 loopback alarmd: STM301 MINOR INIT Array: '/dev/md0' (/boot) Status: currently being rebuilt.

Nov 11 16:20:43 loopback alarmd: STM301 MINOR INIT Array: '/dev/md1' (ntvg) Status: currently being rebuilt.

Nov 11 16:21:33 loopback ngss_sip_mtc: SIPM500 NONE INFO SIP Gateway Maintenance Change [Administrative : Locked -> Locked] [Operational : Disabled -> Enabled] [Control : Not Suspended] [Procedural : Not Terminating -> Not Terminating] [User Requested : Yes] [Reason : Unsuspend command issued] [Web User ID : webuser]

Nov 11 16:21:34 loopback ngss_sip_mtc: SIPM500 NONE INFO SIP Gateway Maintenance Change [Administrative : Locked -> Unlocked] [Operational : Enabled -> Enabled] [Control : Suspended -> Not Suspended] [Procedural : Not Terminating -> Not Terminating] [User Requested : No] [Reason : Unlock command issued] [Web User ID : webuser]

Appendix B - Alarms

Note that this appendix does not yet contain alarms relating to the hardware specific issues (e.g.: power supply failures, temperature, etc.).

Alarm Id (ITU-T X.733)

ID	Type	ID	Type
1	Adapter error	30	Material supply exhausted
2	Application subsystem failure	31	Multiplexer problem
3	Bandwidth reduced	32	Out of memory
4	Call establishment error	33	Output device error
5	Communications protocol error	34	Performance degraded
6	Communications subsystem failure	35	Power problem
7	Configuration or customization error	36	Pressure unacceptable
8	Congestion	37	Processor problem
9	Corrupt data	38	Pump failure
10	CPU cycles limit exceeded	39	Queue size exceeded
11	Dataset or modem error	40	Receive failure
12	Degraded signal degradedSignal	41	Receiver failure
13	DTE-DCE interface error	42	Remote node transmission error
14	Enclosure door open	43	Resource at or nearing capacity
15	Equipment malfunction	44	Response time excessive
16	Excessive vibration	45	Retransmission rate excessive
17	File error	46	Software error
18	Fire detected	47	Software program abnormally terminated
19	Flood detected	48	Software program error
20	Framing error	49	Storage capacity problem
21	Heating/ventilation/cooling	50	Temperature unacceptable
22	Humidity unacceptable	51	Threshold crossed
23	I/O device error	52	Timing problem
24	Input device error	53	Toxic leak detected
25	LAN error	54	Transmit Failure
26	Leak detected	55	Transmitter Failure

ID	Type	ID	Type
27	Local node transmission error	56	Underlying resource unavailable
28	Loss of frame	57	Version mismatch
29	Loss of signal	101	Authentication Failure ^a
102	Breach of Confidentiality	103	Cable Tamper
104	Delayed Information	105	Denial of Service
106	Duplicate Information	107	Information Missing
108	Information Modification Detected	109	Information Out of Sequence
110	Intrusion Detection	111	Key Expired
112	Non Repudiation Failure	113	Out of Hours Activity
114	Out of Service	115	Procedural Error
116	Unauthorized Access Attempt	117	Unexpected Information
118	Unspecified Reason		

a. ITU-T X.733 alarm ids from 58 to 100 are reserved - not assigned yet

Appendix C - Commish Human Machine Interface

This appendix captures screenshots of the commish tool.

This is the introductory stage

```
47.174.73.243 - PuTTY
System Setup, Copyright 2003 Nortel Networks, All Rights Reserved
-----
Setup Stages | Introduction to System Setup
-----
Introduction | -----
Hostname    |
IPAddress   |      Welcome to the system setup tool.
Netmask     |
Gateway     |
Timezone    |
NTP         |
Logs        |
NetNodes    |
Location    |
SNMP        |
Summary     |
-----
              | -----
              | | Abort |                               | Next>> |
              | -----
              | This tool will help you to bring this server into service.
              | Use the <TAB> key to move and select fields
              | and the <ENTER> key to confirm the selection
```

This stage allows the user to enter a hostname

```
47.174.73.243 - PuTTY
System Setup, Copyright 2003 Nortel Networks, All Rights Reserved
-----
Setup Stages | Configure the server hostname
-----
Introduction | -----
Hostname     |
IPAddress    | Please enter a hostname for this server
Netmask      |
Gateway      | [rtpgss2]
Timezone     |
NTP          |
Logs         |
NetNodes     |
Location     |
SNMP         |
Summary      |
-----
              | <<Back | | Next>> |
              | -----
              | The hostname is a textual description of this server.
              | For example: 'sipserve' or 'sipserver.nortel.com'
              | Use '<' and '>' keys to move if left and right arrows don't work
```

This stage allows the user to enter an IP address

```
47.174.73.243 - PuTTY
System Setup, Copyright 2003 Nortel Networks, All Rights Reserved
-----
Setup Stages | Configure the server IP address
-----
Introduction | -----
Hostname     |
IPAddress    | Please enter an IP address for this server
Netmask      |
Gateway      | [47.174.73.243]
Timezone     |
NTP          |
Logs         |
NetNodes     |
Location     |
SNMP         |
Summary      |
-----
              | <<Back | | Next>> |
              | -----
              | The IP address is a numerical identifier used to
              | uniquely identify this server.
              | For example: '192.168.1.5'
```

This stage allows the user to enter a network mask IP address

```
47.174.73.243 - PuTTY
System Setup, Copyright 2003 Nortel Networks, All Rights Reserved
-----
Setup Stages |
-----
Introduction | Configure the server netmask
-----
Hostname |
IPAddress | Please enter a netmask for this server
Netmask |
Gateway | [255.255.255.224]
Timezone |
NTP |
Logs |
NetNodes |
Location |
SNMP |
Summary |

-----
| <<Back | | Next>> |
-----

The netmask is a numerical value used determine which
range of addresses are part of the network this server is on
For example: '255.255.255.0'
```

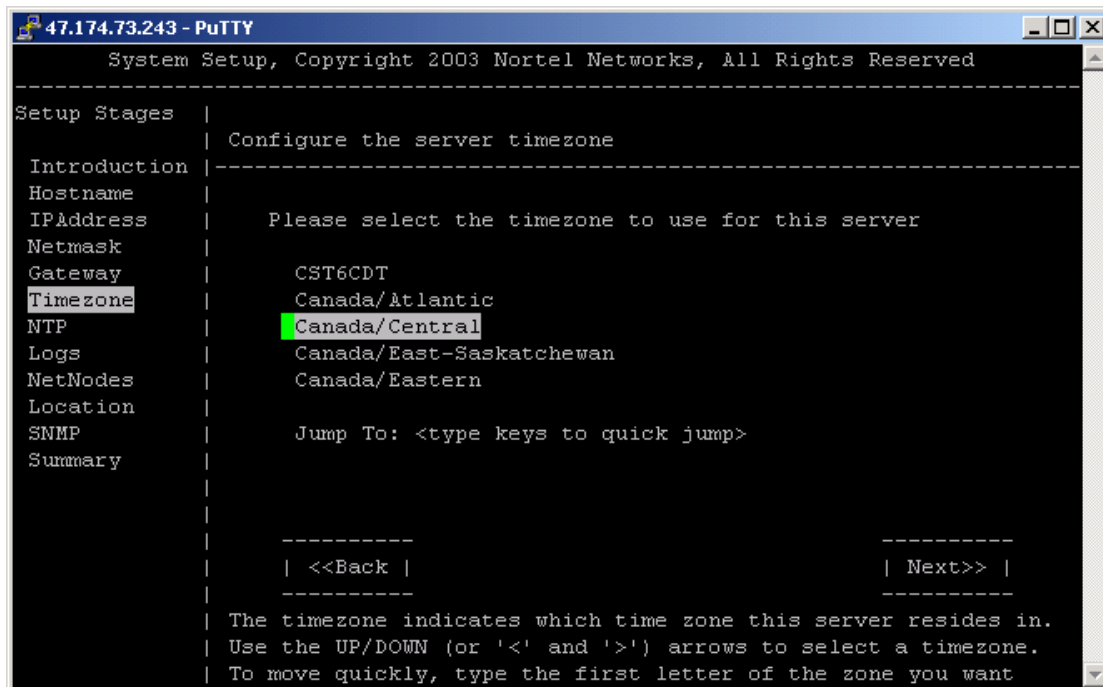
This stage allows the user to enter a gateway IP address

```
47.174.73.243 - PuTTY
System Setup, Copyright 2003 Nortel Networks, All Rights Reserved
-----
Setup Stages |
-----
Introduction | Configure the server default gateway
-----
Hostname |
IPAddress | Please enter a default gateway for this server
Netmask |
Gateway | [47.174.73.225]
Timezone |
NTP |
Logs |
NetNodes |
Location |
SNMP |
Summary |

-----
| <<Back | | Next>> |
-----

The gateway is an IP address of the router which allows
this server's network to communicate with other networks
For example: '192.168.1.1'
```

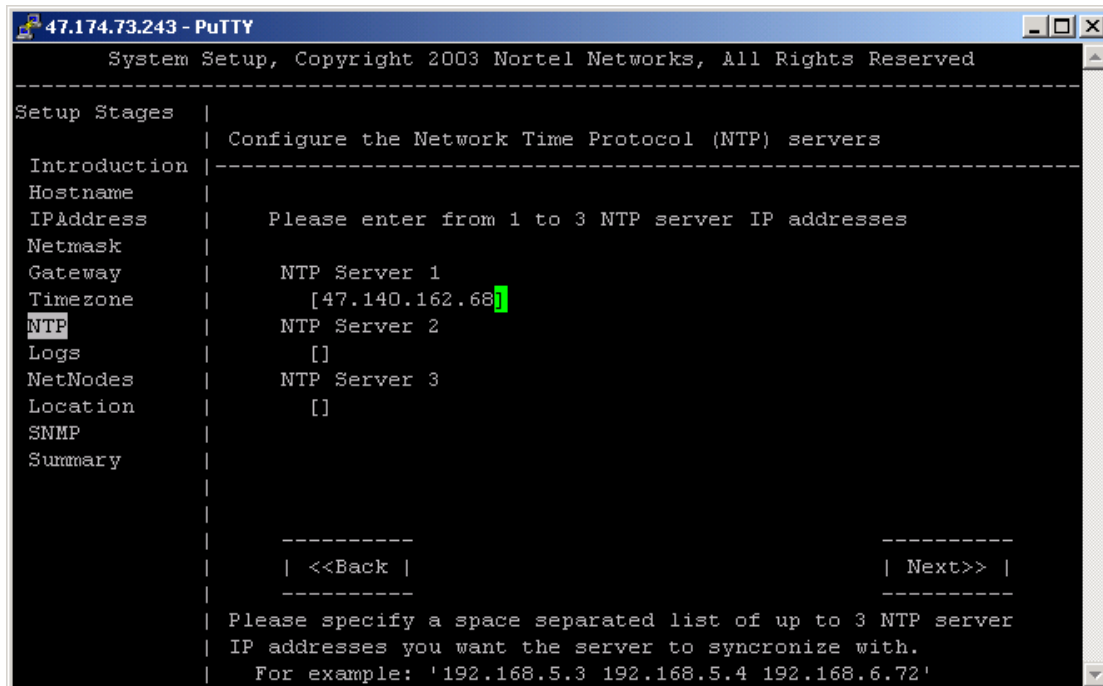

This stage allows the user to select time zone



The screenshot shows a PuTTY window titled "47.174.73.243 - PuTTY". The main text reads "System Setup, Copyright 2003 Nortel Networks, All Rights Reserved". Below this is a table of Setup Stages. The "Timezone" stage is highlighted, showing a list of time zones: Canada/Atlantic, Canada/Central (highlighted with a green cursor), Canada/East-Saskatchewan, and Canada/Eastern. Below the list are navigation options: "<<Back" and "Next>>". A note at the bottom states: "The timezone indicates which time zone this server resides in. Use the UP/DOWN (or '<' and '>') arrows to select a timezone. To move quickly, type the first letter of the zone you want".

```
47.174.73.243 - PuTTY
System Setup, Copyright 2003 Nortel Networks, All Rights Reserved
-----
Setup Stages |
Introduction | -----
Hostname     |
IPAddress    | Please select the timezone to use for this server
Netmask      |
Gateway      | CST6CDT
Timezone     | Canada/Atlantic
             | Canada/Central
NTP          |
Logs         | Canada/East-Saskatchewan
NetNodes     | Canada/Eastern
Location     |
SNMP         | Jump To: <type keys to quick jump>
Summary      |
             | -----
             | | <<Back |           | Next>> |
             | -----
             | The timezone indicates which time zone this server resides in.
             | Use the UP/DOWN (or '<' and '>') arrows to select a timezone.
             | To move quickly, type the first letter of the zone you want
```

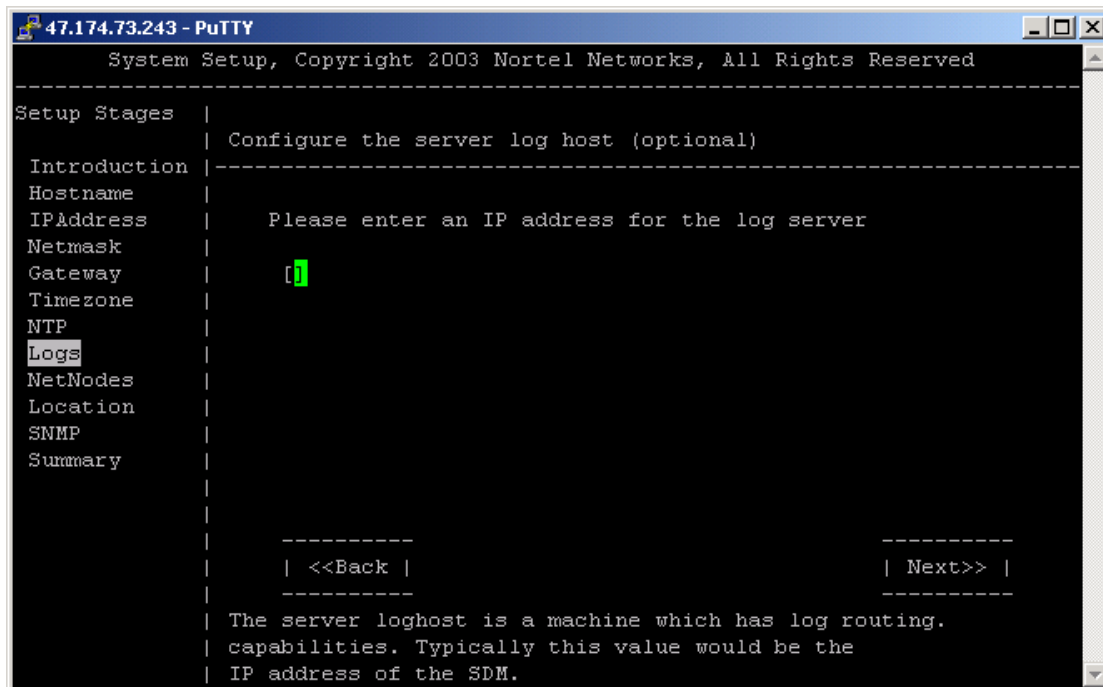
This stage allows the user to enter a NTP server IP address



The screenshot shows a PuTTY window titled "47.174.73.243 - PuTTY". The main text reads "System Setup, Copyright 2003 Nortel Networks, All Rights Reserved". Below this is a table of Setup Stages. The "NTP" stage is highlighted, showing a list of NTP server IP addresses: NTP Server 1 (47.140.162.68), NTP Server 2 ([]), and NTP Server 3 ([]). Below the list are navigation options: "<<Back" and "Next>>". A note at the bottom states: "Please specify a space separated list of up to 3 NTP server IP addresses you want the server to synchronize with. For example: '192.168.5.3 192.168.5.4 192.168.6.72'".

```
47.174.73.243 - PuTTY
System Setup, Copyright 2003 Nortel Networks, All Rights Reserved
-----
Setup Stages |
Introduction | -----
Hostname     |
IPAddress    | Please enter from 1 to 3 NTP server IP addresses
Netmask      |
Gateway      | NTP Server 1
Timezone     | [47.140.162.68]
NTP          | NTP Server 2
Logs         | []
NetNodes     | NTP Server 3
Location     | []
SNMP         |
Summary      |
             | -----
             | | <<Back |           | Next>> |
             | -----
             | Please specify a space separated list of up to 3 NTP server
             | IP addresses you want the server to synchronize with.
             | For example: '192.168.5.3 192.168.5.4 192.168.6.72'
```

This stage allows the user to enter an IP address for log server

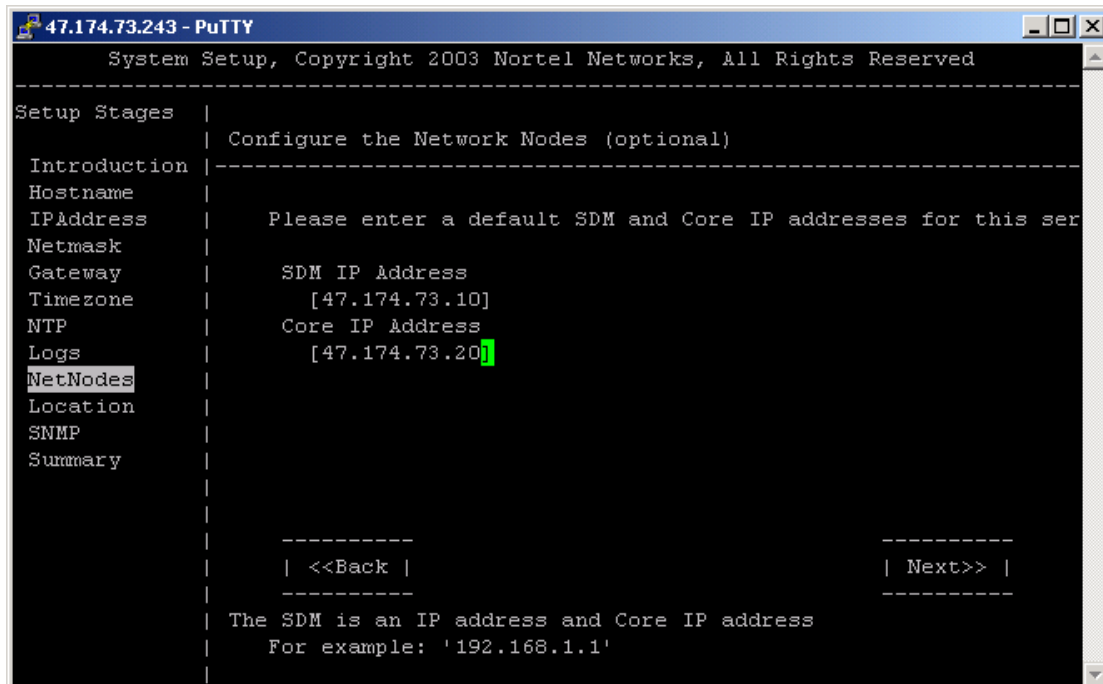


```
47.174.73.243 - PuTTY
System Setup, Copyright 2003 Nortel Networks, All Rights Reserved
-----
Setup Stages | Configure the server log host (optional)
-----
Introduction | -----
Hostname |
IPAddress | Please enter an IP address for the log server
Netmask |
Gateway | [ ]
Timezone |
NTP |
Logs |
NetNodes |
Location |
SNMP |
Summary |

-----
| <<Back | | Next>> |
-----

The server loghost is a machine which has log routing.
capabilities. Typically this value would be the
IP address of the SDM.
```

This stage allows the user to enter SDM and core IP addresses

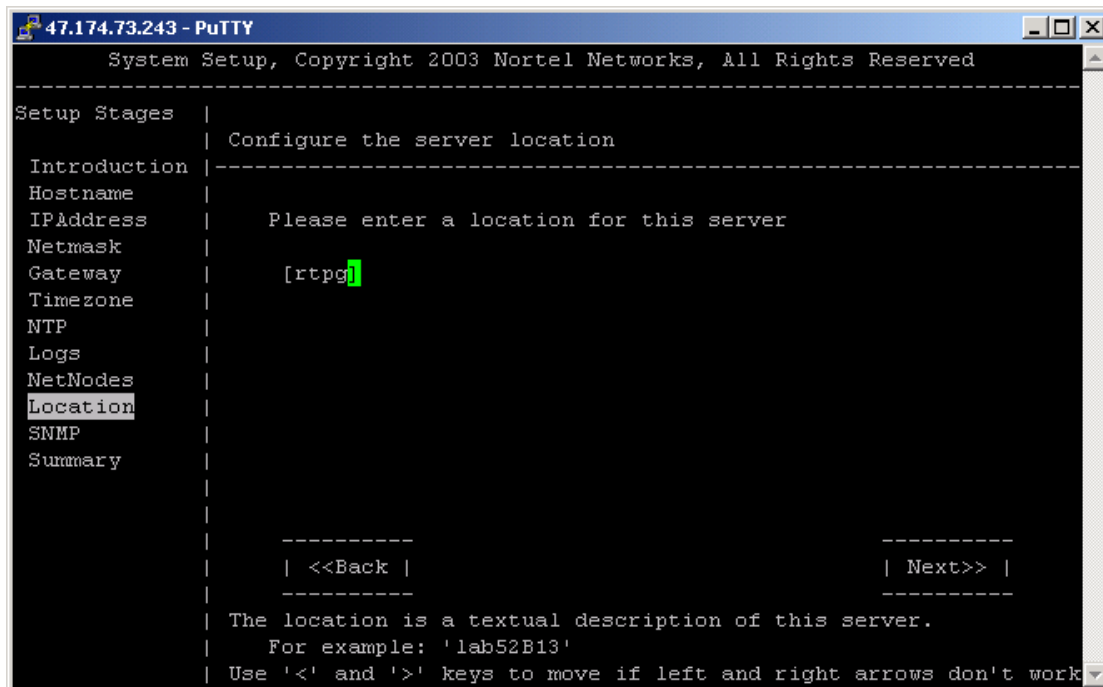


```
47.174.73.243 - PuTTY
System Setup, Copyright 2003 Nortel Networks, All Rights Reserved
-----
Setup Stages | Configure the Network Nodes (optional)
-----
Introduction | -----
Hostname |
IPAddress | Please enter a default SDM and Core IP addresses for this ser
Netmask |
Gateway | SDM IP Address
Timezone | [47.174.73.10]
NTP | Core IP Address
Logs | [47.174.73.20]
NetNodes |
Location |
SNMP |
Summary |

-----
| <<Back | | Next>> |
-----

The SDM is an IP address and Core IP address
For example: '192.168.1.1'
```

This stage allows the user to enter session server location

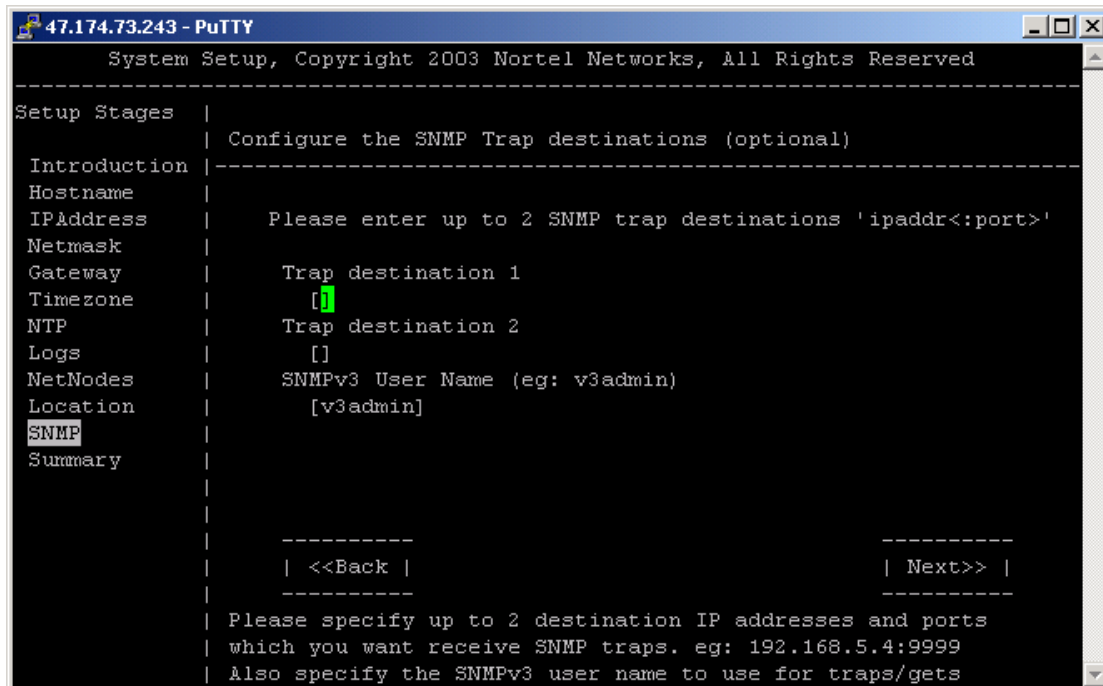


```
47.174.73.243 - PuTTY
System Setup, Copyright 2003 Nortel Networks, All Rights Reserved
-----
Setup Stages |
Introduction | Configure the server location
-----
Hostname |
IPAddress | Please enter a location for this server
Netmask |
Gateway | [rtpp]
Timezone |
NTP |
Logs |
NetNodes |
Location |
SNMP |
Summary |

-----
| <<Back | | Next>> |
-----

The location is a textual description of this server.
For example: 'lab52B13'
Use '<' and '>' keys to move if left and right arrows don't work
```

This stage allows the user to select SNMP trap destination



```
47.174.73.243 - PuTTY
System Setup, Copyright 2003 Nortel Networks, All Rights Reserved
-----
Setup Stages |
Introduction | Configure the SNMP Trap destinations (optional)
-----
Hostname |
IPAddress | Please enter up to 2 SNMP trap destinations 'ipaddr[:port]'
Netmask |
Gateway | Trap destination 1
Timezone | [1]
NTP | Trap destination 2
Logs | []
NetNodes | SNMPv3 User Name (eg: v3admin)
Location | [v3admin]
SNMP |
Summary |

-----
| <<Back | | Next>> |
-----

Please specify up to 2 destination IP addresses and ports
which you want receive SNMP traps. eg: 192.168.5.4:9999
Also specify the SNMPv3 user name to use for traps/gets
```

This is the summary screen

```
47.174.73.243 - PuTTY
System Setup, Copyright 2003 Nortel Networks, All Rights Reserved
-----
Setup Stages | Confirm the system setup
-----
Introduction | -----
Hostname     |
IPAddress    | Select 'Finish' to save or 'Back' to make changes.
Netmask      |
Gateway      |
Timezone     |
NTP          |
Logs         |
NetNodes     |
Location     |
SNMP         |
Summary      |
-----
              |
              | Hostname:      rtpgss2
              | IP Address:   47.174.73.243
              | Netmask:      255.255.255.224
              | Gateway:      47.174.73.225
              | Timezone:     Canada/Central
              | NTP Servers:  47.140.162.68
              | Log Host:
              | Net Nodes:    47.174.73.10 47.174.73.20
              | Location:     rtpg
              | SNMP:         v3admin
              | -----
              | |<<Back |           | Finish |
              | -----
              |
              | This screen allows you to confirm that all of your
              | settings are correct.
```



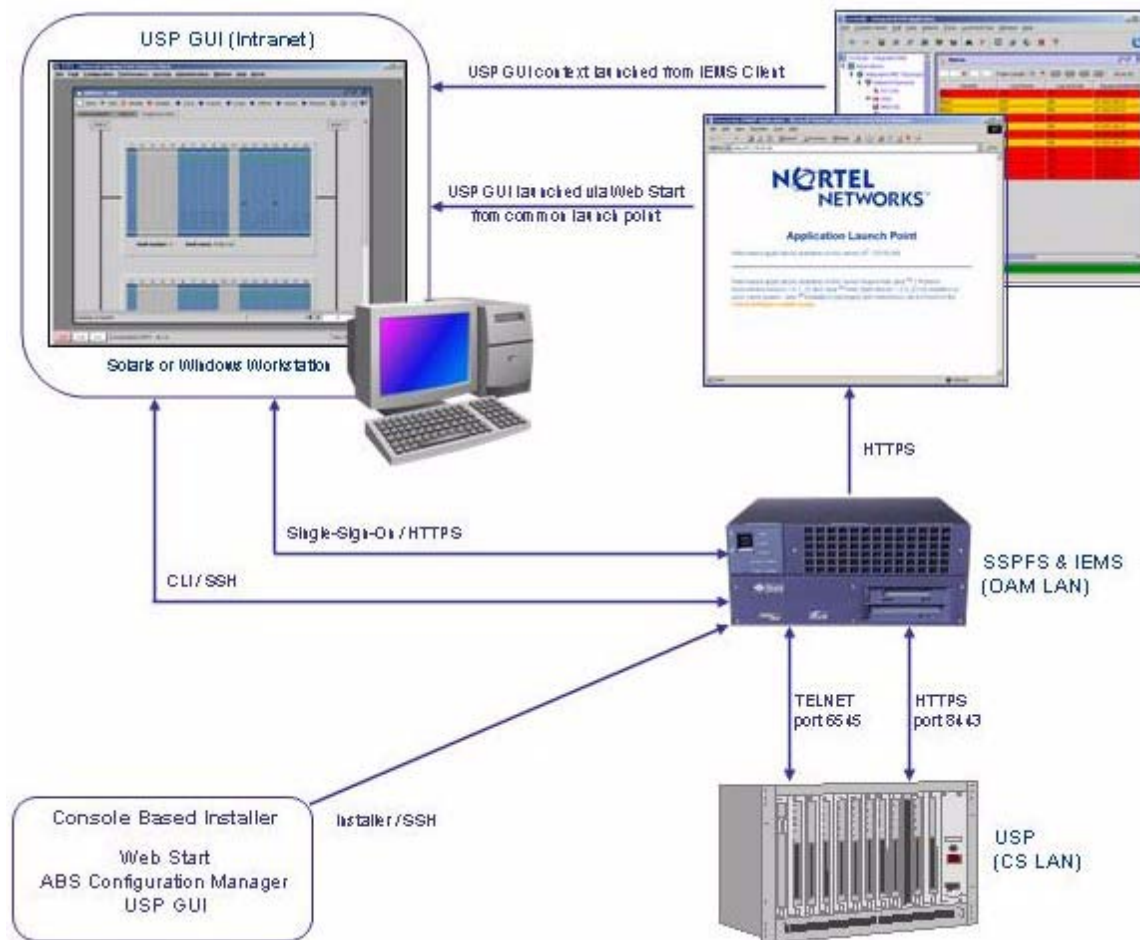
SN07 Feature Deltas

Product = CS 2000

A00004020 -- USP Java GUI Introduction to Succession (PT-IP)

The following figure may be used as a reference architecture throughout this feature description.

SN07 USP GUI Reference Architecture



TELNET and SSH Proxy Support

Due to LAN security requirements, the USP GUI is not allowed to connect directly to the USP. In previous releases this was addressed by the use of a central PC running Citrix Metaframe. Users would connect to the PC via a Citrix client and then launch the USP GUI from the PC to connect to the USP. This function was referred to as "Reach Through."

As of SN07 the GUI will be replaced with a thin Java compiled client GUI which will include the ability to connect to the USP via a TELNET or SSH proxy. For Succession solutions a SSH proxy function will be used on the SSPFS that will eliminate the need for the "Reach Through" PC in the solution.

The proxy function will actually be provided as a two-stage connection process between the GUI, the SSPFS and the USP (transparent to the user through the GUI):

- 1 USP GUI establishes a SSH connection to SSPFS.
- 2 USP GUI then establishes a TELNET from SSPFS to the USP

The configuration of the authentication and proxy function is captured in the following figures.

Site Manager Proxy Configuration - Basic

The screenshot shows the 'site-manager' window with the following configuration details:

- Site Configuration:**
 - site name: uspsite1
 - rtc-12 ipaddress: 10.0.0.1
 - rtc-15 ipaddress: 10.0.0.2
- Authentication Configuration:**
 - authentication scheme: Central Authentication Server
 - authentication server: 10.0.1.1
 - port: 443
- Proxy Configuration:**
 - enable proxy: ☒
 - proxy protocol: Secure Shell (SSH)
 - proxy server: 10.0.1.1
 - port: 22

Buttons on the right: New, Delete, Import..., Export...
Buttons at the bottom: Ok, Cancel, Apply

Site Configuration Export/Import

USP8.1 adds the ability to save a list of configured sites to a text file via the “Export” function. This file may then be distributed to all users and loaded via the “Import” function. This ability has been added due to the fact that we now have more data to configure for each site (authentication and proxy options). This will save the customer time and avoid configuration errors.

Authentication Scheme

Users have the option of selecting “Standard Authentication” or “Central Authentication Server” authentication schemes. The standard authentication will use the supplied user name and password to perform authentication at the USP and proxy (if enabled). To perform advanced authentication the user may wish to use a central authentication server to perform a PAM + Proxy authentication using HTTPS. The standard authentication mechanism is the default authentication scheme for direct connections (no proxy) and the central authentication server mechanism is the default authentication scheme for

proxy connections (proxy enabled). Refer to IEMS Single Sign-on Support for further details on using the PAM + Proxy authentication function.

Authentication IP Address and Port

If the authentication scheme is “Central Authentication Server” then an IP address and port must be supplied of the authentication server. The default port value is the well known HTTPS port.

Proxy Protocol

Users will have the option of selecting TELNET or SSH as the protocol to be used to connect to the proxy. For Succession solutions, SSH will be the required protocol (other customers and solutions may choose to use the TELNET option). If the proxy is enabled, SSH will be the default protocol.

Proxy IP Address and Port

If the proxy function is enabled, then an IP address and port must be supplied for the proxy server. The default port value is the well known Telnet or SSH port (dependent on the proxy protocol chosen).

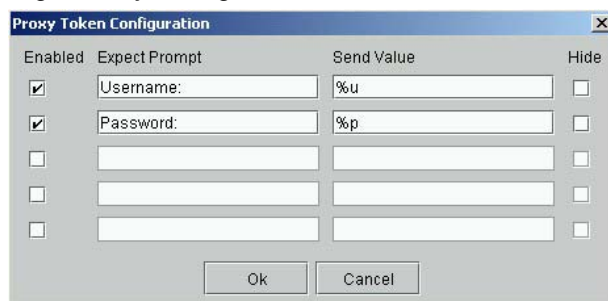
Advanced Tokens

The advanced proxy token configuration allows the user to adapt the behavior of the proxy token matching when connecting through the proxy server. The default token values should be sufficient, but is provided for the ability to adjust the values to work with different Telnet proxy servers. Special keywords are available for the send value to eliminate the need to supply user name, password and/or IP addresses as part of the proxy token matching.

The following special send token values are available:

- **u** – resolves to the current user name
- **p** – resolves to the current password supplied (or special security token if using “central authentication server” authentication scheme)
- **a** – resolves to the IP address of the target end connection point (RTC)
- **h** – resolves to the fully qualified domain name of the target end connection point (RTC)

Site Manger Proxy Configuration - Advanced

The image shows a 'Proxy Token Configuration' dialog box with a title bar containing a close button. The dialog has four columns: 'Enabled', 'Expect Prompt', 'Send Value', and 'Hide'. There are five rows of configuration. The first row has 'Enabled' checked, 'Expect Prompt' as 'Username:', 'Send Value' as '%u', and 'Hide' unchecked. The second row has 'Enabled' checked, 'Expect Prompt' as 'Password:', 'Send Value' as '%p', and 'Hide' unchecked. The third, fourth, and fifth rows have 'Enabled' unchecked, empty 'Expect Prompt' and 'Send Value' fields, and 'Hide' unchecked. At the bottom are 'Ok' and 'Cancel' buttons.

Enabled	Expect Prompt	Send Value	Hide
☒	Username:	%u	☐
☒	Password:	%p	☐
☐			☐
☐			☐
☐			☐

Ok Cancel

Prompt for Password

During the log process or when the GUI is re-establishing a connection to the USP it is possible that the user's password may no longer be valid. For example, consider the case of a secure-id or another "time-to-live" security token. If the user has been logged in and an RTC is reboot the connection will need to be re-established and the user may need to re-authenticate (effort is being made to reduce the likelihood of this occurring). In this case we do not want the user to have to terminate the current simplex connection in order to re-establish the duplex connection. We will simply present the user with the session-login screen and prompt them to re-enter their password.

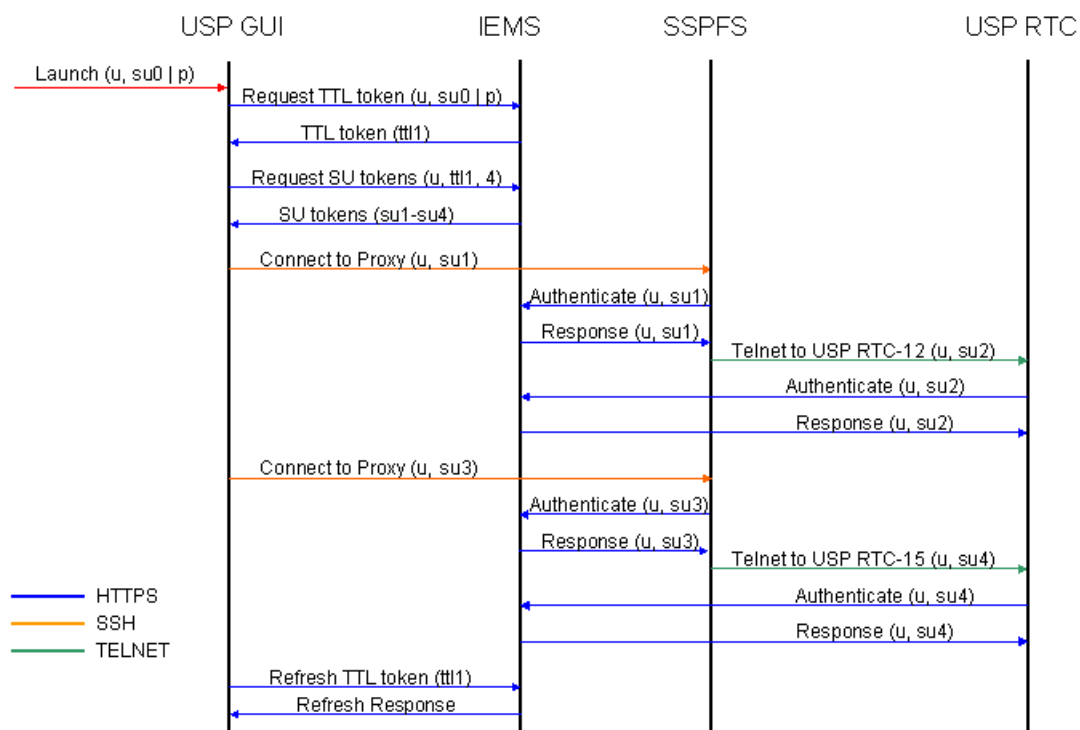
IEMS Single Sign-on Support & Context Launch

The IEMS provides a PAM + Proxy authentication mechanism for the central authentication server scheme. When "Central Authentication Server" authentication scheme is chosen, the GUI will use the supplied IP address and port to establish an HTTPS connection to the IEMS server. Using the supplied user name plus password or supplied security token (if context launched) to request a single time-to-live (TTL) security token from the IEMS. The TTL token will then be used to obtain single-use (SU) security tokens when establishing connections to any other end-points. This will ensure a secure authentication mechanism regardless of connection protocol.

The GUI can be context launched using either the user-name and password or a user-name and single-use security token. The user-name is supplied using the `-u` command line option and is used in conjunction with the `-p` (password) or `-t` (security token) options to perform the initial authentication with the IEMS server.

See the following figure for a single sign-on walkthrough using the IEMS for central authentication.

Single-sign-on Walk Through



Web Start Support

In the past customers have always installed the GUI either on their local desktop or on the reach-through PC running Citrix Metaframe. As of USP9.0, users will still be able to install the GUI locally but will have the additional option of installing the GUI on a central web server and launching via Java Web Start. This is the option that will be used for Succession in SN07. The Web Server is provided by the SSPFS platform. Refer to Figure 1 as a reference.

Console Based Installer

The USP uses Install Anywhere™ to manage software installation. For a UNIX based installation (as used by Succession SN07) a console based install option is available. This eliminates the need to use the graphical version via remote display (i.e. Exceed). The installer provides the same functionality as the graphical version. A user would simply insert the CD-ROM into the SSPFS platform (or FTP a copy of the CD image onto the SSPFS from a remote location), SSH (or TELNET) into the SSPFS and execute the installer with the `-i console` option.

A simulated trace of a console based install process is provided below:

```
$ ./install.bin -i console
```

```
Preparing CONSOLE Mode Installation...
```

```
=====
Universal Signaling Point v9.0.0      (created with InstallAnywhere by
Zero G)
-----
```

```
=====
Introduction
-----
```

InstallAnywhere will now guide you through the installation of the Universal Signaling Point software components.

It is strongly recommended that you quit all programs before continuing with this installation.

Respond to each prompt to proceed to the next step in the installation. If you want to change something on a previous step, type 'back'.

You may cancel this installation at any time by typing 'quit'.

Press <ENTER> to continue:

```
=====
Component Selection
-----
```

Enter a comma separated list of numbers representing the software components that you would like to install. To view a detailed description of each software component enter '?<COMPONENT-NUMBER>'

- 1- [X] USP Software Loads and ABS Manager
- 2- [X] USP Graphical Interface Client
- 3- [X] USP User Manuals and Documentation Suite
- 4- [] USP GR-310 Mediation Application

Enter software component numbers and press <ENTER> to continue:

```
=====Installation Directory
-----
```

Default installation directory: /data/usp

Enter an absolute path, or press <ENTER> to accept the default:

=====

Installation...started. This may take a few minutes to complete.

Installation...completed.

The selected Universal Signaling Point software components have been successfully installed.

Press <ENTER> to exit

Product = CS 2000

A00004036 -- AIN Update Message Query, Response Enhancement (Succession on DMS)

Functional Description

This activity addresses the development associated with enabling in the DMS the update and/or query capabilities for the service listed in the Chapter 5 Section 5.7 of GR-1298 “Information Revision Messages”, which outlines specific groups as well as the services and/or functions relevant to each group.

Given that the appropriate network architecture is available, with the addition of this set of capabilities in the DMS, subscribers will have the ability to both query the status and/or programmed information (if applicable) as well as activate/deactivate and update their corresponding service.

While the first iterations will rely heavily on Advanced Intelligent Network (AIN) (the initial protocol support is Abstract Syntax Notation 1 (ASN.1) via Signaling System No. 7 (SS7)), it should be understood that the intention is for the individual update and/or query service event handlers *not* be protocol dependent nor coupled to AIN directly.

There is much to benefit, however, in abiding by GR-1298; primarily compliance but it also provides an initial set of requirements and capabilities that are already generally available. The following sections outline GR-1298’s Service Data Function (*SDF*) groups as well as their corresponding capabilities and relevant services.

This development allows end user to activate/deactivate the service as if he/she have done from their own phone. Based on the service provider's interface for the end-user it take out the complexity to activate, deactivate, add, change, delete or edit service specific data faced by end-user using a phone.

Functional Behavior

Recognizing that the scope of this activity does not go beyond development in the Core, "[Functional Behavior Diagram](#)" on page 1654 below illustrates the basic control capabilities this activities intends to enable Off-board service control (given an AIN network solution). The following steps outline the basic tasks:

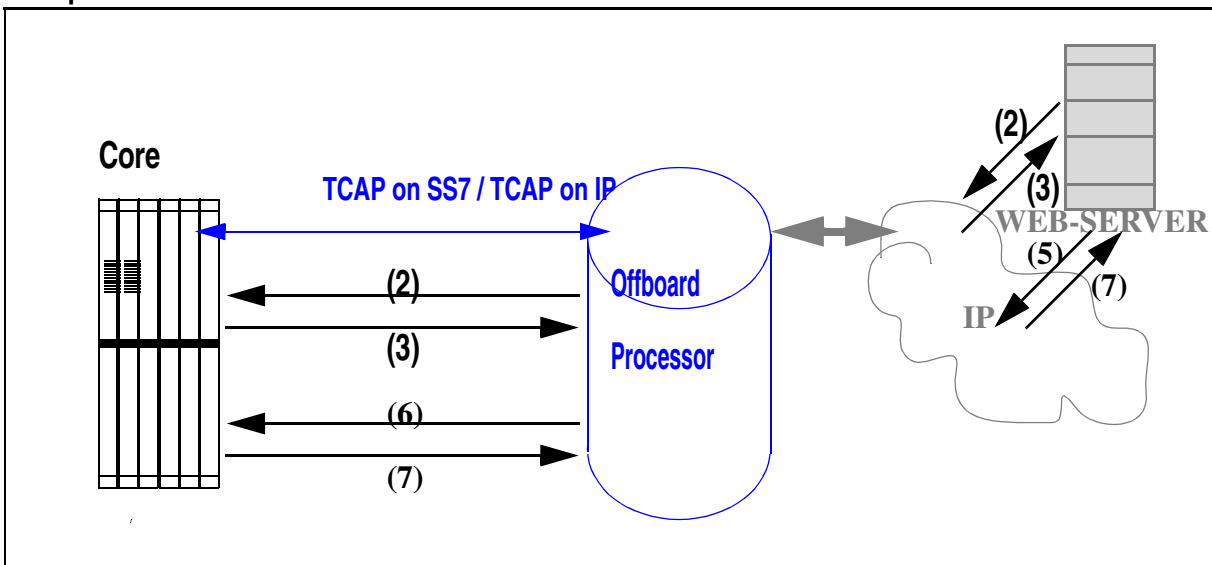
1. The subscriber logs into the Provider's network and, via Web or PC Client based application, gains access to his or her subscriber service control level. From here, the subscriber can generate a request for information about subscribed to services and/or an update to change, for example, the status of a service.
2. The subscriber's update/query request is delivered to the Provider's Network Server where a properly encoded message is created and dispatched to the SCP enabled in the Provider's network.
3. The update/query request is delivered to the SCP where a properly encoded message is created and dispatched via (SS7 or TCAP/IP) to the End-Office serving the subscriber.
4. The End-Office handles the request and replies with the appropriate response. A query response, for example, contains the information requested (e.g. status of a service).
5. The response is delivered to the Provider's Network Server where it is put into a format understood by the application serving the subscriber and, finally,
6. The formatted response makes gets delivered to the subscriber's application where the information is displayed.

Functional Behavior Diagram

Note: It should be understood that the behavioral diagram outlined above represents only one of several possible network solutions and, while it represents the most plausible configuration in the short term, should not be considered the only alternative.

Sample Data Flow

The Figure , "Sample Data Flow" for the service management feature is described below:

Sample Data Flow

1. The end-user browses the web-site, logs into the his / her account. E.g.: Myaccount@MyServiceProvider.com.
2. The Web client triggers a Query to the Off-board Processor, the Off-board Processor in turn generates a TCAP Query Request (NCR) to the Core.
3. The Core responds with the TCAP Query Response (NCR) message which return the users current profile, i.e. the current features assigned to the subscriber, their activation status and relevant attributes.
4. The end-user may decide to change certain services, for e.g.: SLE lists, call forward DN, or turn the call forward busy on the line. The user submits these changes.
5. This triggers the Offboard processor, which could be either of the SCP, IMS or an independent box.
6. The off-board processor in turn Builds TCAP Non Call Related Messages (e.g.: Update Message) and sends to the Core /Switch.
7. The Core / Switch will process the request and respond with the outcome of the request.
8. The Web-server could further use other Query Requests and Update Message to retrieve updated information for a user profile and change the feature attributes.

DN Validation

The DN Validation requires TCAP query for certain services. GR-1298 is not clear on how to allow the DN validation for Non-CallP services. However, we are able to provide DN Validation using TCAP query. The following is the details for the DN Validation behavior for Non-CallP query and update request from the SCP:

SDF Group 1

Group1 services are those generally provided with the ability to

- activate and/or deactivate
- retrieve the status

The following is a list of services GR-1298-Core classifies as Group1.

- Message Waiting Indicator (MWT, CMWI, AINMWT etc.)
- Visual Message Waiting Indicator (MWL, CMWI, AINMWT etc.)
- Anonymous Call Rejection (ACRJ)
- Automatic Callback (deactivation or *cancellation* only) (ACB)
- Automatic Recall (deactivation or *cancellation* only) (AR)
- Call Screening (CSMI)

- Outside Calling Area Alerting (LDSA)
- Calling Identity Delivery and Suppression (activation -> *set the pps to public* and deactivation -> *set the pps to private*) (SUPPRESS)
- Call Waiting (CWTACT)

The following service is not classified by GR-1298-Core but supported by CM under Group 1:

- Make Set Busy (MSB)

Note: Appendix A describes the encoding/decoding of MSB.

SDF Group 2

Group2 services are those generally provided with the ability to

- activate and/or deactivate
- update a corresponding delay interval value.
- retrieve the status and/or delay interval value.

The following is a list of services GR-1298-Core classifies as Group2.

- Audio Message Waiting Indicator (PRN)

SDF Group 3

Group3 services are those generally provided with the ability to

- activate and/or deactivate
- add/delete list entries corresponding to a specified Directory Number (DN), Speed Call Code or Incoming Memory Slot
- delete all list entries
- delete all private entries
- retrieve the status, list entries and/or list size

The following is a list of services GR-1298-Core classifies as Group3.

- Distinctive Ringing/Call Waiting
- Selective Call Rejection

The following service is not classified by GR-1298-Core but supported by CM under group 3:

- Simultaneous Ringing (SIMRING)

Note: The Section describes the encoding/decoding of Simring.

SDF Group 4

Group4 services are those generally provided with the ability to

- activate and/or deactivate
- set or clear forwarding (remote) DN
- retrieve the status and/or forwarding DN

The following is a list of services GR-1298-Core classifies as Group4.

- Call Forwarding Variable
- Call Forwarding Don't Answer
- Call Forwarding Busy Line

Note: Please refer to section for support of AINDigits Parm. This parm is not supported for Group4 in GR-1298 and GR-1299.

SDF Group 5

Group5 services are those generally provided with the ability to

- activate and/or deactivate
- add/delete list entries corresponding to a specified DN, Speed Call Code or Incoming Memory Slot
- delete all list entries
- delete all private entries
- set or clear forwarding (remote) DN
- retrieve the status, list entries, list size and/or forwarding DN

The following is a list of services GR-1298-Core classifies as Group5.

- Selective Call Forwarding
- Selective Call Acceptance

Note: Please refer to section for support of AINDigits Parm. This parm is not supported for Group5 in GR-1298 and GR-1299.

SDF Group 6

Group6 services are those generally provided with the ability to

- update the relevant delay interval for number of rings prior to forwarding
- retrieve the delay interval value

The following is a list of services GR-1298-Core classifies as Group6.

- Ring Control

SDF Group 7

Group7 services are those generally provided with the ability to

- invoke the DMS-based CNDB or CNAB features

The following is a list of services GR-1298-Core classifies as Group7.

- Calling Number Delivery Blocking
- Calling Name Delivery Blocking

SDF Group 8

Group8 services are those generally provided with the ability to

- invoke a service

The following is a list of services GR-1298-Core classifies as Group8.

- Customer Originated Trace
- Cancel Call Waiting

SDF Group 9

Group9 services are those generally provided with the ability to

- change speed calling list entry to specified DN

The following is a list of services GR-1298-Core classifies as Group9.

- Speed Calling

For more information, please refer to GR-1298-Core, section 6.4.

Nortel has developed different variants of the GR's Speed Calling feature. For instance, Nortel's Speed Calling Short (SCS) allows an end user to store a maximum of ten (i.e., 0 to 9) often dialed DN's; therefore, SCS supports a single Speed Calling cell digit access. Nortel's Speed Calling Long (SCL) allows an end user to store up to seventy (i.e., 00 to 69) often dialed DN's; therefore, SCL supports two digits for Speed Calling Cell access.

Note: for SCL (i.e., L30, L50 or L70), the end user must dial both digits of the two digit Speed Calling code, even if the first digit is zero.

This design intent makes the assumption that from the Speed Calling Cell digits provided (from the end user), a single Speed Calling (SC) digit indicates SCS, and two SC digits indicate SCL or Speed Calling User (SCU)¹.

GR-1298-Core allows for Group9 Update request(s); however, it does not provide for a Group9 Query message in order to retrieve/query the user's

Speed Call data. However, Nortel will utilize the Extension Parm to retrieve/query a Block of 20 DNs (per Group9 Query Message). Each Query Block (of DNs) are labeled 0 to 5. For instance:

Nortel's Group9 Query Action Block_x: where x = 0 through 5:

- Query Action Block₀ contains DNs associated with Speed Call Codes 0 to 19
- Query Action Block₁ contains DNs associated with Speed Call Codes 00 to 19
- Query Action Block₂ contains DNs associated with Speed Call Codes 20 to 39
- Query Action Block₃ contains DNs associated with Speed Call Codes 40 to 59
- Query Action Block₄ contains DNs associated with Speed Call Codes 60 to 79
- Query Action Block₅ contains DNs associated with Speed Call Codes 80 to 99

Nortel's Group9 Query Action Block₀ is utilized for Speed Call Short only. Since Nortel's Speed Call Short list could contain up to a maximum of 10 DNs associated with a Speed Call Code, only the first 10 indexes (0 to 9) of Block₀ will be utilized for a Speed Call query. The remaining indexes (10 to 19) will contain NIL DNs.

Nortel's Group9 Query Action Blocks 1-5 (i.e., Blocks1 through Blocks5) are utilized for Speed Call Long only.

Speed Calling directory number validation will be performed if the Speed Calling Validation (SCVAL) option is provisioned in Table CUSTSTN.

Please reference the appendix for Nortel's Group9 Query implementation, which utilizes the Extension Parm. Also, please refer to section for support of AINDigits Parm. This parm is not supported for Group9 in GR-1298 and GR-1299.

Hardware Requirements or Dependencies

In order to enable this capability for affected subscribers, the following must be present in the provider's network:

-
1. SCU - Speed Calling User: this user is allowed (if provisioned with the SCU Servord line option) to have access to a Speed Calling Long list. However, for this feature deployment, the SCU user is not allowed to add, change or query the Speed Calling list - only the SCL controller is allowed to modify or to query their SCL list.

- EO Switch providing the affected services must be enabled to handle the corresponding update and/or queries request via SS7.

Software Requirements or Dependencies

A number of services are controlled via software optionality control (SOC). In order to use these services, appropriate SOC's must be activated in the switch. Therefore, this development depends on the following SOC's:

- AIN00002 - Essentials
- AIN00006 - Call Management
- AIN00210 - Service Enablers
- RES00008 - Long Distance Indicator
- RES00059 - LDA Enhancement
- RES00047 - Call Screening
- RES00053 - Enhanced CSMI
- RES00060 - Usage Sensitive Call Forwarding
- RES00073 - SLE/ACBAR NO TCAP
- RES00081 - Simultaneous Ring
- RES00085 - SimRing Virtual DN
- RES00102 - Enh Do Not Disturb

Limitations and restrictions

As discussed previously, the initial release of this capability is coupled to AIN, specifically for signaling support and primary message (ASN.1) encoding/decoding functions.

Because each group/service pair has its own unique set of limitations/restrictions, a table is being provided to capture what, if any, limitations are present for each application.

Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
1	Message Waiting Indicator	To support MWI, MSRID is required to be sent by off-board processor and it has to be data filled in Table MSRTAB in the DMS. In the response of the query for MWI status, the ON/OFF status is sent back to the off-board system. The requestor DN which is stored against the agent will not be sent because GR-1298-Core does not support any additional data. The DMS supports following type of Message Waiting Indicator and Services: Message Waiting Lamp - for Integrated Business Network (IBN) and Key Set (KSET) lines in business Stutter Dial Tone (STD) - for Residential (RES) lines in residential and IBN lines in business environment. Class Message Waiting Indicator (CMWI) for RES lines in form of STD. All existing Message Waiting (MWT) limitations and restrictions for activation and deactivation are the same and applicable to query and update messages for MWT. Also, please refer to AIN Service Implementation Guide (SIG) for more details.
1	Visual Message Waiting Indicator	To support MWI, MSRID is required to be sent by off-board processor and it has to be data filled in Table MSRTAB in the DMS. In the response of the query for MWI status, the ON/OFF status is sent back to the off-board system. The requestor DN which is stored against the agent will not be sent because GR-1298-Core does not support any additional data. The DMS supports following type of Message Waiting Indicator and Services: Message Waiting Lamp - for IBN and KSET lines in business STD - for RES lines in residential and IBN lines in business environment. CMWI for RES lines in form of STD. The DISPLAY TEXT is not supported. All existing MWT limitations and restrictions for activation and deactivation are the same and applicable to query and update messages for MWT. Also, please refer to AIN SIG for more details.
1	Anonymous Caller Rejection	All existing Anonymous Caller Rejection (ACRJ) limitations and restrictions for activation and deactivation are the same and applicable to query and update messages for ACRJ.

Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
1	Automatic Callback	The only portion is supported to deactivate the Automatic Callback (ACB) as per GR-1298-Core. The activation request for ACB is rejected. All existing Automatic Callback (ACB) limitations and restrictions for deactivation are the same and applicable to query and update messages for ACB.
1	Automatic Recall	The only portion is supported to deactivate the Automatic Recall (AR) as per GR-1298-Core. The activation request for AR is rejected. All existing Automatic Recall (AR) limitations and restrictions for deactivation are the same and applicable to query and update messages for AR.
1	Call Screening	The Call Screening, Monitoring and Intercept (CSMI) is supported for both residential and business lines. All existing CSMI limitations and restrictions for activation and deactivation are the same and applicable to query and update messages for CSMI.
1	Outside Calling Area Alerting	The Outside Calling Area Alerting is known as long distance alerting (LDA) in DMS. The LDA service along with LDA Enhancement (LDAE) supports LDSV, LDSO, LDSA, LDSR and LDST options in DMS switch. Out of these options, the only option allows end user to activate/deactivate is LDSA using access code. The query and update messages are only applicable to LDSA state and activation/deactivation. If LDS_AUTO_PROV_ENABLED office parameter is set to "Y", the LDSA is automatically provisioned to line if the LDSV option is data filled in Table LINEATTR. User action to deactivate is ignored by the LDSA service. The update message for LDSA is ignored. All existing LDSA limitations and restrictions for activation and deactivation are the same and applicable to query and update messages for LDSA.

Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
1	Calling Identity Delivery and Suppression	The Calling Identity Delivery and Suppression (SUPPRESS) is only supported for the PUBLIC network. The query returns the current status of the line as public or private. The update request to activate change the status pps to public. The update request to deactivate change the status pps to private. If current status is public and deactivate request is received, no change made to the status. If current status is private and activate request is received, no change made to the status. All existing SUPPRESS limitations and restrictions for activation and deactivation are the same and applicable to query and update messages for SUPPRESS.
1	Call Waiting	The call waiting (CWT) service is always active on all the lines when assigned in the switch. It is only deactivated when Cancel Call Waiting (CCW) access code is dialed. In the response to the query request following is sent for CWT: If only CWT option is assigned to the line than the status of CWT is active. If CWTACT is also assigned to the line than the status of CWTACT. In the response to the update request following activation/deactivation are done: If only CWT option is assigned to the line than activate/deactivate request are rejected because we can not change the status of CWT on the line. If CWTACT is also assigned to the line than the activate request change the status to active and deactivate request change the status to inactive. Prior to this release CWTACT was only supported for the business lines. This feature also makes CWTACT available to RES lines as well. All existing CWT and CWTACT limitations and restrictions for activation and deactivation are the same and applicable to query and update messages for CWT and CWTACT.

Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
1	Make Set Busy	The Make Set Busy (MSB) is not required nor supported by GR-1298-Core and GR-1299-Core. This is a group 1 service supported by this activity as additional supported service. The activate request turns MSB “ON” and deactivate request turns MSB “OFF”. All existing MSB limitations and restrictions for activation and deactivation are the same and applicable to query and update messages for MSB. For encoding/decoding of MSB, please refer to Section .
2	Audio Message Waiting Indicator	The GR-1298 defined Audio Message Waiting Indicator (AMWI) allows control of both MWT indication for the line in terms of ping ring at a programmable interval. This is the main difference between MWT in group1 and AMWI in group2. The DMS service PRN falls under AMWI category while all other flavor of MWT in DMS are Group1 services. The delay interval is not supported. The CM feature Periodic Ringing Notification (PRN) can only be activated or deactivated because PRN does not allow to control the ring interval or delay interval.

Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
3	Distinctive Ringing/Call Waiting	GR-219-Core provides the following guidance with respect to Distinctive Ringing/Call Waiting (DRCW) Traffic Measurements: Hourly peg counts and usage counts with a usage scan rate of 1 per 10 seconds for SCRJ screen editing, for attempts to invoke control procedures as a result of dialing either SCF service access code (*61 or *81) The end-office will peg any DRCW editing attempt as though the subscriber had instigated the editing session via service access code, therefore, the existing set of DRCW OMs will be used to reflect the measurements for both service access code and/or off-board service control attempts. For more information, please refer to the chapter discussing performance. DRCW editing will be denied if DOR option present. In such instances, a result cause of <i>denied unsuccessful update (27)</i> will be provided in the update response. DRCW editing will be denied if DENY DRCW option present. In such instances, a result cause of <i>denied unsuccessful update (27)</i> will be provided in the update response. Attempts to add Extension DNs to an IBN subscriber's DRCW list is not supported.^a TCAP DN validation will not be performed for ADDs in which the source of the DN to be added is either incoming call memory or an existing SpeedCall cell entry. The office parameter that controls the maximum number of SLE programmers allowed at any given time (SLE_MAX_PROGRAMMERS) will have no affect on SLE programming performed via the off-board service control interface. A response of <i>confAllAnonymousEntriesRemoved</i> will be returned for <i>Delete All Anonymous Entries</i> update requests in which no private DNs are present in the subscriber's list. When editing DRCW via Universal Access, the initial edit/query attempt will automatically add DRCW to the subscriber's line and take on the characteristics of DRCW as defined in table RESOFC. Edit attempts with SOCOption AIN00322 IDLE will result in a SLE106 log being generated. A response of <i>deniedUnsuccessfulUpdate</i> will be returned for ADD attempts in which DN validation fails. For entire list queries in which the number of DNs in the list exceeds 32, only the first 32 entries will be reported in the query response and a SLE106 log will be generated.

Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
3	Selective Call Rejection	- GR-218-Core provides the following guidance with respect to Selective Call Rejection (SCRJ) Traffic Measurements: <i>Hourly peg counts and usage counts with a usage scan rate of 1 per 10 seconds for SCRJ screen editing, for attempts to invoke control procedures as a result of dialing either SCF service access code (*60 or *80)</i> - The end-office will peg any SCRJ editing attempt as though the subscriber had instigated the editing session via service access code, therefore, the existing set of SCRJ OMs will be used to reflect the measurements for both service access code and/or off-board service control attempts. For more information, please refer to the chapter discussing performance. - SCRJ editing will be denied if DOR option present. In such instances, a result cause of <i>denied unsuccessful update (27)</i> will be provided in the update response. - SCRJ editing will be denied if DENY SCRJ option present. In such instances, a result cause of <i>denied unsuccessful update (27)</i> will be provided in the update response. - Attempts to add Extension DN's to an IBN subscriber's SCRJ list is not supported. - TCAP DN validation will not be performed for ADDs in which the source of the DN to be added is either incoming call memory or an existing SpeedCall cell entry. - The office parameter that controls the maximum number of SLE programmers allowed at any given time (SLE_MAX_PROGRAMMERS) will have no affect on SLE programming performed via the off-board service control interface. - A response of <i>confAllAnonymousEntriesRemoved</i> will be returned for <i>Delete All Anonymous Entries</i> update requests in which no private DN's are present in the subscriber's list. - When editing SCRJ via Universal Access, the initial edit/query attempt will automatically add SCRJ to the subscriber's line and take on the characteristics of SCRJ as defined in table RESOFC. - Edit attempts with SOCOption AIN00322 IDLE will result in a SLE106 log being generated. - A response of <i>deniedUnsuccessfulUpdate</i> will be returned for ADD attempts in which DN validation fails. - For entire list queries in which the number of DN's in the list exceeds 32, only the first 32 entries will be reported in the query response and a SLE106 log will be generated.

Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
3	Simultaneous Ringing	- The <i>EditSpecificEntry</i> field values of “add” or “delete” will be interpreted to add or delete only the NON-Pilot Member DN of a SIMRING group. <i>EditAllEntries</i> field with a value of “deleteAllEntries” is interpreted as deleting only the Non-Pilot Member DNs in the SIMRING group. <i>EditSpecificEntry</i> field with value of “delete” will result in SIMRING getting deactivated on the PILOT DN if no entries remain on the list. <i>EditAllEntries</i> field with a value of “deleteAllEntries” will result in SIMRING getting deactivated on the PILOT DN. <i>EditAllEntries</i> field with a value of “deleteAllPrivateEntries” is NOT valid for SIMRING. The update message with this action field will result in UnavailableResources result Cause being sent back as return error component. - The UPDATE message cannot edit the Non Pilot Member DN list during a SIMRING call (i.e. while all the member DNs are ringing). - Attempts to add NON-Pilot Member DNs via the ICM or given SpeedCall cell entry are not supported for SIMRING. - Edit attempts with SOCOption AIN00327 IDLE will result in a SLE106 log being generated. - A response of <i>deniedUnsuccessfulUpdate</i> will be returned for ADD attempts in which DN validation fails.
4	Call Forwarding Variable	Courtesy call during activation is not supported. No AIN triggers will be encountered during programing. ISDN agents are not supported. In a case involving updating the activation data for a call forward keylist, consistency will be retained between this feature and the present DMS call forwarding code as to what constitutes a successful updating. When the call forward service is deactivated, it will not clear the forwarding DN. This is to maintain consistency with the current DMS implementation. When the forwarded to DN is cleared, the call forwarding service will also be deactivated. The forwarded to DN may be up to 30 digits in length. CFU Per Key is not supported.

Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
4	Call Forwarding Don't Answer	Courtesy call during activation is not supported. No AIN triggers will be encountered during programing. Integrated Services Digital Network (ISDN) agents are not supported. In a case involving updating the activation data for a call forward keylist, consistency will be retained between this feature and the present DMS call forwarding code as to what constitutes a successful updating. When the call forward service is deactivated, it will not clear the forwarding DN. This is to maintain consistency with the current DMS implementation. When the forwarded to DN is cleared, the call forwarding service will also be deactivated. The forwarded to DN may be up to 30 digits in length. CFB Per Key is not supported.
4	Call Forwarding Busy Line	Courtesy call during activation is not supported. No AIN triggers will be encountered during programing. ISDN agents are not supported. In a case involving updating the activation data for a call forward keylist, consistency will be retained between this feature and the present DMS call forwarding code as to what constitutes a successful updating. When the call forward service is deactivated, it will not clear the forwarding DN. This is to maintain consistency with the current DMS implementation. When the forwarded to DN is cleared, the call forwarding service will also be deactivated. The forwarded to DN may be up to 30 digits in length. CFD Per Key is not supported.

Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
5	Selective Call Forward	- GR-217-Core provides the following guidance with respect to Selective Call Forwarding (SCF) Traffic Measurements (section 3.5.4): <i>Hourly peg counts and usage counts with a usage scan rate of 1 per 10 seconds for SCF screen editing, for attempts to invoke control procedures as a result of dialing either SCF service access code (*63 or *83)</i> - The end-office will peg any SCF editing attempt as though the subscriber had instigated the editing session via service access code, therefore, the existing set of SCF OMs will be used to reflect the measurements for both service access code and/or off-board service control attempts. For more information, please refer to the chapter discussing performance. - SCF editing will be denied if DOR option present. - SCF editing will be denied if DENY SCF option present. - If there are no entries in the list <i>and</i> no forwarding DN present, attempts to enable SCF will fail with a result cause of <i>denied invalid Forward DN</i>(17). - Attempts to add Extension DNs to an IBN subscriber's SCF list is not supported. - TCAP DN validation will not be performed for ADDs in which the source of the DN to be added is either incoming call memory or an existing SpeedCall cell entry. - The office parameter that controls the maximum number of SLE programmers allowed at any given time (SLE_MAX_PROGRAMMERS) will have no affect on SLE programming performed via the off-board service control interface. - A response of <i>confAllAnonymousEntriesRemoved</i> will be returned for <i>Delete All Anonymous Entries</i> update requests in which no private DNs are present in the subscriber's list. - When editing SCF via Universal Access, the initial edit/query attempt will automatically add SCF to the subscriber's line and take on the characteristics of SCF as defined in table RESOFC. - Edit attempts with SOCOption AIN00322 IDLE will result in a SLE106 log being generated. - A response of <i>deniedUnsuccessfulUpdate</i> will be returned for ADD attempts in which DN validation fails. - For entire list queries in which the number of DNs in the list exceeds 32, only the first 32 entries will be reported in the query response and a SLE106 log will be generated.

Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
5	Selective Call Acceptance	- GR-1298-Core provides for Selective Call Acceptance (SCA) to define the <i>no call acceptance treatment</i> as being a forwarding DN. Nortel Network's version of SCA does not allow for this capability. - The end-office will peg any SCA editing attempt as though the subscriber had instigated the editing session via service access code, therefore, the existing set of SCA OMs will be used to reflect the measurements for both service access code and/or off-board service control attempts. For more information, please refer to the chapter discussing performance. - SCA editing will be denied if DOR option present. - SCA editing will be denied if DENY SCA option present. - Attempts to add Extension DNs to an IBN subscriber's SCA list is not supported. - TCAP DN validation will not be performed for ADDs in which the source of the DN to be added is either incoming call memory or an existing SpeedCall cell entry. - The office parameter that controls the maximum number of SLE programmers allowed at any given time (SLE_MAX_PROGRAMMERS) will have no affect on SLE programming performed via the off-board service control interface. - A response of <i>confAllAnonymousEntriesRemoved</i> will be returned for <i>Delete All Anonymous Entries</i> update requests in which no private DNs are present in the subscriber's list. - When editing SCA via Universal Access, the initial edit/query attempt will automatically add SCA to the subscriber's line and take on the characteristics of SCA as defined in table RESOFC. - Edit attempts with SOCOption AIN00322 IDLE will result in a SLE106 log being generated. - A response of <i>deniedUnsuccessfulUpdate</i> will be returned for ADD attempts in which DN validation fails. - For entire list queries in which the number of DNs in the list exceeds 32, only the first 32 entries will be reported in the query response and a SLE106 log will be generated.
6	Ring Control	Only supported for a ring control type of PRGRING. One ring will last 8s for lines off of non-RDT peripherals and 6s for lines off of Remote Digital Terminal (RDT) peripherals. The number of rings can range between what the OFCENG parm RINGCTRL_MIN_VALUE is set to and 9.
7	Calling Number Delivery Blocking	A DN's Permanent Presentation Status (PPS) is stored in table DNATTRS under the SUPPRESS option. The CNDB feature allows the caller to override the Number portion of the PPS on a per-call basis. The line must be subscribed to the CNDB line or customer group option or the CNDB Universal option. The agent must be off-hook and in the dialing state for the CNDB service to be invoked.

Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
7	Calling Name Delivery Blocking	A DN's Permanent Presentation Status (PPS) is stored in table DNATTRS under the SUPPRESS option. The CNAB feature allows the caller to override the Name portion of the PPS on a per-call basis. The line must be subscribed to the CNAB line or customer group option or the CNAB Universal option. The agent must be off-hook and in the dialing state for the CNAB service to be invoked.
8	Customer Originated Trace	- As per GR-216-Core and the CM implementation of the Customer Originated Trace (COT) feature, two activation levels (ACTLEVEL) are available for conventional users accessing the feature via an access code on telephone. The UPDATE message will allow invoking of the COT feature only for ACTLEVEL of ONELEVEL, which does NOT have any confirmation prompt announcements for the user accessing the feature. - The UPDATE message will not be supporting any announcements or any language related enhancements for the COT feature invocation. - If the COT has already been activated by the user via the access code from a telephone for the last incoming call then if an UPDATE message is used for the COT invocation, then it will be treated like a repeat attempt. The same will be valid in vice-versa scenario.
8	Cancel Call Waiting	- The user can use the UPDATE message to activate Cancel Call Waiting (CCW) only when the user is already off hook and getting a dial tone or is already on a call (single party or multiparty). - If the user invokes CCW through the UPDATE message while being off hook, then the user will not hear any audible confirmation tone for the invocation.

Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
9	Speed Calling	- GR-1299-Core provides numbers 2 through 9 (for Speed Call Short) or numbers 20 through 39 (for Speed Call Long) as the Speed Calling Code(s) for the Group9 Update Message. Nortel will support these GR required Speed Calling Code range. However, Nortel exceeds the GR-1299-Core standard by supporting the following Speed Call Code(s) (from NTP 297-8021-350, Standard 14.02, May 2001): - single digit Speed Call Cell range 0 to 9 for Speed Call Short (SCS), and - two digit Speed Call Cell range 00 to 69 for Speed Call Long (SCL) or Speed Call User (SCU) - GR-1299-Core does not provide for a Group9 Query message in order to retrieve/query the user's Speed Call data. However, Nortel will utilize the Extension Parm to retrieve/query a Block of 20 DNs (per Group9 Query Message). Each Query Block (of DNs) are labeled 0 to 5. For example: Nortel's Group9 Query Action Block_X: where X = 0-5: - Query Action Block₀ contains DNs associated with Speed Call Codes 0 to 19 - Query Action Block₁ contains DNs associated with Speed Call Codes 00 to 19 - Query Action Block₂ contains DNs associated with Speed Call Codes 20 to 39 - Query Action Block₃ contains DNs associated with Speed Call Codes 40 to 59 - Query Action Block₄ contains DNs associated with Speed Call Codes 60 to 79 - Query Action Block₅ contains DNs associated with Speed Call Codes 80 to 99 - Nortel's Group9 Query Action Block₀ is utilized for Speed Call Short only. Since Nortel's Speed Call Short list could contain up to a maximum of 10 DNs associated with a Speed Call Code, only the first 10 indexes (0 to 9) of Block₀ will be utilized for query. The remaining indexes (10 to 19) will contain NIL DNs. - Nortel's Group9 Query Action Blocks 1-5 (i.e., Blocks₁ through Blocks₅) are utilized for Speed Call Long only.

Limitations and Restrictions for each service

Group	Service	Limitations/Restrictions
9	Speed Calling	- GR-1299-Core provides that the Group9 Update Speed Call DN be a maximum of 10 digits per Speed Call Cell. Note: Nortel will support the GR-1299-Core requirement for a 10 digit Speed Call DN per Cell. In addition, Nortel will support an AINDigit DN which supports up to 30 digits for a Speed Call DN per Cell. - Nortel's Speed Call Design intent indicates that from the Speed Calling Cell digits provided (from the end user), a single Speed Calling Cell digit indicates Speed Calling Short, and two Speed Calling Cell digits indicate Speed Calling Long or Speed Calling User (SCU)^b. - Only the Speed Call Controller is allowed to receive or query their Speed Calling List - not a Speed Calling User (SCU). - End to End Speed Call Signaling is not supported. - The Group9 Query Response Extension Parm contains the following fields: - Count: the total number of Speed Calling DN's within this Block_x (up to 20). - DN Bytes: the number of bytes needed to represent the Speed Calling DN. Note: this range is 1 to 15, where 15 bytes represents 30 Digits. - SC Cell: the Speed Calling Cell associated with the Speed Calling DN. - SC DN: the Speed Calling DN. NOTE: if there's an odd number of Speed Calling Digits, the ending nibble will be hex F. - Please reference NTP 297-8021-350, Standard 14.02, May 2001 for all Nortel Speed Call limitations/restrictions. The Group9 Update/Query Event Handler will support the following: - Update Result Causes: - <i>deniedUnsuccessfulUpdate</i> - <i>confServiceActivated</i> - Update Return Result: - <i>UPD_UnavailableResources</i> - <i>UPD_OK</i> - Query Result: - <i>QR_Unavailable_Resources</i> - <i>QR_OK</i>

a. support EXTN DN's is possible given that EXTN is specified in the ADD DN update request - EXTN parm is currently not supported in the protocol but could be added as an extension parm of both group3 and group5 services.

b. SCU - Speed Calling User: this user is allowed (if provisioned with the SCU Servord line option) to have access to a Speed Calling Long list. However for this feature deployment, the SCU user is not allowed to add, change or query the Speed Calling list - only the SCL controller is allowed to modify or to query their SCL list.

Appendix A for A00004036: Supplementary Details

This section contains additional details for the encoding and decoding services which are not supported by the GR-1298 and GR-1299. It also contains the details of Nortel's Extension Parameter(s) to support additional services and functionalities.

Make Set Busy Encoding and Decoding

The Make Set Busy service is not described in the GR-1299, Issue 7, Nov. 2001, ASN.1 encoding. The following extension to the GR-1299 ASN.1 encoding provides the Make Set Busy service accessible via update messages (Page 6-17, Section 6.4.2, GR-1299-Core, Issue 7, Nov. 2001):

```
Service1 ::= ENUMERATED {  
    messageWaitingIndicator (0),  
    visualMessageWaitingIndicator (1),  
    anonymousCallRejection (2),  
    automaticCallback (3),  
    automaticRecall (4),  
    callScreening (5),  
    outsideCallingAreaAlerting (6),  
    callingIdPresentAndSuppress (7),  
    callWaiting (8),  
    makeSetBusy (9)  
}
```

The RequestGroup1 in Section 6.114, Page 6-110 of GR-1299-Core, Issue 7, Nov. 2001 refers to above Service1 for the Query request. The above change also apply to RequestGroup1, Service1 as well to provide the query request of the makeSetBusy service.

The same changes also apply to Page C-57 and C-79, ASN.1 Modules to provide makeSetBusy service under Service1 category.

The following is a hex and ASCII representation of the makeSetBusy Query, makeSetBusy Update request without AMASLPID and makeSetBusy Update request with AMASLPID:

makeSetBusy in Query Request:

BF 72

09

A1

07

81 01 09

82 02 07 80

ProvideInfo

(

RequestGroup1

(

Service1(makeSetBusy)

Request1(activationStatus)

)

)

makeSetBusy in Update Request without AMASLPID (Activate Request):

A2

06

81 01 09

82 01 01

UpdateGroup1

(

Service1(makeSetBusy)

Action1(on)

)

makeSetBusy in Update Request without AMASLPID (Deactivate Request):

A2

06

81 01 09

82 01 00

UpdateGroup1

(

Service1(makeSetBusy)

Action1(off)

)

makeSetBusy in Update Request with AMASLPID (Activate Request):

BF 67

11

A1

07

81 05 16 63 12 53 31

A2

06

81 01 09

82 01 01

8A 05 11 11 11 11 01

SSPUserResource

(

```
SSPUserID
(
  DN(6136213513)
)
UpdateGroup1
(
  Service1(makeSetBusy)
  Action1(on)
)
)
AMASlpID(11111111)
```

makeSetBusy in Update Request with AMASLPID (Deactivate Request):

```
BF 67
11
A1
07
81 05 16 63 12 53 31
A2
06
81 01 09
82 01 00
8A 05 21 43 65 87 09
```

```
SSPUserID
(
  SSPUserID
```

```
(  
    DN(6136213513)  
)  
UpdateGroup1  
(  
    Service1(makeSetBusy)  
    Action1(off)  
)  
)  
AMASlpID(123456789)
```

Simring Encoding and Decoding

The Simring (simultaneousRinging) service is not described in the GR-1299, Issue 7, Nov. 2001, ASN.1 encoding. The following extension to the GR-1299 ASN.1 encoding provides the Simring service accessible via update messages (Page 6-18, Section 6.4.2, GR-1299-Core, Issue 7, Nov. 2001):

```
Service3::=ENUMERATED{  
    distinctiveRingingCallWaiting (0),  
    selectiveCallRejection (1),  
    simultaneousRinging (2)  
}
```

The RequestGroup3 in Section 6.114, Page 6-110 of GR-1299-Core, Issue 7, Nov. 2001 refers to above Service3 for the Query request. The above change also apply to RequestGroup3, Service3 as well to provide the query request of the simring service.

The same changes also apply to Page C-59 and C-80, ASN.1 Modules to provide simring service under Service3 category.

The following is a hex and ASCII representation of the simring query and update requests:

Simring Query Request:

BF 72

09

A3

07

81 01 02

82 02 07 80

ProvideInfo

(

RequestGroup3

(

Service3(simultaneousRinging)

Request3(activationStatus)

)

)

Simring Update Request:

A4

09

81 01 02

A3

04

9F 69 01 00

UpdateGroup3

(

Service3(simultaneousRinging)

EditSpecificEntry

```
(  
    EditListType(addListElement)  
)  
)
```

Support of AINDigits Parameter in Call Forwarding and Speed Call

Call Forwarding and Speed Call are not described in GR-1299 Issue 7, Nov.2001, with having the capability to use up to thirty digit DNs (long DN). The following description captures how up to long DNs can now be used.

Service groups 3, 4, 5 and 9 have the ability to send a update request with long DNs. And service groups 3, 4 and 5 have the ability to receive a query request that contain long DNs.

Long DNs are not used to specify the UserResourceID. They're only permitted for example, when updating the ForwardingDN in a Call Forward Variable (CFU) request.

AdministrableObject Changes:

Service Group 3

Entry::=CHOICE {

[1] IMPLICIT Dn.

[2] IMPLICIT SpeedCallingCode,

[3] IMPLICIT MemorySlot,

[4] IMPLICIT AINDigits

}

-- AINDigits parameter supports up to 30 digits.

Service Group 4

Set::=CHOICE {

[1] IMPLICIT Dn,

[4] IMPLICIT SpeedCallingCode,


```
[5] IMPLICIT AINDigits
```

```
}
```

```
-- AINDigits parameter supports up to 30 digits.
```

Service Group 5

The above new definition, SET, is used indirectly by Service Group 5.

Service Group 9

```
ChangeList::=SEQUENCE {
```

```
[1] IMPLICIT Dn,
```

```
[2] IMPLICIT SpeedCallingCode,
```

```
[3] IMPLICIT AINDigits
```

```
}
```

```
-- AINDigits parameter supports up to 30 digits.
```

InfoProvided Changes:

All Service Groups will use this new query definition.

```
InfoProvided::=[100] IMPLICIT SEQUENCE {
```

```
[1] IMPLICIT ActivationStateCode OPTIONAL
```

```
[2] IMPLICIT EntireList OPTIONAL
```

```
[3] IMPLICIT MemorySlot OPTIONAL
```

```
[4] IMPLICIT ListSize OPTIONAL
```

```
[5] IMPLICIT ForwardToDn OPTIONAL
```

```
[6] IMPLICIT DelayInterval OPTIONAL
```

```
[7] IMPLICIT Empty OPTIONAL,
```

```
[8] IMPLICIT ListSizeVarDN OPTIONAL,
```

```
[9] IMPLICIT ForwardToVarDN OPTIONAL
```

```
}
```

```
ListSizeVarDN ::= SEQUENCE {
```

```
    AINDigits
```

```
}
```

-- ListSizeVarDN is a new field that uses type AINDigits, which supports up to 30 digits.

```
ForwardToVarDN ::= SEQUENCE {
```

```
    AINDigits
```

```
}
```

-- ForwardToVarDN is a new field that uses type AINDigits, which supports up to 30 digits.

Example: Call Forward Query Request Response

BF 64

0B

81 01 00

89 06 80 00 27 43 05 00

InfoProvided

(

 ActivationStateCode(off)

 ForwardToVariableDn(notApplicable odd
unknownOrNotApplicable 7234500)

)

Example: Call Forward Update Request

A5

0D

81 01 00

A3

08

84 06 80 00 27 43 05 00

UpdateGroup4

(

Service4(callForwardingVariable)

ForwardingDN

(

VariableDn(notApplicable odd unknownOrNotApplicable
7234500)

)

)

Example: Speed Call Update Request

AA

11

81 01 00

A2

0C

83 06 80 00 27 43 15 00

82 02 32 33

UpdateGroup9

(

Service9(speedCalling)

ChangeList

(

```
VariableDn(notApplicable odd unknownOrNotApplicable
7234510)

SpeedCallingCode(23)

)

)
```

Speed Call Query Request Extension Parameter

The Speed Calling Query Request Extension Parameter contains the following fields:

- AssignmentAuthority: this field is utilized to identify if this particular Extension Parm is appropriate for this vendor's switch.
- NCRSpeedCallQueryRequest(x), where x = 0-5: the non-call response (NCR) parm identifies the Speed Calling Query Action Block request.

Note: the Speed Calling Query Action Block number (0 through 5) dictates which Speed Calling DN(s) will be retrieved:

- Query Action Block₀ contains DNs associated with Speed Call Codes 0 to 19
- Query Action Block₁ contains DNs associated with Speed Call Codes 00 to 19
- Query Action Block₂ contains DNs associated with Speed Call Codes 20 to 39
- Query Action Block₃ contains DNs associated with Speed Call Codes 40 to 59
- Query Action Block₄ contains DNs associated with Speed Call Codes 60 to 79
- Query Action Block₅ contains DNs associated with Speed Call Codes 80 to 99

Listed below are two Speed Calling Query Request examples: one for Speed Calling Short (SCS), and one for Speed Calling Long (SCL):

- Speed Calling Short (SCS) Query Request example:

Speed Calling SCS Example

```

>qlen 0 0 0 13
-----
LEN:      HOST  00 0 00 13
TYPE: SINGLE PARTY LINE
SNPA: 613
DIRECTORY NUMBER:      6212233
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:      BNR      SUBGRP: 0  NCOS: 0
SIGNALLING TYPE:  DIGITONE
CARDCODE: 6X17AC      GND: N  PADGRP: STDLN  BNV: NL MNO: N
PM NODE NUMBER      :      67
PM TERMINAL NUMBER  :      14
OPTIONS:
DGT SCS
-----

```

Speed Calling SCS Example cont.

```

>t ibnsc
TABLE: IBNSC
IBNSCKEY RESULT
-----
HOST 00 0 00 13 0 SCS 3 8675309 <----- odd number of digits (DN1)
HOST 00 0 00 13 0 SCS 7 9195521200 <--- even number of digits (DN2)

Group 9 Query Request for Action 0:
=====
MESSAGE
qr9extension0:
QueryWithPermission
(
  OriginationTransactionID(0000029D)
  Components
  (
    InvokeLast
    (
      InvokeID(01 00)
      PrivateTCAP
      QueryRequest
      ParameterSequence
      (
        UserID
        (
          DN(6136212233) <---Speed Calling Subscriber
        )
        ExtensionParameter
        (
          AssignmentAuthority(BR549)
          NCRSpeedCallQueryRequest(0) <---Action Block 0
        )
      )
    )
  )
)
;

```

Speed Calling SCS Example cont.

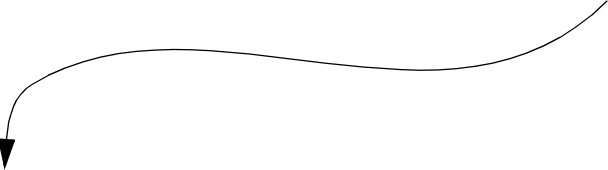
```

Group 9 Query Response for Action 0:
=====
MESSAGE
Response
(
  DestinationTransactionID(0000029D)
  Components
  (
    ReturnResultLast
    (
      CorrelationID(01)
      ParameterSequence
      (
        ExtensionParameter
        (
          AssignmentAuthority(BR549)
          NCRSpeedCallQueryResponse(020403685703F905071959252100)
        )
      )
    )
  )
)
;

```

where 020403685703F905071959252100:

- 02 - Number of Speed Calling DN(s): 2
- 04 - Number of DN Bytes for DN1: 4 bytes
- 03 - Speed Calling Cell assignment: 3
- 685703F9- DN1: 6875309 (Notice the ending hex F for odd number of digits)
- 05 - Number of DN Bytes for DN2: 5 bytes
- 07 - Speed Calling Cell assignment: 7
- 1959252100 - DN2: 9195521200



- Speed Calling Long (SCL) Query Request example:

Speed Calling SCL Example

```

>qlen 0 0 0 13
-----
LEN:      HOST  00 0 00 13
TYPE: SINGLE PARTY LINE
SNPA: 613
DIRECTORY NUMBER:      6212233
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:      BNR      SUBGRP: 0  NCOS: 0
SIGNALLING TYPE:  DIGITONE
CARDCODE:  6X17AC      GND: N  PADGRP: STDLN  BNV: NL  MNO: N
PM NODE NUMBER      :      67
PM TERMINAL NUMBER  :      14
OPTIONS:
DGT SCL 0 L30
-----

```

Speed Calling SCL Example cont.

```
>t ibnsc
TABLE: IBNSC
IBNSCKEY RESULT
-----
HOST 00 0 00 13 0 SCL 23 3362921345 <--- even number of digits (DN1)
HOST 00 0 00 13 0 SCL 29 8675309 <----- odd number of digits (DN2)

Group 9 Query Request for Action 2:
=====
MESSAGE
qr9extension2:
QueryWithPermission
(
  OriginationTransactionID(000002B3)
  Components
  (
    InvokeLast
    (
      InvokeID(01 00)
      PrivateTCAP
      QueryRequest
      ParameterSequence
      (
        UserID
        (
          DN(6136212233) <---Speed Calling Subscriber
        )
        ExtensionParameter
        (
          AssignmentAuthority(BR549)
          NCRSpeedCallQueryRequest(2) <---Action Block 2
        )
      )
    )
  )
)
;
```

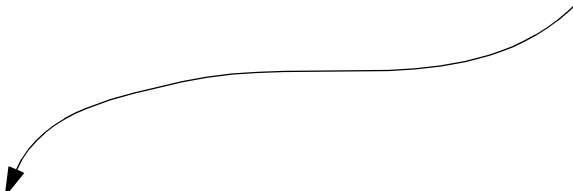
Speed Calling SCL Example cont.

```

Group 9 Query Response for Action 2:
=====
MESSAGE
Response
(
  DestinationTransactionID(000002B3)
  Components
  (
    ReturnResultLast
    (
      CorrelationID(01)
      ParameterSequence
      (
        ExtensionParameter
        (
          AssignmentAuthority(BR549)
          NCRSpeedCallQueryResponse(0205173326293154041D685703F9)
        )
      )
    )
  )
)
;

where 0205173326293154041D685703F9:
02 - Number of Speed Calling DN(s): 2
05 - Number of DN Bytes for DN1: 5 bytes
17 - Speed Calling Cell assignment: 17 hex, 23 dec
3326293154 - DN1: 3362921345
04 - Number of DN Bytes for DN2: 4 bytes
1D - Speed Calling Cell assignment: 1D hex, 29 dec
685703F9 - DN2: 8675309 (Notice the ending hex F for odd number of digits)

```



Extension Parameter ASN.1 Details:- The following details are based on GR1299 Issue 7 requirements and definitions. They follow the ASN.1 notations for Extension Parameter, Assignment Authority and Special Routing Extension Parameter.

ExtensionParameter:-

The following shall be used for the ExtensionParameter (CR6-334 in GR1299 Issue 7, Page 6-77):

```

ExtensionParameter ::= [84] IMPLICIT SEQUENCE {
    assignmentAuthority OBJECT IDENTIFIER,
    parameters ANY DEFINED BY assignmentAuthority
}

```


-- The maximum length of the assignmentAuthority is 15 octets

The parameters field is to be defined by individual service providers. See ITU-T Recommendation X.209 for the encoding rules of OBJECT IDENTIFIERS.

assignmentAuthority:-

The following shall be used for the assignmentAuthority (same as EnvelopeEncodingAuthority - R6-332 in GR1299 Issue 7, Page 6-76):

assignmentAuthority ::= [98] IMPLICIT OBJECT IDENTIFIER

-- Maximum of 15 octets

The following is bit encoding of the assignmentAuthority:

Bit and Octet Encoding of assignmentAuthority

TCAP INFORMATION		ENCODING	In Hex
		HGFEDCBA	
Parameter Identifier	assignmentAuthority (1st octet	10011111	9F
	assignmentAuthority (2nd octet)	01100010	62
Parameter Length		00000111	07
Contents	1st sub-identifier	00101010	2A
	2nd sub-identifier	10000110	86
	3rd sub-identifier	01001000	48
	4th sub-identifier	10000110	86
	5th sub-identifier	11110110	F6
	6th sub-identifier	01111101	7D
	7th sub-identifier	00100100	24

NCRSpeedCallQuery Request:-

The following shall be used for the as NCRSpeedCallQueryRequest (As per ITU-T Recommendation X.209):

NCRSpeedCallQueryRequest ::= [2] CHOICE {

[1] IMPLICIT ActionBlock

}

ActionBlock::=INTEGER (0 .. 5)

-- used to convey to the switch

-- association of Speed Call Codes.

-- 0 indicates that the Speed Call Codes for Speed Call short range from 0 to 9

-- 1 indicates that the Speed Call Codes for Speed Call long range from 00 to 19

-- 2 indicates that the Speed Call Codes for Speed Call long range from 20 to 39

-- 3 indicates that the Speed Call Codes for Speed Call long range from 40 to 59

-- 4 indicates that the Speed Call Codes for Speed Call long range from 60 to 79

-- 5 indicates that the Speed Call Codes for Speed Call long range from 80 to 99

Speed Call Query Response Extension Parameter

The Speed Calling Query Response Extension Parameter contains the following fields:

- **AssignmentAuthority:** this field is utilized to identify if this particular Extension Parm is appropriate for this vendor's switch.
- **NCRSpeedCallQueryResponse:** the non-call response (NCR) parm contains the Speed Calling DN(s) associated with the Query Action Block request.

The NCRSpeedCallQueryResponse contains the following fields:

- **Count:** the total number of Speed Calling DNs within this Action Block_X (up to 20).
- **DN Bytes:** the number of bytes needed to represent the Speed Calling DN. Note: range is 1 to 15, where

- 1 byte - supports 1 or 2 Digits
- 2 bytes - supports 3 or 4 Digits
- 3 bytes - supports 5 or 6 Digits
- 4 bytes - supports 7 or 8 Digits
- 5 bytes - supports 9 or 10 Digits
- 6 bytes - supports 11 or 12 Digits
- 7 bytes - supports 13 or 14 Digits
- 8 bytes - supports 15 or 16 Digits

9 bytes - supports 17 or 18 Digits
 10 bytes - supports 19 or 20 Digits
 11 bytes - supports 21 or 22 Digits
 12 bytes - supports 23 or 24 Digits
 13 bytes - supports 25 or 26 Digits
 14 bytes - supports 27 or 28 Digits
 15 bytes - supports 29 or 30 Digits

- **SC Cell:** the Speed Calling Cell associated with the Speed Calling DN.
- **SC DN:** the Speed Calling DN.

Note: if there's an odd number of Speed Calling Digits, the ending nibble will be hex F.

Please refer to [“Speed Calling SCS Example” on page 1685](#) and [“Speed Calling SCL Example” on page 1686](#) for Speed Calling Query Response examples.

NCRSpeedCallQueryResponse:-

The following shall be used for the as NCRSpeedCallQueryRequest (As per ITU-T Recommendation X.209):

NCRSpeedCallQueryResponse::= [3] IMPLICIT HEX

-- Maximum of 361Octets.

Applicable customer facing sections

Fault Management

Logs	_____X
Alarms	____N/A

Configuration

Data Schema	____N/A
User Interface	____N/A
Element Management	____N/A
Security	____N/A
Service Order	____N/A
Office Parameters	____N/A
Software Optionality Control (SOC)	_____X

Accounting (includes AMA billing)	_____X

Performance (includes operational measurements) _____X

Realtime _____X

Engineering Information _____X

Glossary

Term	Description
CM	Computing Module
SOC	Software Optionality Control
AIN	Advanced Intelligent Network
ASN.1	Abstract Syntax Notation 1
SS7	Signaling System No. 7
TCAP	Transaction Capabilities Application Part
IP	Internet Protocol
SCP	Service Control Point
IBN	Integrated Business Network
KSET	Key Set
SDF	Service Data Function
DN	Directory Number
SIMRING	Simultaneous Ringing
SCS	Speed Calling Short
SCL	Speed Calling Long
SCU	Speed Calling User
SC	Speed Calling
PC	Personal Computer
EO	End-Office
STD	Stutter Dial Tone
RES	Residential
MWT	Message Waiting
CMWI	Class Message Waiting Indicator
ACRJ	Anonymous Caller Rejection

Term	Description
ACB	Automatic Call Back
AR	Automatic Recall
CSMI	Call Screening, Monitoring and Intercept
LDA	Long Distance Alerting
LDAE	Long Distance Alerting Enhancement
SUPPRESS	Calling Identity Delivery and Suppression
CWT	Call Waiting
MSB	Make Set Busy
PRN	Periodic Ringing Notification
DRCW	Distinctive Ringing/Call Waiting
SCRJ	Selective Call Rejection
ISDN	Integrated Services Digital Network
SCA	Selective Call Acceptance
RDT	Remote Digital Terminal
COT	Customer Originated Trace
CCW	Cancel Call Waiting
AMA	Automatic Message Accounting
PPS	Permanent Presentation Status

Configuration for A00004036

Hardware and Software Requirements

NA

Initial Configuration

NA

Office/Subnet parameters (OP/SP) (CM & SESM)

NA

Upgrade Impact

NA

Data schema (DS) (CM, MIBS, RDB)

NA

Service Orders (SO) (CM & SESM)

NA

Software optionality control (SOC)**SOC**

SOC option name:	Off-board Service Control
SOC option title:	Yes
SOC option control type:	state
New SOC option?	Yes
SOC option order code	AIN00321 SVC MGR Basic AIN00322 SVC MGR List Editing AIN00323 SVC MGR Speed Call AIN00324 SVC MGR Call Forward AIN00325 SVC MGR Privacy Control AIN00326 SVC MGR COT and CCW AIN00327 SVC MGR SIMRING
Option defined in DRU:	CNA
Affected products:	SNNCSH07

Element Management

NA

Command interface changes

NA

Security

NA

Configuration Walkthrough

NA

Performance for A00004036

Performance management strategy

Not applicable.

Performance management tools and utilities

Not applicable.

Operational Measurements (OM)

This activity will not be enabling any new OMs, however, similar to operations performed due to service access code driven commands, existing OM groups/registers will be pegged to reflect the relevant incremental update attempts for the same service. For example, an attempt to activate SCF via some off-board interface will be pegged as though the subscriber had gone off-hook and dialed the activation access code for SCF.

For clarity, the following sections will outline in detail what OMs, if any, will be pegged when a request for an off-board service update or change is being processed.

Group1 Services OM Group

The following sub-sections define the OM groups associated with the Group1 services.

The service CSMI and LDS pegs particular OM groups. However, these OM groups are for CallP specific pegging. Therefore, for service control perspective they are not affected nor pegged.

Other Group1 services do not have any OM groups.

ACRJ OM Group

Operational Measures associated with the Anonymous Call Rejection service.

Release history update

Not Applicable

Registers used for Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

ACRJ OM Group Display

ACRJ OM Group Display

>omshow acrj active

ACRJ

CLASS: ACTIVE
START:2003/09/10 08:30:00 WED; STOP: 2003/09/10 09:55:39 WED;
SLOWSAMPLES: 5 ; FASTSAMPLES: 48 ;

ACRJACT ACRJDACT ACRJANN ACRJAUNV
ACRJDUNV ACRJDENY

0				
	0	0	0	0
	0	0		

ACRJACT

Register ACRJACT (Anonymous Call Rejection Activation) will be pegged if the ACRJ Update message successfully activate the ACRJ service.

ACRJDACT

Register ACRJDACT (Anonymous Call Rejection Deactivation) will be pegged if the ACRJ Update message successfully deactivate the ACRJ service.

ACRJAUNV

Register ACRJAUNV (Anonymous Call Rejection Universal Activation) will be pegged if the ACRJ Update message successfully activate the usage based ACRJ service.

ACRJDUNV

Register ACRJDUNV (Anonymous Call Rejection Universal Deactivation) will be pegged if the ACRJ Update message successfully deactivate the usage based ACRJ service.

Register release history update

Not Applicable.

Associated registers

Not applicable.

Associated logs

<None>

AR OM Group

Operational Measures associated with the Automatic Recall service.

Release history update

Not Applicable

Registers used for Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

AR OM Group Display**AR OM Group Display**

```
>omshow ar active
```

```
AR
```

```
CLASS: ACTIVE
```

```
START:2003/09/10 10:00:00 WED; STOP: 2003/09/10 10:13:33 WED;
```

```
SLOWSAMPLES:      1 ; FASTSAMPLES:      1 ;
```

```

      ARATT  ARFDEN  AROVFL  ARLTDA
      ARSTD  ARSTD  ARIMED  ARDLAY
      ARTIME  ARRSCN  ARSCR  ARDATT
      ARPRCD  AROPTO  ARBDIN  ARABT
      ARRACT  ARSTR  ARTSCN  AROSCN
      ARARN  ARNIMED  ARUNIV  ARDENY
      ARPVTBLK  ARPVTALW  ARDSBLID
```

```

0
    0    0    0    0
    0    0    0    0
    0    0    0    0
    0    0    0    0
    0    0    0    0
    0    0    0    0
    0    0    0    0
```

ARDATT

Register ARDATT (Automatic Recall Deactivation ATtempt) will be pegged if the AR Update message to deactivate AR service is received.

ARUNIV

Register ARUNIV (Automatic Recall Universal) will be pegged if the AR Update message to deactivate the Universal AR service is received.

Register release history update

Not Applicable.

Associated registers

Every time Universal AR deactivate request is received, both ARUNIV and ARDATT will be pegged.

Associated logs

<None>

ACB OM Group

Operational Measures associated with the Automatic Call Back service.

Release history update

Not Applicable

Registers used for Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in *bold italics*.

ACB OM Group Display**ACB OM Group Display**

```
>omshow acb active
```

```
ACB
```

```
CLASS: ACTIVE
```

```
START:2003/09/10 08:30:00 WED; STOP: 2003/09/10 10:01:40 WED;
```

```
SLOWSAMPLES: 6 ; FASTSAMPLES: 52 ;
```

```
ACBATT ACBFDEN ACBOVFL ACBLTDA
ACBSTDA ACBSTDT ACBIMED ACBDLAY
ACBTIME ACBRSCN ACBSCR ACBDATT
ACBABT ACBRACB ACBSTR ACBTSCN
ACBOSCN ACBACBN ACBNIMED ACBUNIV
ACBDENY
```

```
0
0 0 0 0
0 0 0 0
0 0 0 0
0 0 0 0
0 0 0 0
0
```

ACBDATT

Register ACBDATT (Automatic Call Back Deactivation ATtempt) will be pegged if the ACB Update message to deactivate ACB service is received.

ACBUNIV

Register ACBUNIV (Automatic Call Back Universal) will be pegged if the ACB Update message to deactivate the Universal ACB service is received.

Register release history update

Not Applicable.

Associated registers

Every time Universal ACB deactivate request is received, both ACBUNIV and ACBDATT will be pegged.

Associated logs

<None>

Group2 Services OM Group

No OM generated for Group2. Therefore, no OM changes identified.

Group3 Services OM Group

Operational Measures associated with the Selective Call Rejection, Distinctive Ring/Call Waiting and Simultaneous Ringing services.

Release history update

Not Applicable

Registers used for SCRJ Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

SCRJ OM Group Display

```
>omshow scrj active
```

```
SCRJ
```

```
CLASS: ACTIVE
```

```
START:2003/10/31 11:30:00 FRI; STOP: 2003/10/31 11:58:19 FRI;
```

```
SLOWSAMPLES: 17 ; FASTSAMPLES: 170 ;
```

```

SCRJEATT SCRJEDEN SCRJEVF SCRJACT
SCRJDACT SCRJEUSG SCRJSAT SCRJSAT2
SCRJSDEN SCRJSBLK SCRJSRJT SCRJUNIV
SCRJDENY SCRJAUNV SCRJDUNV

```

```

0
    0    0    0    0
    0    0    0    0
    0    0    0    0
    0    0    0    0

```

```
>
```

SCRJEATT

Register SCRJEATT (Selective Call ReJection Editing ATtempt) is pegged each time a subscriber updates his/her SCRJ programmed data via some edit session. Similar to the operations performed via service access code controlled edit session, the SCRJEATT register will be pegged for each of the following off-board service update requests.

- addition of DN to a subscriber's SCRJ list
- deletion of a DN from a subscriber's SCRJ list
- request to delete all DNs in a subscriber's SCRJ list
- request to delete all anonymous or private entries in a subscriber's SCRJ list

SCRJEDEN

Register SCRJEDEN (Selective Call ReJection Editing DENial) is pegged each time a subscriber's attempt to update his/her SCRJ programmed data via some edit session is denied. The SCRJEDEN register will be pegged when/if the following is true for a given SCRJ off-board service update request.

- SLE not ENABLED in table CUSTSTN
- SCRJ not ENABLED in table RESOFC

SCRJACT

Register SCRJACT (Selective Call ReJection ACTivation) is pegged each time a subscriber activates his/her SCRJ service. Similar to the operations

performed via service access code controlled activation, the SCRJACT register will be pegged for each occurrence of the an off-board service update activation request.

SCRJDACT

Register SCRJDACT (Selective Call ReJection DeACTivation) is pegged each time a subscriber deactivates his/her SCRJ service. Similar to the operations performed via service access code controlled activation, the SCRJDACT register will be pegged for each occurrence of the an off-board service update deactivation request.

SCRJDENY

Register SCRJDENY (Selective Call ReJection DENY) is pegged each time a subscriber's attempt to update his/her SCRJ programmed data via some edit session is denied due to the presence of the DENY option. The SCRJDENY register will be pegged for each of the following off-board service update request attempts.

- DOR option present on the given SCRJ subscriber's line
- SCRJ enabled office wide and DENY SCRJ option present on the given subscriber's line

Registers used for DRCW Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

DRCW OM Group Display

```
>omshow drew active
```

```
DRCW
```

```
CLASS: ACTIVE
START:2003/10/31 12:00:00 FRI; STOP: 2003/10/31 12:03:59 FRI;
SLOWSAMPLES:    3 ; FASTSAMPLES:    24 ;
```

```

DRCWEATT DRCWEDEN DRCWEOVF DRCWACT
DRCWDACT DRCWEUSG DRCWSAT DRCWSAT2
DRCWSDEN DRCWSBLK DRCWRING DRCWTATT
DRCWTOVF DRCWUNIV DRCWDENY DRCWAUNV
DRCWDUNV
```

```

0
    0    0    0    0
    0    0    0    0
    0    0    0    0
    0    0    0    0
    0
```

```
>
```

DRCWEATT

Register DRCWEATT (Distinctive Ringing Call Wait Editing ATTempT) is pegged each time a subscriber updates his/her DRCW programmed data via some edit session. Similar to the operations performed via service access code controlled edit session, the DRCWEATT register will be pegged for each of the following off-board service update requests.

- addition of DN to a subscriber's DRCW list
- deletion of a DN from a subscriber's DRCW list
- request to delete all DNs in a subscriber's DRCW list
- request to delete all anonymous or private entries in a subscriber's DRCW list

DRCWEDEN

Register DRCWEDEN (Distinctive Ringing Call Wait Editing DENial) is pegged each time a subscriber's attempt to update his/her DRCW programmed data via some edit session is denied. The DRCWEDEN register will be pegged when/if the following is true for a given DRCW off-board service update request.

- SLE not ENABLED in table CUSTSTN
- SCF not ENABLED in table RESOFC

DRCWACT

Register DRCWACT (Distinctive Ringing Call Wait ACTivation) is pegged each time a subscriber activates his/her DRCW service. Similar to the operations performed via service access code controlled activation, the DRCWACT register will be pegged for each occurrence of the an off-board service update activation request.

DRCWDACT

Register DRCWDACT (Distinctive Ringing Call Wait DeACTivation) is pegged each time a subscriber deactivates his/her DRCW service. Similar to the operations performed via service access code controlled activation, the DRCWDACT register will be pegged for each occurrence of the an off-board service update deactivation request.

DRCWDENY

Register DRCWDENY (Distinctive Ringing Call Wait DENY) is pegged each time a subscriber's attempt to update his/her DRCW programmed data via some edit session is denied due to the presence of the DENY option. The DRCWDENY register will be pegged when/if the following is true for a given DRCW off-board service update request.

- DOR option present on the given DRCW subscriber's line

- DRCW enabled office wide and DENY SCA option present on the given subscriber's line

Registers used for SimRing Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

SimRing OM Group Display

```
>omshow simring active
```

```
SIMRING
```

```
CLASS: ACTIVE
```

```
START:2003/10/31 12:00:00 FRI; STOP: 2003/10/31 12:08:27 FRI;
```

```
SLOWSAMPLES: 6 ; FASTSAMPLES: 51 ;
```

```

SIMRACT SIMRDACT SIMREATT SIMREDEN
SIMREOVF SIMRINV SIMRFAIL

```

```

0
    0    0    0    0
    0    0    0

```

```
>
```

SIMRACT

Register **SIMRACT** (SIMultaneous Ringing ACTivation) is pegged each time a subscriber activates his/her SIMRing service. Similar to the operations performed via service access code controlled activation, the **SIMRACT** register will be pegged for each occurrence of the an off-board service update activation request.

SIMRDACT

Register **SIMRDACT** (SIMultaneous Ringing DeACTivation) is pegged each time a subscriber deactivates his/her SIMRing service. Similar to the operations performed via service access code controlled activation, the **SIMRDACT** register will be pegged for each occurrence of the an off-board service update deactivation request.

SIMREATT

Register **SIMREATT** (SIMultaneous Ringing Editing ATtempt) is pegged each time a subscriber updates his/her SIMRing programmed data via some edit session. Similar to the operations performed via service access code controlled edit session, the **SIMREATT** register will be pegged for each of the following off-board service update requests.

- addition of DN to a subscriber's SIMRing list
- deletion of a DN from a subscriber's SIMRing list

SIMREDEN

Register SIMREDEN (SIMultaneous Ringing Editing DENial) is pegged each time a subscriber's attempt to update his/her SIMRing programmed data via some edit session is denied. The SIMREDEN register will be pegged when/if the following is true for a given SIMRing off-board service update request.

- SLE not ENABLED in table CUSTSTN
- SCF not ENABLED in table RESOFC

Register release history update

Not Applicable.

Associated registers

Not applicable.

Associated logs

<None>

Group4 Services OM Group

Operational Measures associated with the Call Forwarding service. Activation and deactivation OMs exist only for POTS CFW. There are no current OMs for RES/IBN CFW activation and deactivation. There are no current OMs for any type of Call Forward Busy or Don't Answer (POTS or RES/IBN).

This service does not operate in a call processing environment. Therefore no call processing related OM will be pegged. Examples of those are OTS (Office Traffic Summary) and traffic separation pegs.

Release history update

Not Applicable

Registers used for Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

CFWPOTS OM Group Display

```

>omshow cfwpots active
CFWPOTS
CLASS: ACTIVE
START:2003/10/03 09:00:00 FRI; STOP: 2003/10/03 09:06:39 FRI;
SLOWSAMPLES: 4 ; FASTSAMPLES: 40 ;
CFWPAATT CFWPSUC1 CFWPSUC2 CFPAOVFL
CFPADENY CFWPFATT CFPFOVFL CFPFDENY
CFWISOV CFBPATT CFBPDENY CFBPOVFL
CFBPISOV CFDPATT1 CFDPATT2 CFDPDENY
CFDPOVFL CFDPNC1 CFDPNC2 CFDPISOV
CFDPFAIL
0
1      1      0      0
0      0      0      0
0      0      0      0
0      0      0      0
0      0      0      0
0

```

CFWPAATT

Register CFWPAATT will be pegged for each activation attempt for POTS CFW.

CFWPSUC1

Register CFWPSUC1 will be pegged each time activation of POTS CFW is successful. Register CFWPSUC2 which is pegged when the courtesy call is successful during POTS CFW programming and activation will not be pegged by this service because courtesy calls are not supported.

CFPADENY

Register CFPADENY is pegged while attempting to set a forward to DN and the forward to DN fails validation for any reason.

CFPAOVFL

Register CFPAOVFL is pegged if there is some software or data storage problem with storing the forward to DN after it has been validated successfully.

Register release history update

Not Applicable.

Associated registers

Not applicable.

Associated logs

<None>

Group5 Services OM Group

Operational Measures associated with the Selective Call Forwarding and Selective Call Acceptance services.

Release history update

Not Applicable

Registers used for SCF Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

SCF OM Group Display

>omshow scf active

SCF

CLASS: ACTIVE

START:2003/08/27 09:30:00 WED; STOP: 2003/08/27 09:31:39 WED;

SLOWSAMPLES: 1 ; FASTSAMPLES: 10 ;

SCFEATT SCFEOVF ***SCFEDEN*** SCFEUSG
SCFACT ***SCFDACT*** SCFFWD SCFFWD2
 SCFSAT SCFSAT2 SCFFAIL SCFOVFL
 SCFSOVFL SCFSDEN SCFSBLK SCFUNIV
SCFDENY SCFAUNV SCFDUNV

0

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	

>

SCFEATT

Register SCFEATT (Selective Call Forwarding Editing ATtempt) is pegged each time a subscriber updates his/her SCF programmed data via some edit session. Similar to the operations performed via service access code controlled edit session, the SCFEATT register will be pegged for each of the following off-board service update requests.

- addition of DN to a subscriber's SCF list
- deletion of a DN from a subscriber's SCF list
- request to delete all DNs in a subscriber's SCF list
- request to delete all anonymous or private entries in a subscriber's SCF list

- set the forwarding DN
- clear the forwarding DN

SCFEDEN

Register SCFEDEN (Selective Call Forwarding Editing DENial) is pegged each time a subscriber's attempt to update his/her SCF programmed data via some edit session is denied. The SCFEDEN register will be pegged when/if the following is true for a given SCF off-board service update request.

- SLE not ENABLED in table CUSTSTN
- SCF not ENABLED in table RESOFC

SCFACT

Register SCFACT (Selective Call Forwarding ACTivation) is pegged each time a subscriber activates his/her SCF service. Similar to the operations performed via service access code controlled activation, the SCFACT register will be pegged for each occurrence of the an off-board service update activation request.

SCFDACT

Register SCFDACT (Selective Call Forwarding DeACTivation) is pegged each time a subscriber deactivates his/her SCF service. Similar to the operations performed via service access code controlled activation, the SCFDACT register will be pegged for each occurrence of the an off-board service update deactivation request.

SCFDENY

Register SCFDENY (Selective Call Forwarding DENY) is pegged each time a subscriber's attempt to update his/her SCF programmed data via some edit session is denied due to the presence of the DENY option. The SCFDENY register will be pegged for each of the following off-board service update request attempts.

- DOR option present on the given SCF subscriber's line
- SCF enabled office wide and DENY SCF option present on the given subscriber's line

Registers used for SCA Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

SCA OM Group Display

```
>omshow sca active
```

```
SCA
```

```
CLASS: ACTIVE
```

```
START:2003/10/30 16:00:00 THU; STOP: 2003/10/30 16:17:59 THU;
```

```
SLOWSAMPLES: 11 ; FASTSAMPLES: 108 ;
```

```

SCAEATT  SCAEDEN  SCAEOVF  SCAACT
SCADACT  SCAEUSG  SCASAT   SCASAT2
SCASDEN  SCASBLK  SCASRJT  SCASRJT2
SCASTRM  SCAUNIV  SCADENY  SCAAUNV
SCADUNV

```

```

0
0      0      0      0
0      0      0      0
0      0      0      0
0      0      0      0
0

```

SCAEATT

Register SCAEATT (Selective Call Acceptance Editing ATtempt) is pegged each time a subscriber updates his/her SCA programmed data via some edit session. Similar to the operations performed via service access code controlled edit session, the SCAEATT register will be pegged for each of the following off-board service update requests.

- addition of DN to a subscriber's SCA list
- deletion of a DN from a subscriber's SCA list
- request to delete all DNs in a subscriber's SCA list
- request to delete all anonymous or private entries in a subscriber's SCA list

SCAEDEN

Register SCAEDEN (Selective Call Acceptance Editing DENial) is pegged each time a subscriber's attempt to update his/her SCA programmed data via some edit session is denied. The SCAEDEN register will be pegged when/if the following is true for a given SCA off-board service update request.

- SLE not ENABLED in table CUSTSTN
- SCF not ENABLED in table RESOFC

SCAACT

Register SCAACT (Selective Call Acceptance ACTivation) is pegged each time a subscriber activates his/her SCA service. Similar to the operations performed via service access code controlled activation, the SCAACT register

will be pegged for each occurrence of the an off-board service update activation request.

SCADACT

Register SCADACT (Selective Call Acceptance DeACTivation) is pegged each time a subscriber deactivates his/her SCA service. Similar to the operations performed via service access code controlled activation, the SCADACT register will be pegged for each occurrence of the an off-board service update deactivation request.

SCADENY

Register SCADENY (Selective Call Acceptance DENY) is pegged each time a subscriber's attempt to update his/her SCA programmed data via some edit session is denied due to the presence of the DENY option. The SCADENY register will be pegged when/if the following is true for a given SCA off-board service update request.

- DOR option present on the given SCA subscriber's line
- SCA enabled office wide and DENY SCA option present on the given subscriber's line

Register release history update

Not Applicable.

Associated registers

Not applicable.

Associated logs

<None>

Group6 Services OM Group

Operational Measures associated with the Call Forwarding Don't Answer Timer service.

Release history update

Not Applicable

Registers used for Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

SPRING OM Group Display

SPRING OM Group Display

> >omshow spring active

SPRING

CLASS: ACTIVE

START:2003/10/30 11:00:00 THU; STOP: 2003/10/30 11:05:57 THU;

SLOWSAMPLES: 4 ; FASTSAMPLES: 36 ;

RCTRLLA RCTRLRA **RCTRLSLA** RCTRLSRA
RCTRLFA

0				
	0	0	0	0
	0			

RCTRLLA

Register RCTRLLA (Ring ConTRoL Local Activation ATtempt) will be pegged if a CFDVT update request is received.

RCTRLSLA

Register RCTRLSLA (Ring ConTRoL Successful Local Activation) will be pegged each time the user is given access to update the CFDVT data whether or not the data is successfully altered or not.

RCTRLFA

Register RCTRLFA (Ring ConTRoL Local FAilure) will be pegged each time there is a failure due to unavailable resources.

Register release history update

Not Applicable.

Associated registers

Not applicable.

Associated logs

<None>

Group7 Services OM Group

No OM generated for Group7. Therefore, no OM changes identified.

Group8 Services OM Group

Customer Originated Trace (COT) OM Group

Operational Measures associated with the Customer Originated Trace (COT) service.

Release history update

Not Applicable

Registers used for Off-board service updates

OM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.

COT OM Group Display

COT OM Group Display

```
>omshow cot active
```

```
COT
```

```
CLASS: ACTIVE
```

```
START:2003/09/10 10:00:00 WED; STOP: 2003/09/10 10:21:58 WED;
```

```
SLOWSAMPLES:    1 ; FASTSAMPLES:    8 ;
```

```

COTATT COTFDEN COTOVFL COTCMPL
COTINCM COTPRCD COTOPTO COTBDIN
COTPFLR COTUNIV COTDENY

```

```

0
    0    0    0    0
    0    0    0    0
    0    0    0

```

COTATT

Register COTATT (Customer Originated Trace Activation Attempt) will be pegged if the COT Update message for the COT service is received.

COTUNIV

Register COTUNIV (Customer Originated Trace Universal) will be pegged if the COT Update message is received for the universal COT service.

Register release history update

Not Applicable.

Associated registers

Not applicable.

Associated logs

<None>

Group9 Services OM Group**Speed Call OM Group**

Operational Measures associated with the Speed Calling service.

Release history update

Not Applicable

Registers used for Off-board service updatesOM group registers display on the MAP terminal as follows. The registers used for pegging off-board service updates are in ***bold italics***.**POTS Speed Call, SC1 or SC2****SCPOTS OM Group Display**

>omshow scpots active

SCPOTS

CLASS: ACTIVE

START:2003/10/24 10:00:00 FRI; STOP: 2003/10/24 10:22:51 FRI;

SLOWSAMPLES: 14 ; FASTSAMPLES: 137 ;

KEY (SC_OM_TUPLES)

SCPAATT SCPAOVFL SCPADENY SCPFATT
SCPFDENY

```

0 SC1_TUPLE
  0      0      0      0
  0
1 SC2_TUPLE
  0      0      0      0
  0

```

SCPAATT

Register SCPAATT (Speed Calling Program Activation ATtempt) will be pegged if the Speed Call Update message successfully added or changed a Speed Call DN.

SCAOVFL

Register SCAOVFL (Speed Calling Activation OVerFlow) is pegged if the Speed Call Update message failed to program the Speed Call Cell because of

a lack of software resources; for example, a lack of HEAP memory in reserve for Speed Calling.

SCADENY

Register SCADENY (Speed Calling Activation DENY) is pegged if the Speed Call Update message failed to program or erase a Speed Call Cell because of an invalid Speed Call Cell number.

Register release history update

Not Applicable.

Associated registers

Not applicable.

Associated logs

<None>

Office Traffic Summary (OTS)

OTS OM Group Display

>omshow ots active

OTS

CLASS: ACTIVE
 START:2003/10/24 10:00:00 FRI; STOP: 2003/10/24 10:22:51 FRI;
 SLOWSAMPLES: 14 ; FASTSAMPLES: 137 ;

KEY ()

NORG NORG2 ORGTRM ORGTRM2
 ORGOUT ORGOUT2 **ORGTRMT** ORGABDN
 ORGLKT **ORGFSET** ORGFSET2 NINC
 NINC2 INCTRM INCTRM2 INCOUT
 INCOUT2 INCTRMT INCABNM INCABNC
 INCLKT INCFSET NSYS NSYS2
 SYSTRM SYSOUT SYSTRMT SYSABDN
 SYSLKT SYSFSET

0

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

ORGFSET

Register ORGFSET (Originating Feature SET) is pegged when a Speed Call feature is successfully programmed by a user via the Speed Call Update message.

ORGTRMT

Register ORGTRMT (Originating Treatment) is pegged if the Speed Call Update message failed to program the Speed Call feature because of an error condition.

Register release history update

Not Applicable.

Associated registers

Not applicable.

Associated logs

<None>

Accounting for A00004036

Accounting strategy

The general accounting strategy for this activity is to continue to perform whatever billing for successful updates that is done today for service activation/deactivation, list editing, etc. In addition to performing the standard billing, a Service Logic Identification Module (module code 039) will be appended to the current record as an AMAslpid is included in the corresponding update request.

CM billing due to Update Requests

The AMA records generated as per the service requirements and the GR1298 requirements (Update and Query messages) for all the service groups whose provisioning and activation is being controlled and queried by the Update and query messages are as follows:

Group1 Services AMA

Only three services--Automatic Call Back (ACB), Automatic Recall (AR) and Make Set Busy (MSB)--generate the AMA record. All other services do not have any AMA record associated with them.

Update Message for ACB (Universal) and AR (Universal)

Consistent with the billing performed as a result of Automatic Call Back (universal - usage based), and Automatic Recall (universal - usage based) being modified via access code, a callcode 330 record (structure code 1030)

will also be provided to record successful deactivation of ACB (universal), and AR (universal).

Update Message for MSB

Consistent with the billing performed as a result of MSB being modified via access code, a callcode 006 record (structure code 510) will also be provided to record successful activation and deactivation of MSB.

Module code 039

When an *AMAslpid* is provided with an update request, a Service Logic Identification Module (module code 039) populated with the *AMAslpid* provided will be appended to any base record associated with the update. The following MAP example figure is in non-printing text.

Example: ACB deactivation - Update message (with AMAslpid)

```
*HEX ID:AA  STRUCTURE CODE:01030C  CALL CODE:330C  SENSOR
TYPE:036C  SENSOR ID:0619351C  REC OFFICE TYPE:036C  REC OFFICE
ID:0619351C  DATE:30929C  CLASS FEATURE:069C  ORIG NPA:613C  ORIG
NUMBER:6215821C  OVERSEAS IND:1C  TERM NPA:00000C  TERM
NUMBER:0000000C  CONNECT  TIME:1508160C  ELAPSED
TIME:000000059C  CLASS FUNCTION:000C  FEATURE STATUS:000C
SCRN LIST SCF:000C  SCRN LIST SCR:000C  SCRN LIST DRCW:000C
MODULE CODE:039C  SLP ID:123456789C  MODULE CODE:000C
```

Example: AR deactivation - Update message (with AMAslpid)

```
*HEX ID:AA  STRUCTURE CODE:01030C  CALL CODE:330C  SENSOR
TYPE:036C  SENSOR ID:0619351C  REC OFFICE TYPE:036C  REC OFFICE
ID:0619351C  DATE:30929C  CLASS FEATURE:068C  ORIG NPA:613C  ORIG
NUMBER:6215821C  OVERSEAS IND:1C  TERM NPA:00000C  TERM
NUMBER:0000000C  CONNECT  TIME:1508160C  ELAPSED
TIME:000000059C  CLASS FUNCTION:000C  FEATURE STATUS:000C
SCRN LIST SCF:000C  SCRN LIST SCR:000C  SCRN LIST DRCW:000C
MODULE CODE:039C  SLP ID:123456789C  MODULE CODE:000C
```

Example: MSB activation- Update message (with AMAslpid)

*HEX ID:AA STRUCTURE CODE:40510C CALL CODE:006C SENSOR TYPE:036C SENSOR ID:0000000C REC OFFICE TYPE:036C REC OFFICE ID:0000000C DATE:80218C TIMING IND: 00000C STUDY IND:0000000C CLD PTY OFF-HK:0C SERVICE OBSERVED:0C OPER ACTION:0C SERVICE FEATURE:000C SIG DIGITS NEXT FIELD:009C ORIG OPEN DIGITS 1:00036340101C ORIG OPEN DIGITS 2:FFFFFFFFF ORIGINATING CHARGE INFO:FFFF DOMESTIC/INTL INDICATOR:1C SIG DIGITS NEXT FIELD:007C TERM OPEN DIGITS 1:00006340102C TERM OPEN DIGITS 2:FFFFFFFFF CONNECT TIME:1451038C ELAPSED TIME:000000138C MODULE CODE:611C GENERIC CONTEXT ID:8002415C GENERIC DIGITS STRING ONE:94A28200000090C
MODULE CODE:039C SLP ID:123456789C MODULE CODE:000C

Group2 Services AMA

No AMA records are generated for Group2 services.

Group3 Services AMA**Update Message for DRCW, SCRJ and SIMRING**

Consistent with the billing performed as a result of Distinctive Ringing / Call Waiting, Selective Call Rejection and Simultaneous Ringing being modified via access code, a callcode 330 record (structure code 1030) will also be provided to record successful DRCW or SCRJ or SIMRING activation, deactivation, list edit operations, etc.

Module code 039

When an *AMAslpid* is provided with an update request, a Service Logic Identification Module (module code 039) populated with the *AMAslpid* provided will be appended to any base record associated with the update.

The following MAP example figure is in non-printing text.

Example: DRCW activation- Update message (with AMAslpid)

*HEX ID:AA STRUCTURE CODE:01030C CALL CODE:330C SENSOR TYPE:036C SENSOR ID:0619351C REC OFFICE TYPE:036C REC OFFICE ID:0619351C DATE:30929C CLASS FEATURE:073C ORIG NPA:613C ORIG NUMBER:6215821C OVERSEAS IND:1C TERM NPA:00000C TERM NUMBER:0000000C CONNECT TIME:1508160C ELAPSED TIME:000000059C CLASS FUNCTION:002C FEATURE STATUS:000C SCRNLIST SCF:FFFF SCRNLIST SCR:FFFF SCRNLIST DRCW:001C
MODULE CODE:039C SLP ID:11111111C MODULE CODE:000C

Example: SCRJ activation- Update message (with AMAslpid)

*HEX ID:AA STRUCTURE CODE:01030C CALL CODE:330C SENSOR TYPE:036C SENSOR ID:0619351C REC OFFICE TYPE:036C REC OFFICE ID:0619351C DATE:30929C CLASS FEATURE:072C ORIG NPA:613C ORIG NUMBER:6215821C OVERSEAS IND:1C TERM NPA:00000C TERM NUMBER:0000000C CONNECT TIME:1508302C ELAPSED TIME:000000081C CLASS FUNCTION:002C FEATURE STATUS:000C SCRNLIST SCF:FFFF SCRNLIST SCR:001C SCRNLIST DRCW:FFFF
MODULE CODE:039C SLP ID:11111111C MODULE CODE:000C

Group4 Services AMA**Updates to Call Forwarding**

Consistent with the billing performed as a result of Call Forwarding being modified via access code, a callcode 31 record (structure code 614) will be provided for successful CFW activation (POTS or IBN/RES) and a callcode 31 record (structure code 96) will be provided for successful CFW deactivation (POTS or IBN/RES).

There are no billing records provided for Call Forward Busy or Don't Answer activation or deactivation for either POTS or IBN/RES.

Module code 039

Impact to be determined.

When an *AMAslpid* is provided with an update request, a Service Logic Identification Module (module code 039) populated with the *AMAslpid* provided will be appended to any base record associated with the update.

The following MAP example figure is in non-printing text.

Example: Call Forward activation- Update message (with AMAslpid)

*HEX ID:AA STRUCTURE CODE:00614C CALL CODE:031C SENSOR TYPE:036C SENSOR ID:0619351C REC OFFICE TYPE:036C REC OFFICE ID:0619351C DATE:30926C TIMING IND:00100C STUDY IND:0000000C SERVICE FEATURE:012C ACTIVATING NPA:613C ACTIVATING NUMBER:6213502C FWD OVERSEAS IND:1C FWD NPA:00613C FWD NUMBER:6212500C ACTIVATION TIME:1426285C
MODULE CODE:039C SLP ID:11111111C MODULE CODE:000C

Example: Call Fwd deactivation- Update message (with AMAslpid)

*HEX ID:AA STRUCTURE CODE:00096C CALL CODE:031C SENSOR TYPE:036C SENSOR ID:0619351C REC OFFICE TYPE:036C REC OFFICE ID:0619351C DATE:30926C TIMING IND:00300C STUDY IND:0000000C SERVICE FEATURE:012C ACTIVATING NPA:613C ACTIVATING NUMBER:6213502C FWD OVERSEAS IND:1C FWD NPA:00613C FWD NUMBER:6212500C ACTIVATION TIME:1426285C ELAPSED TIME:000000265C PRESENT DATE:30926C PRESENT TIME:1426568C
MODULE CODE:039C SLP ID:11111111C MODULE CODE:000C

Group5 Services AMA**Updates to Selective Call Forwarding**

Consistent with the billing performed as a result of Selective Call Forwarding being modified via access code, a callcode 330 record (structure code 1030) will also be provided to record successful SCF activation, deactivation, list edit operations, etc.

Module code 039

When an *AMAslpid* is provided with an update request, a Service Logic Identification Module (module code 039) populated with the *AMAslpid* provided will be appended to any base record associated with the update.

The following MAP example figure illustrates the above as it relates to the extension of a Selective Call Forwarding CLASS AMA record. The Module Code 039 portion of the record is represented as ***bold italics***.

Example: Update message for SCF

*HEX ID:AA STRUCTURE CODE:41030C CALL CODE:330C SENSOR TYPE:036C SENSOR ID:0619351C REC OFFICE TYPE:036C REC OFFICE ID:0619351C DATE:30731C CLASS FEATURE:052C ORIG NPA:000C ORIG NUMBER:0000000C OVERSEAS IND:1C TERM NPA:00000C TERM NUMBER:0000000C CONNECT TIME:0857083C ELAPSED TIME:000000000C CLASS FUNCTION:001C FEATURE STATUS:000C SCRNLIST SCF:001C SCRNLIST SCR:FFFF SCRNLIST DRCW:FFFF
MODULE CODE:039C SLP ID:11111111C MODULE CODE:000C

Group6 Services AMA

No AMA records are generated for Group6 Services.

Group7 Services AMA

Update Messages for CallingNumberDeliveryBlocking

Consistent with the billing performed as a result of CNDB being activated via an access code, a callcode 330 record (structure code 1030) will be provided to record successful CNDB activation.

Module Code 039

When an *AMAsplidid* is provided with an update request, a Service Logic Identification Module (module code 039) populated with the *AMAsplid* will be appended to any base record associated with the update.

Example CNDB Activation

```
*HEX ID:AA STRUCTURE CODE:01030C CALL CODE:330C SENSOR TYPE:036C  
SENSOR ID:0619351C REC OFFICE TYPE:036C REC OFFICE ID:0619351C  
DATE:31030C CLASS FEATURE:075C ORIG NPA:613C ORIG NUMBER:6213513C  
OVERSEAS IND:1C TERM NPA:00613C TERM NUMBER:7234535C CONNECT  
TIME:0949248C ELAPSED TIME:000000000C CLASS FUNCTION:000C FEATURE  
STATUS:000C SCRNLIST SCF:000C SCRNLIST SCR:000C SCRNLIST  
DRCW:000C MODULE CODE:039C SLIP ID:111111111C MODULE CODE:000C
```

Group8 Services AMA

Update Message for COT and CCW

Consistent with the billing performed as a result of Customer Originated Trace and CancelCall Waiting being modified via access code, a callcode 330 record (structure code 1030) will also be provided to record successful COT or CCW invocation.

Module code 039

When an *AMAsplid* is provided with an update request, a Service Logic Identification Module (module code 039) populated with the *AMAsplid* provided will be appended to any base record associated with the update.

The following MAP example figure is in non-printing text.

Example COT activation and LINE 150 Log

*HEX ID:AA STRUCTURE CODE:01030C CALL CODE:330C SENSOR
TYPE:036C SENSOR ID:0619351C REC OFFICE TYPE:036C REC OFFICE
ID:0619351C DATE:30929C CLASS FEATURE:070C ORIG NPA:613C ORIG
NUMBER:6215821C OVERSEAS IND:0C TERM NPA:00613C TERM
NUMBER:6215121C CONNECT TIME:1510368C ELAPSED
TIME:000000000C CLASS FUNCTION:000C FEATURE STATUS:000C
SCRN LIST SCF:000C SCRN LIST SCR:000C SCRN LIST DRCW:000C
MODULE CODE:039C SLIP ID:11111111C MODULE CODE:000C

>open line 150

Done.

RTPT07BD LINE150 SEP29 15:10:36 2600 INFO FULL COT TRACE
SUBSCRIBER LEN: HOST 05 0 08 21 SUBSCRIBER DN: 613 6215821
TRACE DUMP
TIME CALL RCVD: SEP29 15:10:07 DN: 613 6215121
INTRAOFFICE: Y ORIG ADDR TYPE: 003 (UNIQUE)
OUT OF AREA: N CWT: N PRIVATE: N GIC: N
NETWORK: PUBLIC
JIP: 000000
JIP REASON: HOMELRN USED

Group9 Services AMA

No AMA records are generated for Group9 Services.

Other changes

Not applicable.

Product = CS 2000**A00004037 -- USNBD CALEA CMR Interaction Enhancements
(Succession on DMS)*****Functional Description***

Currently there are three types of delivery mechanisms available for CDC messaging; X25, SCTP (supported only on CS2Kdelivery) or call data delivery via Frequency Shift Keying (FSK supported on DMS or in a CS2K hybrid configuration with TDM LTC/LGCs) over a dedicated POTs line. X25 and SCTP mechanisms require Law Enforcement agencies to purchase additional hardware in order to receive the call data messages. Nortel has provided an inexpensive mechanism for the delivery of call data over a

dedicated line. This feature will allow a mechanism for delivery of call data over a Switched Remote trunk.

Functional Description

Currently, FSK supports 2 access types, SL (switched local) and DE (Dedicated). This feature will add a third access type called SR (Switched Remote).

The DTC/SPM or other trunking peripheral does not support the CMR card. In order for the call data to be delivered over a trunk, an LGC/LTC peripheral containing the CMR will allocate a p-side loop around to the trunk. This will allow the data sent from the CM to be looped from the CMR peripheral to the trunk peripheral and out over the trunk.

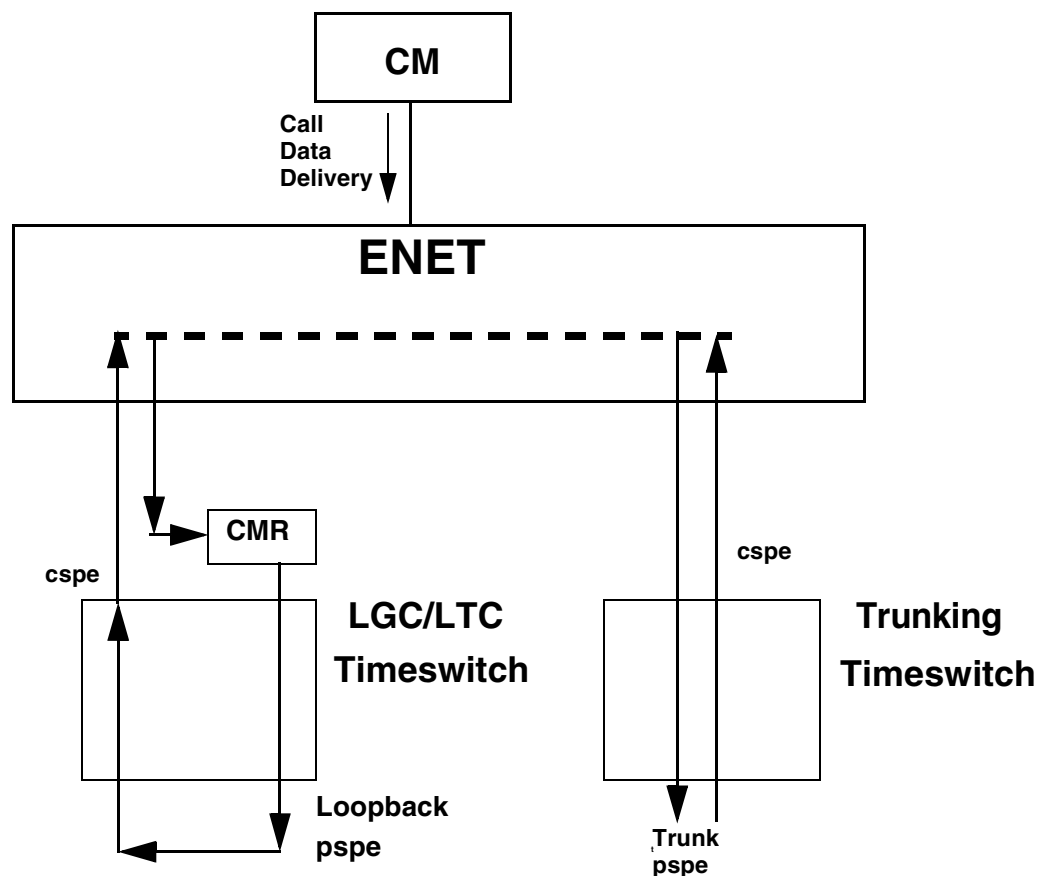
This feature will also support equal access dialing/routing for both Switched-Remote trunk CDCs and Switched CCRs (Note: Switched CCR or dial-out CCR functionality was initially provided in NA014 without equal access support).

To provide support of Equal Access, USNBD Agency command is modified to allow for the provisioning of a PIC and LATA which will be used for all equal access calls to Trunk CDCs and switched CCRs for that agency. If equal access dialing is not desired, the PIC and LATA fields should be set to NILCAR and NILLATA respectively.

Supported trunk types for equal access calls on SR CDCs and Switched CCRs are ISUP IT and ATC trunks with FGD signalling only.

The following figure shows how the connections are made between the CMR card and the outgoing trunk.

CMR card to DTC connection



Modifications to USNBD CI commands

The USNBD CDC and AGENCY commands will be enhanced to allow a new type of transport protocol, SR (switched remote) for FSK CDC over trunks. The following figure illustrates the CDC list command with an SR CDC link added.

Trunk

cdc list all

Index	Type	Access CDC DN	Agency
[Associated SINS]			
1	FSK DE	6136211004	TEST
2	FSK SL	6136211005	TEST
3	FSK SR	16136211006	FBI_WITH_EA
CDC LIST DONE			

The Switched Remote CDC type will utilize Agency data just like the Switched CCRs, for billing information and digit translation.

The Agency command ADD and LIST will be enhanced to add the PIC and LATA fields. The following figure shows the agency list display.

Agency List Display

```
>agency list
AGENCY-NAME STS PRETRANSLATOR LCANAME BILLNO
              PIC              LATA
-----
FBI_NO_EA    613 P621          L613      6135551000
              NILCAR          NILLATA
FBI_WITH_EA  613 P621          L613      6135551001
              ITT             LATA1
AGENCY LIST DONE.
```

The Switched Remote CDC will utilize Agency data just like the existing Switched CCRs, for billing information and digit translation.

The following figure is a calldump of the 110 and 119 billing records which are output for each CCR or CDC call utilizing EA translations.

110 and 119 CALLDUMP logs

```
*HEX ID:AA STRUCTURE CODE:40625C CALL CODE:110C SENSOR TYPE:036C
SENSOR ID:0619351C REC OFFICE TYPE:036C REC OFFICE ID:0619351C
DATE:31215C TIMING IND:00000C STUDY IND:0200000C CLD PTY OFF-HK:0C
SERVICE OBSERVED:0C OPER ACTION:0C SERVICE FEATURE:000C
ORIG NPA:613C ORIG NUMBER:5551000C OVERSEAS IND:0C
TERM NPA:00345C TERM NUMBER:8882400C CONNECT TIME:1016181C
ELAPSED TIME:000000465C IC/INC PREFIX:04881C CC DATE:31215C CC TIME:1016165C
ELAPSED CC:000000482C IC/INC EVENT STATUS:010C TRUNK GROUP NUMBER:40639C
ROUTING INDICATOR:1C DIALING INDICATOR:1C ANI INDICATOR:1C
MODULE CODE:306C OLIP:031C MODULE CODE:000C
```

```
*HEX ID:AA STRUCTURE CODE:40625C CALL CODE:119C SENSOR TYPE:036C
SENSOR ID:0619351C REC OFFICE TYPE:036C REC OFFICE ID:0619351C
DATE:31215C TIMING IND:00000C STUDY IND:0200000C CLD PTY OFF-HK:0C
SERVICE OBSERVED:0C OPER ACTION:0C SERVICE FEATURE:000C
ORIG NPA:613C ORIG NUMBER:5551000C OVERSEAS IND:0C
TERM NPA:00345C TERM NUMBER:8882400C CONNECT TIME:1016180C
ELAPSED TIME:000000465C IC/INC PREFIX:04881C CC DATE:31215C CC TIME:1016163C
ELAPSED CC:000000482C IC/INC EVENT STATUS:010C TRUNK GROUP NUMBER:30639C
ROUTING INDICATOR:0C DIALING INDICATOR:FF ANI INDICATOR:1C
MODULE CODE:306C OLIP:031C MODULE CODE:000C
```

CDC Link Establishment/Termination/Retries

The same rules which apply to Switched Local CDC lines, will be followed for Switched Remote trunks. A detailed list is in the DID section of this document.

Hardware Requirements or Dependencies

Availability of a CMR card in any LGC/LTC on the switch.

Software Requirements or Dependencies

Soc options NBD00003 and NBD00004 turned “ON” for USNBD functionality.

Limitations and restrictions

CM portion of this feature requires the XPM portion of this feature.

Interactions

The feature does not modify the way USNBD interacts with other features. It adds an additional CDC type.

Logs (LG)**New/modified logs**

The existing UNB error and secret logs are enhanced to report the problems specific to Switched Remote CDCs during administration or audits. UNB306 logs will be output if the PIC or LATA fields are deleted.

Data schema (DS)

No new tables are created by this feature and none of the existing tables are modified by this feature.

Office parameters (OP)

No office parameter related changes are made by this feature.

Service orders (SO)

No Service order changes are made by this feature.

Alarms (AL)

No new alarms are added by this feature and none of the existing ones are modified by the feature.

Glossary

Term	Description
CALEA	Communications Assistance for Law Enforcement Act
CLASS	Custom Local Area Signaling Services
CMR	CLASS Modem Resource
FSK	Frequency Shift Keying
LEA	Law Enforcement Agencies
LI	Lawful Interception
PCM	Pulse Code Modulation
USNBD	United States Network Broadcast Delivery

Product = CS2000

A00004045 -- Calling Line Identification Directory Number (CLIDN) for DMS-250 (Succession on DMS, AAL2)

Functional Description

The CLIDN call tracing capability captures call data based on the Called number. Called numbers that require tracing are entered into table CLIDN. Call data is captured during trunk termination and output in a TRK605 log. The TRK605 log contains the call origination number (e.g. Calling Party Number) and additional call information for tracing malicious, threatening or otherwise harassing calls.

Prior to this activity, the CLIDN table existed only in the DMS-100/200 product line as one option for providing CLI call tracing functionality. This feature implements similar DMS-100/200 CLIDN call tracing capability into the UCS DMS-250 product line and uses the same CLIDN table. The UCS DMS-250 functionality supports originations and terminations on the following DMS-250 trunk types: EANT (PTS and SS7), PRI, DAL, ONAL, ONAT and IMT (PTS and SS7). Availability of TRK605 log information is dependent on trunk and signaling type at the time the call information is captured.

Please refer to the following sections for additional information on this capability:

- Software Optionality Control (SOC): UTRS0012
- Table CLIDN
- TRK605 Log
- TRK605 Log Data Capture (Call Processing)

Software Optionality Control (SOC): UTRS0012

The new SOC code UTRS0012 ‘CLIDN for DMS-250’ is introduced by this feature. When UTRS0012 is ON, call attempts on a supported incoming trunk to a called number marked for tracing in table CLIDN will generate a TRK605 log. When UTRS0012 is IDLE, call attempts on a supported incoming trunk to a called number marked for tracing in table CLIDN will not generate a TRK605 log. The following figure shows an example of SOC UTRS0012 in the ON state.

UTRS0012 SOC option

```
>SOC
SOC:
>SELECT OPTION UTRS0012

GROUP:UTRS
OPTION  NAME                RTU STATE  USAGE  LIMIT  UNITS  LAST_CHG
-----  -----
UTRS0012 UCS CLIDN on DMS-250  Y    ON      -      -      -    03/08/28
```

If ACTPATCH KGL03 is active, then SOC UTRS0012 will be set to RTU “Y” and STATE “ON” on ONP to the sourced release.

Table CLIDN

This feature makes table CLIDN functionality available for the UCS DRU. Table CLIDN allows for a maximum of 67 ten-digit directory number (DN) (area code + office code + DN) tuples for which CLI call tracing is provided. For a service code (i.e., 411, 911, etc.) or a seven-digit DN, the letter N (internally translated to 0) must be prefixed to make the total digit count equal to 10.

Table CLIDN is not changed by this feature and is associated with the TRK605 log. When the called number is datafilled in table CLIDN, UTRS0012 SOC option is ON and the incoming trunk is a supported trunk type, the TRK605 log is generated. The following figure shows example datafill for table CLIDN.

Table CLIDN datafill

```

>table clidn
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
DIGITS:
>6136215015
TUPLE TO BE ADDED:
6136215015
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
>list all
TOP
DIGITS
-----
NNNNNNNN411
NNN8765000
6136215015
BOTTOM

```

TRK605 Log

This feature makes TRK605 log functionality available for the UCS DRU. The existing TRK605 log was introduced in the DMS-100/200 by the Inter-Switch Call Trace (ICT) feature AN1658. The TRK605 log is used in a tandem switch to identify the origination number when the called number is being traced. The TRK605 log contains the fields: Incoming trunk, Outgoing trunk, Called number, Originating number, Source, Call ID and Time.

TRK605 Format

This feature does not change the format of the existing TRK605 log. The log report format for TRK605 is as follows:

```

* TRK605 mmmdd hh:mm:ss ssdd ALARM INFO ICT Calling Line Ident
INCOMING TRUNK = <CKT CLI>
OUTGOING TRUNK = <CKT CLI>
CALLED NUMBER = NXXNXXXXXX
SOURCE = CALLING NUMBER/CHARGE
NUMBER/UNAVAILABLE
CALLID = XXXXXX
TIME: MONTH: DAY HH:mm:ss

```

An example of log report TRK605 follows:

* TRK605 SEP27 14:23:29 5908 INFO ICT Calling Line Ident

INCOMING TRUNK = CKT DCEA20C7DR01 1

OUTGOING TRUNK = CKT DCEA21C7DR02 1

CALLED NUMBER = 2018212345

ORIGINATION NUMBER = 8146119871

SOURCE = CALLING NUMBER

CALLID = 852346

TIME: SEP27 14:23:29

TRK605 Log Field descriptions

The following table describes each field in the TRK605 log report.

TRK605 Log Field descriptions

Field	Value	Description
*	Alarm	One asterik indicates that the generation of this log report represents a minor alarm condition.
INCOMING TRUNK	Trunk Group name and member number	This field identifies the CLLI name and member number of the incoming trunk.
OUTGOING TRUNK	Trunk Group name and member number	This field identifies the CLLI name and member number of the outgoing trunk.
CALLED NUMBER	Digits 0-9	This field identifies the called number that is being traced.
ORIGINATING NUMBER	Digits 0-9 or '\$'	This field identifies either the calling number, charge number or billing number from the incoming trunk call information. The CLIDN for DMS-250 feature attempts to get the calling number first. If the calling number is not available, the charge number is used. If the charge number is not available, the billing number is used. If neither the calling, charge nor billing number is available, this field will display '\$'.

TRK605 Log Field descriptions

Field	Value	Description
SOURCE	Calling Number, Charge Number or Unavailable	This field identifies from what the originating number is derived. If the originating number cannot be derived, '\$' will appear in the ORIGINATING NUMBER field and the SOURCE field will display "UNAVAILABLE".
CALLID	6 digit number; Digits 0-9 used	This field identifies the call process id number.
TIME	Month, Day, Hour, Minute and Second	This field identifies the date and time the call was logged.

TRK605 Log Data Capture (Call Processing)

When a supported incoming trunk with the called number datafilled in table CLIDN attempts to terminate on an outgoing trunk, a TRK605 log message is generated. The TRK605 log data is captured from the call information depending on the type of call and incoming trunk call data.

The following three call types may impact the Called number used to index table CLIDN on incoming DMS-250 calls:

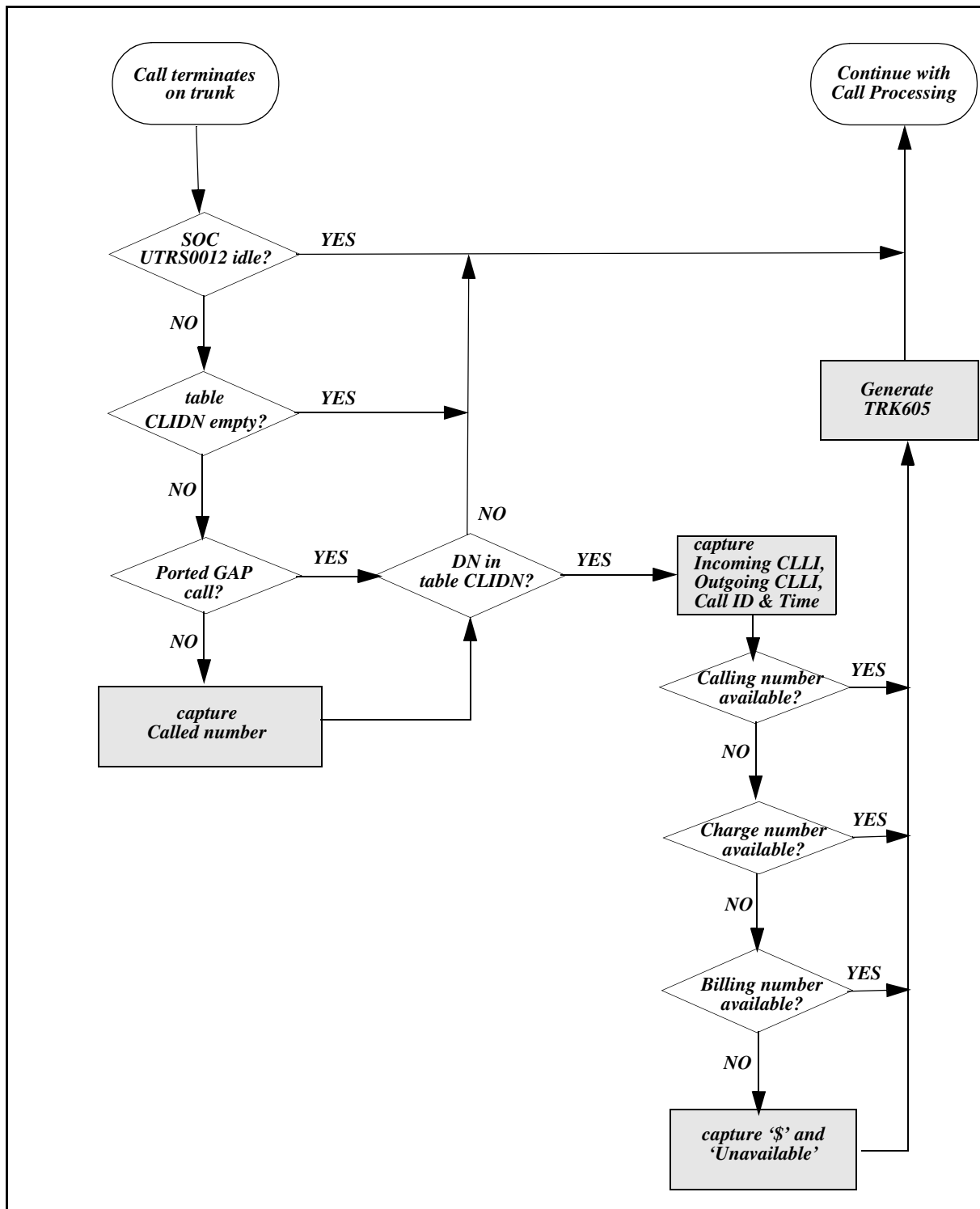
- For typical calls, the Called number from the incoming trunk is used to index table CLIDN for DN tracing.
- Incoming calls in which a ported number Generic Address Parameter (GAP) is signaled in or returned from the database query, the ported number is used to index table CLIDN for DN tracing, otherwise the Called number is used.
- For all CAIN calls that receive a Called number from the database, the returned Called number from the database is used to index table CLIDN for DN tracing.

If the Called number is located in table CLIDN, the TRK605 log is generated with the incoming trunk captured call data. The following table gives a breakdown of how the TRK605 log data is derived. The flow chart in "CLIDN Call behavior" on page 1731 describes the call processing behavior of this feature.

TRK605 log data

TRK605 log field	Information received from
Incoming Trunk	CLLI of incoming trunk
Outgoing Trunk	CLLI of outgoing trunk

TRK605 log field	Information received from
Called Number	Ported number GAP, if ported number is signaled in. The number returned from query, if CAIN alters called number. Called number present in the incoming trunk call data, if typical call.
Origination Number	Calling party number, charge number or billing number. If none of the above info is available, this field will be '\$' (left blank).
Source	'CALLING NUMBER' if Origination number field is calling party number. 'CHARGE NUMBER' if Origination number field is charge number or billing number. 'UNAVAILABLE' if Origination number field is '\$'.
Callid	Call data information
Time	Call data information time

CLIDN Call behavior

Hardware Requirements or Dependencies

None.

Software Requirements or Dependencies

SN07 (UCS20).

Limitations and restrictions

- This functionality will not support the following UCS trunk types: AXXESS.
- Only standard In-switch routed CAIN calls will be supported.
- This feature is patched in SN06 under ACTPATCH KGL03.

Interactions

None.

Applicable customer facing sections

Fault Management

Logs ☒ X

Alarms ☐ N/A

Configuration

Data Schema ☒ X

User Interface ☐ N/A

Element Management ☐ N/A

Security ☐ N/A

Service Order ☐ N/A

Office Parameters ☐ N/A

Accounting (includes AMA billing) ☐ N/A

Performance (includes operational measurements) ☐ N/A

Glossary

Term	Description
ANI	Automatic Number Identification
CAIN	Carrier Advanced Intelligent Network
CLI	Calling Line Identify

Term	Description
CLIDN	Calling Line Identify Directory Number
CLLI	Common Language Location Identification
DAL	Dedicated Access Line
DN	Directory Number
EANT	Equal Access Network Trunk
GAP	Generic Address Parameter
IAM	Initial Address Message of the SS7 signalling
IMT	Inter Machine Trunk
ISUP	Integrated Services digital network User Part
ICT	Inter-Switch Call Trace
LNP	Local Number Portability
ONAL	Off Network Access Line
ONAT	Off Network Access Trunk
ONP	One Night Process
PRI	Primary Rate Interface
RTU	Right to Use
SS7	Signalling System No. 7
SOC	Software Optionality Control
UCS	Universal Carrier Service

Fault Management for A00004045

Fault management strategy

The CLIDN for DMS-250 feature provides the same CLIDN call tracing capability using the TRK605 log as the existing DMS-100/200 CLIDN functionality.

Fault management tools and utilities

N/A.

Logs

Explanation

Log Title: TRK605

Name: ICT Calling Line Identification

Description: This log is generated when the SOC UTRS0012 is ON and the called number is data filled in table CLIDN in a DMS-250 toll switch. The TRK605 log is used in a toll switch to identify the origination number when the called number is being traced.

Event type: Minor alarm condition.

Format

The log report format for TRK605 is as follows:

```
* TRK605 mmmdd hh:mm:ss ssdd ALARM INFO ICT Calling Line Ident
INCOMING TRUNK = <CKT CLLI>
OUTGOING TRUNK = <CKT CLLI>
CALLED NUMBER = NXXNXXXXXX
SOURCE = CALLING NUMBER/CHARGE
NUMBER/UNAVAILABLE
CALLID = XXXXXX
TIME: MONTH: DAY HH:mm:ss
```

An example of log report TRK605 follows:

```
* TRK605 SEP27 14:23:29 5908 INFO ICT Calling Line Ident
INCOMING TRUNK = CKT   DCEA20C7DR01   1
OUTGOING TRUNK = CKT   DCEA21C7DR02   1
CALLED NUMBER  = 2018212345
ORIGINATION NUMBER = 8146119871
SOURCE =          CALLING NUMBER
CALLID =    852346
TIME:  SEP27 14:23:29
```

Field descriptions

The following table describes each field in the log report:

Field descriptions

Field	Value	Description
*	Alarm	One asterik indicates that the generation of this log report represents a minor alarm condition.
INCOMING TRUNK	Trunk Group name and member number	This field identifies the CLLI name and member number of the incoming trunk.
OUTGOING TRUNK	Trunk Group name and member number	This field identifies the CLLI name and member number of the outgoing trunk.
CALLED NUMBER	Digits 0-9	This field identifies the called number that is being traced.
ORIGINATING NUMBER	Digits 0-9 or '\$'	This field identifies either the calling number, charge number or billing number from the incoming trunk call information. The CLIDN for DMS-250 feature attempts to get the calling number first. If the calling number is not available, the charge number is used. If the charge number is not available, the billing number is used. If neither the calling, charge nor billing number is available, this field will display '\$'.
SOURCE	Calling Number, Charge Number or Unavailable	This field identifies from what the originating number is derived. If the originating number cannot be derived, '\$' will appear in the ORIGINATING NUMBER field and the SOURCE field will display "UNAVAILABLE".
CALLID	6 digit number; Digits 0-9 used	This field identifies the call process id number.
TIME	Month, Day, Hour, Minute and Second	This field identifies the date and time the call was logged.

Action

Action to be taken is determined by the local telephone company.

Associated Operational Measurements or Performance Measurements

There are no associated OM registers.

Additional information

On the DMS-250, the TRK605 log is generated for EANT, PRI, DAL, ONAL, ONAT and IMT trunk types.

The TRK605 log was introduced to the DMS-100/200 by feature AN1658.

Alarms

The TRK605 log is a minor alarm condition.

Related documentation

AN1658 - Inter-Switch Call Trace (ICT) Feature

Configuration for A00004045

Hardware and Software Requirements

In order to perform CLIDN call tracing on the DMS-250, SOC UTRS0012 must be ON and the desired termination number(s) must be datafilled in table CLIDN.

Initial Configuration

This feature impacts EANT, PRI, DAL, ONAL, ONAT and IMT trunks.

This feature creates a section for existing table CLIDN (see Section 13.5.1).

Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

Upgrade Impact

Dump and Restore

If ACTPATCH KGL03 (UCS19) is active on Dump side, then UTRS0012 will be set to RTU “Y” and “ON” on ONP to the sourced release (restore side UCS20 and above).

Element Management Upgrade

N/A

Data schema (DS) (CM, MIBS, RDB)

New table

Table CLIDN is new to the UCS DRU, but currently exists in DMS-100/200.

Table CLIDN

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
CLIDN	NEW	UNCHANGED

Table/MIB/Remote Database Schema information

Name: CLIDN

Calling Line Identification Directory Number

Functional description

Table CLIDN allows for a maximum of 67 ten-digit directory number (DN) (area code + office code + DN) tuples for which CLI call tracing is provided. These DNs are external to the switching unit. The ten-digit DNs include an area code + office code + directory number or a service code.

For a service code (i.e., 411, 911, 0, etc.) or a seven-digit DN, the letter N must be prefixed to make the total digit count equal to 10. The system internally translates the letter N to 0.

Table CLIDN is associated with the TRK605 log on the DMS-250 switch. When the called number is datafilled in table CLIDN, UTRS0012 SOC option is ON and the incoming trunk type is supported (trunk types: EANT, PRI, DAL, ONAL, ONAT or IMT), the TRK605 log is generated.

The TRK605 log report contains the following fields:

- the incoming trunk group and number
- the outgoing trunk group and number
- the called party number
- the originating party number
- the date and time

Usage sequence and implications (CM Only)

No other tables need to be datafilled prior to entering data into table CLIDN.

Size**Table size**

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
CLIDN	0	67	

Fields

The following table lists field description for table CLIDN.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DIGITS	N/A		numeric digits 0-9 and N	<i>Digits.</i> The entry is equal to the ten-digit DN of a line external to the switching unit. The letter N must prefix service codes like 411, 911 and 0. This action makes the total digit count equal to 10. The system translates the letter N internally to 0.

Datafill example

The following figure shows an example of datafill for table CLIDN. The example contains a service code, 7-digit DN and 10-digit DN.

MAP example for table CLIDN

TABLE: CLIDN

DIGITS

NNNNNNN411
NNN8765000
2018213456

Table release history update

Design activity A00004045 (CLIDN for DMS-250) introduced log report TRK605 to the UCS DRU in SN07.

Design activity AN1658 (Inter-Switch Call Trace) introduced log report TRK605 in CNA05.

Supplementary information

N/A

Translation verification other tools

Table CLIDN does not use translation verification tools.

Service Orders (SO) (CM & SESM)

N/A

Software optionality control (SOC)**SOC**

SOC option name:	CLIDN for DMS-250
SOC option title:	Yes
SOC option control type:	usage
New SOC option?	Yes
SOC option order code	UTRS0012
Option defined in DRU:	UCS
Affected products:	SN07

Element Management

N/A

Command interface changes

N/A

Security

N/A

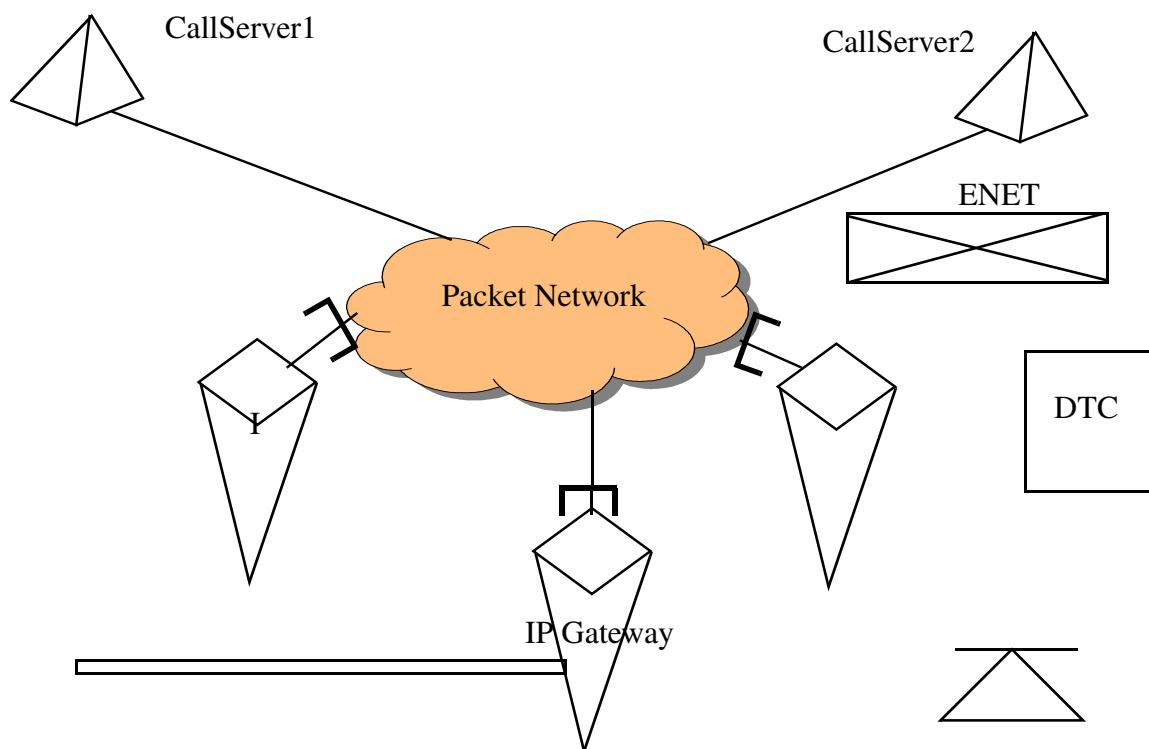
Configuration Walkthrough

In order to perform CLIDN call tracing on the DMS-250, SOC UTRS0012 must be ON and the desired called number(s) must be datafilled in table CLIDN.

Product = CS2000**A00004046 -- ECAN for Trimodal, 9K-IP-IPIW to Legacy (UA-IP)*****Functional Description***

The TriModal call model allows for legacy, AAL1 and IP bearer fabrics to co-exist in the same Call Server VPN. This activity is responsible for ensuring that ECAN resources can and are allocated appropriately within the CallServer VPN. The goal is to ensure that ECAN resources are always applied in IP networks and are applied according to the selected strategy for AAL1 fabric. This entails implementation of an Edge Strategy for IP Networks and either an Edge or Region strategy for AAL1 networks. Edge Strategy requires that ECAN resources are always allocated at the point of entry into a packet network. Region strategy uses a provisioning model that allows the customer to dictate where ECAN resources should be deployed throughout the network.

Edge Strategy



[- Indicates an ECAN resource

The diagram above is an illustration of how an edge strategy could be employed. The salient point is that every point of entry into the network is covered by an ECAN resource.

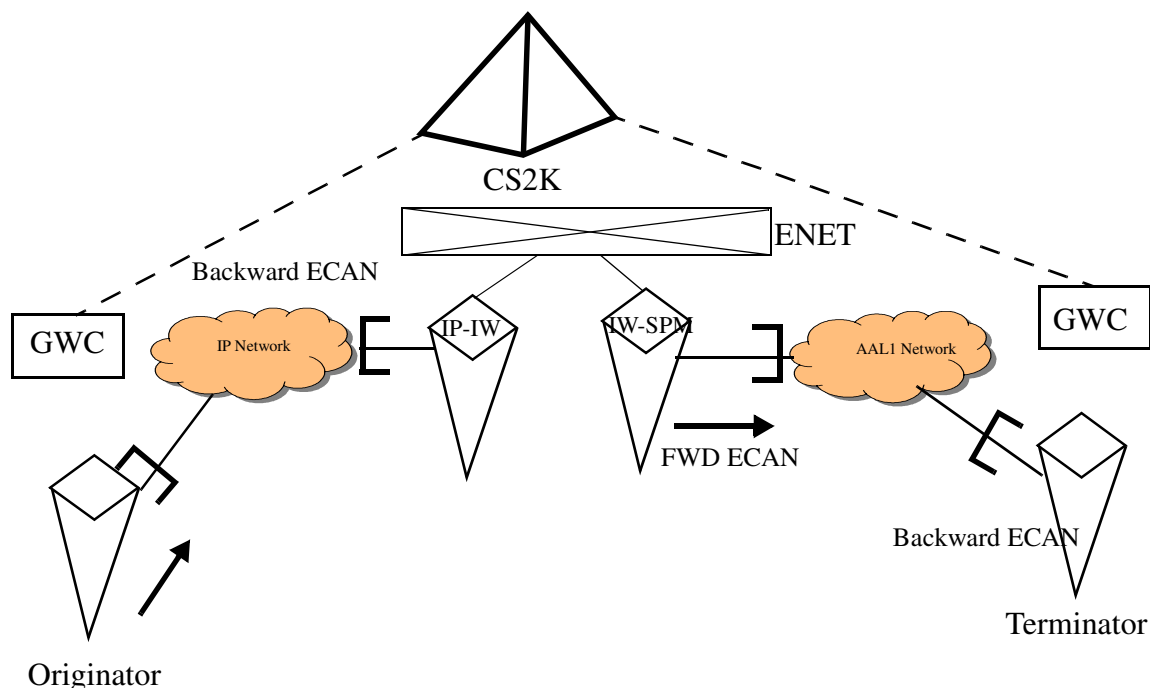
Conversely, a region strategy is dictated by provisioning. The customer, using knowledge of network parameters, provisions the strategic locations within their network where ECAN resources should be applied. It is not assumed that a network device with a packet interface will automatically utilize ECAN resources.

In SN06, feature A89007309, introduced support for an ECAN_EDGE_STRATEGY office parameter which would be used to differentiate between EDGE and REGION strategies on IP and AAL1 networks. A primary goal of activity A00004046 is to ensure that in the TriModal implementation, this strategy continues to be effective.

In SN07, IP, AAL1 and ENET bearer fabrics all co-exists on the same CS2K callserver. At a minimum, every call in this topology must have sufficient ECAN resources. These resources may be provided locally or optimized out of the call if it is subsequently determined that the resource is not required. Fortunately, the SN06 strategy extends itself quite well to the TriModal architecture, ensuring that ECAN is applied consistent with this strategy.

The ECAN edge strategy will be assumed for all packet network types except AAL1. The ECAN strategy for AAL1 will be determined by the value of the EDGE_ECAN_STRATEGY office parameter. Currently, there are scenarios where ECAN resources in a TriModal switch will be duplicated.

TRI-MODAL IP-AAL1 Call



In the call scenario above, 4 ECAN resources will be allocated in the call, depending upon the ECAN_EDGE_STRATEGY value for the AAL1 side. The IP side of the call will always allocate both ECAN resources, however, if the REGION strategy is deployed, the ECAN resource on the AAL1 side of the call, utilizing the IW-SPM, will be deallocated. The manner in which ECAN resources are allocated in this TriModal topology is unchanged from

the manner in which the resources would be allocated if both IP and AAL1 were not converged.

Therefore, in summary, the ECAN_EDGE_STRATEGY parameter will continue to be used in the CS2K to control ECAN allocation in the AAL1 bearer fabric. All other packet bearer fabrics will assume the edge strategy.

Trunk Provisioning

In summary, support for TriModal CS2K should be transparent to the customer. Support for this activity will be provided by the existing infrastructure, developed in the previous release for support of Next Generation Networks.

Hardware Requirements or Dependencies

There are no additional hardware requirements in support of this feature.

Software Requirements or Dependencies

There are no additional software requirements in support of this feature.

Limitations and restrictions

Trunk provisioning pertaining to ECAN is limited to provisioning ECAN resources against a specific trunk sub-group. There are 2 fields in TRKSGRP where this is done. On SPM peripherals, the SPMECIDX option is used to connect a specific ECAN provisioned value with a subgroup. For all other trunks, the ECSTAT field is used to determine whether or not ECAN resources are available, internally or externally.

This mode of operation is unchanged in this activity, however, customers should be aware of the following limitation (once MG4K-IP is available) when determining the ECAN characteristics of SPM based trunk members constituting a trunk group. TRKSGRP table only allows 2 subgroup tuples to be added per trunk group. There are currently 3 bearer fabrics that could potentially differ in their ECAN provisioning requirements in this table.

- Legacy Trunks i.e DMSCP SPM.
- AAL1 Trunks i.e. MG4K
- IP Trunks i.e. MG4K-IP (not available in SN07)

Since only 2 trunk subgroup tuples are allowed per trunk group, if the strategy for a trunk group contains all three component types, 2 of these types must share the same SPMECIDX value. This constraint should be considered during trunk datafill planning.

Interactions

There should be no visible effect in support of ECAN allocation in a TRI-MODAL call server. The extensibility of existing Next-Generation-Networks

ECAN support makes the application of these resources transparent on a TRI-MODAL CS2K.

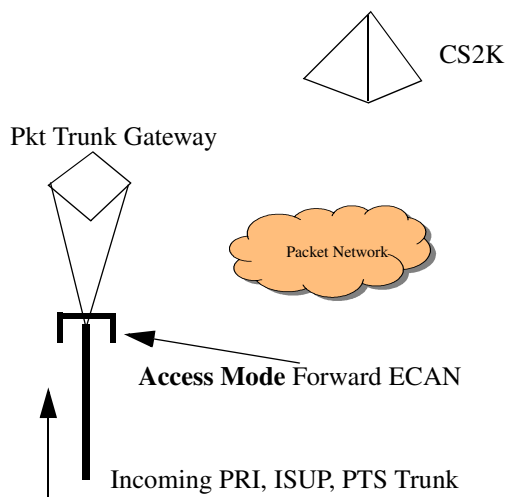
ECAN Terminal Type Cross Matrix

The allocation of resources are described in terms of Forward and Backward ECAN and Network vs. Access Mode allocation. In order to facilitate the understanding of table data, an explanation of these terms is in order.

Forward ECAN refers to ECAN resources that prevent echo from traversing in the forward direction of the call from originator to terminator. Backward ECAN refers to ECAN resources that prevent echo from traversing the call in a backwards direction from terminator to originator.

This concept in conjunction with Access vs. Network mode echo cancellation provides the exact direction and location in the CS2K that the echo cancellers are applied. Access mode ECAN refers to echo cancellers applied towards the facility i.e. The Line or the Trunk entity that is the source of the echo. Network mode ECAN applies echo cancellers toward the ENET. “Towards the ENET” or “Towards the Facility” applies to the “tail of the echo”. The “tail of the echo” can be thought of as the round-trip path from the echo canceller to the source of the echo. The echo cancellers are deployed in the direction of the tail. The following diagrams are provided to help the reader to understand how echo cancellers are applied in conjunction with these concepts.

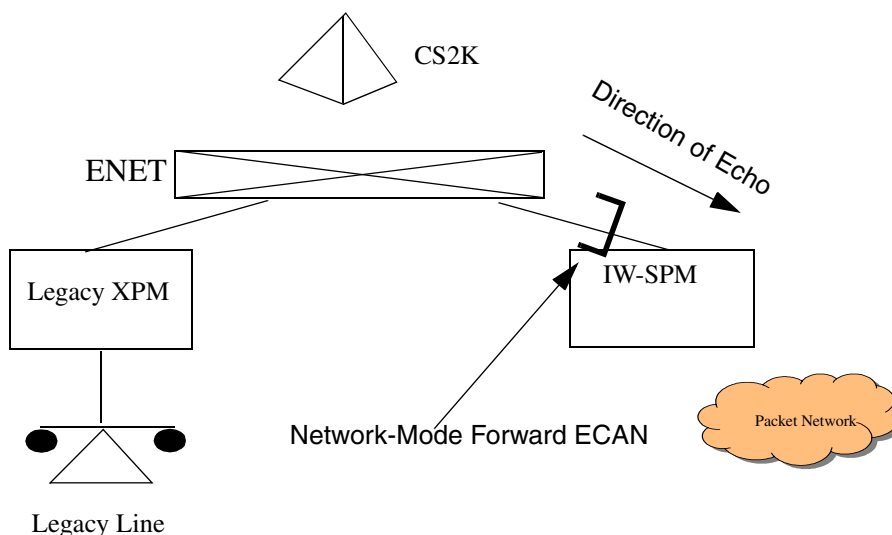
Access Mode ECAN Example



As the preceding figure illustrates, the echo canceller is applied to the incoming trunk, before packetization. It is Access Mode because it is applied to control echo from the Facility. It is “forward” because it is blocking echo in the forward direction towards the terminating side of the call.

Network-Mode echo cancellers are applied toward the ENET. This is the defining characteristic of Network-Mode ECAN. Figure below illustrates this concept.

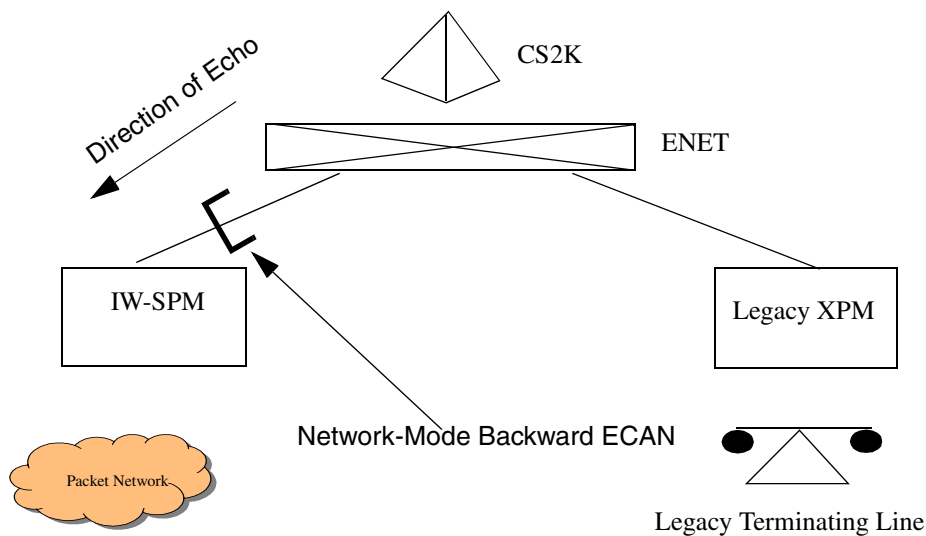
Network Mode Forward ECAN



In the preceding figure, the echo canceller is forward, due to the direction of the echo that is being cancelled. Echo cancellation is applied prior to packetization. However, the same ECAN resource applied in a different configuration can be Network-Mode **Backward** ECAN due to its position within the CS2K VLAN. This is the reason that Forward and Backward are not sufficient to determine the location of an echo canceller in the VLAN.

If the IW-SPM is positioned on the originating side of the CS2K VLAN, as opposed to the terminating side of the CS2K as it is shown in Figure , it is providing Backward ECAN.

The following figure illustrates an IW-SPM providing ECAN resources in this capacity.

Network-Mode Backward ECAN

The following tables provide a high-level view of ECAN allocation for different terminal types. Note that ABI lines and trunks have the same ECAN behavior as a packet line of the same network type. For example, an AAL1 ABI trunk would have the same ECAN behavior as listed in the following tables for an AAL1 line.

ECAN Location for Legacy and IP Interworkings

Call Type	IP IW SPM	IP MG4K	IP Line GW	IP trunk GW
IP line to Legacy agent	Backward ECAN		Forward ECAN	
Legacy agent to IP line	Forward ECAN		Backward ECAN	
IP MG4K trunk to Legacy agent	Backward ECAN	Forward ECAN		
Legacy Agent to IP MG4K trunk	Forward ECAN	Backward ECAN		
IP GWC trunk to Legacy agent	Backward ECAN			Forward ECAN
Legacy Agent to IP GWC trunk	Forward ECAN			Backward ECAN
Legacy Agent to SIPT GWC trunk	Forward ECAN			

ECAN Location for Legacy and IP Interworkings

Call Type	IP IW SPM	IP MG4K	IP Line GW	IP trunk GW
SIPT GWC trunk to Legacy Agent	Backward ECAN			
Note:	It is assumed that all packet trunks are datafilled with access mode ECAN.			

ECAN Location for AAL1 agent Interworkings

Call Type	ECAN_EDGE_STRATEGY = N			ECAN_EDGE_STRATEGY = Y		
	AAL1 IW SPM	AAL1 MG4K	AAL1 line GW	AAL1 IW SPM	AAL1 MG4K	AAL1 line GW
AAL1 line to AAL1 line			Forward & Backward ECAN			Forward & Backward ECAN
AAL1 line to MG4K trunk		Forward & Backward ECAN**	Forward ECAN		Backward ECAN	Forward ECAN
AAL1 line to AAL1 BICC trunk			Forward ECAN			Forward ECAN
MG4K trunk to MG4K trunk		Forward & Backward ECAN			Forward & Backward ECAN	
MG4K trunk to AAL1 line		Forward & Backward ECAN**	Backward ECAN		Forward ECAN	Backward ECAN
MG4K trunk to AAL1 BICC trunk		Forward & Backward ECAN**			Forward ECAN	
AAL1 BICC trunk to AAL1 BICC trunk						
AAL1 BICC trunk to AAL1 line			Backward ECAN			Backward ECAN
AAL1 BICC trunk to AAL1 MG4K trunk		Backward ECAN			Backward ECAN	
Note:	It is assumed that all packet trunks are datafilled with access mode ECAN. **Note: calls involving AAL1 MG4K ISUP trunks when ECAN_EDGE_STRATEGY is set to N will result in two ECAN resources in the same direction even if provisioned to only perform ECAN in only one direction.					

ECAN Location for Legacy and AAL1 Interworkings

Call Type	ECAN_EDGE_STRATEGY = N			ECAN_EDGE_STRATEGY = Y		
	AAL1 IW SPM	AAL1 MG4K	AAL1 line GW	AAL1 IW SPM	AAL1 MG4K	AAL1 line GW
AAL1 line to Legacy agent			Forward ECAN	Backward ECAN		Forward ECAN
Legacy agent to AAL1 line			Backward ECAN	Forward ECAN		Backward ECAN
MG4K trunk to Legacy agent		Forward & Backward ECAN**		Backward ECAN	Forward ECAN	
Legacy Agent to MG4K trunk		Forward & Backward ECAN**		Forward ECAN	Backward ECAN	
Legacy Agent to DPT GWC trunk	Forward ECAN			Forward ECAN		
DPT GWC trunk to Legacy Agent	Backward ECAN			Backward ECAN		
Note:	It is assumed that all packet trunks are datafilled with access mode ECAN. **Note: calls involving AAL1 MG4K ISUP trunks when ECAN_EDGE_STRATEGY is set to N will result in two ECAN resources in the same direction even if provisioned to only perform ECAN in only one direction.					

ECAN Location for IP and AAL1 (edge) Interworkings

Call Type	IP IW SPM	IP MG4K	IP Line GW	IP trunk GW	AAL1 IW SPM	AAL1 MG4K	AAL1 line GW
IP line to AAL1 line	Backward ECAN		Forward ECAN		Forward ECAN		Backward ECAN
IP line to AAL1 BICC trunk	Backward ECAN		Forward ECAN		Forward ECAN		
IP line to AAL1 MG4K trunk	Backward ECAN		Forward ECAN		Forward ECAN	Backward ECAN	
IP GWC trunk to AAL1 line	Backward ECAN			Forward ECAN	Forward ECAN		Backward ECAN
IP GWC trunk to AAL1 BICC trunk	Backward ECAN			Forward ECAN	Forward ECAN		
IP GWC trunk to AAL1 MG4K trunk	Backward ECAN			Forward ECAN	Forward ECAN	Backward ECAN	

ECAN Location for IP and AAL1 (edge) Interworkings

Call Type	IP IW SPM	IP MG4K	IP Line GW	IP trunk GW	AAL1 IW SPM	AAL1 MG4K	AAL1 line GW
IP MG4K trunk to AAL1 line		Forward ECAN			Forward ECAN		Backward ECAN
IP MG4K trunk to AAL1 BICC trunk	Backward ECAN	Forward ECAN			Forward ECAN		
IP MG4K trunk to AAL1 MG4K trunk		Forward ECAN				Backward ECAN	
IP SIPT trunk to AAL1 line	Backward ECAN				Forward ECAN		Backward ECAN
IP SIPT trunk to AAL1 BICC trunk	Backward ECAN				Forward ECAN		
IP SIPT trunk to AAL1 MG4K trunk	Backward ECAN				Forward ECAN	Backward ECAN	
AAL1 line to IP line	Forward ECAN		Backward ECAN		Backward ECAN		Forward ECAN
AAL1 line to IP GWC trunk	Forward ECAN			Backward ECAN	Backward ECAN		Forward ECAN
AAL1 line to IP MG4K trunk		Backward ECAN			Backward ECAN		Forward ECAN
AAL1 line to IP SIPT trunk	Forward ECAN				Backward ECAN		Forward ECAN
AAL1 BICC trunk to IP line	Forward ECAN		Backward ECAN		Backward ECAN		
AAL1 BICC trunk to IP GWC trunk	Forward ECAN			Backward ECAN	Backward ECAN		
AAL1 BICC trunk to IP MG4K trunk	Forward ECAN	Backward ECAN			Backward ECAN		
AAL1 BICC trunk to IP SIPT trunk	Forward ECAN				Backward ECAN		
AAL1 MG4K trunk to IP line	Forward ECAN		Backward ECAN			Forward ECAN	
AAL1 MG4K trunk to IP GWC trunk	Forward ECAN			Backward ECAN	Backward ECAN	Forward ECAN	
AAL1 MG4K trunk to IP MG4K trunk		Backward ECAN				Forward ECAN	

ECAN Location for IP and AAL1 (edge) Interworkings

Call Type	IP IW SPM	IP MG4K	IP Line GW	IP trunk GW	AAL1 IW SPM	AAL1 MG4K	AAL1 line GW
AAL1 MG4K trunk to IP SIPT trunk	Forward ECAN				Backward ECAN	Forward ECAN	
Note:	It is assumed that all packet trunks are datafilled with access mode ECAN.						

ECAN Location for IP and AAL1 (region) Interworkings

Call Type	IP IW SPM	IP MG4K	IP Line GW	IP trunk GW	AAL1 IW SPM	AAL1 MG4K	AAL1 line GW
IP line to AAL1 line	Backward ECAN		Forward ECAN				Backward ECAN
IP line to AAL1 BICC trunk	Backward ECAN		Forward ECAN		Forward ECAN		
IP line to AAL1 MG4K trunk	Backward ECAN		Forward ECAN			Forward & Backward ECAN**	
IP GWC trunk to AAL1 line	Backward ECAN			Forward ECAN			Backward ECAN
IP GWC trunk to AAL1 BICC trunk	Backward ECAN			Forward ECAN	Forward ECAN		
IP GWC trunk to AAL1 MG4K trunk	Backward ECAN			Forward ECAN		Forward & Backward ECAN**	
IP MG4K trunk to AAL1 line		Forward ECAN					Backward ECAN
IP MG4K trunk to AAL1 BICC trunk	Backward ECAN	Forward ECAN			Forward ECAN		
IP MG4K trunk to AAL1 MG4K trunk		Forward ECAN				Backward ECAN	
IP SIPT trunk to AAL1 line	Backward ECAN						Backward ECAN
IP SIPT trunk to AAL1 BICC trunk	Backward ECAN				Forward ECAN		
IP SIPT trunk to AAL1 MG4K trunk	Backward ECAN					Forward & Backward ECAN**	

ECAN Location for IP and AAL1 (region) Interworkings

Call Type	IP IW SPM	IP MG4K	IP Line GW	IP trunk GW	AAL1 IW SPM	AAL1 MG4K	AAL1 line GW
AAL1 line to IP line	Forward ECAN		Backward ECAN				Forward ECAN
AAL1 line to IP GWC trunk	Forward ECAN			Backward ECAN			Forward ECAN
AAL1 line to IP MG4K trunk	Forward ECAN	Backward ECAN					Forward ECAN
AAL1 line to IP SIPT trunk	Forward ECAN						Forward ECAN
AAL1 BICC trunk to IP line	Forward ECAN		Backward ECAN		Backward ECAN		
AAL1 BICC trunk to IP GWC trunk	Forward ECAN			Backward ECAN	Backward ECAN		
AAL1 BICC trunk to IP MG4K trunk	Forward ECAN	Backward ECAN			Backward ECAN		
AAL1 BICC trunk to IP SIPT trunk	Forward ECAN				Backward ECAN		
AAL1 MG4K trunk to IP line	Forward ECAN		Backward ECAN			Forward & Backward ECAN**	
AAL1 MG4K trunk to IP GWC trunk	Forward ECAN			Backward ECAN		Forward & Backward ECAN**	
AAL1 MG4K trunk to IP MG4K trunk		Backward ECAN				Forward ECAN	
AAL1 MG4K trunk to IP SIPT trunk	Forward ECAN					Forward & Backward ECAN**	
Note:	It is assumed that all packet trunks are datafilled with access mode ECAN. **Note: calls involving AAL1 MG4K ISUP trunks when ECAN_EDGE_STRATEGY is set to N will result in two ECAN resources in the same direction even if provisioned to only perform ECAN in only one direction.						

Applicable customer facing sections

Fault Management

Logs

Alarms	_____
Configuration	
Data Schema	_____
User Interface	_____
Element Management	_____
Security	_____
Service Order	_____
Office Parameters	__X__
Accounting (includes AMA billing)	_____
Performance (includes operational measurements)	_____

Glossary

Term	Description
Forward ECAN	Echo Cancellers blocking echo from traversing from originator to terminator
Backward ECAN	Echo Cancellers blocking echo from traversing from terminator to originator

Configuration for A00004046

Initial Configuration

Customers must consider the ECAN requirements of trunk members that will comprise trunk groups within the network. The inability to set more than two simultaneous SPMECIDX values within a trunk group is the source of this constraint.

The SPMECIDX field identifies a particular ECAN configuration tied to trunk members within a trunk subgroup. The existing TRKSGRP table only allows two tuples within the same trunk group. Therefore, for SPM based trunks coexisting with ENET based trunks, there are only 2 possible ECAN alternatives available.

Office parameters (CM)

The ECAN_EDGE_STRATEGY office parameter's role is changing slightly in SN07. This change impacts the role of this office parameter for determining ECAN implementation strategy within the network.

Modified office parameters

Parm table	Parameter name	NEW/CHANGE D/DELETED/R ELOCATED	Domain (CM or Subnet Management)
OFCENG	ECAN_EDGE_STRATEGY	CHANGED	CM

Parameter information**ECAN_EDGE_STRATEGY**

ECAN_EDGE_STRATEGY in table OFCENG.

Functional description

The ECAN_EDGE_STRATEGY is used to determine ECAN resource allocation strategy within the network. The role of this parameter is changing in SN07 to only impact AAL1 networks. The assumption is that all other packet networks are EDGE strategy by default.

Provisioning rules

No Change

Range information

No Change

Activation

No Change

Dependencies

No Change

Consequences

No Change

Verification

No Change

Memory requirements

No Change

Parameter release history update

ECAN_EDGE_STRATEGY in table OFCENG in SN07 and beyond will only apply to AAL1 bearer networks. All other packet network type such as IP will assume the edge ECAN strategy.

Upgrade Impact

Dump and Restore

There is no impact to upgrades.

Element Management Upgrade

Not applicable.

Product = CS2000

A00004271 -- SIP App Server SOC (PT-IP)

Functional Description

This activity implements a mechanism to control the maximum number of SIPT calls that utilize the Next Generation Session Server (NGSS) platform when the far end is a non-CS2K, referred to here as an Application Server. A usage SOC, CS2B0009, is implemented to limit these types of calls (abbreviated as CS2AS in this document).

Another activity, A00004414 SIP Call Server SOC, implements a similar mechanism to control the maximum number of SIPT calls that utilize the NGSS platform when the far end is another CS2K (CS2CS calls). SOC option CS2B0008 is the usage SOC for A00004414.

Both SOC features are part of a set of activities for delivering the Session Server - SIP Gateway application in SN07. The other features are:

- A00003270 SIP Open Interop Call Processing
- A00003271 Session Server Web Server Interface
- A00003272 Session Server Provisioning Framework
- A00003273 SIP Gateway Application Maintenance
- A00003277 Session Server OM Subsystem
- A00003279 SIP on Session Server Link Maintenance and Load Balancing
- A00003280 SIP on Session Server Tracing/Debug Framework
- A00003281 SIP on Session Server Call Audit
- A00003282 SIP on Session Server Datasync
- A00003933 SIP on Session Server Drop 1 ICAF
- A00003934 Session Server Project ICAF

SOC limiting

The usage-controlled CS2B0009 SOC added by this activity applies to calls that have the following characteristics:

- the incoming or outgoing trunk group has the DYNAMIC option with SIPT SIGNALING in table TRKOPTS,
- a match of the incoming or outgoing trunk group is found in the SIPTTRK field of one of the tuples in table SIPLINK²,
- the CONNTYPE field of the tuple in table SIPLINK is set to CS2AS

A counter keeps track of the current number of calls matching the above criteria. For each new CS2AS call, the current value in the counter is checked against the limiting value in the CS2AS SOC. If the addition of a new call of this type would exceed the SOC limit, the call is sent to treatment; otherwise, the counter is incremented and the call is allowed to proceed. When the call is ended, the counter is decremented.

In the following example of table SIPLINK, incoming SIPT calls on trunk group NGSSINC and outgoing calls on trunk group NGSSOUT will increment the usage counter for the CS2AS SOC.

TABLE: SIPLINK

LINKNAME	CONNTYPE	AGNTDATA

NGSSOUTLK	CS2AS ISUPTRK	NGSSOUT
NGSSINLINK	CS2AS ISUPTRK	NGSSINC
LOOPAROUND1	CS2CS ISUPTRK	NGSSLOOP

Here is an example of the output of the SOC SELECT command for the new SOC:

```
>select option CS2B0009
```

```
GROUP:CS2B
```

OPTION	NAME	RTU	STATE	USAGE	LIMIT	UNITS	LAST_CHG
-----	----	---	-----	-----	-----	-----	-----
CS2B0009	CS to AppS Calls	Y	-	127	500	1VC	04/01/19

2. Table SIPLINK is a new table introduced in feature A00003279

OMs

A new OM group, NGSSOM is introduced for tracking the effects of the CS2B0009 SOC limit setting on CS2AS calls. OM fields in the new group relative to this feature are:

- CS2ASOVF - pegged when a CS2AS NGSS call is deflected because allowing the call would have caused the current CS2AS call count to exceed the SOC limit.
- CS2ASHWM - keeps track of the maximum value reached for the CS2AS call counter.

Two other registers are added for feature A00004414 to keep track of CS2CS calls (SOC CS2B0008):

- CS2CSOVF - pegged when a CS2CS NGSS call is deflected because allowing the call would have caused the current CS2CS call count to exceed the SOC limit.
- CS2CSHWM - keeps track of the maximum value reached for the CS2CS call counter.

Sample output for the NGSSOM group:

NGSSOM

CLASS: ACTIVE

START:2003/12/01 06:00:00 MON; STOP: 2003/12/01 06:09:10 MON;

SLOWSAMPLES: 6 ; FASTSAMPLES: 55 ;

	CS2CSHW	CS2CSHW2	CS2ASHW	CS2ASHW2
	CS2CSOV	CS2CSOV2	CS2ASOV	CS2ASOV2
0				
	0	0	125	0
	0	0	0	0

Logs

The NGSS701 log is a new log added for this feature. It is generated when a CS2AS call is rejected because it would exceed the LIMIT setting of the CS2B0009 SOC.

The NGSS700 log is added for feature A00004414 to be output when a CS2CS call is rejected because it would exceed the LIMIT setting of the CS2B0008 SOC.

Hardware Requirements or Dependencies

None

Software Requirements or Dependencies

None

Limitations and restrictions

None

Interactions

The usage SOC introduced by this feature does not take the place of Base DPT usage SOC CS2B0005. The latter is still needed to set the value of office parameter DPT_MAX_PORTS in table OFCVAR. DPT_MAX_PORTS limits the overall number of simultaneous DPT calls.

Calls that peg the new CS2B0009 count will always peg the CS2B0005 count as well.

If the SOC limit set for CS2B0009 exceeds the limit of the Base DPT SOC CS2B0005, the latter is the limiting factor in determining the maximum number of simultaneous CS2AS calls.

Applicable customer facing sections

Fault Management

Logs ☒Alarms ☐

Configuration

Data Schema ☐User Interface ☐Element Management ☐Security ☐Service Order ☐Office Parameters ☐SOC ☒Accounting (includes AMA billing) ☐Performance (includes operational measurements) ☒

Glossary

Term	Description
CS2AS	CS2K Call Server-to-Agent Server
CS2CS	CS2K Call Server-to-CS2K Call Server

Fault Management for A00004271

Fault management strategy

A log is needed to provide real-time indication when a SIPT call is not allowed to proceed due to the SOC LIMIT setting of either CS2B0008 or CS2B0009.

Fault management tools and utilities

DMS logutil system.

Logs

Explanation

Log Title: NGSS 700

Name: CS2CS CALL REJECTED

Description: This log is generated when a SIPT CS2CS call is rejected because it would exceed the LIMIT setting of the CS2B0008 SOC. The SIPT call is not allowed to complete through the NGSS.

Event type: Call setup failure.

Format

```
NGSS700 <mmdd hh:mm:ss ssdd> INFO CS2CS CALL REJECTED
NGSS CS2CS call limit has been reached
A new LIMIT for SOC CS2B0008 may be needed.
```

Field descriptions

There are no fields associated with this log, only text indicating SOC CS2B0008's LIMIT setting is being exceeded.

Action

The SOC LIMIT setting for the SIP Call Server SOC CS2B0008 option may need to be increased.

Associated Operational Measurements or Performance Measurements

The CS2CSOV register in OM group NGSSOM is pegged.

Additional information

None.

Explanation

Log Title: NGSS 701

Name: CS2AS CALL REJECTED

Description: This log is generated when a CS2AS call is rejected because it would exceed the LIMIT setting of the CS2B0009 SOC. The SIPT call is not allowed to complete through the NGSS.

Event type: Call setup failure.

Format

```
NGSS701 <mmdd hh:mm:ss ssdd> INFO CS2AS CALL REJECTED
```

```
NGSS CS2AS call limit has been reached
```

```
A new LIMIT for SOC CS2B0009 may be needed.
```

Field descriptions

There are no fields associated with this log, only text indicating SOC CS2B0009's LIMIT setting is being exceeded.

Action

The SOC LIMIT setting for the SIP Call Server SOC CS2B0009 option may need to be increased.

Associated Operational Measurements or Performance Measurements

The CS2ASOV register in OM group NGSSOM is pegged.

Additional information

None.

Related documentation

Performance for A00004271

Performance management strategy

The system needs to monitor and provide output as to whether the limit settings for SOC's CS2B0008 and CS2B0009 are being exceeded, as well as what the high water usage mark is for each. A new DMS OM group is the method chosen to capture this information.

Performance management tools and utilities

The DMS OM system.

Performance Measurements (PM), Operational Measurements (OM), and stats

PM, OM, and stats format

N/A

OM Group NGSSOM

OM description

The NGSSOM group provides information on the maximum number of simultaneous calls that utilize the NGSS platform as well as indication of the number of times the limit settings of the CS2B0008 and CS2B0009 usage SOC's have been exceeded.

Release history update

The OM group is created in SN07.

Registers

OM group registers display on the MAP terminal as follows:

OM Group Display

CS2CSHW	CS2CSHW2	CS2ASHW	CS2ASHW2
CS2CSOV	CS2CSOV2	CS2ASOV	CS2ASOV2

Group structure

OM group provides 1 tuple for the entire CS2K.

Key field: N/A

Info field: N/A

Associated OM groups

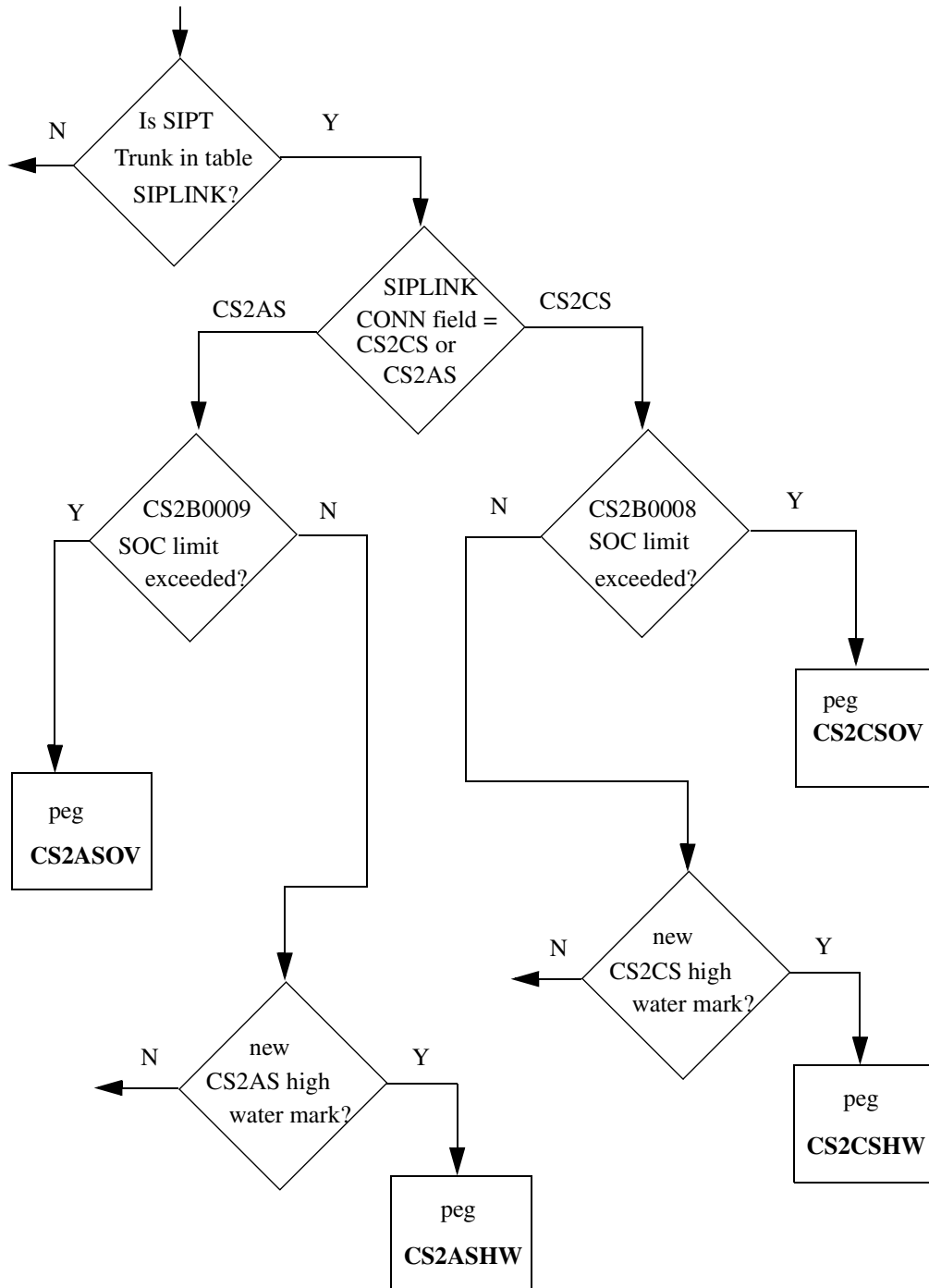
None

Associated functional groups

None

Associated functionality codes

None

NGSSOM registers logic flow chart

Register CS2CSHW

Register description

Holds the value of the highest number of simultaneous SIPT calls that utilize the NGSS platform to handle a call to or from another CS2K.

Register release history update

Register is created in SN07

Associated registers

Overflow register is CS2CSHW2

Associated logs

None

Register CS2CSOV

Register description

Holds the number of times a SIPT call did one of the following:

- attempted to utilize the NGSS platform to reach a far-end CS2K and was not allowed to complete because it would have exceeded the limit set by the usage SOC CS2B0008.
- was received from a far-end CS2K via the NGSS platform and was not allowed to complete because it would have exceeded the limit set by the usage SOC CS2B0008.

Register release history update

Register is created in SN07

Associated registers

Overflow register is CS2CSOV2

Associated logs

None

Register CS2ASHW

Register description

Holds the value of the highest number of simultaneous SIPT calls that utilize the NGSS platform to reach a far-end SIP application server.

Register release history update

Register is created in SN07.

Associated registers

Overflow register is CS2ASHW2

Associated logs

None

Register CS2ASOV**Register description**

Holds the number of times a SIPT call did one of the following:

- attempted to utilize the NGSS platform to reach a far-end SIP application server and was not allowed to complete because it would have exceeded the limit set by the usage SOC CS2B0009.
- was received from a far-end SIP application server via the NGSS platform and was not allowed to complete because it would have exceeded the limit set by the usage SOC CS2B0009.

Register release history update

Register is created in SN07.

Associated registers

Overflow register is CS2ASOV2.

Associated logs

None

Product = CS2000**A00004391 -- ACD Agent Expansion from 9,999 to 30,000 Agents
(Succession on DMS)*****Functional Description***

Currently, the maximum number of ACD agents that can be provisioned in a single SL-100 or DMS-100 switch is 9,999. This feature extends that maximum to 30,000 agents.

This activity does not increase the number of ACD groups per switch nor the number of ACD agents per group. It only increases the switch-wide maximum number of total ACD agents.

This feature will be controlled via usage based SOC. The maximum number of ACD agents in the switch will be determined by the level of SOC which has been purchased but cannot exceed 30,000 agents.

Background

The maximum number of ACD agents that can be provisioned in a DMS-100 or SL-100 is currently determined by the value of an office parameter. The parameter MAX_NUM_ACD_AGENTS_PER_SWITCH is found in table OFCOPT and can be set to any value in the range of 0 to 9999.

When an attempt is made to create a new ACD agent, the current count of agents in the switch is compared to the value of the office parameter. If the limit has already been reached, the new agent cannot be created. For this activity, the range of the office parameter will be increased to 30000.

Other factors which contribute to the current maximum of 9,999 ACD agents per switch include the ACD agent position ID (POSID) and login ID (LOGINID). The POSID is defined via SERVORD when a new ACD agent is created, and LOGINIDs are defined via tables ACDLOGIN and ACDENLOG.

The POSID and LOGINID are both four digit values with a range of 0001 to 9999. Though neither POSID nor LOGINID is directly correlated to the number of agents in the switch, it would be impractical to have more than 9,999 agents if the POSID and LOGINID remain limited to 4 digits. Therefore, the range of POSID and LOGINID will be increased to 30000.

The external impact of making these changes is briefly described in the sections that follow. More detailed information can be found in Section on page 1774.

Office parameter MAX_NUM_ACD_AGENTS_PER_SWITCH

The office parameter MAX_NUM_ACD_AGENTS_PER_SWITCH currently has a maximum value of 9999. The range of this parameter will be increased to have a maximum value of 30000. The actual value of this parameter can no longer be changed by the end user. In order to change the value of the parameter, the SOC usage limit must be changed. The value in the office parameter will then be automatically updated to reflect the new SOC limit.

See Section on page 1775 and Section on page 1786 for detailed information.

Table ACDLOGIN

Table ACDLOGIN currently supports a maximum of 9,999 tuples. LOGINIDs between 0001 and 9999 can be datafilled here for use by individual ACD agents. This table will be expanded to support up to 30,000 tuples.

Expansion to 30,000 LOGINIDs requires that the LOGINID field be expanded from a 4 digit value to a 5 digit value. Existing 4 digit LOGINIDs will be padded with a leading 0 during ONP.

See Section on page 1776 for detailed information.

Table ACDENLOG

Table ACDENLOG currently supports up to 1024 partitions with a maximum of 9,999 tuples each. LOGINIDs between 0001 and 9999 can be datafilled in each partition for use by individual ACD agents. This table will be expanded to support up to 30,000 LOGINIDs in each partition.

Expansion to 30,000 LOGINIDs per partition requires that the LOGINID field be expanded from a 4 digit value to a 5 digit value. Existing 4 digit LOGINIDs will be padded with a leading 0 during ONP.

See section Section on page 1776 for detailed information and examples.

Table ACDGRP

This activity adds a new field in table ACDGRP. The new field will be called IDSIZE and will specify the number of login digits to be used by all agents in the group. IDSIZE can be set to a value of 4 or 5. The default value will be 4.

When IDSIZE equals '4', all agents in the ACD group will login using 4 digit login IDs. When IDSIZE equals '5', all agents in the ACD group will login using 5 digit login IDs.

During ONP from a load which does not include this feature to a load which does, IDSIZE will be defaulted to '4' for all ACDGRP tuples.

All existing agents will continue to login using their existing 4 digit login IDs. The operating company can continue to add agents to these groups and/or create new groups with IDSIZE = 4 provided that there are available login IDs in the range of 00001 to 09999. Availability depends on datafill in table ACDLOGIN and/or ACDENLOG.

When login IDs 00001 through 09999 have been exhausted, the next agent added must use a 5 digit login ID. This means that the agent's entire ACD group must be converted to 5 digit login.

Converting a group to 5 digit login

To convert an ACD group from 4 digit login to 5 digit login, field IDSIZE in table ACDGRP must be changed to '5'. No other switch based changes will be required. However, all agents in that ACD group must be notified to begin using 5 digit login. Existing agents can simply use their old 4 digit login ID but manually pad it with a leading 0. For example, an agent using a login ID of

1234 will begin using the login ID 01234. If they attempt to login without the leading 0, the login will fail.

New agents that are added to a group already using 5 digit login IDs can use any available login ID in the range of 00001 to 30000. Availability depends on existing datafill in table ACDLOGIN and/or ACDENLOG.

See Section on page 1776 for detailed information and examples.

Table KSETLINE

Table KSETLINE defines the DN keys on all keysets. This activity makes a field change for KSETLINE tuples that meet the following criteria:

- FORMAT = 'ACD'
- ACDKEY = 'INCALLS'
- IDNUM = 'Y'

For these tuples, field POSID (position ID) is required. This activity expands the POSID field from 4 digits to 5 digits. Existing 4 digit POSIDs will be padded with a leading 0 during ONP.

The maximum value for POSID will be 30000.

See Section on page 1776 for detailed information and examples.

Table KSETFEAT

Table KSETFEAT defines the feature assignments on keysets. This activity makes a field change for KSETFEAT tuples that meet the following criteria:

- FEATURE = 'SUPR'
- IDNUM = 'Y'

For these tuples, field POSID (position ID) is required. This activity expands the POSID field from 4 digits to 5 digits. Existing 4 digit POSIDs will be padded with a leading 0 during ONP.

The maximum value for POSID will be 30000.

See Section on page 1776 for detailed information and examples.

Table IBNFEAT

Table IBNFEAT defines the feature assignments on IBN sets. This activity makes a field change for IBNFEAT tuples that meet the following criteria:

- FEATURE = 'ACD' or 'SUPR'
- IDNUM = 'Y'

For these tuples, field POSID (position ID) is required. This activity expands the POSID field from 4 digits to 5 digits. Existing 4 digit POSIDs will be padded with a leading 0 during ONP.

The maximum value for POSID will be 30000.

See section Section on page 1776 for detailed information and examples.

SERVORD

Some Servord commands used by ACD offer a prompt for POSID. Currently, any value between 0000 and 9999 is accepted as valid input for the POSID. This activity will change the acceptable value of POSID to be a 5 digit value in the range of 00000 to 30000.

This change affects command prompting for NEW, ADO, NEWACD, and CHF commands.

See Section on page 1785 for detailed information and examples.

Tools

ACDDEBUG and ACDSHOW are Command Interface (CI) tools that will require changes by this feature in order to handle a 5 digit position ID. ACDDEBUG is a CI tool created to display ACD data structures. Currently, a ACDDEBUG command uses a 4 digit position ID as an index in order to display ACD agent data. This activity will extend the command so that the data structures of an ACD agent with a 5 digit position will be displayed.

ACDSHOW is a CI tool that displays specific information concerning a current ACD configuration such as the list of agent positions in a ACD group and agent information for a given user login ID. Currently, ACDSHOW commands use a 4 digit position ID as an index in order to display information concerning an ACD configuration. This activity will extend the command so that the information of an ACD agent with a 5 digit position will be displayed.

For more information on ACDDEBUG and ACDSHOW, please refer to Section on page 1787.

Intelligent Call Management (ICM)

ICM is a product that connects a host computer to a DMS-100 or MSL-100. ICM defines a switch to computer message set and a computer to switch message set that enables services to a telephone subscriber. Call event messages are sent from the switch to the host computer. Whereas call control messages, are sent from the host computer to the switch. Specific ICM call event messages or ICM call control message can contain a 'positionID' parameter and/or 'loginID' parameter. Currently, the 'positionID' parameter and the 'loginID' parameter in ICM messages handle only 4 digits.

This activity will allow the switch to send ICM call event messages to the host computer with a 5 digit 'positionID' parameter and/or a 5 digit 'loginID' parameter. This activity will also allow call control ICM messages sent from the host computer to the switch to have a 5 digit 'positionID' parameter or 5 digit 'loginID' parameter. Once the call control message is received on the switch, the 5 digit 'positionID' or 5 digit 'loginID' will be checked for validity.

ACD Management Information System (MIS)

ACD MIS is a hardware and software option which provides customer premise equipment (CPE) downstream processor (DSP) with information concerning ACD events occurring in an associated DMS-100 switch. The DSP can request and collect ACD information from the switch. There are two types of ACD MIS messages: messages sent from the switch to the DSP and message sent from the DSP to the switch.

The following are categories of messages sent from the switch to the DSP:

- Switch Control messages
- Initialization Data messages
- ACD VFG OM messages,
- ACD call/agent position event messages and
- Load Management Event messages.

Specific ACD MIS messages can contain a 'positionID' parameter and/or 'loginID' parameter. Currently, the 'positionID' parameter and the 'loginID' parameter in ACD MIS messages handle only 4 digits. This activity will allow ACD MIS messages sent from the switch to the DSP to have a 5 digit 'positionID' parameter or 5 digit 'loginID' parameter.

There following are categories of messages sent from the DSP to the switch:

- DSP Control Messages
- Inquire Switch Data Messages
- Remote Load Management Request messages.

This activity will allow ACD MIS message sent from the DSP to the switch to have a 5 digit 'positionID' parameter and/or a 5 digit 'loginID' parameter. The 5 digit 'positionID' will be checked for validity.

SOC Control

This feature will be controlled by a standard usage based SOC. The usage limit will define the maximum number of agents for the switch (i.e. the total number of lines that can have the ACD option assigned).

The default usage limit will be 0 ACD agents. During ONP from previous loads, the SOC usage limit will be set to match the value of office parameter MAX_NUM_ACD_AGENTS_PER_SWITCH. Thus there will be no impact to existing customers who do not purchase this SOC.

When the SOC is purchased, the usage limit can be increased by any number of agents up to a maximum value of 30,000 agents.

When the usage limit is changed via SOC, the value in office parameter MAX_NUM_ACD_AGENTS_PER_SWITCH will automatically be updated to reflect the SOC usage limit. The value in the office parameter can no longer be changed manually. The SOC usage limit must be changed first.

The SOC will not control the ability to use the optional 5 digit login IDs, nor will it control the ability to datafill extra login IDs for future use.

See Section on page 1786 for detailed information.

Hardware Requirements or Dependencies

Not applicable

Software Requirements or Dependencies

Not applicable

Limitations and restrictions

- Once an ACD group is converted to 5 digit login (see section 2.2.5), all of the agents in that group will be required to login using 5 digits. Pre-existing 4 digit login IDs can be used by dialing a leading zero.
- Once an ACD group is converted to 5 digit login, it cannot be converted back to 4 digit login.
- Login IDs 00001 through 09999 can be used by any ACD agent in the switch. If the agent's group is using 4 digit login (as defined in table ACDGRP), the agent will dial the last 4 digits only. If the agent's group is using 5 digit login, the agent must dial all 5 digits.
- Login IDs 10000 through 30000 can only be used by agents in groups which use 5 digit login.
- Although 5 digit login is optional per ACD group, it should be noted that 5 digit login will be required as soon as the login IDs 00001 through 09999 are exhausted. At that point, the next agent added must use a 5 digit login ID. This means that the entire group to which this agent belongs must be converted to 5 digit login. The other agents in the group can continue to use their previous login IDs, but they must now include a leading zero when logging in.

- Individual ACD agents cannot be moved between two ACD groups which do not use the same number of login digits. Field IDSIZE in table ACDGRP must match for an agent to be moved from group to group by any means.

Interactions

Load Management / Remote Load Management

Load Management / Remote Load Management allows ACD agents to be moved from one ACD group to another. This activity restricts movement of agents between groups which do not use the same number of login digits. Field IDSIZE in table ACDGRP must match or the agent movement will not be allowed.

Applicable customer facing sections.

Fault Management

Logs	__X__
Alarms	_N/A_

Configuration

Data Schema	__X__
User Interface	_N/A_
Element Management	_N/A_
Security	_N/A_
Service Order	__X__
Office Parameters	__X__

Accounting (includes AMA billing)	_N/A_

Performance (includes operational measurements)	_N/A_

Glossary

Term	Description
ACD	Automatic Call Distribution
ACDMIS	ACD Management Information Systems
ASN	Abstract Syntax Notation
CI	Command Interface
DMS	Digital Multiplex System

Term	Description
DN	Directory Number
DSP	Downstream Processor
IBN	Integrated Business Network
ICM	Intelligent Call Management
ONP	One Night Process
SCAI	Switch Computer Application Interface
SOC	Software Optionality Control

Fault Management for A00004391

Fault management strategy

There are 3 existing logs which are slightly modified for this feature. The modified logs are E911212, E911213, and E911214.

The modification is very minor. Each of these logs prints out a position ID and login ID when the 911 PSAP is using ACD. The fields used to display these IDs are increasing from 4 digits to 5 digits.

Fault management tools and utilities

Not Applicable

E911 212 Logs

Explanation

Log Title: E911 212

Name: E911 Call Event Record

Description: All E911 calls produce this log when either party disconnects.

Format

This is an existing log. Its function and basic format is unchanged by this activity.

If the E911 PSAP is using an ACD group for its agents, this log will print a position ID (POSID) and a login ID (LOGINID) associated with the agent who took the call. This feature expands these ID fields from 4 digits to 5 digits and extends their range to a maximum of 30000.

Field descriptions

Field descriptions

Field	Value	Description
POSID	00001 to 30000	This feature increases the size of this field to 5 digits and its range to a maximum of 30000.
LOGINID	00001 to 30000	This feature increases the size of this field to 5 digits and its range to a maximum of 30000.

Action

No new action is required beyond the standard procedures for E911 212 logs.

Associated Operational Measurements or Performance Measurements

Not Applicable.

Additional information

None.

E911 213 Logs

Explanation

Log Title: E911 213

Name: ACD PSAP Agent Login

Description: This log is produced when an ACD PSAP Agent logs in.

Format

This is an existing log. Its function and basic format is unchanged by this activity.

When an ACD PSAP agent logs in, this log is produced. It contains an AGENT POSITION ID and an AGENT LOGIN ID associated with the agent logging in. This feature expands these ID fields from 4 digits to 5 digits and extends their range to a maximum of 30000.

Field descriptions

Field descriptions

Field	Value	Description
AGENT POSITION ID	00001 to 30000	This feature increases the size of this field to 5 digits and its range to a maximum of 30000.
AGENT LOGIN ID	00001 to 30000	This feature increases the size of this field to 5 digits and its range to a maximum of 30000.

Action

No new action is required beyond the standard procedures for E911 213 logs.

Associated Operational Measurements or Performance Measurements

Not Applicable.

Additional information

None.

E911 214 Logs

Explanation

Log Title: E911 214

Name: ACD PSAP Agent Logout

Description: This log is produced when an ACD PSAP agent logs out.

Format

This is an existing log. Its function and basic format is unchanged by this activity.

When an ACD PSAP agent logs out, this log is produced. It contains an AGENT POSITION ID and an AGENT LOGIN ID associated with the agent logging out. This feature expands these ID fields from 4 digits to 5 digits and extends their range to a maximum of 30000

Field descriptions**Field descriptions**

Field	Value	Description
AGENT POSITION ID	00001 to 30000	This feature increases the size of this field to 5 digits and its range to a maximum of 30000.
AGENT LOGIN ID	00001 to 30000	This feature increases the size of this field to 5 digits and its range to a maximum of 30000.

Action

No new action is required beyond the standard procedures for E911 214 logs.

Associated Operational Measurements or Performance Measurements

Not Applicable.

Additional information

None.

Alarms

Not Applicable

Related documentation

None.

Configuration for A00004391**Hardware and Software Requirements**

Not applicable.

Initial Configuration

Not applicable.

Office parameters (OP)

New/modified office/subnet parameters

New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management)
OFCOPT	MAX_NUMBER_ACD_AGENTS _PER_SWITCH	CHANGED	CM

Parameter information

MAX_NUMBER_ACD_AGENTS_PER_SWITCH

Maximum Number of Automatic Call Distribution Agents Per Switch

Functional description

This is a pre-existing office parameter which specifies the maximum number of ACD agent positions that the operating company can assign on the switching unit.

The purpose of this parameter will not be changed by this activity.

The range of this parameter will be increased to have a maximum value of 30,000 agents. The ability to assign a new value to this parameter will be restricted. A new value can only be assigned by changing the limit of the feature SOC.

When the SOC usage limit is increased or decreased, the value stored in the office parameter will be automatically updated to reflect the new limit. See section 13.7 for SOC information.

Range information

Range Information

Minimum	Maximum	Default
0	30000	0

This activity increases the maximum value of the office parameter.

Memory requirements

No memory impact.

Parameter release history update

The maximum value is being increased from 9999 to 30000 for SN07.

Upgrade Impact

Dump and Restore

This feature requires no operating company intervention during dump/restore or any other phase of ONP.

Element Management Upgrade

Not applicable.

Data schema (DS)

New/modified tables, MIBs, or Database Schema

New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
ACDGRP	CHANGED	UNCHANGED
KSETLINE	CHANGED	UNCHANGED
KSETFEAT	CHANGED	UNCHANGED
IBNFEAT	CHANGED	UNCHANGED
ACDLOGIN	CHANGED	UNCHANGED
ACDENLOG	CHANGED	UNCHANGED

Table/MIB/Remote Database Schema information

Name: ACDGRP

ACD Group Info

Functional description

ACDGRP is an existing table. This table defines ACD groups. A new field is introduced by this activity to specify the size (number of digits) of the Login ID. The size is either 4 or 5 digits. Default value is 4 digits.

Usage sequence and implications (CM Only)

Current datafill order unchanged.

Size

The size of table ACDGRP is not impacted by this activity.

Fields

The following table lists fields for ACDGRP.

A new field IDSIZE is added to this table. All other fields of this table are unchanged.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
IDSIZE	New	None	4 or 5	Size of the Login ID in number of digits.

Datafill example

The following example shows sample datafill for table ACDGRP. In this example, group ACDTEST1 is using 5 digit login IDs while the other 2 groups are using 4 digit login IDs.

Example tuples from table ACDGRP

ACDNAME	CUSTGRP	ACDRNGTH	THROUTE	NSROUTE	PRIOPRO	DBG	MAXCQSIZ	MAXWAIT	ACDMIS	MSQS	DISTRING	OBSWTONE	FRCNGTSV	IDSIZE	OPTIONS
ACDGRP2	CGA	12	OFR3	1											
	OFR3	1	0	N	12	20									
					N	NONE			N						N
				N										4	
ACDTEST1	IBNTST	0	OFRT	41											\$
	OFRT	43	0	N	1	256									N
					N	NONE			N						
				N										5	
							(VARWRAP 100) (	ACDCPK N)\$							
ACD1CGA	CGA	12	OFR3	1											
	OFR3	1	0	N	12	20									
					N	NONE									N
				N										4	
															\$

Table release history update

Since BCS18.

Supplementary information

Dump and Restore impact. There will be upgrade impact to table ACDGRP due to the new field IDSIZE introduced by this activity. The reformat procedures will default the value of this field to 4 during ONP.

Translation verification other tools

ACDGRP does not use translation verification tools.

Name: KSETLINE

Key Set Line Information table

Functional description

KSETLINE is an existing table. This table defines INCALLS KEY to key number 1 on ACD set. This activity changes the field POSID, which is the ACD position ID associated with the INCALLS KEY. The POSID will be changed to a 5 digit number.

Usage sequence and implications (CM Only)

Current datafill order unchanged.

Size

The size of table KSETLINE is not impacted by this activity.

Fields

The following table lists fields for KSETLINE.

The existing field POSID is changed in this table. All other fields of this table are unchanged.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
POSID	Changed	None	5-digit number between 00001 and 30000.	ACD Position ID associated with the INCALLS key.

Datafill example

The following example shows sample datafill for table KSETLINE. Note the 5 digit POSIDs.

Example tuples from table KSETLINE

KSETKEY	FORMAT	DNRESULT
KSFMTID	KSFMTARE	

HOST 05 0 00 06 1	ACD Y 7502338	
	CGA 2 0 909	
INCALLS	CGAACD3 1 Y 00332	(3WC) (MSB) (ACDNR)\$
	MBS	
HOST 05 1 00 06 1	ACD Y 7502339	
	CGA 2 0 909	
INCALLS	CGAACD4 1 Y 00443	(MSB) (ACDNR)\$
	MBS	
SRCM 04 0 01 01 1	ACD Y 7502331	
	CGA 2 0 909	
INCALLS	CGAACD1 1 Y 00112	(PRK) (MSB) (ACDNR)\$
	MBS	

Table release history update

Since BCS10.

Supplementary information

Dump and Restore impact. There will be upgrade impact to table KSETLINE due to the change to the field POSID introduced by this activity. The reformat procedures will prefix a digit 0 to all ACD Position IDs upgraded during ONP.

Translation verification other tools

KSETLINE does use translation verification tools but are not impacted by this activity.

Name: KSETFEAT

Key Set Feature Information table

Functional description

KSETFEAT is an existing table. This table defines SUPR feature data when assigned to a keyset feature key. This activity changes the field POSID, which is the ACD position ID associated with the supervisor feature. The POSID will be changed to a 5 digit number.

Usage sequence and implications (CM Only)

Current datafill order unchanged.

Size

The size of table KSETFEAT is not impacted by this activity.

Fields

The following table lists fields for KSETFEAT.

The existing field POSID is changed in this table. All other fields of this table are unchanged.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
POSID	Changed	None	5-digit number between 00001 and 30000.	ACD Position ID associated with the SUPR key.

Datafill example

The following example shows sample datafill for table KSETFEAT. Note the 5 digit POSIDs.

Example tuples from table KSETFEAT

FEATKEY						FEATURE		KVAR			
HOST	00	0	19	02	1	SUPR	SUPR	ACDTEST2	1	Y	01111
HOST	00	1	08	01	1	SUPR	SUPR	ACDTEST2	1	Y	02222
HOST	01	0	00	14	1	SUPR	SUPR	CGAACD5	1	Y	05555
HOST	01	1	01	24	1	SUPR	SUPR	CGAACD2	1	Y	07777
HOST	05	1	00	06	1	SUPR	SUPR	CGAACD4	1	Y	04444

Table release history update

Since BCS10.

Supplementary information

Dump and Restore impact. There will be upgrade impact to table KSETFEAT due to the change to the field POSID introduced by this activity. The reformat procedures will prefix a digit 0 to all SUPR Position IDs upgraded during ONP.

Translation verification other tools

KSETFEAT does use translation verification tools but are not impacted by this activity.

Name: IBNFEAT

IBN Line Feature Information table

Functional description

IBNFEAT is an existing table. This table defines ACD and SUPR feature data when assigned to IBN sets. This activity changes the field POSID which is the ACD position ID associated with the ACD or SUPR options on the set. The POSID will be changed to a 5 digit number.

Usage sequence and implications (CM Only)

Current datafill order unchanged.

Size

The size of table IBNFEAT is not impacted by this activity.

Fields

The following table lists fields for IBNFEAT.

The existing field POSID is changed in this table. All other fields of this table are unchanged.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
POSID	Changed	None	5-digit number between 00001 and 30000.	ACD Position ID associated with the ACD or SUPR option.

Datafill example

The following example shows sample datafill for table IBNFEAT. Note the 5 digit POSIDs.

Example tuples from table IBNFEAT

	LEN	DNNO	DF	FEATURE				DATA
HOST	01	1 02 00						
		0	ACD	ACD	CGAACD2	1	Y	00020
		(ACDNR) \$						
HOST	05	1 01 05						
		0	ACD	ACD	ACDTEST1	1	Y	05115
HOST	05	1 01 05						
		0	SUPR	SUPR	ACDTEST1	1	Y	05225

Table release history update

Since BCS10.

Supplementary information

Dump and Restore impact. There will be upgrade impact to table IBNFEAT due to the change to the field POSID introduced by this activity. The reformat procedures will prefix a digit 0 to all ACD Position IDs upgraded during ONP.

Translation verification other tools

IBNFEAT does use translation verification tools but are not impacted by this activity.

Name: ACDLOGIN

ACD Login Table

Functional description

ACDLOGIN is an existing table. This table maps ACD Login IDs to a corresponding password, if needed. This table also maps Customer groups to the corresponding ACD Login ID, if requested. This table is indexed by Login ID.

Usage sequence and implications (CM Only)

Current datafill order unchanged.

Size

Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ACDLOGIN	0	30,000	Memory is allocated dynamically through the use of SEGSTOR in blocks of 512. Two words of protected store is needed per tuple.

Fields

The following table lists fields for ACDLOGIN.

A range of the LOGINID field is changed by this activity. Remaining fields of this table are not changed.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
LOGINID	Changed	None	5-digit number between 00001 and 30000	The range of ACD Login ID is expanded to accommodate 30,000 Login IDs.

Datafill example

The following example shows sample datafill for table ACDLOGIN. Note the 5 digit LOGINIDs.

Example tuples from table ACDLOGIN

```

LOGINID CUSTGRP PSWD OPTIONS
-----
00551 Y CGA N (VARWRAP 100) $
01001 N N $
01002 Y IBNTST Y 1234 $
01003 Y IBNTST Y 1234 (VARWRAP 60) (PAQ 1) $
02001 N N $
02002 Y COMKODAK Y 1234 $
02003 Y COMKODAK Y 1234 (VARWRAP 60) (PAQ 1) $
04120 Y CGA N (VARWRAP 100) $

```

Table release history update

Since BCS18.

Supplementary information

Dump and Restore impact. There will be upgrade impact to table ACDLOGIN due to change in field LOGINID made by this activity. The reformat procedures will prefix a digit 0 to all Login Ids upgraded during ONP.

Translation verification other tools

ACDLOGIN does not use translation verification tools.

Name: ACDENLOG

ACD Enhanced Login

Functional description

Table ACDENLOG is an existing table. It allows multiple customer groups the full range of Login IDs for their ACD agents. This table is indexed by a two-part key, made up of the Partition Number (PARTNO) and Login ID (LOGINID). The table format is same as table ACDLOGIN with one additional field, ACTIVATE.

Usage sequence and implications (CM Only)

Current datafill order unchanged.

Size

Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ACDENLOG	0	30,000	Memory is allocated dynamically through the use of SEGSTOR in blocks of 512. Two words of protected store is needed per tuple.

Fields

The following table lists fields for ACDENLOG.

The range of the LOGINID field is changed by this activity. Remaining fields of this table are not changed.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
LOGINID	Changed	None	5-digit number between 00001 and 30000	The range of ACD Login ID is expanded to accommodate 30,000 Login IDs.

Datafill example

The following example shows sample datafill for table ACDENLOG. Note the 5 digit LOGINIDs.

Example tuples from table ACDENLOG

PARTNO	LOGINID	ACTIVATE	CUSTGRP	PSWD	OPTIONS
121	00551	N Y	CGA N	(VARWRAP 100)	\$
121	01001	N N	N	\$	
124	00551	N Y	IBNTST Y	1234	\$
125	01003	N Y	IBNTST Y	1234 (VARWRAP 60)	(PAQ 1) \$
131	02001	N N	N	\$	
133	02002	N Y	COMKODAK Y	1234	\$
205	02002	N Y	COMKODAK Y	1234 (VARWRAP 60)	(PAQ 1) \$
212	04120	N Y	CGA N	(VARWRAP 100)	\$

Table release history update

Since BCS20.

Supplementary information

Dump and Restore impact. There will be upgrade impact to table ACDENLOG due to change in field LOGINID made by this activity. The reformat procedures will prefix a digit 0 to all Login Ids upgraded during ONP.

Translation verification other tools

ACDENLOG does not use translation verification tools.

Service Orders (SO)

This activity does not introduce any new Service Order commands, LCCs, or options.

Service order change details

When the ACD option is added to a line (ADO, NEW, NEWACD commands), or when ACD option data is changed (CHF command), one of the prompts offered by Servord is POSID. Currently, any value between 0001 and 9999 is accepted as valid input for the POSID. This activity will change the acceptable value of POSID to be a 5 digit value in the range of 00001 to 30000.

How service order commands are presented**Description**

The range of valid input for the POSID prompt has changed. Previously, the POSID was entered as a 4 digit value in the range of 0001 to 9999. It will now be entered as a 5 digit value in the range of 00001 to 30000.

Applicability

The POSID prompt is applicable to Servord commands ADO, NEW, NEWACD, and CHF only when they are used to manipulate the data associated with the ACD or SUPR line option.

Example

The following figures show an example of adding the ACD option to an existing business set using the ADO command. Note that when the system prompts for POSID, the user must now provide a 5 digit value in the range of 00001 to 30000. Previously, a 4 digit value would have been accepted.

Example of the ADO command in prompt mode

```

SO:
>ado
SONUMBER:      NOW    3 11  6 AM
>
DN_OR_LEN:
>6218000
OPTKEY:
>1
OPTION:
>acd
ACDGROUP:
>acdtest1
ACDSGRP:
>0
IDNUM:
>Y
POSID:
>00018
OPTKEY:
>$
COMMAND AS ENTERED:
ADO NOW 3 11 6 AM 6218000 ( 1 ACD ACDTEST1 0 Y 0009 ( ) ( ) ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>Y

```

Example of the ADO command in no-prompt mode

```

SO:
>ado $ 6218000 1 acd acdtest1 0 y 00018 $

```

The NEW, NEWACD, and CHF commands also offer the POSID prompt when used to manipulate ACD data. Examples of these commands are not provided because the effect of this change is identical to the ADO example shown above. POSID must now be input as a 5 digit value.

Command prompts

The valid input has changed for system prompt POSID.

Valid input for POSID

Prompt	Valid input	Description	Areas affected by prompt
POSID	00001 to 30000	ACD agent position ID.	Affects Servord commands ADO, NEW, NEWACD, and CHF when used to manipulate ACD option data.

Software optionality control (SOC)

This feature will be controlled by a standard usage based SOC. The usage limit will define the maximum number of ACD agents in the switch.

The default usage limit will be 0 ACD agents. During ONP from previous loads, the SOC usage limit will be set to match the value of office parameter

MAX_NUM_ACD_AGENTS_PER_SWITCH. Thus there will be no impact to existing customers who do not purchase this SOC.

The SOC usage limit will control the maximum number of ACD agents in the switch. The office parameter MAX_NUM_ACD_AGENTS_PER_SWITCH will automatically be updated to match the SOC usage limit anytime the SOC usage limit is changed (increased or decreased).

The other aspects of this feature including 5 digit login optionality, ability to use login IDs between 10000 and 30000, and mandatory use of 5 digit POSIDs are not controlled in anyway by the SOC.

SOC

SOC option name:	ACD00101
SOC option title:	ACD Agent Expansion
SOC option control type:	USAGE
New SOC option?	YES
SOC option order code	00037650
Option defined in DRU:	CCM
Affected products:	NA100, SL100

Element Management

Not applicable.

Command interface changes

Command: ACDDEBUG

Command type: NON-MENU

Command target: All

Command availability: RES

Command description

ACDDEBUG is a CI tool created to display ACD data structures in both dynamic and static environments.

The available commands are:

QUERY - Allows display of ACD data structures

CPIDTOAGT - Displays LEN and DN for entered line cpid or CLLI and member number for an entered trunk cpid.

QUIT - Quits from ACDDEBUG environment

Currently, the Query command uses a 4 digit positionID as an index in order to display ACD agent data. This activity will extend the command so that the data structures of an ACD agent with a 5 digit position will be displayed.

Command syntax for changed parameters

ACDDEBUG command parameters and variables

Command	Parameters and variables
QUERY AGENTDATA	ALL, GROUP, POSID
Parameters and variables	Description
ALL	Displays all agent data on the switch
GROUP	Displays agent data in a particular ACDGROUP
POSID	Displays agent data for a particular position ID. The positionID must be 5 digits.

Qualifications and warnings

NA

Responses

Wrong type

CI outputs with associated meanings and actions

ACDDEBUG
Wrong type: <ACD_posid?> {1 TO 30,000} Enter: <ACD_posid?> [<Form?>]
Meaning: The user has input an invalid position ID.
System or user actions: Input a valid position ID from 1 to 30,000

Example**Usage examples for ACDDEBUG Query command**

Description of task:	Display the ACD agent data
Command:	QUERY agentdata posid 12300
MAP response:	ACD GROUP NUMBER 5 ("ACDTEST1") - - ACD AGENT DATA Protected Data - Index 22 Address 59443834 Incalls Cp_id: HOST 01 0 06 04 DN 6136212200 KEY 1 Agent Position ID: 12300 SCAI agent: NO Unprotected Data - Index 22 Address 4EC906E0 ECM_ASSOCIATED: N ECM_USER_DATA_PTR: FFFF0000 ECM_IDX_IN_AGT_LIST: -515 ECM_NETNODEID: 4261281277 Agent Login ID: 11300 Agent Login Partition NO.: 0 Status: ACDIDLE Not Ready Active: N

Command: ACDSHOW**Command type: NON-MENU****Command target: All****Command availability: RES****Command description**

ACDSHOW is a CI tool that displays specific information concerning a current ACD configuration such as the a list of agent positions in a ACD group and agent information for a given user login ID. Currently, ACDSHOW commands use a 4 digit positionID as an index in order to display information

concerning an ACD configuration. This activity will extend the command so that the information of an ACD agent with a 5 digit position will be displayed.

The available commands are:

ACDSHOW		
ACDDNS	HELP	QUIT
ACDSHOW	LOADMGMT	STATUS
ADMINGROUP	LOGINID	SUPERVISOR
AGTPOS	MODE	TABENTRY
AUDIOGROUP	NSAUDGRP	THRESHOLD
COUNTS	NSROUTE	THROUTE
GROUPINFO	OVFLROUTE	VALIDAUDIO
GROUPNAME	PASSWORD	VALIDROUTES
FIAUDGRP	FOAUDGRP	CLRROUTE
RENQTOUT	RENQRTE	RENQAUD

Command syntax for changed parameters

ACDSHOW command parameters and variables

Command	Parameters and variables
AGTPOS	ALL, GROUP, POSID, LEN, DN, CLI,
LOGINID	ID
Parameters and variables	Description
ALL	Displays all agent data on the switch.
GROUP	Displays agent data in a particular ACDGROUP.
POSID	Displays agent data for a particular position ID. The positionID will be 5 digits.
LEN	Displays agent data for a particular LEN.
DN	Displays agent data for a particular DN.
CLI	Displays agent data for a particular CLI.
ID	Displays agent data for a particular login ID. The loginID will be 5 digits.

Qualifications and warnings

NA

Responses**Wrong type****CI outputs with associated meanings and actions**

ACDSHOW
Wrong type: <ACD_posid?> {1 TO 30,000} Enter: <ACD_posid?> [<Form?>]
Meaning: The user has input an invalid position ID.
System or user actions: Input a valid position ID from 1 to 30,000

Example**Usage examples for ACDSHOW AGTPOS command**

Description of task:	Show ACD information by ACD agent positionID
Command:	AGTPOS POSID 12300
MAP response:	Agent: HOST 01 0 06 04 DN 6136212200 KEY 1 Agent Login ID: 11300 Status: IDLE Loginid Partition: 0

Usage examples for ACDSHOW LOGINID command

Description of task:	Show ACD information by ACD agent loginID
Command:	LOGINID 11300 brief ibntst
MAP response:	Agent Position ID: 12300 Agent Login ID: 11300 Status: IDLE Loginid_Partition: 000

Usage examples for ACDSHOW LOGINID command

Command:	LOGINID 11300 full ibntst		
Map response:	Agent Position ID:	12300	
	Agent Login ID:	11300	
	Status:	IDLE	
	Loginid_Partition:	000	
	Agent:	HOST 01 0 06 04	DN 6136212200 KEY 1
	ACD Group:	ACDTEST1	
	ACD Subgroup:	0	
	SCAI Agent:	NO	

Security

Not applicable

Configuration Walkthrough

Not applicable

Product = CS2000**A00004414 -- SIP Call Server SOC (PT-IP)*****Functional Description***

This activity implements a mechanism to control the maximum number of SIPT calls that utilize the Next Generation Session Server (NGSS) platform when the far end is another CS2K. A usage SOC, CS2B0008, is implemented to limit these types of calls (abbreviated as CS2CS in this document).

Another activity, A00004271 SIP App Server SOC, implements a similar mechanism to control the maximum number of SIPT calls that utilize the NGSS platform when the far end is non-CS2K, referred to here as an Application Server. SOC option CS2B0009 is the usage SOC for A00004271.

Both SOC features are part of a set of activities for delivering the Session Server - SIP Gateway application in SN07. The other features are:

- A00003270 SIP Open Interop Call Processing

- A00003271 Session Server Web Server Interface
- A00003272 Session Server Provisioning Framework
- A00003273 SIP Gateway Application Maintenance
- A00003277 Session Server OM Subsystem
- A00003279 SIP on Session Server Link Maintenance and Load Balancing
- A00003280 SIP on Session Server Tracing/Debug Framework
- A00003281 SIP on Session Server Call Audit
- A00003282 SIP on Session Server Datasync
- A00003933 SIP on Session Server Drop 1 ICAF
- A00003934 Session Server Project ICAF

SOC limiting

The usage-controlled CS2B0008 SOC added by this activity applies to calls that meet the following criteria:

- the incoming or outgoing trunk group has the DYNAMIC option with SIPT SIGNALING in table TRKOPTS,
- a match of the incoming or outgoing trunk group is found in the SIPTTRK field of one of the tuples in table SIPLINK³,
- the CONNTYPE field of the tuple in table SIPLINK is set to CS2CS.

A counter keeps track of the current number of calls matching the above criteria. For each new CS2AS call, the current value in the counter is checked against the limiting value in the CS2AS SOC. If the addition of a new call of this type would exceed the SOC limit, the call is sent to treatment; otherwise, the counter is incremented and the call is allowed to proceed. When the call is ended, the counter is decremented.

In the following example of table SIPLINK, incoming and outgoing SIPT calls on trunk group NGSSLOOP will increment the usage counter for the CS2AS SOC.

TABLE: SIPLINK

LINKNAME	CONNTYPE	AGNTDATA
NGSSOUTLK	CS2AS ISUPTRK	NGSSOUT
NGSSINLINK	CS2AS ISUPTRK	NGSSINC
LOOPAROUND1	CS2CS ISUPTRK	NGSSLOOP

Here is an example of the output of the SOC SELECT command for the new SOC:

3. Table SIPLINK is a new table introduced in feature A00003279

```
>select option CS2B0008
GROUP:CS2B
OPTION      NAME                RTU  STATE  USAGE  LIMIT  UNITS  LAST_CHG
-----
CS2B0008   CS to CS Calls      Y   -    127   500    1VC   04/01/19
```

Hardware Requirements or Dependencies

None

Software Requirements or Dependencies

None

Limitations and restrictions

None

Interactions

The usage SOC introduced by this feature does not take the place of Base DPT usage SOC CS2B0005. The latter is still needed to set the value of office parameter DPT_MAX_PORTS in table OFCVAR. DPT_MAX_PORTS limits the overall number of simultaneous DPT calls.

Calls that peg the new CS2B0008 count will always peg the CS2B0005 count as well.

If the SOC limit set for CS2B0008 exceeds the limit of the Base DPT SOC CS2B0005, the latter is the limiting factor in determining the maximum number of simultaneous CS2AS calls.

Feature A00004271 SIP App Server SOC introduces new OM group NGSSOM for tracking the effects of the CS2B0008 SOC limit setting on CS2CS calls.

Feature A00004271 SIP App Server SOC adds a new NGSS700 log that is generated when a CS2CS call is rejected because it would exceed the LIMIT setting of the CS2B0008 SOC.

Applicable customer facing sections

Fault Management

Logs

Alarms

Configuration

Data Schema

User Interface

Element Management	_____
Security	_____
Service Order	_____
SOC	___X___
Office Parameters	_____
Accounting (includes AMA billing)	_____
Performance (includes operational measurements)	_____
Indicate with an X if you are completing the sections of the DDOC listed below. Indicate with “N/A” if these sections do not apply to this functionality.	
Realtime	_____
Engineering Information	_____

Glossary

Term	Description
New term	Definition

Configuration for A00004414

Hardware and Software Requirements

N/A

Initial Configuration

N/A

Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

New/modified office/subnet parameters

New or modified parameter

Parm table	Parameter name	NEW/CHANGE D/DELETED/RE LOCATED	Domain (CM or Subnet Management

Parameter information

<abbreviated parameter name>

<long parameter name>

Functional description

Provisioning rules

Range information

Range Information

Minimum	Maximum	Default

Activation

Dependencies

Consequences

Verification

Memory requirements

No memory impact.

Units per memory block = <10>

Words per memory block = <510>

If the parameter value = <25>

words required = (((parameter value - 1)/units per block) + 1) *words per block = <>

Parameter release history update

Upgrade Impact

N/A

Dump and Restore

Element Management Upgrade

Data schema (DS) (CM, MIBS, RDB)

N/A

New/modified tables, MIBs, or Database Schema

New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)

Table/MIB/Remote Database Schema information

Name: <abbreviated name of table, MIB, or Database if applicable>

<long name of table>

Functional description

Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

<abbreviated names of tables before the current table if applicable>

<abbreviated name of the current table>

<abbreviated names of tables after the current table if applicable>

OR

There is no requirement to datafill tables in a specific order.

OR

Current datafill order unchanged.

Size

Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
DDPACDEV	0	8 000 000	Memory is automatically allocated for 16 DPC devices.

Fields/OIDs

The following table lists fields/OIDs for <abbreviated name of table/MIB>.

<conditional information>

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action

Datafill example

The following example shows sample datafill for table <abbreviated name of table>.

Table release history update

Supplementary information

Translation verification other tools

The following example shows the output from <ToolName> when it is used to verify <abbreviated name of table>.

<abbreviated name of table> does not use translation verification tools.

Service Orders (SO) (CM & SESM)

N/A

Service order change details

LCC and options

Meridian digital centrex feature assignment requirements

Feature	500 2500	MDC SET	ISDN SET	MDC Set ISDN Set Relationship							
				S E T	S U B S E T	K E Y	D N	D E D K E Y	L A M P	C O D E	D I S P L A Y
AABSAUTOMATIC ANSWERBACK	N	Y		X				X	X		
AUTODISP** AUTOMATIC DISPLAY	N	Y			X						X

The feature in the table above requires a handsfree Business Set. This feature must be assigned to key 1.

New commands

How service order commands are presented

Description

Applicability

Example

Example of the <abbreviated command name> command in prompt mode

Example of the <abbreviated command name> command in no-prompt mode

Command prompts

The system prompts for <abbreviated command name> are shown in order of their appearance.

System prompts for <abbreviated command name>

Prompt	Valid input	Description	Areas affected by prompt

How service order options are presented

Description

Example

Example of the <abbreviated option name> option in prompt mode

Example of the <abbreviated option name> option in no-prompt mode

Example of the <abbreviated option name> option in no-prompt mode for SERVORD+

Option prompts

System prompts for <abbreviated option name> option

Prompt	Valid input	Description	Areas affected by prompt

Line class code compatibility

<abbreviated option name> compatibility to LCC

Line class code	Compatible?
1FR-1MR	Yes/No

Assignability

The following functionalities apply to this option:

- set functionality: <yes or no>
- subset functionality: <yes or no>
- DN functionality: <yes or no>
- key functionality: <yes or no>

Option prerequisites

<abbreviated option name> has the following prerequisites:

Notes

The following notes apply to <abbreviated option name>:

Feature identification

Functionality: <functional group>

Feature number: <feature number>

SERVORD+ Exceptions

Software optionality control (SOC)

SOC

SOC option name:	CS to CS calls
SOC option title:	Yes/No
SOC option control type:	usage
New SOC option?	Yes
SOC option order code	CS2B0008
Option defined in DRU:	MSH
Affected products:	SN07

Element Management

N/A

New/modified GUIs

New or modified GUIs

GUI name	NEW, CHANGED, or DELETED

GUI information

GUI name: <abbreviated name of GUI>

<long name of GUI>

Functional description

GUI usage and implications

GUIs must be used in the following sequence:

<abbreviated names of GUI before the current GUI if applicable>

<abbreviated name of the current GUI>

<abbreviated names of GUIs after the current GUI if applicable>

OR

There is no requirement to datafill GUIs in a specific order.

OR

Current datafill order unchanged.

GUI size

New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory

GUI fields

The following table lists fields for GUI or pull down menu <abbreviated name of GUI>.

<conditional information>

GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry

Usage example

The following example shows sample datafill or menu selection for GUI <abbreviated name of GUI>:

GUI release history update

Supplementary information

CLUI Interface

Command interface changes

N/A

Directory: <directory name/MAP level>

Directory description

Accessing directory: <directory name>

Access to directory or MAP level and return to CI

Command: <command name>

Command type: <NON-MENU, Listed MENU, Unlisted MENU>

Command target: <NT40, SUPERNODE, BRISC, All, Other>

Command availability: <RES, NONRES or OTHER>

Command description

Command syntax

<CommandName> command parameters and variables

Command	Parameters and variables
<command name> for example, CNTRS	<Plane Number> (0,1) <Display what> Card (0 to 10) All Proc
Parameters and variables	Description
Card	Displays ECC error counts for the specified card only
All	Displays ECC error counts for all the cards on the specified plane. This includes the processor ECC error counts.
Proc	Displays ECC error counts for only the processor memory

Qualifications and warnings

Responses

<response>

MAP outputs with associated meanings and actions

Command
<RESPONSE>: <description> Meaning: System or user actions: Example: WARNING: The CPUs are out of sync due to a problem with mismatches. The mismatch logs and minfo should be analysed before a manual resyncing is performed. Do you wish to continue? Please confirm ("Yes", "Y", "No", "N"). Meaning: <description> for example "This response warns users that the CPUs are out of sync due to a mismatch and that the cause of the mismatch should be determined before resyncing." System or user actions: <description> for example "You should analyze the mismatch logs and minfo to determine the type of faults in the system and deal with those problems before resyncing."
<RESPONSE>: <description> Meaning: System or user actions:

Example

Usage examples for <CommandName> command

Description of task:	
Description of task	Synchronize the two CPUs of the CM without matching memory after synchronization and without displaying any warnings regarding possible side effects beforehand.
Command: MAP response:	Example: SYNC Nomatch Noprompt Example: SYNCHRONIZATION SUCCESSFUL

Security

N/A

Network configuration

Key management

Protocol

Authentication

Configuration Walkthrough

N/A

Product = CS 2000

A00004422--Enhanced 911 Dynamic Packet Trunks Session Initiation Protocol-Telephony Call Trace (Succession on DMS)

Functional Description

Description

This feature provides the ability to trace established intra and inter office calls involving SIP-T DPT for Call Server 2000 (CS2K). Before the development of this feature, CS2K-Core had the ability to trace intra office line to line and inter office line to trunk/line and trunk to trunk/line calls for emergency situations (police, fire, hospital etc.) for only TDM trunks.

This feature enhances the trace abilities of CS2K to identify which SIP-T DPT (originating and/or terminating) is associated with an active call within the call server by means of SIP-T DPT callid.

This feature works for all calls and not just E911 calls.

The trunk information is provided through a new man-machine command interpreter (CI) command "SIPTRACE"⁴. The syntax and permissible input and output parameters of SIPTRACE are described in the following sections.

The input trunk information consists of:-

- trunk group and trunk member for TDM trunks.
- SIP-T DPT call-id for SIP-T DPT.

This command tool utility is limited to SIP-T DPT and TDM trunks as input to this command, while the output can be SIP-T DPT, TDM trunks or lines.

4. Henceforth, in this document, all references to new CI command utility would refer to new CI command "SIPTRACE".

The new CI command “SIPTRACE” has the following syntax:-

```
SIPTRACE <Input trunk> {  
    {T    <TDM trunk group> STRING  
        <TDM trunk member> {0 TO 9999}},  
    {D    <DPT SIP-T call-id> STRING}}
```

Output on the CI prompt for the above command is of the following format:-

<input> is currently connected to <output>

where

<input> is either

- “TDM trunk <trkgrp> <trkmem>” if a TDM trunk was entered or
- “SIP-T DPT <trkgrp> callid <SIP-T callid>” if a SIP-T callid was entered. The SIP-T callid entered on the command prompt during SIPTRACE command execution, is enclosed in single quotes.

<output> is one of the following:

- “TDM trunk <trkgrp> <trkmem>” if the connected party is a TDM trunk member
- “SIP-T DPT <trkgrp> callid <SIP-T callid>” if the connected party is a SIP-T DPT.
- “LINE <lineid>” DN is displayed, if the connected party is a line terminal.

For call scenarios in which the output TDM agent is found to be a C7ISL member, the tool automatically traverses the ISL and presents the final agent of the call. In such cases, multiple output lines are displayed on the CI.

Call scenarios involving SIP-T loop-arounds where SIP-T DPT looped around on the same or different GWC(s), are also supported by the new CI command SIPTRACE. In such cases, the output SIP-T call-id retrieved from the GWC is used to recursively trace the final output agent of the call and multi-line outputs are displayed on the CI.

The new CI command utility is at the top level of CI and the user is able to invoke this new command, at any level built over CI (e.g. MAPCI, LOGUTIL etc.)

The following are the error/information messages to be displayed on the CI.

Error/Information messages displayed on the CI

Sr. No.	Error/Information messages displayed on the CI	Cause of the error/information message
1	<Input trunk> ^a is currently connected to a line whose DN is not available	The output end-point is found to be a line but its Tid is not mapped to a DN datafilled in tables on the Core
2	TDM trunk group not datafilled in table CLLI	Invalid TDM trunk group entered
3	TDM trunk group not datafilled in table TRKGRP	TDM Trunk group not datafilled in table TRKGRP
4	TDM trunk group not datafilled in table TRKSGRP	TDM Trunk group not datafilled in table TRKSGRP
5	SIP-T DPT <SIP-T DPT trkgrp> callid <SIP-T call-id> not associated with any active call	SIP-T callid does not exist within the GWC(s) and when the SIP-T DPT trunk group is available.
6	<Input trunk> is currently connected to an unsupported agent type <CP selector>	Output agent is not supported by this feature
7	TDM trunk <trkgrp> <trkmem> not associated with any active call	The input TDM trunk member information entered at the CI does not map to a live call
8	SIP-T DPT callid <SIP-T call-id> not associated with any active call	CS2K-Core is unable to send broadcast message to GWC(s) to retrieve associated DPT Tid(s) or when the GWC response messages have arrived in the Core but unable to determine the output agent details and the SIP-T DPT trunk group is not available.
9	Unable to identify far-end C7ISL member for TDM trunk (C7ISL) <trkgrp> <trkmem>	The output agent is found to be a TDM C7ISL agent but the far end TDM C7ISL trunk group and trunk member details datafilled in table C7ISL are not available.
10	Trunk group datafilled as DPT in Table DPTRKMEM	DPT trunk group entered using option T while SIPTRACE command execution
11	Number of SIP-T DPT loop-arounds exceeded allowed limit	For call scenarios in which the number of SIP-T to SIP-T loop-arounds in the same call server has exceeded 9 (highly unlikely)

a. <Input trunk> refers to: {T <Input TDM trunk group> <Input TDM trunk member>, D <SIP-T DPT trkgrp> callid <SIP-T call-id>}

The snapshots of various combinations of call scenarios involving TDM and SIP-T DPT trunks is shown in the following examples; the SIPTRACE command execution is shown on the CI prompt for simplicity purpose but same can be executed on any level built over CI (e.g. MAPCI, LOGUTIL, etc.):-

1. TDM to line inter-working in CS2K

```
CI> SIPTRACE T ETSIV1LPA 2  
  
TDM trunk ETSIV1LPA 2 is currently connected to LINE 1158206005
```

2. SIP-T DPT to line inter-working in CS2K

```
CI> SIPTRACE D '0026.4030-10-16-49-02.67@CS2K4_84'  
  
SIP-T DPT K4SIP1LOOPFR3 callid 0026.4030-10-16-49-02.67@CS2K4_84  
is currently connected to LINE 1158206007
```

3. TDM to TDM inter-working in CS2K

```
CI> SIPTRACE T ETSIV1LPB 2  
  
TDM trunk ETSIV1LPB 2 is currently connected to TDM trunk  
UKISUPLPA 10
```

4. TDM to SIP-T DPT inter-working in CS2K

```
CI> SIPTRACE T ETSIV1LPB 2  
  
TDM trunk ETSIV1LPB 2 is currently connected to SIP-T DPT  
K4SIP1LOOPFR3 callid 0026.4030-10-16-49-02.67@CS2K4_84
```

5. SIP-T DPT to TDM inter-working in CS2K

```
CI> SIPTRACE D '0026.4030-10-16-49-02.67@CS2K4_84'  
  
SIP-T DPT K1SIP1V1 callid 0026.4030-10-16-49-02.67@CS2K4_84 is  
currently connected to TDM trunk ETSIV1LPA 2
```

6. SIP-T DPT to SIP-T DPT inter-working in CS2K

```
CI> SIPTRACE D '0026.4030-10-16-49-02.67@CS2K4_84'  
  
SIP-T DPT K1SIP1V1 callid 0026.4030-10-16-49-02.67@CS2K4_84 is  
currently connected to SIP-T DPT K4SIP1LOOPFR3 callid 0026.4030-  
10-16-49-02.95@CS2K4_84
```

7. Output TDM identified as C7ISL member

```
CI> SIPTRACE T ETSIV1LPB 2  
  
TDM trunk ETSIV1LPB 2 is currently connected to TDM trunk (C7ISL)  
ETSIV1LPA 3  
TDM trunk (C7ISL) UKISUPLPA 4 is currently connected to LINE  
1158206005
```

8. Input TDM identified as C7ISL member

```
CI> SIPTRACE T ETSIV1LPB 2  
  
TDM trunk (C7ISL) ETSIV1LPB 2 is currently connected to TDM trunk  
UKISUPLPA 8
```

9. SIP-T DPT loop-arounds (Case-1) - Posting the SIP-T call-id that is not a part of the SIP-T loop-around

```
CI> SIPTRACE D '0026.4030-10-16-49-02.67@CS2K4_84'  
  
SIP-T DPT K1SIP1UK3 callid 0026.4030-10-16-49-02.67@CS2K4_84 is  
currently connected to SIP-T DPT K1SIP1V1 callid 0026.4030-10-16-  
49-02.95@CS2K4_84  
SIP-T DPT K2SIP1CZ1 callid 0026.4030-10-16-49-02.95@CS2K4_84 is  
currently connected to LINE 1158206005
```

10. SIP-T DPT loop-arounds (Case-2) - Posting the SIP-T call-id which is a part of the SIP-T loop-around

```
CI> SIPTRACE D '0026.4030-10-16-49-02.67@CS2K4_84'

SIP-T DPT K1SIP1UK3 callid 0026.4030-10-16-49-02.67@CS2K4_84 is
currently connected to SIP-T DPT K1SIP1V1 callid 0026.4030-10-16-
49-02.95@CS2K4_84
SIP-T DPT K2SIP1CZ1 callid 0026.4030-10-16-49-02.67@CS2K4_84 is
currently connected to LINE 1158206005
```

11. Invalid input option

```
CI> SIPTRACE abcd

Next par is: <Input trunk> {T <TDM trunk group> <TDM trunk
member>,
D <DPT SIP-T call-id>}

Enter: <Input trunk>
CI>
```

12. No option entered with new CI command

```
CI> SIPTRACE

Next par is: <Input trunk> {T <TDM trunk group> <TDM trunk
member>,
D <DPT SIP-T call-id>}

Enter: <Input trunk>
CI>
```

13. Incomplete input entered with option T

```
CI> SIPTRACE T ETSIV1LPA  
  
Next par is: <TDM trunk member> {0 TO 9999}  
  
Enter: <TDM trunk member>  
CI>
```

14. Incomplete input entered with option D

```
CI> SIPTRACE D  
  
Next par is: <DPT SIP-T call-id> {STRING}  
  
Enter: <DPT SIP-T call-id>  
CI>
```

15. Invalid input TDM trunk group name

```
CI> SIPTRACE T ABCD 2  
  
TDM trunk group not datafilled in Table CLLI
```

16. TDM trunk group not datafilled in table TRKGRP

```
CI> SIPTRACE T UASBLDNANN 2  
  
TDM trunk group not datafilled in Table TRKGRP
```

17. TDM trunk group not datafilled in table TRKSGRP

```
CI> SIPTRACE T ETSIV2LPB 2  
TDM trunk group not datafilled in Table TRKSGRP
```

18. Invalid input TDM trunk member number

```
CI> SIPTRACE T ETSIV1LPA -2  
Out of range: <TDM trunk member> {0 TO 9999}  
Enter: <TDM trunk member>  
CI>
```

19. SIP callid does not exist / does not map to any live call.

```
CI> SIPTRACE D '0026.4030-10-16-49-02.67@CS2K4_84'  
SIP-T DPT K2SIP1CZ1 callid 0026.4030-10-16-49-02.67@CS2K4_84 not  
associated with any active call
```

20. Input TDM parameters do not map to any live call.

```
CI> SIPTRACE T ETSIV1LPA 2  
TDM trunk ETSIV1LPA 2 not associated with any active call
```

21. Output agent is not supported for TDM input

```
CI> SIPTRACE T ETSIV1LPA 2
```

```
TDM trunk ETSIV1LPA 2 is currently connected to an un-supported  
agent type 10
```

22. Output agent is not supported for SIP-T DPT inputs

```
CI> SIPTRACE D '0026.4030-10-16-49-02.67@CS2K4_84'
```

```
SIP-T DPT K2SIP1CZ1 callid 0026.4030-10-16-49-02.67@CS2K4_84 is  
currently connected to an un-supported agent type 12
```

23. Output line DN not identifiable for TDM inputs

```
CI> SIPTRACE T ETSIV1LPA 2
```

```
TDM trunk ETSIV1LPA 2 is currently connected to a line whose DN  
is not available
```

24. Output line DN not identifiable for SIP-T DPT inputs

```
CI> SIPTRACE D '0026.4030-10-16-49-02.67@CS2K4_84'
```

```
SIP-T DPT K2SIP1CZ1 callid 0026.4030-10-16-49-02.67@CS2K4_84 is  
currently connected to a line whose DN is not available
```

25. Output agent is TDM C7ISL but unable to find far-end C7ISL agent

```
CI> SIPTRACE T ETSILPB 2

TDM trunk ETSILPB 2 is currently connected to TDM trunk (C7ISL)
UKISUPLPA 3
Unable to identify far-end C7ISL member for TDM trunk (C7ISL)
UKISUPLPA 3
```

26. Input DPT trunk group entered with option T

```
CI> SIPTRACE T K2SIP1CZ1 2

Trunk group datafilled as DPT in Table DPTRKMEM
```

27. Unable to send GWC request message or unable to determine output agent for SIP-T DPT input

```
CI> SIPTRACE D '0026.4030-10-16-49-02.67@CS2K4_84'

SIP-T DPT callid 0026.4030-10-16-49-02.67@CS2K4_84 not
associated with any active call
```

Hardware Requirements or Dependencies

None.

Software Requirements or Dependencies

Software load from SN07 onwards.

Limitations and restrictions

- The new command interpreter (CI) command “SIPTRACE” is supported only for SIP-T DPT. It is not supported for networks using BICC protocol.
- TDM trunks and SIP-T DPT are the only input parameters allowed. Line is not allowed as input parameter.
- TDM trunks, SIP-T DPT and Line DNs are the only output parameters.

- If a line directly maps to a DN, the DN is displayed as <lineid> with area-code, office-code and station-number as datafilled in table DNINV.
- Lines, discovered as output agents, not mapped to DNs are not supported by the new CI command SIPTRACE.
- Feature interactions like 3WC or any other multi-linked calls with the new CI command SIPTRACE, are not supported by the new CI command SIPTRACE.

Interactions

Features supported by the new CI command SIPTRACE include, but not limited to, 3WC, CFB, CFU, CFDA, SDN, MLH.

Applicable customer facing sections

Fault Management

Logs __N/A__

Alarms __N/A__

Configuration

Data Schema __N/A__

User Interface __X__

Element Management __N/A__

Security __N/A__

Service Order __N/A__

Office Parameters __N/A__

Accounting (includes AMA billing) __N/A__

Performance (includes operational measurements) __N/A__

Glossary

Term	Description
3WC	Three way conference
BICC	Bearer Independent Call Control
CI	Command Interpreter
C7ISL	CCS7 ISUP Signalling Loop-back
CFB	Call Forward Busy

Term	Description
CFD/CFDA	Call Forward Don't Answer
CFU	Call Forward Universal
CS2K	Communication Server 2000
DMS	Digital Multiplex System
DN	Directory Number
DPT	Dynamic Packet Trunking
E911	Enhanced 911 services
ISUP	ISDN User Part
ISDN	Integrated Services Digital Network
GWC	GateWay Controller
MLH	Multi Line Hunt-group
SIP-T	Session Initiation Protocol-Telephony
SDN	Secondary Directory Number
TDM	Time Division Multiplexing
VRDN	Virtual Routing Distribution Node

Product = CS 2000

A00004554--SDM FX System Backup Enhancements (Succession on DMS)

This feature implements scheduling of the system image backup to both SDM tape drives and the capability to configure the "Backup Required Alarm."

The following are the purposes of this activity.

- Automate the backup process and allow the user to schedule the backups for each drive (Dat 0 and Dat 1).
- Allow the user to Configure "Backup required "alarm, so that he can Enable/Disable the backup required alarm.

Scheduling Interface

This is the interface the user employs to add new schedules and disable or modify existing schedules. The options provided by this interface are

- Schedule Dat 0
- Schedule Dat 1

These two options allow the user to add new schedules and disable or modify an existing schedule.

- List Schedules

The List Schedule option will show all the schedule details for each drive.

Other Features

The other features are:

- In case of a failure it will raise a “Backup Failure” alarm.
- It won’t start the system image backup if a “Backup Failure” alarm exists.
- Necessary customer logs will be generated during the execution of the scheduled backup.
- It will support the existing way of taking the backup also.

Alarm Configure Interface

This is an interface for setting the “Backup Required” alarm status. The options provided by this interface are:

- Disable the “Backup Required” alarm
- Enable the “Backup Required” alarm
- List the Current status of “Backup Required” alarm

Note: The existing backup “InProgress” alarm will be there even if the “Backup Required” alarm status is Disabled.

Screen Captures for the Main Menus

Main Menu

```
***      *****
***      SuperNode Data Manager
***
***      System Image Backup and Restore Menu
***      *****
***
```

```
***
*** 0. Exit
***
*** 1. Help
***
*** 2. Backup & Restore System image
***
*** 3. Alarm Configure
***
***
***
***
*** Please enter your selection (0 to 3) ? ==>
```

Backup and Restore Menu

```
*** *****
*** SuperNode Data Manager
***
*** System Image Backup and Restore Menu
*** *****
***
***
*** 0. Exit
***
*** 1. Previous Menu
***
*** 2. Create a System Image on Tape (S-tape)
***
*** 3. List Contents of the System Image Tape (S-tape)
***
*** 4. Restore Files from the System Image Tape (S-tape)
***
*** 5. Schedule Backup
***
```

*** Please enter your selection (0 to 5) ? ==>

Scheduled Backup Menu

```
***
***      *****
***
***      SuperNode Data Manager
***
***
***      Schedule Backup Configure Menu
***      *****
***
***
***
***      0. Exit
***
***      1. Previous Menu
***
***      2. Schedule Dat 0
***
***      3. Schedule Dat 1
***
***      4. List Backup Schedules
***
***
***      Please enter your selection (0 to 4) ? ==>
```

Product = CS 2000

A00004713--1+1 Speedometer Support (Succession on DMS)

Functional Description (FN)

This feature updates the Speedometer to support 1+1 configuration in release CSP20. It provides capacity prediction for 1+1 configuration within the accuracy target of +/-10% when the utilization is above 15%. It allows the users to change the value of Rated Power to 1 through table OFCENG.

Hardware Requirements or Dependencies

N/A

Software Requirements or Dependencies

N/A

Limitations and restrictions

None

Interactions

In the releases without this feature, the smallest value of Rated Power allowed is 2. In this feature, the users are able to modify the value of Rated Power to the smallest of 1.

Applicable customer facing sections

Fault Management

Logs N/A

Alarms N/A

Configuration

Data Schema N/A

User Interface N/A

Element Management N/A

Security N/A

Service Order N/A

Office Parameters X

Accounting (includes AMA billing) N/A

Performance (includes operational measurements) N/A

Configuration for A00004713**Hardware and Software Requirements**

N/A

Initial Configuration

N/A

Office parameters (OP) (CM & SESM)

Modified office parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management)
OFCENG	RATED_POWER	CHANGED	CM

Parameter information

Rated_Power

Functional description

This parameter defines the number of PEs engineered in the switch. The Speedometer uses the value of this parameter to calculate capacity prediction.

Provisioning rules

N/A

Range information

Minimum	Maximum	Default
1	7	3

Activation

N/A

Dependencies

N/A

Consequences

N/A

Verification

The users can verify and/or update the value of Rated_Power via table (OFCENG) control.

Memory requirements

No memory impact.

Parameter release history update

N/A

Upgrade Impact

N/A

Data schema (DS) (CM, MIBS, RDB)

N/A

Service Orders (SO) (CM & SESM)

N/A

Software optionality control (SOC)

N/A

Element Management

N/A

Command interface changes

N/A

Security

N/A

Configuration Walkthrough

N/A

Product = CS 2000**A00004868--FTP Proxy for SDM and CBM (Succession on DMS)*****Design Description excerpts*****Purpose**

The purpose of this feature is to provide passthrough (file transfer) to the CM from the ftp client (downstream machine) via SDM/CBM in a Non-DCE environment.

FTPProxy will be used by an external ftp client for transferring files between client and CORE, client and SDM/CBM (In case of CORE it will be without the files ever residing on the SDM/CBM). Certain amount of security will be provided by giving the passthrough (file transfer) facility to the ftp users based on their unix groups. FTP Proxy will provide all of the facility provided by the current File transfer Service(SDM_BASE.fts) implementation on SDM19.

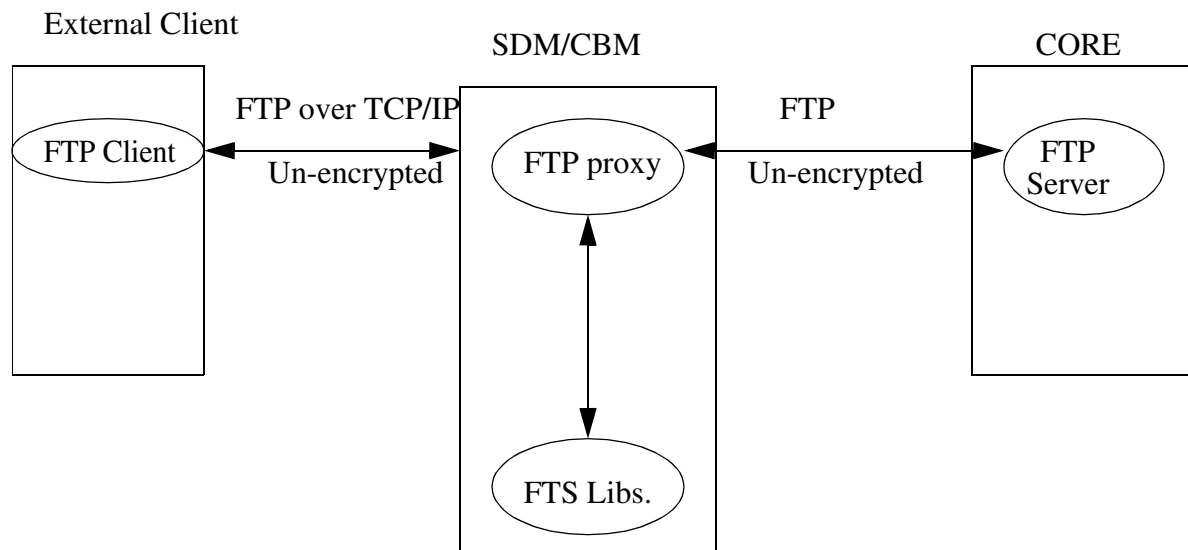
On SDM, SFT application provides the passthrough capability to the ftp users. So, the FTPProxy and SFT application will be mutually exclusive, at one point only either of them can reside on SDM. Whereas on CBM, SFT is not

available, so the FTPProxy can reside independent of other CBM applications, but it will be mutually exclusive with SSPFS's ProFTPD service.

FTPProxy feature will be provided to the customer as an optional application on SDM and CBM. It will also include the functionalities such as creating ftp users dynamically and deleting them after the file transfer is over, and parallel sessions will also be supported.

Refer to the following figure for FTP functionality.

FTP Functionality



Logs

New customer logs will be generated to provide information regarding the file transfers between FTP Client and CORE, and who ftp-users are logged on to CORE.

Log format for file transfers

```
Feb 16 02:24:52 sspfs_server ftpd[20103]: SDM739 NONE  
INFO FTS ftp-user request for file PML successful
```


Log format for login information

```
Feb 16 02:24:40 sspfs_server ftpd[20103]: SDM739 NONE  
INFO FTS ftp-user hari logged on to CORE  
successfully.
```

Glossary

Term	Description
AIX	IBM UNIX operating system on the SDM FX
CBM	Core and Billing Manager
CM	Command Module (the CPU of the DMS)
CMFT	Command Module File Transfer Script
Core	DMS switch computing engine
DCE	Distributed Computer Environment
FTP	File transfer protocol
FTS	File transfer System (Nortel proprietary code)
IP	Internet Protocol
SCFT	SSH Core File Transfer
SDM	SuperNode Data Manager
SSH	Secure Shell protocol
SSHD	Secure Shell protocol Daemon

Product = CS2000**A00004872 -- MIDCALL Tones /Services for CS2K (UA-IP, IAW)*****Functional Description***

This SN07 activity provides support for the following services in both the North American and International markets:

- Automatic Call Distribution Observe (ACD OBS): allows an ACD supervisor to monitor the quality of service offered to callers. As an option, an observe warning tone may be provided to the agent prior to the observation. The tone is heard when the observation is invoked and at the start of each new call while an observation is in effect. This tone is heard

by the ACD agent and not the caller.

There are various types of observe:

- a. Basic - Basic observe allows the supervisor to monitor an agent within its group that is involved in an active call. To activate OBS, a supervisor presses the OBS key and enters the INCALLS DN of the agent to be monitored. The supervisor is provided with a one way listen path into a call between an ACD agent and caller. A two way speech path can be achieved by pressing the CAG key.
- b. Extended - Extended Observe enhances the observe functionality to allow a supervisor to observe any agent that has an INCALLS key in any ACD group within the same customer group.
- c. Enhanced - When the ACD observe agent enhanced feature is in effect, the supervisor can observe the INCALLS key and a datafilled SDN using the AGENT key. Once the supervisor enters the observe mode, pressing the AGENT key after dial tone is received allows the supervisor to switch back and forth between observing the INCALLS key and the SDN as the agent switches between talking on the two keys.
- d. Flexible Call Observing (FOBS) - FOBS enhances the current ACD feature by providing an ACD OBS means for ACD supervisors to begin monitoring service given to a call before an agent has answered the call. The basic OBS feature imposes the restriction that a call must be in the talking state in order for OBS to be used. FOBS allows observation of a call to begin from the time it is first queued in the ACD system. This gives the supervisor an opportunity to gain knowledge of the overall handling of the incoming call. The supervisor continues to monitor the call if it is rerouted under enhanced overflow or NACD, if it is presented to an agent, and if the agent answers the call. Activation of FOBS instigates the monitoring of the next call to the ACD group, ACD subgroup or ACDDN. Monitoring ceases when the caller disconnects, or if the call is routed outside the ACD environment

NOTE: ASL functionality cannot be supported at this time. Although the provisioning of this functionality is not restricted, the behavior is not supported in solutions using an audio server. Solutions using an MTM to provide this observe conferencing should work with ASL. Furthermore, OBS and 3WC interactions are supported using the AMS for conferencing, but it is not supported on the UAS due to protocol restrictions on the UAS.

- Automatic Call Distribution Emergency Key, Emergency Key Backup (ACD EMK)- The EMK feature enables an ACD agent to immediately conference in a supervisor and/or an auxiliary device in the event of threatening or abusive calls. When the EMK key is pressed, the lamp

flashes on the agent set if the supervisor is available. The supervisor set rings and the Answer Emergency Key (AEMK) lamp flashes. When the supervisor answers the AEMK key the supervisor is conferenced into the call. The EMK and AEMK lamps are steadily lit. If the call is not answered by the supervisor within 30 seconds the feature is taken down. The EMK key can only be activated while the agent is active on an ACD call. The agent who initiates the emergency call must remain on the call for the duration of the feature. Emergency Key Backup provides a method for redirecting EMK calls made from an ACD agent position to a supervisor set AEMK key when the supervisor set is already active on an AEMK call, or the supervisor set is unavailable (i.e. supervisor does not answer the EMK call.) Redirection is accomplished by placing ACD supervisor AEMK (Answer Emergency) DN's in a hunt group via tables HUNTGRP and HUNTMEM.

- Camp-on for MDC lines (MBSCAMP) - this feature allows a MBS set to “camp-on” to a busy group member. When the MBSCAMP subscriber receives a call and attempts to transfer to another member of the customer group, if that line is busy so that the call would normally receive busy treatment, the MBSCAMP feature provides a call-waiting type indication to the busy line and camps onto the busy line. The MBSCAMP line is provided ringback or audio as an indication of the camping.
- Music on Hold (LMOH, KSMOH, pre-recorded music announcement on hold for ACD) - this feature provides an audio source to a line placed on hold by a line with this option (either on the line or the customer group).
- Executive Busy Override/Executive Busy Override Exempt (EBO/EBX) - the EBO feature allows a member of a customer group to override a busy indication from a called line in the group and connect into the call in progress. The EBO line can be connected as a third party or can either flash (on an IBN set) or press an EBO key again (on an MBS set) to drop the extra party and only be connected to the called party. Just prior to connecting the EBO party into the call, an EBO warning tone is provided to both parties of the current call. The EBX feature prevents a line with EBO from barging into a call. That is, when a subscriber with EBO attempts to override a call to another subscriber with EBX, the EBO feature is denied.
- Directed Call pick-up Barge In (DCBI) - this feature allows a member of a customer group to pickup an incoming call to a member of a customer group and also allows the member to barge-in to that call if it is answered prior to the completion of the pickup attempt. In that case, the DCBI line is connected as a third party to the call, and prior to the connection, an optional DCBITONE barge-in indication tone is provided to both parties of the initial call.

These services should have the same basic functionality in Succession as in the Legacy environment, but it must be noted that in Succession the tones

associated with the services are supplied by another device and therefore are a product of those elements.

Hardware Requirements or Dependencies

No new hardware is introduced by these services. However, as noted above, in Succession the tones required for these services are requested of a gateway (GW), either a network audio server (i.e. Universal Audio Server (UAS) or Audiocodes Media Server (AMS)) or a local GW.

Note there is a limitation with respect to the UAS. See the limitations section for more information.

Software Requirements or Dependencies

The SN07 software loads are required of the Succession elements.

Limitations and restrictions

These services function in Succession as they do in Legacy; that is, any limitations existing in Legacy also exist in Succession. An exception is that ASL functionality cannot be supported at this time. Although the provisioning of this function is not restricted, the behavior is not supported in solutions using an audio server. Solutions using an MTM to provide this observe conferencing should work with ASL.

The UAS does not support some of the signalling used for the ACD OBS interactions with 3WC (a null events descriptor in the H.248 protocol). Therefore this interaction is not supported with the UAS. This functionality is supported on the AMS.

For Music On Hold, the music is a pre-recorded music announcement.

Interactions

There are no new interactions with these services in SN07.

Applicable customer facing sections

Fault Management

Logs	_n/a_

Alarms	_n/a_

Configuration

Data Schema	_X_

User Interface	_n/a_

Element Management	_n/a_

Security	_n/a_

Service Order	_n/a_
Office Parameters	_n/a_
Accounting (includes AMA billing)	_n/a_
Performance (includes operational measurements)	_n/a_

Glossary

Term	Description
ACD	Automatic Call Distribution
AEMK	ACD Answer Emergency key
AMS	Audiocodes Media Server
CAG	Call Agent key
EBO	Executive Busy Override
EBX	Executive Busy Override Exempt
EMK	ACD Emergency key
FOBS	Flexible Call Observe
GW	Gateway
IBN	Integrated Business Network
KSMOH	Keyset Music on Hold
LMOH	Line Music on Hold
MOH	Music on Hold
OBS	ACD Observe
PRECONF	Preset Conference
SDN	Secondary Directory Number
UA-IP	Universal Access - Internet Protocol
UAS	Universal Audio Server

Configuration for A00004872

Hardware and Software Requirements

These services are configured in Succession as they are in Legacy. The tones provided by these services for a pure Succession network are provided by a gateway (GW), and therefore the physical characteristics of those tones are a product of the GW playing the tone. Information pertaining to this tones must be configured before the tone can be provided for Legacy offices where the tones are provided by the MTM. For Succession lines, since the tone is provided by the GW, no tone datafill is required.

Initial Configuration

Not applicable.

Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable.

Upgrade Impact

Dump and Restore

Not applicable.

Element Management Upgrade

Not applicable.

Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

Datafill in Table STN is not required for a pure Succession office.

Table/MIB/Remote Database Schema information

Name: Table STN

Special Tones

Functional description

Table STN is used to provision the hardware associated with special tones, typically played from a MTM circuit pack. With this activity, datafill is not required to support a purely Succession switch. If Legacy lines exist on the switch, this datafill is still required as it exists today in order to provide tones from the MTM.

Usage sequence and implications (CM Only)

Current datafill order unchanged.

Size

There is no change to the size limits to Table STN.

Fields/OIDs

There are no new fields for Table STN.

Datafill example

The following example shows sample datafill for table STN for Legacy, which is not required for Succession.

STN EBOT 1 MTM 5 14 3X68AC 10 0

Table release history update

Not applicable.

Supplementary information

The services of this activity that require special tones to be configured must now state that the tone can be provisioned via Table STN for Legacy lines, but this is no longer a requirement for packet lines. Also, the “typical” tone characteristics can be stated but if the tone is played by the GW, these characteristics are a product of the GW providing the tone.

The following table lists examples of current documentation and notes on the changes required.

Changes required for special tones via Table TONES

Document type	Current information	Modification needed
Data Schema for Table TONES description (volume 10 in LEC017)	Functional description states: The special tones listed below are generated on cards located on a trunk module (TM) or maintenance trunk module (MTM), and defined in table STN instead of table TONES: *BVTONE: IBN busy verification tone *CWT: call waiting tone *DISTCWT: distinctive call waiting tone *EBOT: executive busy override tone *ERWT: expensive route warning tone *OHQT: offhook queuing tone *ROH: receiver offhook tone	It should be noted that these tones may exist in Table STN when the tone is played by the TM/MTM device for Legacy/TDM lines.

Changes required for special tones via Table TONES

Document type	Current information	Modification needed
Translations Guide for DCBI feature (volume 11 in LEC017)	Description states: Both parties of the current call can receive an optional warning tone before the barging-in of the activating station occurs. The application of this tone is a customer group option. The DCBI tone contains 440 Hz at 13dbm. Datafill sequence show Table STN as a table requiring datafill for feature, stating: You must enter data in table STN to define the special tones used with DCBI.	It is suggested that the actual tone be stated as “typically” 440hz at 13dbm (since the characteristics can now be dependent on the GW configuration). It should be noted that the DCBITONE is not required for packet lines
Data Schema for Table CUSTSTN DCBITONE (volume 3 in LEC017)	CUSTSTN option DCBITONE states: Tone circuits in table STN with the code EBOT supply the warning tones	The TONE EBOT may be provided from a GW so that Table STN datafill is not required
Translations Guide for MBS Busy Override (volume 14 in LEC017)	Operation of feature states that when the calling party presses the EBO key, the called party and the party connected to the called party hears 500 ms of EBO warning tone. The translations table flow mentions defining EBOT in table STN for this feature. Datafilling table STN describes the provisioning required.	The “typical” tone length is 500 ms. The EBOT tone datafill is not a requirement for packet lines.
Translations Guide for Station camp on for Meridian Business Set (volume 15 in LEC017)	Translations table flow states: Table STN is required for tones that require trunk cards and allows MBSCAMP to work to another MBS. A 3X68AC... is required along with CWT datafill. The summary of table flow defines table STN and gives datafill for CWT tone.	The CWT tone is no longer needed for MBSCAMP to a Succession pphone (standard CWT buzz is now supplied). However it is still required of a Legacy pphone.
Translations Guide for ACD OBS (volume 16 in LEC017)	Description states “If OBSWTONE is set to Y, make an entry in table STN. Refer to the data schema section of this document for additional information on table STN.”	An entry is not required in table STN for a packet line.

Translation verification other tools

Table STN does not use translation verification tools.

Service Orders (SO) (CM & SESM)

Not applicable

Software optionality control (SOC)

Not applicable.

Element Management

Not applicable

Command interface changes

Not applicable

Security

Not applicable

Configuration Walkthrough

In order to configure the SN07 services ACD OBS, EBO, and DCBI to play tones from the GWs, if the office is a legacy office which plays the tone through the MTM, the current TABLE STN provisioning is still used. For provisioning these services on packet lines using audio servers for conferencing, no tones datafill is required.

Product = CS 2000

A00004922-4923 -- DMS-250 N449 PRI Enhancements (PT-IP)

Synopsis

This FN documents the functionalities provided by features A00004922 (DMS-250 N449 PRI Enhancements - GWC) and A00004923 (DMS-250 N449 PRI Enhancements - SPM) in Succession environment.

A00004922 covers the functionalities required to support the following N449 Primary Rate Interface (PRI) enhancements:

- Support of CodeSet 0 (CS0) parameterized Network Specific Facilities Information Element (NSF IE) with Out-Of-Band (OOB) data in Facility message.
- Support of CS6 Facility IE, Billing IE, and Item IE in Facility message.
- Support of CS0 and CS7 User-to-User Information (UI) if present in PRI Disconnect message.

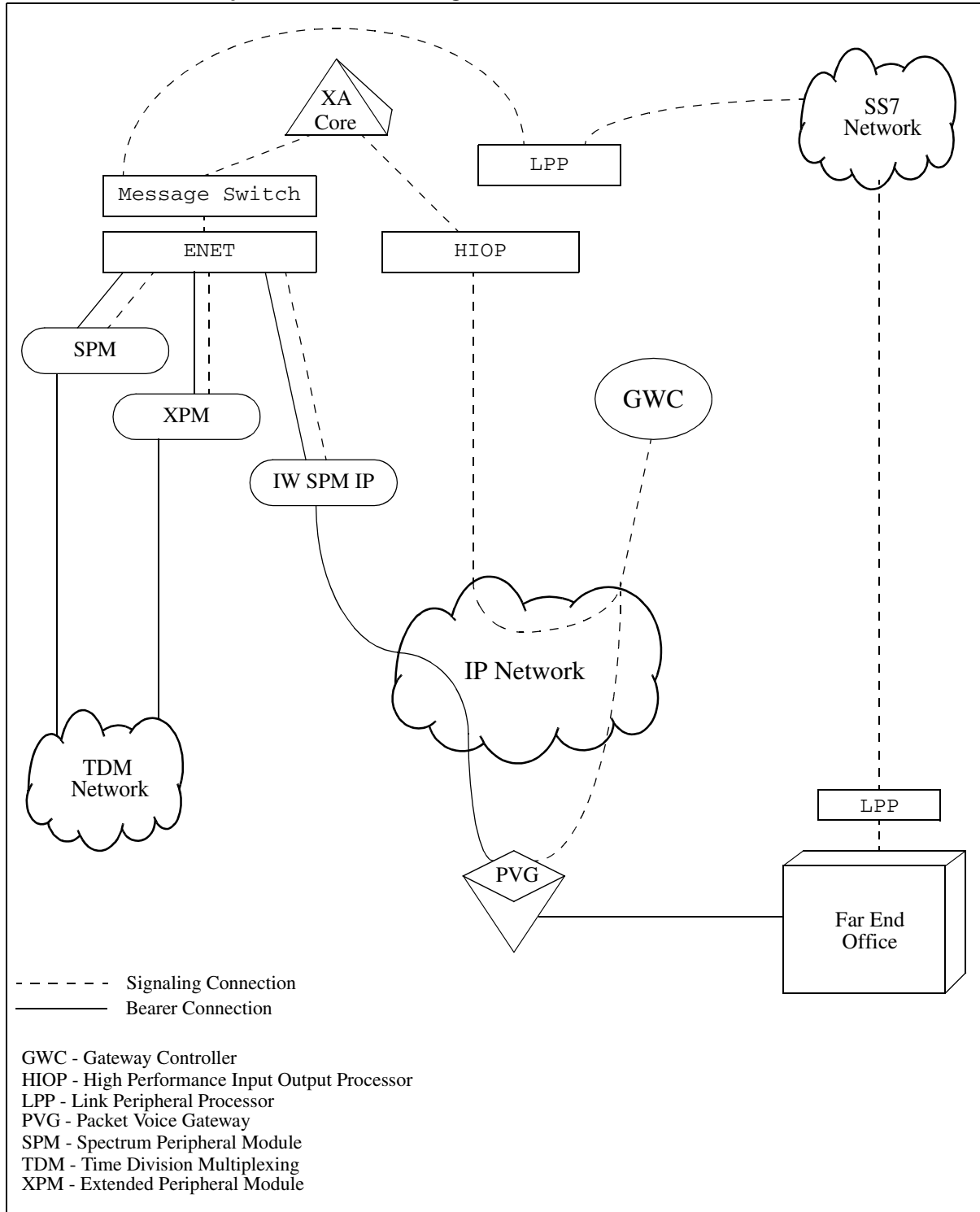
A00004923 covers the functionalities required to support the following N449 PRI enhancements:

- Support of CS0 parameterized NSF IE with OOB data in SETUP and Facility messages.
- Support of CS6 Facility IE in Facility message.

Background

A brief description of Succession environment and its components is presented in this section as the background information.

The following figure, Sample Succession Configuration, shows a switch that is capable of Time Division Multiplexing (TDM) as well as Succession environment.

Sample Succession Configuration

A description of the IP components is presented in the following table.

IP Components

IP Component	Explanation
XA-Core	Performs the call processing functions for a TDM and/or IP based solution. Also known as the computing module (CM).
Gateway Controller	Functions as the interface between the XA-Core and gateways such as the PVG. The GWC handles signaling from the core that was previously handled by the TDM SPM/XPM. Examples of this include Integrated Services Digital Network User Part (ISUP) and PRI. To communicate with gateways; the GWC also supports protocols such as ASPEN, ISDN User Adaptation Protocol (IUAP), and H.248.
Interworking SPM IP	Provides trunking capability from a TDM network to the IP network. TDM voice flows in the IW SPM IP from the ENET and is sent to the PVG in the form of IP packets. The reverse function is also performed. It is important to note that trunks do not hang off the IW SPM IP as they do with TDM SPMs.
Packet Voice Gateway	Functions as a gateway to the network for the bearer (i.e. speech) path. Bearer voice over IP packets are received from peripherals such as the IW SPM IP and sent to the outside network in the form of IP packets or TDM voice.
Link Peripheral Processor	This SS7 entity is the switch's link to the SS7 network. It functions in the IP world exactly as it does in the TDM world. In a TDM environment, the SPM/XPM sends an ISUP Initial Address Message (IAM) to the destination switch by bouncing the IAM through the core to the LPP to the SS7 Network. In an IP environment, the GWC sends an ISUP IAM to the destination switch in exactly the same way.
High Performance Input Output Processor	Provides the XA-Core a 100 Base ethernet access to the IP network. This allows communication between the core and the gateway controller.

Feature Description

A00004922 DMS-250 N449 PRI Enhancements - GWC

The functionalities provided by GWC for N449 PRI are documented in the following subsections.

Support of CS0 Parameterized NSF IE with OOB data in Facility Message

This feature supports three new NSF service identifiers in CS0 for the N449 PRI. The service identifier is sent in the Service Parameter field of the NSF IE in a Facility message. The new service identifiers are:

- OOB triggers and data allowed (0001100)
- Only OOB triggers allowed (0001101)
- Network Managed Data (NMD) (0001110)

The GWC supports the receipt of the following parameterized values in a Facility message.

Parameterized Network Specific Facilities Information Element.

Octet	Values
Octet 1	00100000 (NSF IE identifier)
Octet 2	Length of NSF IE
Octet 3:	00000000 (Length of network identification)
Octet 4: Bit 8	0 (Parameterized)
Octet 4: Bit 7	1 (Extension)
Octet 4: Bit 6	0 (Feature)
Octet 4: Bit 5-1	01001 (Available Feature Indicator)
Octet 5: Bit 8	0 (Spare)
Octet 5: Bits 7-1	Service Parameter Field
	0001100 OOB Triggers Allowed - Data Allowed
	0001101 OOB Triggers allowed - Data Not Allowed
	0001110 Network Managed Data (NMD)

Support of CS6 Facility IE in Facility Message

This feature supports a CS6 Facility IE length of up to 200 octets in an N449 PRI Facility message. A sample format of CS6 Facility IE supported is shown below. The highlighted operation values are the new values supported.

Parameterized Network CS6 Facility IE

Octet	Values
Octet 1	Service Discriminator = 10001
Octet 2	Component Type Tag = 10100001 (Invoke)
Octet 3:	Component Length
Octet 4: Bit 8	Invoke ID Tag = 00000010 (Invoke ID tag)
Octet 4: Bit 7	Invoke ID Length
Octet 4: Bit 6	Invoke ID
Octet 4: Bit 5-1	Operation Value Tag = 00000010 (Operation Value Tag)

Octet	Values
Octet 5: Bit 8	Operation Value Length
Octet 5: Bits 7-1	Operation Value
	11001110 (Redirect Call)
	11001111 (Put Calling Party on Hold)
	11010000 (Retrieve Calling Party From Hold)
	11010001 (Drop TP)
	11010011 (User Data Transfer)
	11001100 (Billing Operation)
	11010010 (Application Specific Call Status)
	10001111 (Request Feature)
	Q.931 IE tag = 01000000

Support of CS6 Billing IE, and Item IE in Facility Message

This feature provides the capability to receive and transmit an N449 PRI Facility message containing CS6 Billing Service Data IE, and/or CS6 Item IE.

The Billing Service Data IE can be received in a Facility message on a call after a Call Proceeding message has been received or sent.

The content of the Billing Service Data IE is presented in “Billing Service Data Information Element” on page 1838. Up to 100 octets of billing service data is supported. The Billing Service Data IE may appear in a Facility message as long as the total number of octets within the message does not exceed the maximum.

Billing Service Data Information Element

Octet	Values
Octet 1	01011000 (Billing Service Data IE identifier)
Octet 2	Length of Billing Service Data IE
Octet 3: Bit 8	1 (Extension)
Octet 3: Bits 7-5	000 (spare)
Octet 3: Bits 4-1	Type of Billing Service Data
	0011 Append To Record: Non-Mutilated Data
	0100 Append To Record: Mutilated Data
Octet 4 - 103	Billing Service Data

The content of the Item IE is presented in the following table.

Item Information Element

Octet	Values
Octet 1:bit 8	0 Set value
Octet 1:bits 7-1	1001101 (Item IE Identifier)
Octet 2	Length of Item IE
Octet 3: Bit 8	1 (Extension)
Octet 3:Bits 7-1	Item 0100001 Billing Closure 0101001 Send Close Message

Support of CS0 and CS7 UII IE

This feature provides the capability to receive and transmit CS0 and/or CS7 UII IE if present in an N449 PRI Disconnect message.

The content of UII IE is presented in the following table.

User-to-User Information Element

Octet	Values
Octet 1:bit 8	0 Set value
Octet 1:bits 7-1	1111110 (UII IE Identifier)
Octet 2	Length of UII IE
Octet 3+	User Information (See notes)

Notes: The contents of user information are structured according to the user application.

A00004923 DMS-250 N449 PRI Enhancements - SPM

The functionalities provided by SPM for N449 PRI are documented in the following subsections.

Support of CS0 Parameterized NSF IE with OOB data in SETUP and Facility Message

This feature supports three new NSF service identifiers in CS0. The service identifier is sent in the Service Parameter field of the NSF IE in a SETUP and Facility message.

Refer to [“Support of CS0 Parameterized NSF IE with OOB data in Facility Message” on page 1836](#) for more information.

Support of CS6 Facility IE in Facility Message

This feature supports a CS6 Facility IE length of up to 200 bytes in a Facility message.

Refer to [“Support of CS6 Facility IE in Facility Message” on page 1837](#) for more information.

Hardware Requirements or Dependencies

Not Applicable.

Software Requirements or Dependencies

Not Applicable.

Limitations and restrictions

Not Applicable.

Interactions

Not Applicable.

Applicable customer facing sections

Fault Management

Logs

Alarms

Configuration

Data Schema

User Interface

Element Management

Security

Service Order

Office Parameters

Accounting (includes AMA billing)

Performance (includes operational measurements)

Indicate with an X if you are completing the sections of the DDOC listed below. Indicate with “N/A” if these sections do not apply to this functionality.

Realtime

Engineering Information

Glossary

Term	Description
AMA	Automatic Message Accounting
ASPEN	Nortel's Media Gateway Control Protocol
CM	Computing Module
CS	CodeSet
CS0	CodeSet 0
CS6	CodeSet 6
CS7	CodeSet 7
GWC	Gateway Controller
HIOP	High performance Input Output Processor
H.248	Media Gateway Control Protocol
IAM	Initial Address Message
ISUP	Integrated Services Digital Network User Part
IUAP	ISDN User Adaptation Protocol
IW-SPM IP	Interworking Spectrum Peripheral Module IP
LPP	Link Peripheral Processor
NMD	Network Managed Data
NSF IE	Network Specific Facility Information Element
OOB	Out-Of-Band
PRI	Primary Rate Interface
PVG	Packet Voice Gateway
SS7	Signaling System No. 7
SPM	Spectrum Peripheral Module
TDM	Time Division Multiplexing
UUI	User-to-User Information
XPM	Extended Peripheral Module

Product = CS 2000

A00005007--Cause Indicators parameter support for DTAG AMA Enhancement (PT-IP)

Functional Description

This feature addresses the specific requirements defined by Deutsche Telekom AG (DTAG) for reporting the cause indicator parameter in the AMA records for an Avst (International Gateway Switch).

This feature is in continuation with feature A00003007 AMA Enhancements for DTAG International Gateway.

Overview.

The DTAG specifications states that the cause indicator of the release message be captured in AMA records.

This feature captures the Cause Indicator for ETSI ISUP to ETSI ISUP non-INAP tandem call for the following scenarios.

- GWC sends a Clear Forward Message.
- GWC sends a Clear Back Message.
- GWC reports the Release message to the CM.

In a Tandem (or Gateway) switch, for most of the cases, the release message is bounced on the GWC and not sent to the CM. Upon receiving a release message, the GWC sends a CLEAR_FORWARD or CLEAR_BACKWARD message to the CM to tear down the call.

This feature introduces a mechanism to transport CI parameter from GWC to CM in CLEAR_FORWARD or CLEAR_BACKWARD message. Figure2 explains the mechanism.

A new office parameter REPORT_ISUP_CI_TO_CM will be created in table OFCENG, which will govern the functionality.

- If the office-parameter is set to 'Y', functionality is enabled
- If the office-parameter is set to 'N', functionality is disabled.

Example datafill of REPORT_ISUP_CI_TO_CM

Table OFCENG REPORT_ISUP_CI_TO_CM N

The Extraction of Cause Indicator will be fully invoked if

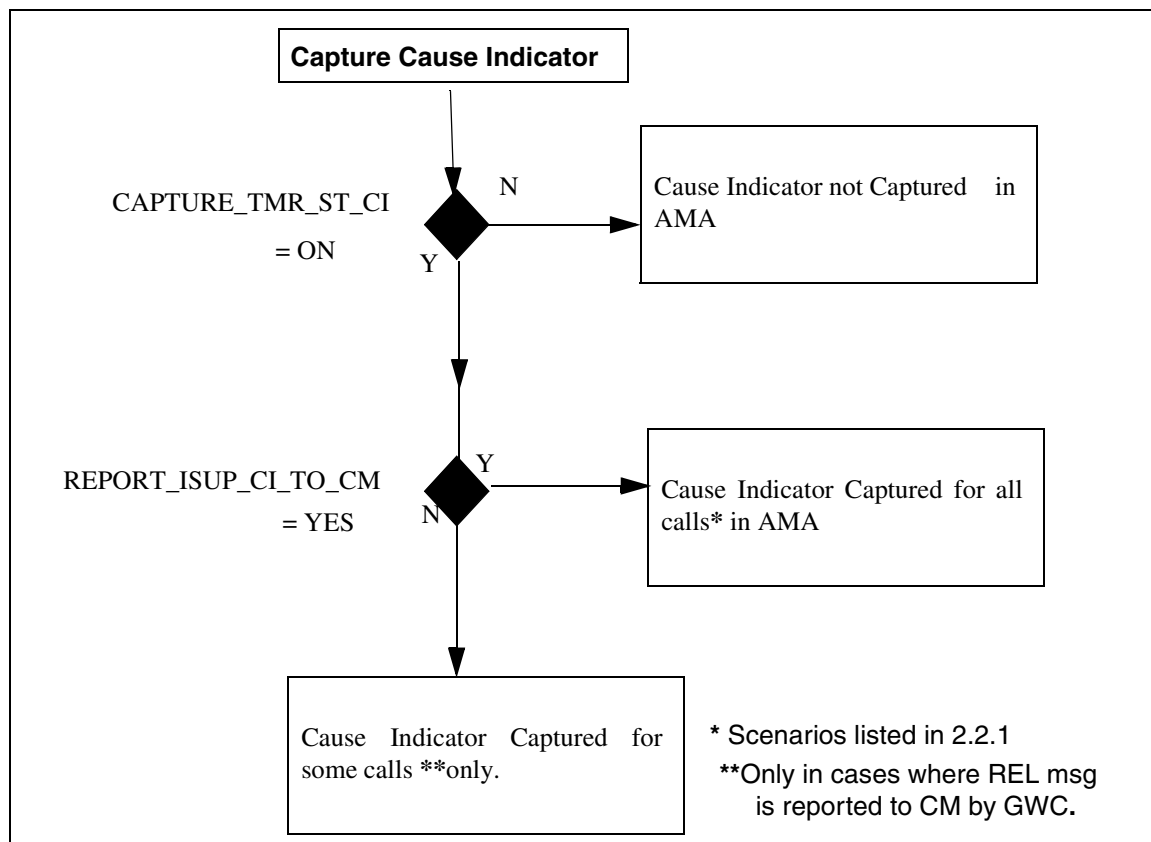
- The Office Parameter CAPTURE_TMR_ST_CI of TABLE AMAOPTS is ON.
- The Office Parameter REPORT_ISUP_CI_TO_CM of TABLE OFCENG is set to YES.

While data filling CAPTURE_TMR_ST_CI in table AMAOPTS, this feature introduces additional **warning** to data fill REPORT_ISUP_CI_TO_CM to YES to ensure complete functionality.

Warning while data filling CAPTURE_TMR_ST_CI.

```
TABLE: AMAOPTS
>pos capture_tmr_st_ci
    CAPTURE_TMR_ST_CI                                OFF
>cha
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
AMASEL: OFF
>ON
TUPLE TO BE CHANGED:
    CAPTURE_TMR_ST_CI                                ON
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
Note: Additional AMA MC611 (context ID 80100) will be
generated for all ETSI ISUP tandem (non-INAP) calls.
Warning : Please ensure that the office parameter
REPORT_ISUP_CI_TO_CM in table OFCENG is set to YES to
enable full functionality of capturing Cause Indicator.
TUPLE CHANGED
JOURNAL FILE INACTIVE
```

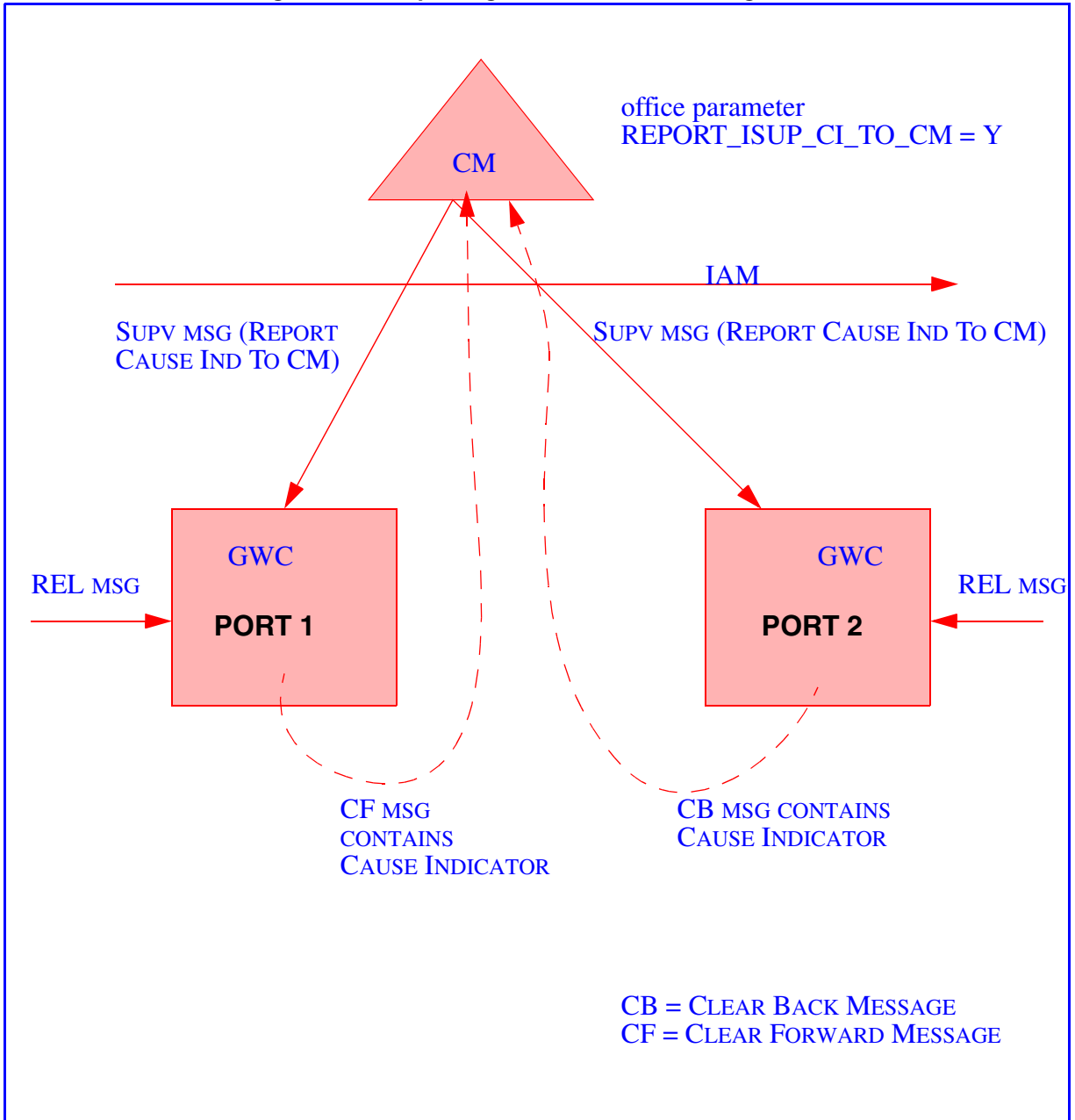
The cause indicator will be stored in AMA record in AMA generic module code 611 with context id 80100 (TMR_ST_CI).

Capturing of Cause Indicator in AMA records

The Cause Indicator will appear in AMA records as below.

Cause Indicator parameter in AMA records.

MODULE CODE:	611C	GENERIC MOD: ONE DGT STR FMT
GENERIC CONTEXT ID:		
PARSE RULES	80100	TMR/SERVTYPE/CAUSE IND
SIGNIFICANT DIGITS	00C	NIL
GENERIC DIGIT STRING ONE:		
TRANSMISSION MEDIUM REQ	003	
SERVICE TYPE	000	
CODING STANDARD	0	ITU-T
LOCATION	00	U
CAUSE VALUE (CLASS PORTION)	1	NORMAL EVENT
CAUSE VALUE (VALUE PORTION)	00	
UNUSED	000C	
MODULE CODE:	000C	FINAL MODULE

Message flow for reporting CI in CB or CF message**Hardware Requirements or Dependencies**

-N/A-

Software Requirements or Dependencies

-N/A-

Limitations and restrictions

For scenarios in which the CS2K releases the call, cause indicator is not captured in AMA records (Module 611, Context id 80100)

The figure below shows the values of CI which will appear AMA in such scenarios.

CDefault Cause Indicator in AMA records

MODULE CODE:	611C	GENERIC MOD: ONE DGT STR FMT
GENERIC CONTEXT ID:		
PARSE RULES	80100	TMR/SERVTYPE/CAUSE IND
SIGNIFICANT DIGITS	00C	NIL
GENERIC DIGIT STRING ONE:		
TRANSMISSION MEDIUM REQ	003	
SERVICE TYPE	000	
CODING STANDARD	0	ITU-T
LOCATION	00	U
CAUSE VALUE (CLASS PORTION)	0	NORMAL EVENT
CAUSE VALUE (VALUE PORTION)	00	
UNUSED	000C	
MODULE CODE:	000C	FINAL MODULE

Interactions

-N/A-

Applicable customer facing sections.

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema _____

User Interface _____

Element Management _____

Security _____

Service Order _____

Office Parameters X

Accounting (includes AMA billing) X

Performance (includes operational measurements) _____

Glossary

Term	Explanation
CS2K	Call Server 2000
DTAG	Deutsche Telekom AG
GWC	Gateway Controller
CB	Clear Back
CF	Clear Forward
CI	Cause Indicator

Recommended Reading/References

- [1] 163TR75 - DTAG specification for the Telekom-ISUP (T-ISUP)
- [2] 163TR76 -DTAG specification for the Gateway-ISUP (G-ISUP)
- [3] 163TR80 - DTAG interworking specification (R2, G-ISUP, T-ISUP)
- [4] A00003007- AMA Enhancements for DTAG Intl GW
- [5] KDS:IN specification, DTAG, release date unknown.
- [6] „Tarifizierung von IN-Verbindungen“, FTZ 163 TL 50 Teil 1/10.94, Anhang AA, DTAG, Oct 1994.
- [7] „Beschreibung der Kommunikationsdatenerfassung für IN“, FTZ 163 TL 500 Teil 1200/10.94, Anhang D, DTAG, Oct 1994.
- [8] KDS:N specification (163 TL 500 Teil 1202/10.94, Anhang C), DTAG, Oct 1994.
- [9] KDS:A specification („Technische Spezifikation MSP-T, Anhang A: Datenformat NAKODA (KDS:A)“, Version 1.0, DTAG, Mar 28th, 2002.
- [10] TZ 163 TR 75.97 „T-ISUP“, DTAG, Aug 25th, 1997.
- [11] TZ 163 TR 76.98 „Anwendungsspezifikation für das Zeichengabesystem Nr. 7 - G-ISUP“, DTAG, Apr 1998.
- [12] TZ 163 TR 78.96 „T-INAP“ Teil 1+3+4, DTAG, Apr 1996.

[13] TZ 163 TR 80.98 Annex 3 „Tarifizierung von IN-Verbindungen“, DTAG, Apr 1998.

Configuration for A00005007

Hardware and Software Requirements

Not Applicable to the activity A00005007.

Initial Configuration

Not Applicable to the activity A00005007

Office/Subnet parameters (OP/SP) (CM & SESM)

New/modified office/subnet parameters

New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCENG	REPORT_ISUP _CI_TO_CM	NEW	CM

Parameter information

Name: REPORT_ISUP_CI_TO_CM

Reporting of Cause Indicator to CM.

Functional description

This parameter will enable sending of supervision to GWC for reporting of the cause indicator of Release message to CM. The cause indicator will be attached to the Clear Forward or Clear Back Message.

This implementation of this parameter is being done in ISN07 (SNWCSH07).

Provisioning rules

This parameter enables sending of supervision when set to TRUE and disables when set to FALSE.

Range information

Range Information

Minimum	Maximum	Default
Boolean {N,Y}	n/a.	N

Activation

Any changes are activated immediately.

Dependencies

None.

Consequences

None

Verification

No verification required for this parameter.

Memory requirements

No memory impact.

Parameter release history update

Creating Office Parameter REPORT_ISUP_CI_TO_CM in table OFCENG.

Upgrade Impact

Not Applicable to the activity A00005007.

Data schema (DS) (CM, MIBS, RDB)

Not Applicable to the activity A00005007.

Service Orders (SO) (CM & SESM)

Not Applicable to the activity A00005007.

Software optionality control (SOC)

Not Applicable to the activity A00005007.

Element Management

Not Applicable to the activity A00005007.

Command interface changes

Not Applicable to the activity A00005007.

Security

Not Applicable to the activity A00005007.

Configuration Walkthrough

Not Applicable to the activity A00005007.

Product = CS 2000

A00005073--SBA Outbound Connection Security (Succession on DMS)

Functional Description

This feature provides optional secure outbound file transfer using OpenSSH sftp client. The sftp client protects all data including sensitive users' password by encrypting the data before it leaves SDM/CBM and decrypting the data after it arrives the downstream OSS. The sftp also provides data integrity check to ensure that no one has tampered the data during the transfer.

The SBA user can configure the secure file transfer by adding or changing an existing schedule tuple in billmtc. For SN07, the user has to manually accept the downstream host key for each destination before configuring secure outbound file transfer to the destination. The actual configuration details are documented in the configuration section.

This feature also enhances SBA password protection scheme by using SDM/CBM private data manager (documented in A00005074) to store all the passwords for OSS access. The private data manager is responsible for storing the data in an encrypted form.

Hardware Requirements or Dependencies

No new hardware requirements or dependencies are introduced by this feature.

Software Requirements or Dependencies

Software requirements for downstream system

A SSH sftp-server⁵ which is compatible with OpenSSH sftp client must be running on the downstream Operations Support System (OSS) in order for SBA to transfer data with OpenSSH sftp client.

Software requirements for SDM.

The OpenSSH and its dependencies should be installed on the SDM/CBM. If this software is unavailable, SBA user will not be able to use the SFTPW protocol for outbound file transfer. There is no explicit check done by the SBA software to determine if this package/fileset is installed during SFTPW configuration time. If the SBA SFTPW application fails to find the sftp program, it raises a SFTPW alarm and terminates the transfer event immediately.

For CBM, this feature depends on the OpenSSH packages as well as NTutil.

5. SFTP server subsystem

For SDM, this feature depends on SDM_OpenSSH.base and SDM_BASE.util files must be installed manually.

Limitations and restrictions

- As described in Section “Software Requirements or Dependencies” on page 1850, that the SFTPW is only available if OpenSSH and the SDM base util software is installed. SBA currently uses OpenSSH software (version 3.7.1p2 or later) for secure file transfer.
- Public keys authentication is not supported in this release. All users are authenticated with userid/password to the downstream OSS.
- The overall billing data traffic rate is lower than that of a FTPW with a given SBA CPU usage. For more information, please refer to the SDM EI section.
- The initial host key acceptance of the downstream processor should be done manually before it can use the SFTPW⁶ to transfer files from SDM/CBM. Figure shows how to accept a host key manually. The .ssh/known_hosts file in maint's home directory will be edited by SSH software to include the host key. After that SBA can use sftp to send file to the downstream OSS as maint/root. This procedure must be done for each downstream destination. This step must be done prior to schedule tuple configuration for SFTPW.
- The SSH-2 server running on the downstream OSS must be compatible with OpenSSH sftp client.
- Due to government restrictions on export/import of encryption software, secure file transfer will not be available on SDM/CBM loads that shipped to some countries with restrictions on the strength of encryption.
- Does not secure data transfer for AFT, RTB and sendtape applications.

6. SFTPW - Secure File Transfer Protocol Wrapper which controls sftp client to send files using SSH protocol

Host key acceptance

```

In AIX
> login: root
> root's Password: xxxx
> su - maint
> /usr/bin/ssh -l maint wcary2p3
The authenticity of host 'wcary2p3 (47.135.213.53)' can't be established.
RSA key fingerprint is ef:f8:b9:b5:4e:15:71:66:09:82:0d:93:fa:ce:58:ff.
Are you sure you want to continue connecting (yes/no)? yes

```

Interactions

None

Applicable customer facing sections

Fault Management

Logs ☒ XAlarms ☒ X

Configuration

Data Schema ☐ N/AUser Interface ☒ XElement Management ☐ N/ASecurity ☐ N/AService Order ☐ N/AOffice Parameters ☐ N/AAccounting (includes AMA billing) ☐ N/APerformance (includes operational measurements) ☐ N/ARealtime ☐ N/ASDM Engineering Information ☒ X

Glossary

Term	Description
SDM	Supernode Data Manager
CBM	Core Billing Manager
SBA	SDM/CBM billing application
SSH	Secure Shell
FTP	File Transfer Protocol
SFTP	Secure File Transfer Protocol (SSH internal protocol)
OSS	Operations Support System

Fault Management for A00005073

Fault management strategy

In case of file transfer error, SDMB375 is generated on the Core with the proper information. The SDMB375 is not a new log. It is also raises a major or critical alarm on certain error conditions.

Fault management tools and utilities

NA

Logs

Explanation

Log Title: SDMB375

Name: SDM BILLING FILE TRANSFER

Description: To indicate an error occur in SBA secure file transfer

Event type: N/A

Format

*SDMB375 <date> <time> <seq#> SDM BILLING FILE TRANSFER

STREAM=<stream>:<destination>:<specific error>

Field descriptions

Field	Value	Description
Stream	string SIZE(4)	stream name
destination	string SIZE(15)	The name of the destination
specific error (variable field)	string SIZE varies	sftp specific error message and the possible action should be taken

Action

Follow the recommended action in the specific error field.

Associated Operational Measurements or Performance Measurements

NA

Alarms

On error conditions, an alarm is raised on SDMBIL alarm slot.

Alarm format: SFTW

C

The corresponding log will also be generated.

Configuration for A00005073

Hardware and Software Requirements

- OpenSSH installed on SDM/CBM
- SDM/CBM Private Data Manager running
- SBA installed and InSv

Initial Configuration

Configure and activate an SBA stream.

Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

Upgrade Impact

NA

Data schema (DS) (CM, MIBS, RDB)

N/A

Service Orders (SO) (CM & SESM)

N/A

Software optionality control (SOC)

N/A

Element Management

N/A

Command interface changes

N/A

Security

N/A

Configuration Walkthrough**Host key acceptance for downstream OSS****Host key acceptance**

```
In AIX
> login: root
> root's Password: xxxx
> su - maint
> /usr/bin/ssh -l maint wcary2p3
The authenticity of host 'wcary2p3 (47.135.213.53)' can't be established.
RSA key fingerprint is ef:f8:b9:b5:4e:15:71:66:09:82:0d:93:fa:ce:58:ff.
Are you sure you want to continue connecting (yes/no)? yes
```

SBA specific configuration

SBA secure outbound file transfer can be configured by adding or changing an existing schedule tuple after the user has done a host key acceptance. The following shows an example on how a user can configure secure outbound file transfer. The text in bold indicates the field values that are different from FTPW

Prompts for schedule add

```
Valid streams are {'OCC'}.
Press Enter to accept 'OCC'.
Enter Stream: occ

Valid file format types are {'DIRP'}.
Press Enter to accept 'DIRP'.
Enter File_Format_Type:

Destination can have between 1 and 15 alphanumeric characters.
Enter Destination: OOS

Valid protocols are {'FTPW', 'RFTPW' 'SFTPW'}.
Press Enter to accept 'FTPW'.
Enter Protocol: SRTFPW

Primary destination must follow IP address format (i.e. N.N.N.N
where N indicates a number between 0 and 255).
Enter Primary_Destination: 47.135.213.53

Primary port can be 22 or between 1025 and 65535.
Press Enter to accept '22'.
Enter Primary_Port:

Alternate destination must follow IP address format (i.e. N.N.N.N
where N indicates a number between 0 and 255).
Enter Alternate_Destination: 47.135.213.53

Alternate port can be 22 or between 1025 and 65535.
Press Enter to accept '22'.
Enter Alternate_Port: 22

... (con't on next figure)
```


Prompts for Schedule add (con't)

Start time is in time of day format (hh:mm) where hh is hours between 0 and 23 and mm is minutes between 0 and 59.

Enter Start_Time: 00:00

Stop time is in time of day format (hh:mm) where hh is hours between 0 and 23 and mm is minutes between 0 and 59.

Enter Stop_Time: 23:00

Interval can be between 5 and 1440 minutes.

Press Enter to accept '120'.

Enter Interval: 5

Remote storage directory can have between 1 and 255 characters.

Enter Remote_Storage_Directory: /billing

Remote login can have between 1 and 20 characters.

Enter Remote_Login: test

Remote password can have between 1 and 20 characters.

Enter Remote_Password:

Re-enter Remote_Password:

Maximum retries can be between 0 and 10.

Press Enter to accept '3'.

Enter Maximum_Retries:

Retry wait time can be between 1 and 60 seconds.

Press Enter to accept '1'.

Enter Retry_Wait_Time:

File extension can have between 0 and 3 characters.

Enter 'Blank' for no file extension.

Press Enter to accept 'Blank'.

Enter File_Extension:

Field separator can have 1 character.

Press Enter to accept '.'.

Enter Field_Separator:

WARNING: Billing files associated with this tuple will not transfer downstream when Active is set to No.

Valid active values are {'No', 'n', 'Yes', 'y'}.

Press Enter to accept 'No'.

Enter Active: y

Product = CS 2000

A00005074--OMDD: Outbound Connection Security (Succession on DMS)

Functional Description

The OM Data Delivery (OMDD) application on the SDM/CBM collects OM reports from the core, processes them in to CSV files and sends the CSV files to downstream destinations (OSS). Prior to this activity, the outbound transfer of CSV files from SDM/CBM to downstream was always insecure because it used only the standard ftp protocol to do the transfer. The standard ftp protocol sends out user password as well as data in cleartext, making them vulnerable to reading by a third party by intercepting them in the network.

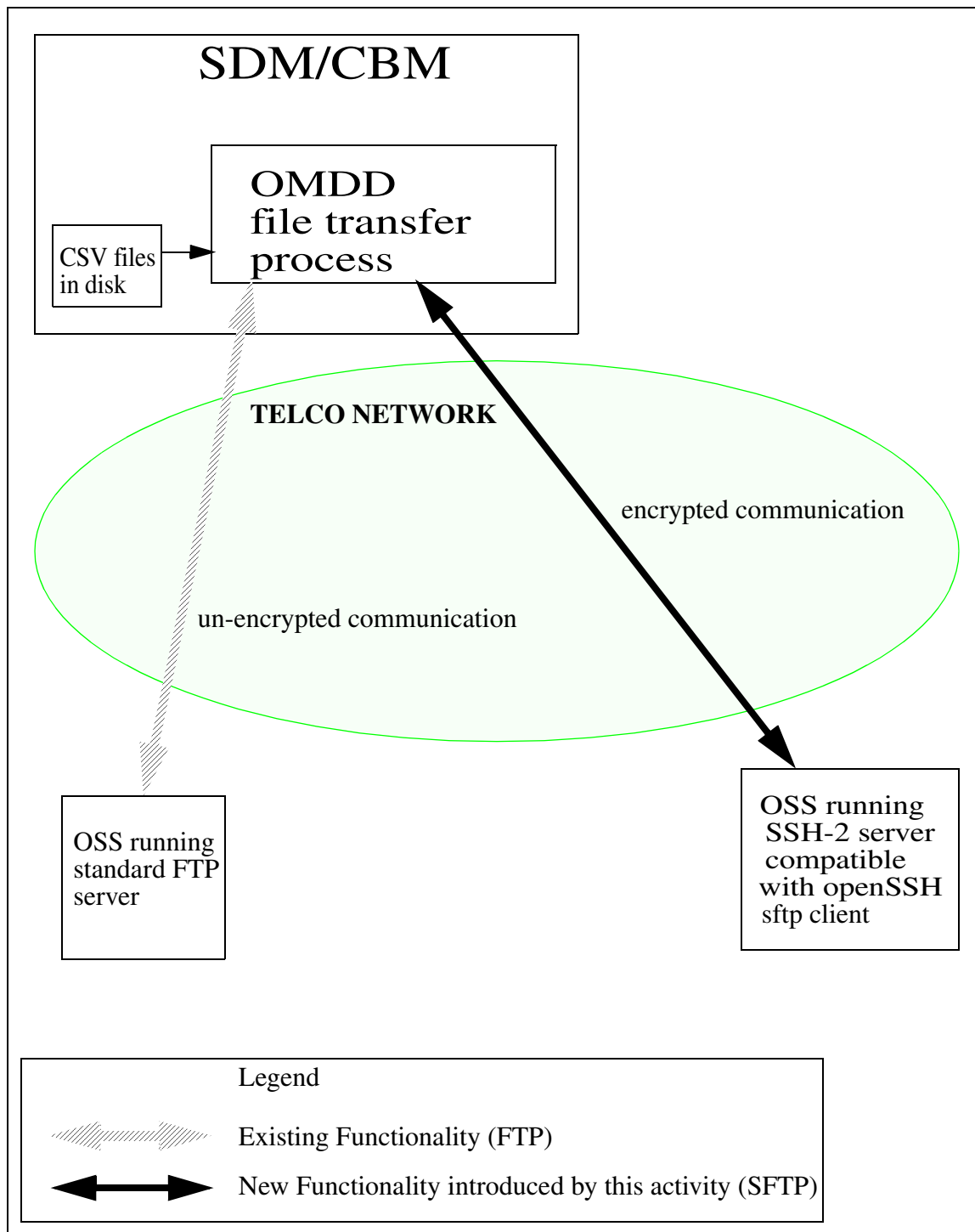
This activity provides an optional mechanism to prevent OMDD outbound transfers from sending out clear text passwords and data in the network. The mechanism uses the OpenSSH secure ftp client for doing outbound file transfers from SDM/CBM to the downstream destination. OpenSSH encrypts all data (including passwords) exchanged between the SDM/CBM and downstream, thus making them resistant to reading by a third party by intercepting them in the network.

The following figure shows the OMDD outbound file transfer functionality after this activity. It should be noted that secure file transfer is only an optional mechanism and the user can still choose standard ftp for file transfers. This choice can be done while configuring or modifying file transfer destinations.

The user configures file transfer destinations on the SDM/CBM using the OMDD User Interface program (OMUI). It is the configuration tool for OMDD. This activity modifies the Add and Modify File Transfer Destination menus of OMUI. From now on, when a user adds or modifies a file transfer destination, he/she will be asked to select the type of file transfer for the destination in addition to the already existing parameters. The choices for the type of file transfer will be "Standard" and "Secure." The default choice will be "Standard."

The following figure shows examples of adding file transfer destinations (both secure and standard) using the OMUI tool.

While doing the actual file transfer, OMDD will invoke either the standard FTP client or the secure FTP client by looking at the choice made by the user at the time of configuration. A customer log SDMO375 will be generated if the OM file transfer fails.

OMDD File Transfer view

Additionally, this feature develops a Private Data Manager on the SDM./CBM for encrypting data by all applications. OMDD will contact the Private Data Manager for storing downstream destination passwords in encrypted format.

Hardware Requirements or Dependencies

No hardware requirements or dependencies are introduced by this feature.

Software Requirements or Dependencies

The customer's downstream machine (the OSS) should be running a SSH-2 server compatible with SFTP client of OpenSSH. The OpenSSH filesset should be installed on the SDM/CBM too.

Limitations and restrictions

- The additional overhead of encrypting/decrypting all data will affect the capacity of OMDD if secure ftp is used.
- Public keys authentication is NOT supported in this release. All users are authenticated with userid/password with the downstream OSS.
- The initial host key acceptance of the downstream processor should be done manually before it can use the SSH protocol to transfer file from SDM/CBM. Figure shows an example how to accept a host key. The /home/maint/.ssh/known_hosts file will be edited by ssh to include the host key. After that user can use SSH for OMDD file transfer. OMDD will use the /home/maint/.ssh/known_hosts file when invoking the sftp client.
- The SSH-2 server running on the downstream OSS should be compatible with the OpenSSH sftp client.
- Due to government restrictions on export/import of encryption software, this feature will not be available on SDM/CBM loads shipped to some countries.

Example of adding the host key of downstream processor to the known_hosts file

```
cbm:/home/maint> ssh user1@47.135.214.66
The authenticity of host '47.135.214.66 (47.135.214.66)' can't be established.
RSA key fingerprint is fd:3b:18:27:1f:85:55:83:ff:e6:16:7e:fd:5e:33:f8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '47.135.214.66' (RSA) to the list of known hosts.
user1@47.135.214.66's password:
```

User input - Blue
System Output -Black

Interactions

Not Applicable

Applicable customer facing sections

Fault Management

Logs __N/A__

Alarms __N/A__

Configuration

Data Schema __N/A__

User Interface __X__

Element Management __N/A__

Security __N/A__

Service Order __N/A__

Office Parameters __N/A__

Accounting (includes AMA billing) __N/A__

Performance (includes operational measurements) __N/A__

Realtime __N/A__

Engineering Information

___X__

Glossary

Term	Description
SDM	Supernode Data Manager
CBM	Core Billing Manager
OMDD	Operational Measurements Data Delivery
OMUI	OMDD User Interface
CSV	Comma Separated Value
SSH	Secure Shell
FTP	File Transfer Protocol
SFTP	Secure File Transfer Protocol
OSS	Operations Support System

Configuration for A00005074

Hardware and Software Requirements

OMDD application running on the SDM/CBM is InSv. OpenSSH is installed on the SDM/CBM.

Initial Configuration

The initial configuration of OMDD is not changed by this activity.

Element Management

New/modified GUIs

GUI name	NEW, CHANGED, or DELETED
OMUI	Changed

GUI information

The OMUI “Add File Transfer Destination” and “Modify File Transfer Destination” menus are modified by this activity.

GUI name: OMUI

OMDD User Interface

Functional description

The “Add File Transfer Destination” menu in OMUI enables the user to configure a destination where OMDD can transfer OM reports. The “Modify File Transfer Destination” menu enables the user to modify an already configured file transfer destination.

This activity modifies the Add and Modify File Transfer Destination menus of OMUI. From now on, when a user adds or modifies a file transfer destination, he/she will be asked to select the type of file transfer for the destination in addition to the already existing parameters. The choices for the type of file transfer will be “Standard” and “Secure.”

If the user chooses “Secure”, a warning message will be printed along with the confirmation prompt. This warning message informs the user that secure file transfer would fail if OpenSSH was not installed on the SDM/CBM.

The following figure shows an example configuration of file transfer destination using the modified menu. The same change is made in the “Modify File Transfer Destination” menu also.

OMUI File Transfer Destination menu

Add File Transfer Destination (for a secure file transfer destination)
File Transfer Destination name > ftd1
Destination IP Address > 1.1.1.1
Type of File Transfer: Standard/Secure > Secure
Destination Port [22] >
Destination Login > user1
Destination Password >
**WARNING: File Transfer to this destination will fail if OpenSSH is not installed.
Please install OpenSSH if it is not already installed.**
Add File Transfer Destination(Y/N)?

Add File Transfer Destination (for a standard file transfer destination)
File Transfer Destination name > ftd2
Destination IP Address > 1.1.1.2
Type of File Transfer: Standard/Secure > Standard
Destination Port [21] >
Destination Login > user1
Destination Password >
Add File Transfer Destination(Y/N)?

SDM/CBM output - black
User input - blue
Step newly added by this activity - red

Configuration Walkthrough

This activity introduces an additional step in the add and modify file transfer destination menus of OMUI. This does not change the existing configuration methods of OMDD.

Product = CS 2000

A00005190--nSDM (Takoma) OC3 Node and Link Maintenance (Succession on DMS)

Functional Description

A market was identified to replace the aging billing storage device known as the DPP (Distributed Processing Peripheral). The function of the DPP is to receive billing records from the core through an IOC interface and store them on redundant hard disks. A modem link is used to poll the DPP for billing records and transfer them downstream to an OSS.

The chosen platform for DPP replacement was the next generation SDM or Core and Billing Manager (CBM) on the SSPFS platform. However, core connectivity became a problem since DPP's are connected to BRISC cores via IOC connectivity but the CBM only provided IP connectivity.

A prototype was built to prove that OC3 could be used to connect a CBM 800 to an MS in a similar manner to the SDM FX which is connected through DS512 links to the MS.

The OC3 connectivity resolves several issues including security and capacity.

This solution builds on the existing infrastructure that is used for the SDM FX platform and the Node maintenance infrastructure that was developed for the Ethernet connected SDM and the CBM 850.

This activity provides the modifications in node maintenance on the core to support the OC3 connected CBM.

Hardware Requirements or Dependencies

None

Software Requirements or Dependencies

None.

Limitations and restrictions

None.

Interactions

None.

Applicable customer facing sections**Fault Management**

Logs _____N/A

Alarms _____N/A

Configuration

Data Schema _____X

User Interface _____X

Element Management _____N/A

Security _____N/A

Service Order _____N/A

Office Parameters _____N/A

Accounting (includes AMA billing) _____N/A

Performance (includes operational measurements) _____N/A

Realtime _____X

Engineering Information _____X

Glossary

Term	Description
CBM	Core and Billing Manager

Fault Management for A00005190**Fault management strategy**

No change.

Fault management tools and utilities

No change.

Link Condition Change Log

Explanation

Log Title: SDM267

Name: SDM LINK CONDITION CHANGE

Description: CBM custlog log to indicate a change in the condition of a CBM link.

Event type: Info

Format

```
SDM267 NONE INFO SDM LINK CONDITION CHANGE
Link: Domain <domain num> Port <port num>
From: <previous link condition>
To: <new link condition>
```

```
SDM267 NONE INFO SDM LINK CONDITION CHANGE
Link: Domain 0 Port 0
From: closed
To: mtc-open
```

Field descriptions

Field	Value	Description
Link: Domain	0 or 1	MS number
Link: Port	0	NTL9X63 port number
From:	closed, mtc-open, open	previous link condition
To:	closed, mtc-open, open	new link condition

Action

None.

Associated Operational Measurements or Performance Measurements

None.

Links Crossed Log

Explanation

Log Title: SDM314

Name: SDM LINKS CROSSED

Description: CBM custlog log to indicate two link connections are physically crossed.

Event type: Major

Format

SDM314 MAJOR FAIL SDM LINKS CROSSED

link <recv link num> on domain <recv domain num> port <recv port num> crossed with link <send link num> on domain <send domain num> port <send port num>

SDM314 MAJOR FAIL SDM LINKS CROSSED

link 0 on domain 0 port 0 crossed with link 1 on domain 1 port 0

Field descriptions

N/A

Action

Reconnect crossed links from MS port to correct ATM card.

Associated Operational Measurements or Performance Measurements

None

Core Heartbeat Alarm

Associated alarm message: No response to core heartbeat

Severity: Critical

Condition: CBM-800 node maintenance heartbeat not responded to in 15 seconds.

Action: Report the full text of the alarm to the support group.

ATM Hardware Alarm

Associated alarm message: ATM card fault: <description>

Severity: Critical, Major, Minor

Condition: ATM diagnostics return card fault

Action: Report the full text of the alarm to the support group.

Configuration for A00005190

Hardware and Software Requirements

Tables IPNETWRK and MSCDINV must be data filled before table SDMINV.

Initial Configuration

No hardware needs to be present to configure an SDM or CBM connected by DS512 or OC3 on the Core.

Office/Subnet parameters (OP/SP) (CM & SESM)

No change.

Upgrade Impact

No change.

Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
SDMINV	CHANGED	UNCHANGED

Table/MIB/Remote Database Schema information

Name: SDMINV

DS512 connected SDM inventory table

Functional description

This table contains the PEC codes, location, link information, and IP address information related to a DS512 connected SDM. This activity adds a new PEC for a simplex CBM which is OC3 connected.

Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

Current datafill order unchanged.

Size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SDMINV	0	1	No change

Fields/OIDs

The following table lists the changed field for table SDMINV.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SHELFPEC	Changed	none	NTRX50DA NTRX50EB NTRX51EL NTRX51LS	NTRX51LS is being added for the simplex CBM OC3 connected shelf type.

Datafill example

```
>table sdminv
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: SDMINV
>lis all
TOP
SDM CONFIG FLOOR ROW POSITION CABTYPE CABPEC CABNUM SHELFPEC SHELFPOS
          IPADDR LINKRATE          LINKS
-----
  0  SIMP      1  A      1  MISC NT0X02AB      1 NTRX51LS      2
 10  40  15   3  SR256      ( 8 0 )$
BOTTOM
```

Translations verification other tools

Not applicable

Service Orders (SO) (CM & SESM)

Not applicable

Software optionality control (SOC)

Not applicable

Element Management

Not applicable.

Command interface changes

MAP level:mapci;mtc;appl;sdm

SDM MAPCI screen CSP19

CM	MS	IOD	Net	PM	CCS	Trks	Ext	APPL
.	01MBCD	AMA B	.	.	.	...	.	.
		C						
SDM		OAMAP		SDM	SWMTC	SDMBIL		
0 Quit		.		.	.	.		
2								
3	SDM 0	OffL		Links_OOS: 4				
4								
5 Trnsl								
6								
7 Bsy								
8 RTS								
9 OffL								
10								
11								
12								
13								
14 QuerySDM								
15 Locate								
16								
17								
18 Platform								
admin								
Time 15:57								>

SDM MAPCI screen CSP20

CM	MS	IOD	Net	PM	CCS	Trks	Ext	APPL
.	01MBCD	AMA B	.	.	.	...	.	.
		C						
SDM		OAMAP		SDM	SWMTC	SDMBIL		
0 Quit		.		.	.	.		
2								
3	SDM 0	OffL		Links_OOS: 4 of 4				
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
admin								
Time 15:57								>

MAP level description

This map level displays the state information related to the SDM.

It also provide commands to query additional status as well as control the state of a DS512 connected SDM.

To the existing mapci screen, small modifications are being added to support an OC3 connected CBM.

From the customer's perspective, there is little visual difference between the two supported environments. The differences are as follows:

- Only 2 links are supported to a CBM.
- The platform, locate, querysdm status, querysdm config, and querysdm loads commands are not supported on a CBM.
- The querysdm flt command will only display core side faults for a CBM.
- A new field is visible as long as there is heartbeating with the CBM which presents the overall application status of the CBM. i.e."Applications started" and "Applications stopped".

Accessing path: appl:SDM

Access to directory or MAP level and return to CI

mapci;mtc;appl;sdm

Command: QuerySDM

Command type: Listed MENU

Command target: All

Command availability: RES

Command description

This is an existing command to query information concerning the SDM.

The command will be missing parameters when CBM connected and will only return Core side faults on a CBM.

Command syntax

QuerySDM command parameters and variables

platform	Parameters and variables
sdm	QuerySDM: Query information about the SDM. Parms: [<QuerySDM Option> {FLT, LOADS, STATUS, CONFIG}]

QuerySDM command parameters and variables

platform	Parameters and variables
cbm	QuerySDM: Query information about the SDM. Parms: [<QuerySDM Option> {FLT}]

Qualifications and warnings

No change

Responses

No change in response

Command: Locate

Command type: Listed MENU

Command target: All

Command availability: RES

Command description

Displays the card location of all cards on an SDM FX.\

On a CBM, this command is not supported.

Command syntax

The locate command has no parameters.

Qualifications and warnings

No Change

Responses

<response>

The response for a CBM will be:

Locate command is not supported for shelf pec NTRX51LS.

Command: rebootsdm

Command type: Unlisted MENU

Command target: All

Command availability: RES

Command description

Sends a message to the SDM instructing it to reboot. This command is not supported on a CBM.

Command syntax

No parameters

Qualifications and warnings

no change

Responses**<response>**

The response for a CBM will be:

Locate command is not supported for shelf pec NTRX51LS.

Command: haltsdm

Command type: Unlisted MENU

Command target: All

Command availability: RES

Command description

Sends a message to the SDM instructing it to halt. This command is not supported on a CBM.

Command syntax

No parameters

Qualifications and warnings

No change

Responses**<response>**

The response for a CBM will be:

Locate command is not supported for shelf pec NTRX51LS.

Security

Not applicable

Product = CS 2000

A00005192--CBM 800 OC3 BRISC connectivity and OC3 node and link maintenance (Succession on DMS)

Functional Description

Description

This feature provides OC3 connectivity between a CBM 800 and the MS of a BRISC or XA-Core. Physical connectivity consists of two OC3 fibers connected between two ATM interface cards on the Solaris Netra-240 and two NTL9X63 paddleboards, one on each MS.

This feature provides the following software components:

- CBM 800 MTS/IP/FTS driver
- CBM 800 link maintenance
- CBM 800 node maintenance

The MTS/IP/FTS driver provides an MTS socket and IP socket interface to allow CBM 800 software components to send and receive MTS and IP messages to and from core software components.

CBM 800 link maintenance sets the conditions of the two OC3 links displayed at the Core level (figure 2) of the cbmmtc UI. Link conditions are set in response to node state change commands invoked from the SDM level of MAPCI (as seen in the following figures) and port / card state changes invoked from the MS Card level of MAPCI. The following table gives the MAPCI node state and the cbmmtc link conditions for various mtce actions.

MAPCI SDM Level

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
AMDI	.	1IOCOS	.	2 SPM	3 RS	.	29CCd	1 Maj	SDM
C		M		*C*	*C*		*C*	M	M
SDM		OAMAP	ATMFW	SDM	SPMCP	SWMTC	SDMBIL	PKT	TOPSIP
0 Quit		.	.	ISTb	.	.	.	.	.
2									
3		SDM 0	ISTb	Links_OOS:	.				
4									
5 Trnsl									
6									
7 Bsy	SDM:								
8 RTS									
9 Offl									
10									
11									
12									
13									
14 QuerySDM									
15 Locate									
16									
17									
18 Platform									
admin									
Time 15:57	>								

cbmmtc Core Level

CBM	MATE	NET	APPL	Sys	HW	CLLI: SNM2
IsTb	UnEq	.	.	.	M	Host: pcarylrr
M						


```

Core
0 Quit
2 Core
3 # Communication Path State Core Address Node Address
4 1 VIA OC3 . 192.168.101.196 192.168.101.101
5 link 0: Open
6 link 1: Open
7
8
9 Note: link conditions are:
10 - Closed
11 - MTC_Open
12 - Open
13
14 QueryCBM
15
16
17 Help
18 refresh
root
Time 13:43 >

```

Node State and Link Conditions

Mtce Action	Node State	Link 0 Condition	Link 1 Condition
Offline node	Offl	Closed	Closed
Busy node	ManB	Mtc-open	Mtc-open
RTS node	InSv / ISTb	Open	Open
Busy link 0	InSv / ISTb	Closed	Open
Busy link 1	InSv / ISTb	Open	Closed
Busy all links when node state InSv	SysB (NA)	Closed	Closed
Busy all links when node state ManB	ManB (NA)	Closed	Closed
Faults on both links	SysB (NA)	Closed	Closed

The CBM node state in the banner of the second figure may **not** be the same as the SDM node state in the first figure due to the fact that the two node states are different data points. The CBM alarm state in the banner of the second figure will match the SDM alarm state in the first figure when the CBM 800 is in-service.

CBM 800 node maintenance sets the Core Heartbeat State at the Net level of the cbmmtc UI (see the following figure). The heartbeat state will be InSv if at least one of the OC3 links is in a mtc-open or open condition. If faults are raised on both links, the link conditions will change to closed and the heartbeat state will change to SysB. The NET alarm in the banner will also change to SysB.

If an ATM card alarm is raised, the HW alarm in the banner will indicate a HW problem. The ATM HW alarm can be queried from the HW level of the cbmmtc UI.

CBM 800 link mtce generates cust logs for link condition changes and crossed links.

```

CBM Net Connectivity Level
  CBM  MATE  NET  APPL  SYS  HW  CLLI: SNM2
  IstB SysB  .    .    .    .    Host: pcarylrr
  M     M
Net
0 Quit
2 Core
3
4 Logs
5
6 NTP
7
8
9
10
11
12
13
14 QueryCBM
15
16
17 Help
18 refresh
root
Time 13:43 >

```

Hardware Requirements or Dependencies

None

Software Requirements or Dependencies

None

Limitations and restrictions

None

Interactions

This feature interacts with the following features:

- A00005337 CBM 800 OC3 BRISC Paddleboard Connectivity
 - provides datafilling of an NTL9X63 paddleboard in a non-cmic slot of a Supernode or SNSE MS shelf.
- A00005190 CBM 800 OC3 Node and Link Maintenance
 - provides core side node and link maintenance components
- A00002822 CBM User Interface Manager
 - provides user interface manager for CBM 800 and CBM 850

Applicable customer facing sections

Fault Management

Logs

___X___

Alarms	__X__
Configuration	
Data Schema	__NA__
User Interface	__NA__
Element Management	__NA__
Security	__NA__
Service Order	__NA__
Office Parameters	__NA__
Accounting (includes AMA billing)	__NA__
Performance (includes operational measurements)	__NA__

Glossary

Term	Description
CBM	Core and Billing Manager on SSPFS platform
CBM 800	OC3 connected simplex CBM
CBM 850	IP connected high availability CBM
SSPFS	Succession Solaris Platform Foundation Software

Fault Management for A00005192

Fault management strategy

Unchanged

Fault management tools and utilities

Unchanged

Link Condition Change Log

Explanation

Log Title: SDM633

Name: SDM LINK CONDITION CHANGE

Description: CBM custlog log to indicate a change in the condition of a CBM link.

Event type: Info

Format

```
SDM633 NONE INFO SDM LINK CONDITION CHANGE
      Link: Domain <domain num> Port <port num>
      From: <previous link condition>
      To: <new link condition>

SDM633 NONE INFO SDM LINK CONDITION CHANGE
      Link: Domain 0 Port 0
      From: closed
      To: mtc-open
```

Field descriptions

Field	Value	Description
Link: Domain	0 or 1	CBM domain number
Link: Port	0	CBM port number
From:	closed, mtc-open, open	previous link condition
To:	closed, mtc-open, open	new link condition

Action

None.

Associated Operational Measurements or Performance Measurements

None

Core Heartbeat Alarm Logs

Associated alarm message: No heartbeat response received.

Severity: Major

Condition: response to CBM 800 heartbeat not received from core.

Action: Check for link faults at cbmmtc HW level. Check for closed link conditions at cbmmtc core level.

Log Title: SDM336 MINOR, SDM636 NONE

Examples

```
SDM336 MAJOR Alarm raised or updated
Heartbeat alarm
TimeStamp: Tue Apr 27 12:52:52 2004
ComponentID: CLASS=NET;NETTYPE=CORE
```

Category: Communications
Probable Cause: communicationsProtocolError
Specific Problem: No heartbeat response received.

SDM636 MAJOR Alarm raised or updated
Heartbeat alarm
TimeStamp: Tue Apr 27 15:38:12 2004
ComponentID: CLASS=NET;NETTYPE=CORE
Category: Communications
Probable Cause: noProbableCause
Specific Problem: Heartbeat response received.

Crossed Link Alarm Logs

Associated alarm message: Crossed Link: link 0 (domain 0 port 0) crossed with link 0 (domain 0 port 1)

Severity: Major

Condition: two link connections are physically crossed.

Action: Fix the crossed link connections.

Log Title: SDM314 MAJOR, SDM614 NONE

Examples:

Alarm Raised Log:

SDM314 MAJOR Alarm raised or updated.
Major Crossed Link: link 0 (domain 0 port 0) crossed with link 1 (domain 0 port 1)
TimeStamp: Mon Mar 29 17:47:26 2004
ComponentID: CLASS=HW;HWTYPE=CROSS_LINK_0
Category: Communications
Probable Cause: configurationOrCustomizationError
Specific Problem:

Alarm Cleared Log:

SDM614 NONE Alarm raised or updated.
Cleared Crossed Link: link 0 (domain 0 port 0) crossed with link 1 (domain 0 port 1)
TimeStamp: Mon Mar 29 17:47:26 2004
ComponentID: CLASS=HW;HWTYPE=CROSS_LINK_0
Category: Communications
Probable Cause: noProbableCause

Specific Problem:

OC3 Card Fault Alarm

Associated alarm message: OC3 Card Fault: [receive/transmit] fault on link <num> (domain <num> port <num>)

Severity: Major

Condition: signal on receive/transmit fibre to OC3 card is faulty or not present.

Action: check receive/transmit fibre connection.

Log Title: SDM334 MAJOR, SDM634 NONE

Examples:

Alarm Raised Log:

SDM334 MAJOR Alarm raised or updated.
Major OC3 Card Fault: receive fault on link 0 (domain 0 port 0)
TimeStamp: Mon Mar 29 20:07:21 2004
ComponentID: CLASS=HW;HWTYPE=OC3_FAULT_0
Category: Communications
Probable Cause: equipmentMalfunction
Specific Problem:

Alarm Cleared Log:

SDM634 NONE Alarm raised or updated.
Cleared OC3 Card Fault: receive fault on link 0 (domain 0 port 0)
TimeStamp: Mon Mar 29 19:01:10 2004
ComponentID: CLASS=HW;HWTYPE=OC3_FAULT_0
Category: Communications
Probable Cause: noProbableCause
Specific Problem:

Link Fault Alarm

Associated alarm message: Link Fault: <fault description> on link <num> (domain <num> port <num>)

Severity: Minor

Condition: diagnostics indicate minor link fault

Action: Report the full text of the alarm to the support group.

Log Title: SDM335 MINOR, SDM635 NONE

Examples:Alarm Raised Log:

SDM335 MINOR Alarm raised or updated.
Minor Link Fault: Bad Incoming CRCs on link 0 (domain 0 port 0)
TimeStamp: Mon Mar 29 19:47:06 2004
ComponentID: CLASS=HW;HWTYPE=LINK_FAULT_0
Category: Communications
Probable Cause: equipmentMalfunction
Specific Problem:

Alarm Cleared Log:

SDM635 NONE Alarm raised or updated.
Cleared Link Fault: Bad Incoming CRCs on link 0 (domain 0 port 0)
TimeStamp: Mon Mar 29 19:47:06 2004
ComponentID: CLASS=HW;HWTYPE=LINK_FAULT_0
Category: Communications
Probable Cause: noProbableCause
Specific Problem:

Related documentation

NA

Product = CS 2000**A00005193 -- 9+1 Performance Measurements Tools Support
(Succession on DMS)*****Functional Description***

This CSP20 feature implements changes required to support the XA-Core 9+1 configuration. Specifically, this feature will allow a Rated Power of 9.

Hardware Requirements or Dependencies

N/A

Software Requirements or Dependencies

N/A

Limitations and restrictions

None

Interactions

For releases prior to this feature, the largest value allowed for the office parm Rated_Power in table OFCENG is 7. With this feature, users are able to modify the value of Rated_Power up to a maximum of 9.

Applicable customer facing sections**Fault Management**

Logs	N/A

Alarms	N/A

Configuration

Data Schema	N/A

User Interface	N/A

Element Management	N/A

Security	N/A

Service Order	N/A

Office Parameters	X

Accounting (includes AMA billing)	N/A

Performance (includes operational measurements)	N/A

Configuration for A00005193**Hardware and Software Requirements**

N/A

Initial Configuration

N/A

Office/Subnet parameters (OP/SP) (CM & SESM)**New/modified office/subnet parameters**

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
OFCENG	RATED_POWER	CHANGED	CM

Parameter information**RATED_POWER****Functional description**

This parameter defines the number of PEs engineered in the switch. The Speedometer uses the value of this parameter to calculate the capacity prediction for the switch.

Provisioning rules

N/A

Range information**Range Information**

Minimum	Maximum	Default
1	9	3

Activation

N/A

Dependencies

N/A

Consequences

N/A

Verification

To verify, users can modify and display the value of RATED_POWER on table OFCENG via table control.

Memory requirements

No memory impact.

Parameter release history update

N/A

Upgrade Impact

N/A

Data schema (DS) (CM, MIBS, RDB)

N/A

Service Orders (SO) (CM & SESM)

N/A

Software optionality control (SOC)

N/A

Element Management

N/A

Command interface changes

N/A

Security

N/A

Configuration Walkthrough

N/A

Product = CS 2000**A00005363--CAIN and CDR Support for GNS Personal Toll Free Service (Succession on DMS)*****Functional Description*****Description**

Additional information is needed that is not currently collected and presented in CDR records. This information will be made available in new CDR fields, that are used by the Flexible CDR capability. Some of this information comes from new CAIN message processing. The Flexible CDR capability is controlled by the existing SOC UBFR0001.

The processing of this new information is controlled by a new SOC CAIN0202 - CAIN FlexCDR Enhancements.

The new CAIN message processing consists of:

1. Support for a new CAIN parameter, AMABusinessCustomerId in some incoming messages.
2. Support for a digits id (300) for an existing CAIN parameter, AMADigitsDialedWC.
3. Support for recording all the digits for a currently supported digits id (301) for the existing CAIN parameter AMADigitsDialedWC
4. Support for retaining the first occurrence of an existing CAIN parameter, AMASlpID. Currently, only the last occurrence of this parameter is retained.
5. Support for 4 new parameters in the CDRTMPLT table: SLPID1ST, BUSCSTID, DGI300 and DGI301. This feature does not create a new predefined template. The customer must either modify their existing template or create a new template which includes the 4new parameters.

Functional Overview

CAIN: AMABusinessCustomerId

Prior to this feature, the AMABusinessCustomerId parameter was not supported by the DMS-250. This feature provides support for this parameter, including enhancements to the CAIN simulator to generate this parameter in the messages listed below. The value for this parameter is 11 digits.

The call processing support consists of parsing the incoming parameter, and making the data available for use by the billing component - it will not affect call processing (either by its value, presence or absence) in any other way. Only the last occurrence of this parameter will be retained for use by the billing component. This parameter will be supported in the DMS-250 being received in the following messages from an SCP:

- Analyze_Route
- Disconnect
- Send_To_Resource

This includes display of this parameter in the VAMP log.

CAIN: AMADigitsDialedWC

Prior to this feature, the AMADigitsDialedWC was not supported for a digits id of 300. This feature adds this support, which consists of parsing the incoming parameter for this digits id, and making the data available for use by the billing component. Only the last occurrence of a AMADigitsDialedWC with a digits id of 300 will be retained for use by the billing component (as is the case today with other such AMADigitsDialedWC digits id). The maximum

supported length for the value of this digits id is 24 digits (with the three digit of the digits id makes a maximum total length of 27 digits).

The AMADigitsDialedWC parameter is currently supported by the DMS-250 for various incoming messages from the SCP, and this activity does not alter that support - that is to say that the DMS-250 will support receiving a AMADigitsDialedWC parameter with a digits id of 300 in all cases that reception of a AMADigitsDialedWC parameter is valid. However, the functionality added by this feature (recording the value received in a AMADigitsDialedWC parameter with digits id = 300) will only be supported for the following messages:

- Analyze_Route
- Disconnect
- Send_To_Resource

This includes display of this new digit id in the VAMP log.

CAIN: AMADigitsDialedWC - 301

Prior to this feature, only the first four digits in the AMADigitsDialedWC parameter with digits id = 301 were recorded (in field PINDIGS). This feature records the entire parameter (the 3 digits of the digits id plus 24 digits) in the new field DGI301. When this feature is active, the AMADigitsDialedWC parameter with digits id = 301 is no longer recorded in field PINDIGS, but only in field DGI301.

CAIN: AMASlpId

Prior to this feature, only the last AMASlpId parameter for a call received in a message from the SCP was retained for use by the billing component. This feature adds support for also retaining the first AMASlpId parameter for a call received in a message. This support applies to all messages from the SCP that contain an AMASlpId parameter. Note that in the case that there is only one such AMASlpId parameter received during a call, the first and last AMASlpId values will be the same. The AMASlpId parameter is currently supported by the DMS-250 for various incoming messages from the SCP, and this activity does not alter that support. The functionality added by this feature (retaining the first AMASlpId) will however only be supported for the following messages:

- Analyze_Route
- Disconnect
- Send_To_Resource

CAIN: Simulator changes

To support the changes to the CAIN simulator for the new parameter and AMADigitsDialedWC digits, the following CAIN simulator tables are changed. Table Control Changes.

Table	Desc
CAINRESP	A new parameter, AMABusinessCustomerId, with a value of 11 digits, is supported in the following operation types: - Analyze_Route - Disconnect - Send_To_Resource This new parameter is also supported in the “non-restricted” message (as are all parameters). For the existing parameter AMADIGITS, a new digits type, 300, is supported.
CAINREXT	For the existing parameter AMADIGS, a new digits type, 300, is supported.

CDR: Table changes

To allow the recording of Dialed digits, Customerid and the first received Amaslpid, the following changes are made to the CDRTMPLT table.

Table	Desc
CDRTMPLT	4 new parameters for the FIELDS and REORIGCP sub-fields of table CDRTMPLT are added to record the data collected for the AMADigitsDialedWC, AMABusiness-CustomerId, and AMASlpID CAIN parameters.

Sample datafill for table **CDRTMPLT**:

NAME ACTIVE PRIMARY FIELDS REORIGCP

VZN_FLXCDR Y N (SEQNUM) (CIC) (ORIGTIME) (ORIGDATE)
(ANSTYPE) (TIMECHNG) (ORIGAMPM) (INCINTL) (DISCTIME)
(DISCDATE) (ANISUFF) (DISCAMPM) (INCBILL) (FILL1) (CALLDUR)

(PINDIGS) (ANISP) (INFODIG) (BILLNUM) (ACCTCD) (CLGPTYNO)
 (RLTCDR) (ACCTV) (UNIVACC) (DIALEDNO) (CALLEDNO)
 (OUTPULNO) (FILL4) (ORIGOPRT) (PREDIG) (CNPREDIG) (OPART)
 (TPART) (QUEUED) (FILL3) (FILL3) (FILL4) (RTENO) (NETSEC)
 (OPCHOICE) (COLLTIME) (ADIN) (LNPCHECK) (NUMWBCKT)
 (WBCKTS) (FINSID) (BILLTYPE) (ORIGGRP) (DISCTYPE) (ORIGMEM)
 (PASSTHRU) (TERMGRP) (PRESIND) (TERMMEM) (OSRASSOC)
 (DIGDATA) (FINTKGRP) (TRAP) (COSOVE) (FINTKMEM) (SCPBILL)
 (FILL3) (FILL3) (FILL3) (FILL2) (FILL3) (FILL2) (TRTMTCD)
 (COMPCODE) (CRID) (DNIS) (ORIGPVN) (TERMPVN) (ORIGLRN)
 (PORTEDNO) (CAINCT) (ACG) (DNISNOA) (FILL1) (MLTCOSID)
 (FILL4) (FILL1) (COSINDEX) (FILL2) (CARRSEL) (**SLPID1ST**)
 (**BUSCSTID**) (**DGI300**) (**DGI301**) (FILL8) \$ \$

CDR: New Field Description

The new data captured by this activity will be formatted into the CDR record using the following layout:

Field Name	Bits	CDR Field Description
DGI300	27	Contains the Digit ID "300" followed by the dialed digits which are contained in the SCP message whenever the digits id = 300. This will be performed as described in section 2.3.2.
DGI301	27	Contains the Digit ID "301" followed by the dialed digits which are contained in the SCP message whenever the digits id = 301. This will be performed as described in section 2.3.3.
BUSCSTID	11	Contains the customer id which is received in the SCP message. This field is populated based on the description in section 2.3.1.
SLPID1ST	9	Contains the first AMASLPID received. This field is populated as described in section 2.3.4.

Sample CDR Log (new fields in bold):

```

RTPE_B115BH   CDR273 FEB04 21:44:14 4200 INFO CDR_CALL_ENTRY
250X15AY      CDR273 FEB09 13:44:20 0800 INFO CDR_CALL_ENTRY

RECCD      F0          TEMPLID      016
ACTIDX      6          TOOLGEN      Y
USEEDIT     N          VARLNGTH     N
SEQNUM      00001      CIC          5676
ORIGTIME    34992      ORIGDATE    035
ANSTYPE     03        TIMECHNG     N
ORIGAMPM    1          INCINTL     N
DISCTIME    35052      DISCDATE    035
ANISUFF     1          DISCAMPM    1
INCBILL     1          CALLDUR     00013107

```

PINDIGS	6987	ANISP	5124599628
INFODIG	1	BILLNUM	50854321499779000001234
ACCTCD	802000012345	CLGPTYNO	214684552900000
RLTCDR	Y	ACCTV	3
UNIVACC	8007654321	DIALEDNO	508345214997799
CALLEDNO	508543214997790	OUTPULNO	508345129479970
ORIGOPRT	501	PREDIG	1
CNPREDIG	1	OPART	511
TPART	31	QUEUED	Y
OPCHOICE	232	COLLTIME	060
ADIN	12	LNPCHECK	7
NUMWBCKT	16	WBCKTS	10000000 10000000 00000000
FINSID	111	BILLTYPE	35
ORIGGRP	0353	DISCTYPE	1
ORIGMEM	0101	PASSTHRU	2
TERMGRP	0355	PRESIND	1
TERMMEM	0101	OSRASSOC	N
DIGDATA	Y	FINTKGRP	09999
TRAP	N	COSOVE	Y
FINTKMEM	62843	SCPBILL	FE17700B
TRTMTCD	010	COMPCODE	3
CRID	684149400	DNIS	214684149400000
ORIGPVN	214684149400000	TERMPVN	214684466200000
ORIGLRN	2146841494	PORTEDNO	2146844662
CAINCT	1	ACG	Y
DNISNOA	103	MLTCOSID	0001
COSINDEX	0001	CARRSEL	02
SLPID1ST	032401234	BUSCSTID	02532401234
DGI300	300997799912345678901234567	DGI301	301997799912345678901234567

Software Optionality Control

The actual recording of the four items, DGI300,DGI301, BUSCSTID, and SLPID1ST is controlled by a new SOC, CAIN0202 - CAIN FlexCDR Enhancements.

Hardware Requirements or Dependencies

No new hardware dependencies are introduced by these features.

Software Requirements or Dependencies

No new customer software or firmware dependencies are introduced by these features.

Limitations and restrictions

None

Interactions

None.

Applicable customer facing sections

Fault Management

Logs

___X___

Alarms

___na___

Configuration

Data Schema	__X__
User Interface	__na__
Element Management	__na__
Security	__na__
Service Order	__na__
Office Parameters	__na__

Accounting (includes AMA billing) __X__

Performance (includes operational measurements) __na__

Realtime __X__

Engineering Information __X__

Glossary

Term	Description
AMA	Automatic Message Accounting
CAIN	Carrier AIN
CDR	Call Detail Recording
SCP	Service Control Point
SOC	Software Optionality Control

Fault Management for A00005363**Fault management strategy**

Logs are used for fault management.

Fault management tools and utilities

The VPTRACE tool is used to turn on VAMP logs.

Logs**VAMP901**

The VAMP901 log is enhanced for the following two purposes:

- to display the new Business Customer ID parameter, and

- the AMA Digits parameter has an additional value possible in the Digits Type subfield (300)

Explanation

Log Title: VAMP901

Name: Variable AIN Message Platform 901 Log

Description: The VAMP901 log report is generated when a message is received via the VAMP framework. The VAMP framework captures the messages only when message logging has been enabled with the VPTRACE tool. For more detailed information, refer to NTP 297-2621-370--UCS DMS-250 NetworkBuilder Application Guide. This log is intended for lab use only and is not suitable for live switches due to the number and size of reports.

Event type: Info

Format

The new Business Customer ID parameter appears in the VAMP901 log with the other parameters. Its display format is shown below.

BUSCSTID: <string of digits>

Field descriptions

The new field AMABUSCSTID consists of a string of digits

Field	Value	Description
AMABUSCSTID	Vector of 11 digits	Digits

Field name: AMABUSCSTID

Field optionality: optional, variable

Type: Alphanumeric

Size: 7 bytes

Value(s): See field descriptions above

Descriptions: See field descriptions above

NTP table reference: N/A

Action

None

Associated Operational Measurements or Performance Measurements

None

Additional information

None

Related documentation

None

Configuration for A00005363**Hardware and Software Requirements**

No new hardware or software requirements are created by this activity.

Initial Configuration

Standard configuration applies

Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable

Data schema (DS) (CM, MIBS, RDB)**New/modified tables, MIBs, or Database Schema**

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
CAINRESP	changed	unchanged
CAINREXT	changed	unchanged
CDRTMPLT	changed	unchanged

Table/MIB/Remote Database Schema information**Name: CAINRESP**

CAIN Simulator Response

Functional description

This feature adds a new parameter, AMABusinessCustomerId, to the operation types:

- Analyze_Route
- Disconnect
- Send_To_Resource

This feature also add a new digits id type (300) to the AMADIGS parameter.

Usage sequence and implications (CM Only)

The current table datafill order is unchanged.

Size

Unchanged

Fields/OIDs

The following table lists the changed fields/OIDs for CAINRESP

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CAIN_PARAMETER_VALUE	changed	subfield	AMABUSCUSTID	The range of this subfield is expanded to include the AMABusinessCustomerId parameter.
AMADIGSTYPE	changed	subfield	001, 002, 003, 004, 005, 006, 011, 012, 300, 301, 302, 303, 304, 305, 999	The range of this subfield is expanded to include the value of 300

Datafill example

The following example shows sample datafill for table CAINRESP.

TABLE: CAINRESP

RESPKEY

DATAAREA

RESP123CR 0 RESP INVL ANALYZE_ROUTE (CLDNO NATL ISDN 2149201234) (AMABUSCUSTID
01234567890) (AMADIGS 300 9876543210) \$ \$ \$**Table release history update**

Not applicable.

Supplementary information

None.

Translation verification other tools

None.

Name: CAINREXT

CAIN Simulator Response Extension Parameters

Functional description

This feature adds a new digits id type (300) to the AMADIGS parameter.

Usage sequence and implications (CM Only)

The current table datafill order is unchanged.

Size

Unchanged

Fields/OIDs

The following table lists the changed fields/OIDs for CAINRESP

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
AMA_DIGS _TYPE	changed	subfield	001, 002, 003, 004, 005, 006 , 011, 012, 300, 301, 302, 303, 304, 305, 999	The range of this subfield is expanded to include the value of 300

Datafill example

The following example shows sample datafill for table CAINREXT.

TABLE: CAINREXT

REXTKEY

DATAAREA

REXT123

NT (AMA_BUS_CUSTID 01234567890) (AMADIGS 300 9876543210) \$ \$ \$

Table release history update

Not applicable.

Supplementary information

None.

Translation verification other tools

None.

Name: CDRTMPLT

CDR template table

Functional description

This feature adds 4 new parameters to the FIELDS and REORIGCP subfields of table CDRTMPLT.

Usage sequence and implications (CM Only)

The current table datafill order is unchanged.

Size

Unchanged

Fields/OIDs

The following table lists the changed fields/OIDs for CAINRESP

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
FIELDS	changed	subfield	BUSCSTID, SLPID1ST, DGI300, DGI301.	The range of this subfield is expanded to include the BUSCSTID, SLPID1ST, DGI300 and DGI301 parameters.
REORIGCP	changed	subfield	BUSCSTID, SLPID1ST, DGI300, DGI301.	The range of this subfield is expanded to include the BUSCSTID, SLPID1ST, DGI300 and DGI301 parameters.

Datafill example

The following example shows sample datafill for table CDRTMPLT.

TABLE: CDRTMPLT

NAME ACTIVE PRIMARY FIELDS REORIGCP

```
-----
VZN_FLXCDR Y N (SEQNUM) (CIC) (ORIGTIME) (ORIGDATE)
(ANSTYPE) (TIMECHNG) (ORIGAMPM) (INCINTL) (DISCTIME)
(DISCDATE) (ANISUFF) (DISCAMPM) (INCBILL) (FILL1) (CALLDUR)
(PINDIGS) (ANISP) (INFODIG) (BILLNUM) (ACCTCD) (CLGPITYNO)
(RLTCDR) (ACCTV) (UNIVACC) (DIALEDNO) (CALLEDNO)
(OUTPULNO) (FILL4) (ORIGOPRT) (PREDIG) (CNPREDIG) (OPART)
(TPART) (QUEUED) (FILL3) (FILL3) (FILL4) (RTENO) (NETSEC)
(OPCHOICE) (COLLTIME) (ADIN) (LNPCKECK) (NUMWBCKT)
(WBCKTS) (FINSID) (BILLTYPE) (ORIGGRP) (DISCTYPE) (ORIGMEM)
```


(PASSTHRU) (TERMGRP) (PRESIND) (TERMMEM) (OSRASSOC)
(DIGDATA) (FINTKGRP) (TRAP) (COSOVE) (FINTKMEM) (SCPBILL)
(FILL3) (FILL3) (FILL3) (FILL2) (FILL3) (FILL2) (TRTMTCD)
(COMPCODE) (CRID) (DNIS) (ORIGPVN) (TERMPVN) (ORIGLRN)
(PORTEDNO) (CAINCT) (ACG) (DNISNOA) (FILL1) (MLTCOSID)
(FILL4) (FILL1) (COSINDEX) (FILL2) (CARRSEL) (SLPID1ST)
(BUSCSTID) (DGI300) (DGI301) (FILL8) \$ \$

Table release history update

Not applicable.

Supplementary information

None.

Translation verification other tools

None.

Service Orders (SO) (CM & SESM)

Not applicable

Software optionality control (SOC)

The CAIN0202 SOC is added by this feature

SOC option name:	CAIN0202
SOC option title:	CAIN FlexCDR Enhancements
SOC option control type:	state
New SOC option?	Yes
SOC option order code	CAIN0202
Option defined in DRU:	UCS
Affected products:	DMS-250

Element Management

Not Applicable.

Command interface changes

Not Applicable.

Security

Not Applicable.

Configuration Walkthrough

Not applicable

Product = CS 2000

A00005268 -- SBA: Multi-volume Support for Core Backup (Succession on DMS)

Description

Architectural Description.

Currently 2 volumes can be assigned on a per stream for SBA on the CM as backup storage. These volumes are used to store the billing records whenever the stream goes to backup mode on the CM. This configuration does not meet the backup storage requirement for some of the markets.

This feature will focus on increasing the backup storage capacity available for SBA on the CM from current 2 volumes allotted per stream to 69 volumes or the maximum supported by the underlying hardware whichever is less per stream.

High Level Description.

As part of this feature new MAPCI commands will be introduced. The new CI commands will allow user to add / remove more than one volume at a time per stream.

This feature is core only scope and affects TL layer.

Hardware requirements

Under investigation.

Limitations and restrictions

None

Interactions

None.

Logs (LG)

The following logs have been changed as part of this activity.

SDMB531 :

The conf log (SDMB531) has been changed. Following shows a sample output of the current SDMB531 log format.

3PC_TDM07CD SDMB531 MAY06 09:43:32 0500 INFO SDM BILLING
CONFIG

STREAM= SBA0:

NEWVOLUMES =

SD00AMA1	SD00AMA2	SD00AMA3	SD00AMA4
SD00AMA5			
SD00AMA6	SD00AMA7	SD00AMA8	SD00AMA9
SD00AMA10			
SD00AMA11	SD00AMA12	SD00AMA13	SD00AMA14
SD00AMA15			
SD00AMA16	SD00AMA17	SD00AMA18	SD00AMA19
SD00AMA20			
SD00AMA21	SD00AMA22	SD00AMA23	SD00SNS
SD00AMA			
SD01AMA1	SD01AMA2	SD01AMA3	SD01AMA4
SD01AMA5			
SD01AMA6	SD01AMA7	SD01AMA8	SD01AMA9
SD01AMA10			
SD01AMA11	SD01AMA12	SD01AMA13	SD01AMA14
SD01AMA15			

OLDVOLUMES =

SD00AMA1	SD00AMA2	SD00AMA3	SD00AMA4
SD00AMA5			
SD00AMA6	SD00AMA7	SD00AMA8	SD00AMA9
SD00AMA10			

SD00AMA11 SD00AMA12 SD00AMA13 SD00AMA14
SD00AMA15

SD00AMA16 SD00AMA17 SD00AMA18 SD00AMA19
SD00AMA20

SD00AMA21 SD00AMA22 SD00AMA23 SD00SNS
SD00AMA

SD01AMA1 SD01AMA2 SD01AMA3 SD01AMA4
SD01AMA5

SD01AMA6 SD01AMA7 SD01AMA8 SD01AMA9
SD01AMA10

SD01AMA11 SD01AMA12 SD01AMA13 SD01AMA14
SD01AMA15

SD01AMA16 SD01AMA17 SD01AMA18 SD01AMA19
SD01AMA20

SDMB820

The logs raised when any of BAK** alarms are raised have also been changed.
Following is a sample output of the log generated.

```
3PC_TDM07CD *** SDMB820 MAY06 11:20:51 2876   SDM BILLING
BACKUP
STREAM= SBA0: WARNING, 50% or less of Backup space is free.
VOLUMES=
SD00AMA13 SD00AMA15 SD01AMA11 SD01AMA12
SD01AMA13
```

Data schema (DS)

New/modified tables

New or modified tables

Table name	NEW, CHANGED or DELETED	Table Control (NEW/OLD/UNCHANGED)
SDMBILL	Changed	Unchanged

Office parameters (OP)

None.

Service orders (SO)

No change.

Alarms (AL)

No change.

Command interface (CI)**New/modified commands****Table 1 New or modified commands**

Command name	NEW, CHANGED OR DELETED	New name (if renamed)	Directory/MAP level name	MENU/NON-MENU /HIDDEN
CONF	changed		SDMBIL	Menu
ADDVOL	new		SDMBIL	Menu
REMOVOL	new		SDMBIL	Menu

Operational measurements (OM)

No change.

AMA/Billing information (AM)

No change.

Software optionality control (SOC)

No change.

Glossary

Term	Description
New term	definition
SBA	Supernode Billing Application
SDM	Supernode Data Manager
CM	Computing Module

Product = CS 2000

A00005485 -- SAM21 Platform Installation on SSPFS (PT-IP, UA-IP, IAC, IAW)

Excerpts from the Design Description

Purpose

To allow the installation of the SAM21 Platform Package from CDROM on to the SSPFS box.

In SN07, the new SSPFS box does not contain a DAT Tape Drive but only a CD/DVD ROM drive. Therefore, the Platform Installation tool will be further enhanced to allow the user to extract the SAM21 Platform Package from CD where it is stored in a "RPM" format.

What this means is that this tool will now be used in ALL Solutions to allow the user to install the SAM21 Platform Loads using a DAT tape, to be backward compatible, and CDROM moving forward. The CDROM will be of ISO format containing the following files:

- SAM21 Platform Fileset (This is used for installation on the AIX SDM)
- SAM21 Platform TAR file
- SAM21 Platform RPM file

If the solution contains an AIX SDM, the user will be prompted for a roo passwd for the SDM so that the fileset will be Secure Copied onto the SDM.

Note: The implementation of this activity will also satisfy the problem described by CR.Q00808578 -

This tool will be further expanded to allow the user to install the Call Agent and Message Controller Linux loads from CDROM. It must be noted that the SOS images will not be extracted from CD using this tool.

Product = CS 2000

A00005734 -- Multiple Time Zone (MTZ) support for CICM lines (IAW)

Functional Description

Description

CICM lines can exist in multiple time zones as there is no geographical limitation that the call server and the agents should co-exist in the same time zone.

With the existing implementation line features, billing, logs etc. work on the switch time for all users irrespective of their local times.

This activity provides Multiple Time Zone (will be called by abbreviation MTZ henceforth) by providing the ability to store the local time of the user on the switch so that the features can be activated in terms of the local time of the user.

Activity A59038784 provided the same functionality for subscriber visible services for IBN and RES sets.

This activity extends the support to CICM KSET lines.

The services addressed by this feature are

- WUCR (Wakeup Call Request)
- ARDDN (Automatic Recall Directory Number)
- QTD (Query Time and Date)

No changes are made to Logs and Billing records.

This new functionality reuses existing table MULTITM which can be datafilled with different time zones along with Day Light Savings if any. The items that can be entered in table MULTITM are shown in the following figure.

Items in table MULTITM (Range of MULTITM)

ENTRY NAME	ENTRY TYPE
-----	-----
MTZNAME	MULTITM_KEY
TMSENSE	MODIFY
MINUTES	MTZMINSTYPE
DST	YES_NO
DSTSENSE	MODIFY
DSTMINS	DSTMINSTYPE
STRTYEAR	MTZYEARTYPE
STRTMON	MONTHS
STRTDAY	DAYS
STRTHOUR	HOURS
STRTMIN	MINUTES
ENDYEAR	MTZYEARTYPE
ENDMON	MONTHS
ENDDAY	DAYS
ENDHOUR	HOURS
ENDMIN	MINUTES

The following figure shows a sample entry for table MULTITM. It shows that the timezone BERL is offset from the standard by 60 minutes, and that DST of plus 60 minutes begins on March 31st at 0200, and ends on October 27th at 0300. Similarly AZOR is offset with a negative 60 (behind by 60 mins).

There is one pre-registered key in table MULTITM: 'LOC'. This key is used to show when the time local to the CM is applying DST. This is to cover situations such as the USA and the UK, whose DST start times are often one week apart.

Sample entries in Table MULTITM

	MTZName	TMSense	Minutes	DST	DSTSense	DSTmins	STRTYear	STRTMon	STRTDAY	STRTHour	STRTMIn	ENDYear	ENDMon	ENDDay	ENDHour	ENDMin

LOC	POS	0	N	POS	0	2002	JAN	1	0	0	2002	JAN	1	0	0	

BERL	POS	60	Y	POS	60	2002	MAR	31	2	0	2002	OCT	27	3	0	

AZOR	NEG	60	N	POS	0	2002	JAN	1	0	0	2002	JAN	1	0	0	

This activity introduces a new option 'MTZ' for KSET lines, details about this option are:

- This option is a Set option, can be assigned to any key. (DN key (key 1) or any other vacant key).

- It is 'data feature' option, has one parameter, which is any key in table MULTITM. Table MULTITM is datafilled with different possible timezones. A KSET agent's timezone if different from the switch timezone is configured by associating the corresponding entry in MULTITM through MTZ option

- MTZ option if applied to a Set affects the specified features (QTD, WUCR and ARDDN) on all DN appearances of the set.

- It is 'Code access' feature, does not require a key press to activate the feature. Also there is no explicit activation required, effective once assigned.

- No Lamp be lit by this option

- MTZ option is applicable to only M5216 LCC (It is the only supported KSET LCC on CICM currently)

The following figure shows how to datafill a line with the MTZ option. The subsequent figure shows the qdn and qlen output.

Assigning MTZ option

```
SO:
>ado
SONUMBER:      NOW    2    2 19 PM
>
DN_OR_LEN
>9915022
OPTkey:
>1
OPTION:
>MTZ
SO_MTZ_NAME:
>ber1
OPTKEY:
>$
COMMAND AS ENTERED
ADO NOW 2 2 19 PM 9915022 (1 MTZ LOC)$
ENTER Y TO CONFIRM, N TO REJECT OR E TO eDIT
>Y
```

QDN and QLEN output

```
-----
>qdn 9915022
```

```
DN: 9915022
TYPE: SINGLE PARTY LINE
SNPA: 919 SIG: N/A LNATTIDX: N/A
LINE EQUIPMENT NUMBER: HOST 00 0 15 17
LINE CLASS CODE: M5216 SET
KEY: 1
CUSTGRP: POTSDATA SUBGRP: 0 NCOS: 0 RING: Y
CARDCODE: 6X21AC GND: N PADGRP: PPHON BNV: NL MNO: Y
PM NODE NUMBER : 38
PM TERMINAL NUMBER : 498
DNGRPS OPTIONS:
NETNAME:PUBLIC
NAME: RTPH CO
OPTIONS:
MTZ BERL
```

```
>qlen 9915022
```

```
LEN: HOST 00 0 15 17
TYPE: SINGLE PARTY LINE
SNPA: 919
DIRECTORY NUMBER: 9915022
LINE CLASS CODE: M5216 SET
CUSTGRP: POTSDATA SUBGRP: 0 NCOS: 0 RING: Y
CARDCODE: 6X21AC GND: N PADGRP: PPHON BNV: NL MNO: Y
PM NODE NUMBER : 38
PM TERMINAL NUMBER : 498
DNGRPS OPTIONS:
NETNAME:PUBLIC
NAME: RTPH CO
OPTIONS:
MTZ BERL
  KEY DN
  --- --
  1 DN 9199915022
KEY FEATURE
  --- -----
1      MTZ
```

In this example the Set is configured to belong to BERL timezone. This timezone is 60 mins ahead of the switch time (see figure 2 - BERL tuple).

With above datafills if the CM clock is as below,

Date is THU. 26/FEB/2004 16:45:58 ,

Invoking QTD (Query Time and Date) on the KSET set will display

“Date is THU. 26/FEB/2004 17:45:58”

Hardware Requirements or Dependencies

N/A

Software Requirements or Dependencies

SN07 or equivalent CM load.

Limitations and restrictions

The information in table MULTITM, including time offsets and start and end points for daylight savings time, will have to be entered manually each year. Since it is up to each country or region to set their own DST dates, any routine to automatically generate these dates is in danger of becoming obsolete very quickly. An effort has been made to make the table as human readable as possible, to make the task of entering the data as easy as it can be.

When adding a tuple to table MULTITM, the starting and ending dates of the DST entries can be at most switch year+1. Any entry with a year greater than that value are rejected.

This activity tests MTZ feature only on CICM KSET line though the implementation is in the switch which does not differentiate a CICM line from other lines like MG9K etc...The feature is not restricted to other lines but as a part of this activity the functionality is tested only on CICM and testing on other lines like lines on MG9K are out of scope.

M5216 is the only LCC supported on CICM currently and is the only affected LCC by this activity.

MTZ assigned on a CICM line affects the date and time on the 3 specified features only viz. ARDDN, QTD and WUCR and does not affect the time provided by the CICM gateway for the Inbox, Outbox etc.... on the CICM line.

No changes to billing records or logs for the affected features are included in this activity.

There is no restriction on the number of lines that can have this feature.

Interactions

This feature alters any customer activated feature where the time of day is a factor. Wake Up Call Request is an obvious example, where the user enters the time at which they wish to receive a call to wake them. The full list is:

1. WUCR (Wake Up Call Request)
2. ARDDN (Automatic Recall Dialable Directory Number)
3. QTD (Query Time and date) - pphone only

Applicable customer facing sections

Fault Management

Logs	n/a
Alarms	n/a
Configuration	
Data Schema	n/a
User Interface	n/a
Element Management	n/a
Security	n/a
Service Order	x
Office Parameters	n/a
Accounting (includes AMA billing)	n/a
Performance (includes operational measurements)	n/a

Glossary

Term	Description
ARDDN	Automatic Recall Directory Number
CICM	Centrex IP Client Manager
DST	Daylight Savings Time
MTZ	Multiple Time Zone
QTD	Query Time and Date
WUCR	Wake Up Call Request

Configuration for A00005734

Hardware and Software Requirements

All CM processors (PPC, 68K etc.) and any SN07 or equivalent CM load

Initial Configuration

To configure this feature, you must datafill table MULTITM with any relevant timezones, including local time (during non-DST, this is zero offset from the CM clock. During DST, this is the offset from the CM clock to go back to non-DST)

Any lines that required this feature must have the MTZ option added through SERVORD.

Upgrade Impact

n/a

Data schema (DS) (CM, MIBS, RDB)

None

Service Orders (SO) (CM & SESM)

New line option MTZ

Description

The option MTZ is used on any line that is physically located in a different time zone to the controlling CM. When the user activates other time related features (Such as Wake Up Call Request), the time will be converted to their local time, rather than the CM time.

Example

Example of the MTZ option

```
SO:
>ado
SONUMBER:      NOW      2      2      19      PM
>
DN_OR_LEN
>7205011
OPTkey:
>1
OPTION:
>MTZ
SO_MTZ_NAME:
>loc
OPTKEY:
>$
COMMAND AS ENTERED
ADO NOW 2 2 19 PM 7205011 (1 MTZ LOC)$
ENTER Y TO CONFIRM, N TO REJECT OR E TO eDIT
>Y
```

Option prompts

System prompts for MTZ option

Prompt	Valid input	Description	Areas affected by prompt
TIMEZONE	Keys in table MULTITM		

Assignability

The following functionalities apply to this option:

- set functionality: Yes
- subset functionality: no
- DN functionality: no
- key functionality: no

Option prerequisites

Table MULTITM must have data in it.

Configuration Walkthrough

Datafill table MULTITM with timezone information. Add option MTZ to relevant lines. Feature is activated automatically.

Product = CS2000**A00005758 -- ESUP over Telnet support (Succession on DMS)*****Functional Description***

ESUP, Enhanced SDM Upgrade Procedure, is the recommended upgrade procedure for the SuperNode Data Manager from/to SDM20/CS2E00070.

The Major limitation of ESUP was its restriction on the usage of the Active System console to perform the upgrade. This feature provides the support for performing the ESUP upgrade over remote login sessions (telnet) as well.

This is achieved by the usage of the Open Source third party software 'SCREEN', a full-screen window manager that multiplexes a physical terminal between several processes.

ESUP process is launched with 'SCREEN' support. The usage of 'SCREEN' is transparent to the user.

The framework for a semi-automatic recovery in case of an ESUP failure is also introduced as part of this feature. Semi-automatic recovery here refers to the user-initiated recovery procedure to recover the system from upgrade failures.

Hardware Requirements or Dependencies

No new hardware requirements or dependencies are introduced by this feature.

Software Requirements or Dependencies

Software requirements for downstream system

No new hardware requirements or dependencies are introduced by this feature.

Software requirements for SDM.

Open Source software 'SCREEN' is to be installed on the system.

Limitations and restrictions

'Telnet' is the only remote login supported.

Interactions

No

Applicable customer facing sections

Fault Management

Logs

Alarms

Configuration

Data Schema

User Interface

Element Management

Security

Service Order

Office Parameters

Accounting (includes AMA billing)

Performance (includes operational measurements)

Glossary

Term	Description
SDM	Supernode Data Manager
CBM	Core Billing Manager
OSS	Operations Support System
ESUP	Enhanced SDM Upgrade Procedure



SN07 Feature Deltas

Product = CS 2000

A00005986 -- EM integration with PAM+ proxy (IAW)

Overview

Succession user authentication services are migrating to a single centralized 3rd party server, which provide authentication services to succession management systems via a Pluggable Authentication Module (PAM) on the SSPFS platform. By using PAM, Succession management systems can interact with any pluggable authentication technology of a customers choosing, without having to make any changes to succession management applications. The use of a centralized authorization database via PAM also provides the advantage of having a single account management interface for use by all succession management tools.

This feature integrates the CICM-EM into this wider strategy for user authentication on Succession.

The CICM-EM now interfaces to PAM via the HTTPS PAM+ proxy on SSPFS.

The CICM-EM User Interface requires a username/password login. Prior to this feature, only a single user level was supported – which provided full access to all the provisioning, maintenance and admin functions of the CICM-EM. With the introduction of this feature, the CICM-EM can be configured to access the HTTPS PAM+ proxy, passing it the username and password, and the SSPFS then returns a user authentication level to the CICM-EM, or rejects the username and password if they are not a valid combination. This user authentication level is then used by the CICM-EM to restrict access to functions that are not appropriate for particular user groups.

Detail

Prior to this feature, the username and password supplied when logging into the element manager corresponded to local user accounts on the CICM-EM.

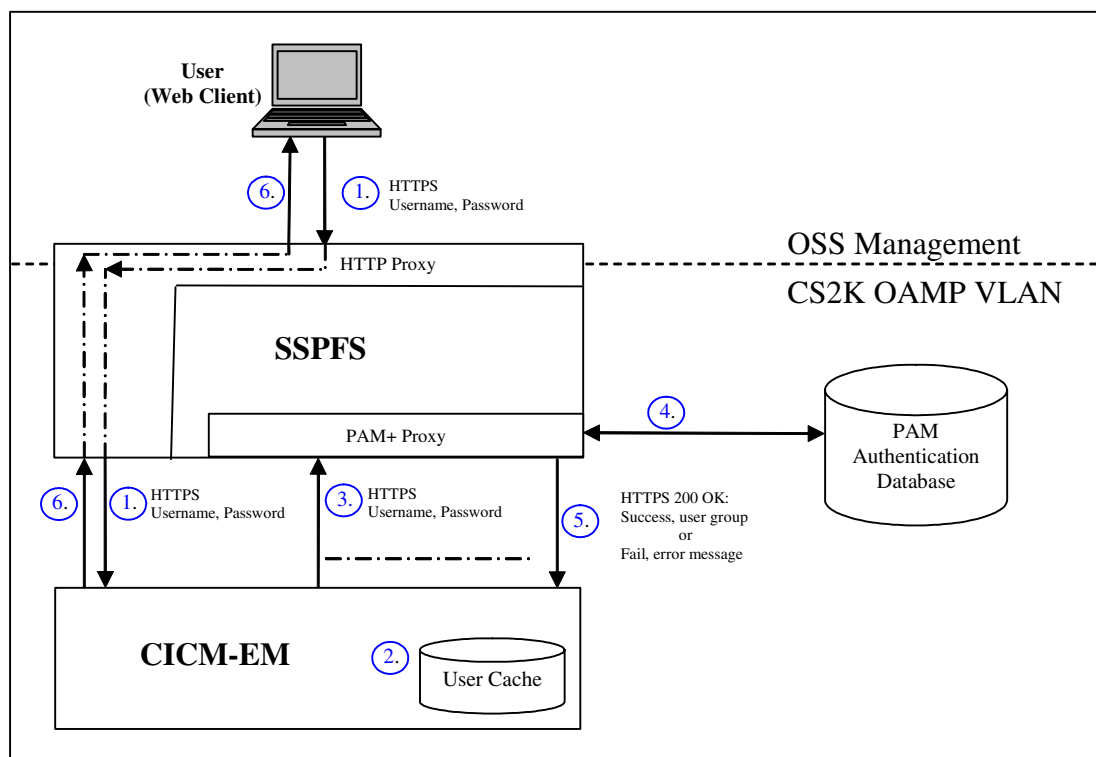
For SN07 Succession deployments, username and password can be configured to be a global Succession account managed on a centralized authentication database, which interfaces to Succession management tools via the PAM+ proxy located on the SSPFS.

Local user account management and user authentication on the CICM-EM is preserved for TDM deployments, where the SSPFS platform is not used. For Succession deployments, a method of local user authentication is also provided for use when connectivity is lost to the SSPFS platform.

User authentication via SSPFS PAM Proxy

The behavior provided by CICM-EM user authentication via the PAM proxy running on the SSPFS, is outlined in the functional behavior diagram below.

Functional Behaviour Diagram: HTTPS PAM+ proxy and CICM-EM integration



- 1 Using a web client, the user attempts to log into the CICM-EM through the HTTP proxy located on the SSPFS. The supplied username and password are for a global Succession user account which is managed on a centralised authentication database. The Web Client sends an HTTPS request to the CICM-EM with the username and password built into the HTTP authentication header.
- 2 The CICM-EM uses the supplied username and password as a key to search a cache of recently authenticated users. Each user entry in the cache contains a corresponding username and password for a temporary local user account assigned to that user. If the user is present in the cache, the mapped local username and password is passed back to the PAM authenticator and we go directly to step 5 (with successful authentication).
- 3 The CICM-EM sends an authentication request to the HTTPS PAM+ proxy located on the SSPFS.
- 4 The PAM+ proxy authenticates the user on a centralised authentication database via PAM.
- 5 If the authentication is successful, the PAM+ proxy responds with a list of succession user groups to which the user belongs. The CICM-EM has a list of pre-defined local user groups that are equivalent to the user groups returned by the PAM proxy. The CICM-EM creates a temporary local user account on the CICM-EM when a response to a user authentication request is successful. The temporary local user account is added to the pre-defined local user groups that are equivalent to the Succession user groups returned by the PAM proxy.

Additionally, the CICM-EM adds the authenticated username/password and the corresponding temporary local username/password to the user cache. This entry is held in the local cache for a pre-determined amount of time. Whilst this entry is present in the cache, subsequent authorisation requests for this user do not need to be processed through the PAM proxy. This reduces the processing load on both the CICM-EM and PAM proxy.

The CICM-EM also replaces the global Succession username/password in the HTTPS authentication request with the username/password of the temporary local user account. The temporary local username and password combination is then authenticated locally by standard user authentication. If the authentication is unsuccessful, then the CICM-EM rejects the user's attempt to log in.

- 6 If the authentication is successful, then the CICM-EM provides the user with the required webpage. If the authentication is unsuccessful, then the CICM-EM denies access to the requested webpage.

Succession User authentication levels on the PAM+ proxy are organised into five separate domains, with each domain containing 5 separate levels of user authentication. This provides a total of 25 user authentication levels, as shown below:

Access level	User Domain				
	Trunks	Lines	MGC	MG	EMS
Administrator	trkadm	lnadm	mgcadm	mgadm	emsadm
Read-Write	trkrw	lnrw	mgcrw	mgrw	emsrw
Provisioning	trkprov	lnsprov	mgcprov	mgprov	emsprov
Maintenance	trkmtc	lnmtc	mgcmtc	mgmtc	emsmtc
Read-Only	trkro	lnro	mgcro	mgro	emsro

The PAM proxy returns a list of groups against which the user has been successfully authentication. The user domains relevant to the CICM Element Manager are Lines, MG and EMS.

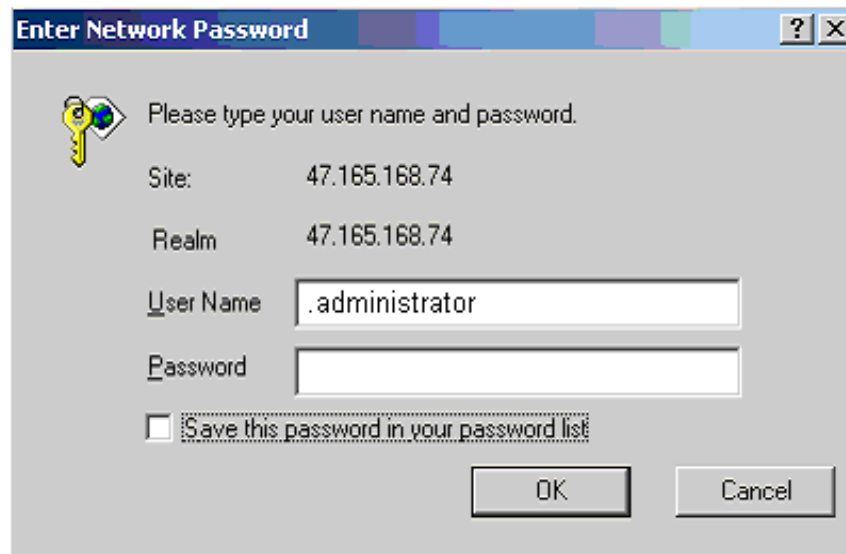
All CICM-EM web pages are configured with access control levels that are appropriate to their functionality.

Local User authentication

Centralised user authentication via the SSPFS PAM proxy is not available to TDM deployments of CICM. In addition, if connectivity is lost between the CICM EM and the SSPFS, it is important to provide the ability to access the CICM-EM to provide continued access to the functionality that it offers.

The CICM-EM will check if it is running in a TDM or Succession CICM deployment before it attempts to process the authentication via the PAM proxy. For TDM deployments, the authentication functionality will immediately pass control of the authentication back to the standard mechanism used for CICM.

For Succession deployments, users will be able to select local authentication by prefixing their username with a period (“.”). This will allow users to access the CICM-EM when the PAM proxy is out of service (provided they have a local user account on the CICM-EM). Therefore, to access the CICM-EM when the SSPFS is not accessible, the user can log in as shown below:



The image shows a Windows-style dialog box titled "Enter Network Password". It has a yellow key icon on the left. The text inside says "Please type your user name and password." Below this, there are labels for "Site:" and "Realm:", both with the value "47.165.168.74". There are input fields for "User Name" (containing ".administrator") and "Password" (empty). At the bottom, there is a checkbox labeled "Save this password in your password list" which is unchecked. There are "OK" and "Cancel" buttons at the bottom right.

Site:	47.165.168.74
Realm	47.165.168.74
User Name	.administrator
Password	
☐ Save this password in your password list	

Configuration

The configuration of the IP address to use for the SSPFS PAM+ proxy is configured during the EM preboot stage as follows:

Screen capture of initial configuration of the EM

```
+-----+
| STEP n : Configure the SSPFS PAM Proxy
+-----+

This CICM Element Manager can use Pluggable Authentication Module (PAM)
on the Succession Server Platform Foundation Software (SSPFS) platform
(if available).

Will this Element Manager use the PAM on the SSPFS to authenticate users?
[Y|N, default=N]:
Y

Will this EM connect to the PAM server using HTTPS [Y|N, default = N]
N

Please enter the IP address of the SSPFS PAM proxy:
1.2.3.4

You have entered the IP address of the SSPFS PAM proxy as 1.2.3.4
Is this correct [Y|N, default=N]
Y
```

The user can select to use HTTP or HTTPS (secure HTTP) to communicate with the PAM proxy. If HTTPS is selected, the user will be prompted to enter the Fully Qualified Domain Name (FQDN) of the PAM server. HTTPS requires that a certificate from a valid signing authority is installed on the SSPFS.

Limitations and restrictions

Authentication using the SSPFS will only occur when the user is accessing the CICM-EM via the web interface. This feature will not change the method used for authenticating users who are logging in using a Telnet session.

Logs (LG)

This feature interacts with A00003718 “CICM Osmine readiness – Faults, alarms and performance monitoring”, to log the following events on the IEMS:

- User successfully authenticated through PAM.
- User authentication through PAM failed.

- Request Timeout on PAM proxy.

The CICM-EM will also raise an alarm on the IEMS when a request to the PAM proxy times out. This alarm is cleared the next time an authentication request is successfully processed through the PAM server.

Glossary

Term	Description
CICM	Centrex IP Client Manager
CICM-EM	CICM Element Manager
HTTP(S)	Hypertext Transfer Protocol (Secure)
IP	Internet Protocol
PAM	Pluggable Authentication Module
SSPFS	Succession Server Platform Foundation Software
TDM	Time Division Multiplexed
VLAN	Virtual Local Area Network

References

- A00005985 “CICM Security”
- A00001912 “Centralised Security Administration”
- A00003718 “CICM Osmine readiness – Faults, alarms and performance monitoring”

Product = CS 2000

A00005988 -- XPe OS Evolution and platform boot (IAW)

Functional Description

Overview

Scope

This document covers the following areas:

- Changes to CICM and CICM EM Hardware.
- Details of the new Windows XP Embedded OS to be used for this release.
- Process for network boot and remote download of CICM/CICM-EM image.

- Details of Integration with SAM21 Chassis, SAM21 Element Manager and SDM/SSPFS.

Description

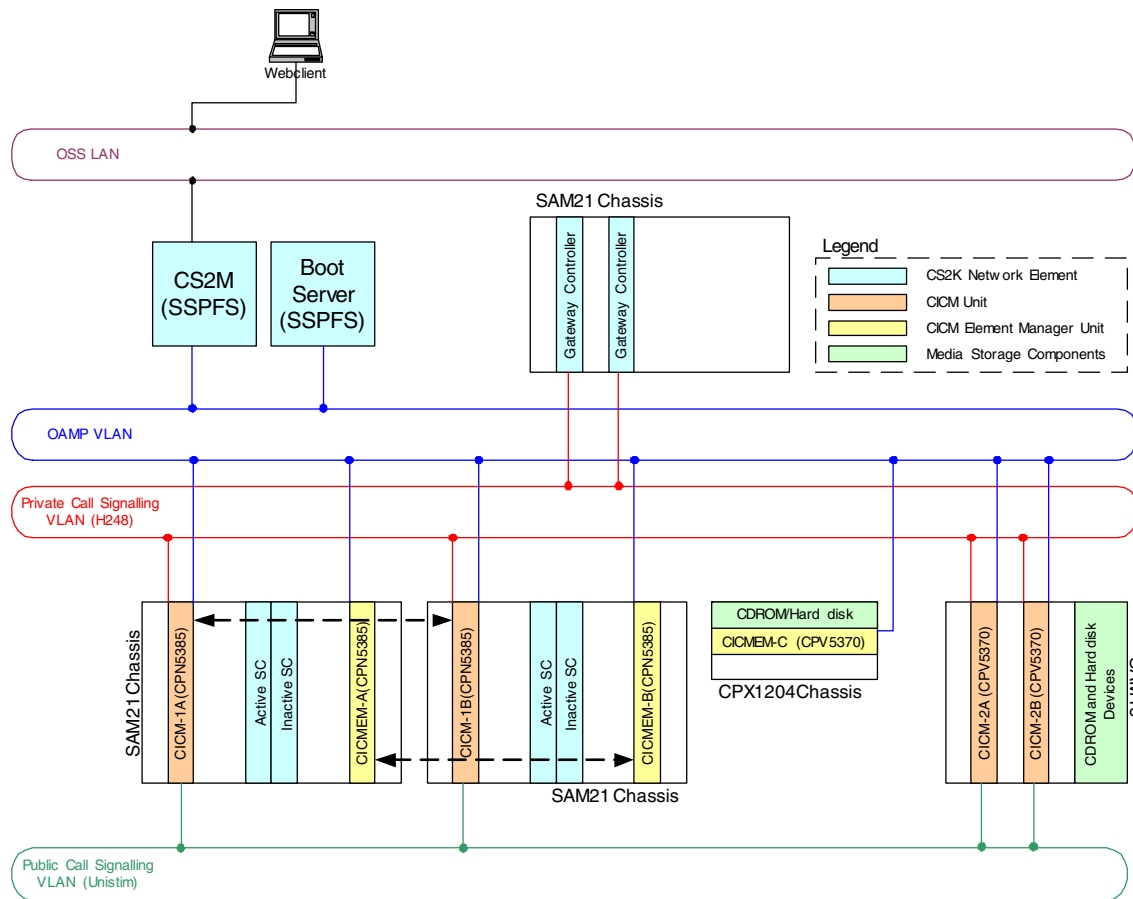
This feature integrates the CICM and the CICM EM into the SAM21 chassis. The SAM21 is a Motorola Chassis (CPX8221) used to host many of the Succession components including the Gateway Controller, 3PC, USP and STORM. It comprises of 17 IO slots used for Slave CPU cards and 2 Master CPU Card Slots used for the two SAM21 Shelf Controller CPUs.

The CICM and CICM EM platforms running in the SAM21 chassis are able to remote boot and configure themselves in conjunction with the SAM21 Element Manager and the CS2K Boot Server (SDM/SSPFS).

CICM has the following changes introduced in SN07 as a result of this integration:

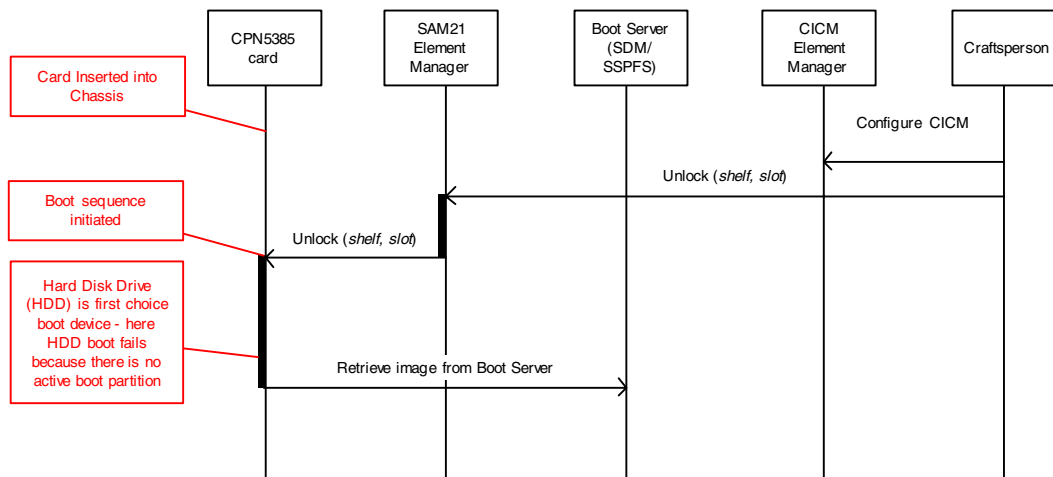
- New Hardware Platform – CPN5385 CPU Card.
 - Compatibility with SAM21 chassis provides the ability for CICM to share a chassis with other Succession components leading to a reduced footprint
- Change of OS to Windows XP Embedded from Windows NT4 Embedded.
 - XP Embedded is the latest embedded operating system, and therefore has more advanced features and a longer shelf-life than NT4 Embedded.
- Automatic Network Boot and Installation of CICM and CICM EM Software Image and instead of using CDROM install process. (Although the CDROM process will still be used for backwards compatibility with existing hardware)
 - Network booting provides reduced commissioning costs by allowing more of the commissioning process to be run remotely.
- Configuration of OS and Software settings via the Element Manager

The following figure shows how the new and existing CICM and CICM-EM components fit into the Succession network.

CICM and CICM-EM Network Diagram**Detail**

The following figure shows a simplified flowchart for the process of network booting, imaging and installing the CICM CPN5385 card in the Succession environment.

Network Boot and Installation Process Overview for CICM on CPN5385



Hardware Considerations

This section briefly describes changes to the CICM hardware for SN07. It also discusses backwards compatibility for old platforms.

Motorola CPN5385 Slave CPU Card

To permit the integration of the CICM into the SAM21 Chassis, the CICM has moved from a Master Slot CPU card to a Slave Slot CPU card. Slave cards only require power and PCI connectivity from the Chassis to run. It is not possible for them to use external storage devices in the chassis so a dedicated onboard storage device is required.

Specification

The specification for the CPN5385 card and associated components is as follows: -

- Processor - 1200 MHz Mobile Pentium III Processor – M.
- RAM - 512 MB DDR SDRAM.
- Storage – Ramix PMC243 Ultra133-TX2 Promise Controller including 40GB 2.5” Slim line Hard Disk.
- Network – One Intel 82559 100base-T Adapter and Two Intel 82544EI 1000base-T Adapters, all on Rear Transition Module.
- Keyboard/Mouse – 3 Rear USB Ports.
- Serial – One DB-9 COM Port on Front Board, Two DB-9 COM Port on Rear Transition Module.

Please note that the CPN5385 card requires an additional card (the Transition Module) to provide the required input and output connectivity.

To order this hardware, please refer to the Nortel Product Equipment Code (PEC) and description below:

NTRX51HJ CPN5385, 1.2 GHZ, 512MB SDRAM, HD PMC

NTRX51HK CPTM85 TRANSITION MODULE (this is the Rear I/O card for the 5385)

Mean Time Before Failure (MTBF) Analysis

A Mean Time Before Failure analysis provides a statistical determination of the lifetime of components and systems. The following MTBF figures are relevant for a CICM system running on the CPN5385 based system:

CPN5385 Card = 190,000 hours

PMC243 drive carrier and controller = 380,000 hours

2.5" Slim line Hard disk = 298,000 hours

The combined MTBF for the system can be calculated using the following equation.

Combined MTBF

$$\frac{1}{m^t} = \frac{1}{m^1} + \frac{1}{m^2} + \dots + \frac{1}{m^n}$$

Where m^t is the combined (or total) MTBF and m^n is the MTBF for a component system.

Thus the combined MTBF for the CPN5385 system is in the region of 88,000 hours. Therefore, in a system with 1000 CPN5385 systems in service over 5 years you would expect subsystem failures in approximately 500 systems.

Backwards Compatibility

The SN07 release will support the following hardware platforms: -

- CPN5385 Slave CPU Card in SAM21 Chassis – For CICM and CICM-EM.
Order codes:
 - NTRX51HJ CPN5385, 1.2 GHZ, 512MB SDRAM, HD PMC

- NTRX51HK CPTM85 TRANSITION MODULE
- CPV5370 Master CPU Card in CPX8216T Chassis – For CICM. Order codes:
 - NTRX51VB CPV5370, 700MHZ, PENTIUM III
 - NTRX51VC CPTM-04 TRANSITION MODULE
- CPV5370 Master CPU Card in CPX1204 Chassis – For CICM-EM. Order codes (same as CPX8216T based system):
 - NTRX51VB CPV5370, 700MHZ, PENTIUM III
 - NTRX51VC CPTM-04 TRANSITION MODULE

Platforms based around the CPV5370 Master CPU are not be able to network boot and must be installed from a CD. This is because the SAM21 Chassis and its associated Shelf Controllers are required to facilitate the automatic configuration of BOOTP entries for the CICM (to allow network boot) and only the CPN5385 is supported in this chassis.

Intel Pre-Execution Environment

The Intel Ethernet Adapters on the CPN5385 are pre-flashed with a network ROM conforming to the Intel Pre-Execution Environment (PXE) Specification. When this is enabled, it allows an Ethernet Adapter to boot and then download and execute a small Network Bootstrap Program (NBP). This NBP will then facilitate the download and execution of a simple OS e.g. DOS or Linux.

Base OS Evolution

Previous releases of the CICM product have been based around the Windows NT Embedded Service Pack 6 OS. In SN07, this feature introduces the use of the latest Microsoft Embedded OS, Windows XP Embedded (XPE) Service Pack 1.

The CICM Element Manager will continue to use Windows 2000 Server Edition.

Installation process

The installation process is as follows:

- 1 Configure the card on the SDM or SSPFS (please refer to feature A00001935 “Provisioning Support for Centrex-IP Nodes and Lines” for details)
- 2 Configure the card on the CICM EM (refer to feature A00005987 “Provisioning, backup and restore” for details)

- 3 Insert the CPN5385 card into the SAM21 chassis
- 4 Unlock the card from the SDM/SSPFS
- 5 The CICM card will now network boot fully and start the imaging process
- 6 After the reboot...
 - After the reboot it will attempt to pull down configuration information from the element manager, (this should have previously been saved on the element manager by running through the configuration web pages). If the information is successfully found and downloaded the CICM will come into service.
 - If the CICM cannot contact the element manager it will assume it is operating in high security mode and will wait for certain security information to be entered. This is entered by connecting to the serial port of the CICM node in question using --9600 bits per second, eight data bits, no parity and one stop bit. Log in using username administrator, and password Administrator (case sensitive).
- 7 After rebooting, the CICM will be operational

The time required for the CICM card to network boot and come into operation (measured from when the Unlock command is received) is expected to be no longer than 15 minutes.

Re-installation process

It may be necessary to reinstall the base image on the hard disk in certain situations. For example if an OS fix can not be applied as a patch, a new base image may need to be installed. To allow reinstallation of the base image the network boot process must be run again. This can be achieved by using a maintenance page on the Element Manager to send a message to a card which results in the card being rebooted, and a network boot to be initiated.

Initiating a restart

Prior to this activity, the only supported method to restart the CICM was to use the CICM Element Manager to restart the node. Now, when running on the CPN5385 card, the CICM can also be restarted by locking and then unlocking the card from the SDM/SSPFS. The CICM node must be inactive before it can be locked. Therefore, if the CICM node is the active node, the CICM service must be stopped prior to locking. The CICM service is stopped from the maintenance webpage on the CICM-EM.

Software Requirements or Dependencies

The following components must be running their SN07 software loads prior to attempting to configure an SN07 CICM:

- SAM21 EM
- Shelf Controller
- CS2M Management Platform
- CICM-EM

Limitations and restrictions

When viewing a CICM running on the CPN5385 chassis on the CICM Element Manager, the card status overview is no longer provided. This is as a result of being able to have multiple CICM pairs within one SAM21 shelf, and so a graphical representation of the status of the whole shelf would provide potentially misleading information.

Both versions are shown below for reference.

Example CPN5370, SAM16 based CICM status page on the CICM-EM

Centrex IP Client Manager - Microsoft Internet Explorer provided by Nortel Networks

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Go

Links Address http://47.165.168.75/centrexip/ Go

Centrex IP Client Manager

CICM
status
configuration
terminals
users
maintenance

CICM-EM
status
synchronization

profiles
audio
enterprise
language
network
user
feature

diagnostics
diagnostics

cxip120 cicm status

CXIP120 - Status - Active Refresh 11:56:00

Slot	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
Fault																
Active							●	●	●							
Maint																

Node A, cxip120a Service = **running**
Status = Online
Node State = slave
Fault code=0
No faults detected

Node B, cxip120b Service = **running**
Status = Online
Node State = master
Fault code=0
No faults detected

virtual media gateways

VMG instance	Node A	Node B
VMG00	Hot Standby	In Service

network

IP address	Adapter	Active
47.165.168.120	Node A, Adapter 1	Yes
47.165.168.121	Node A, Adapter 2	Yes
47.165.168.125	Node B, Adapter 1	Yes
47.165.168.126	Node B, Adapter 2	Yes

terminals

Node	Status
Node A	Started
Node B	Started

summary
perform maintenance on cxip120
view status of chassis components
performance monitoring
Connections
view the status of
cicm-140

CICM-EM Version 7.1.157

Done Internet

Example CPN5385, SAM21 based CICM status page on the CICM-EM

The screenshot shows the Centrex IP Client Manager web interface in a Microsoft Internet Explorer browser window. The address bar shows the URL <http://47.165.168.74/centrexip/>. The page title is "Centrex IP Client Manager".

The left sidebar contains a navigation menu with the following items:

- CICM
 - status
 - configuration
 - terminals
 - users
 - maintenance
- CICM-EM
 - status
 - synchronization
- profiles
 - audio
 - enterprise
 - language
 - network
 - user
 - feature
- diagnostics
 - diagnostics

The main content area displays the "cxip180 cicm status" page. It shows the status of CXIP180 as "Active" with a "Refresh 11:37:02" link. Below this, there are two nodes:

Node	Service	Status	Node State	Fault code	Faults detected
Node A, 47.165.168.180	running	Online	master	0	No faults detected
Node B, 47.165.168.185	running	Online	slave	0	No faults detected

Below the node status, there is a section for "virtual media gateways" with a table:

VMG instance	Node A	Node B
CXIP180	In Service	Hot Standby

The "network" section shows a table of IP addresses and their status:

IP address	Adapter	Active
47.165.168.180	Node A, Adapter 1	Yes
47.165.168.181	Node A, Adapter 2	Yes
47.165.168.185	Node B, Adapter 1	Yes
47.165.168.186	Node B, Adapter 2	Yes

The "terminals" section shows a table of node status:

Node	Status
Node A	Started
Node B	Started

At the bottom of the main content area, there are links for "cicms" and "home".

The right sidebar contains a list of actions:

- summary
- perform maintenance on cxip180
- view status of chassis components
- performance monitoring
 - Connections
- view the status of
 - cicm-140

The bottom status bar shows "Done" and "Internet".

Interactions

N/A

Glossary

Term	Description
CICM	Centrex IP Client Manager
CICM-EM	CICM Element Manager
CPU	Central Processing Unit

XPe	XP Embedded
SAM16	Motorola Chassis (CPX8216T)
SAM21	Motorola Chassis (CPX8221)
SDM	Supernode Data Manager
SSPFS	Succession Server Platform Foundation Software
USP	Universal Signalling Point

References

A00005987 “Provisioning, backup and restore”

A00001935 “Provisioning Support for Centrex-IP Nodes and Lines”

Product = CS 2000

A00006405 -- Multi Point Code Expansion (Succession on DMS, AAL2)

Functional Description

This activity expands the number of Point Codes (PC) that can be defined in an SSP office in table C7NETWRK from 16 to 31.

Product = CS 2000

A00006483 -- Audio Server Node Announcement Capacity Increase to 1280 (PT-IP, AAL2)

Functional Description

This activity provides the capability to increase the number of simultaneous announcement calls which can be supported in the CS2K for an Audio Server Node from 300 to 1280.

Hardware Requirements or Dependencies

The audio server gateways subtending the Gateway Controller (GWC) that is datafilled as an Audio Server node must have the appropriate configuration to support 1280 ports.

Software Requirements or Dependencies

This functionality requires both the Core and GWC to be at the SN07 releases or later.

Limitations and restrictions

With the ANNC option set to 1280, this reduces the number of conference resources available on for the Audio Server node. Please refer to A89009843 “UAS Announcement Traffic Distribution” for how to calculate conference and announcement availability.

Prior to SN06, the ANNC option did not exist. When the Core is upgraded to SN06, the reformat procedure for table SERVSINV assigns by default the ANNC option. The default value specified for the ANNTERMS field is 300 if no other options (i.e. 3PORT or 6PORT) are datafilled. The default value will not change in SN07. If 3PORT or 6PORT is datafilled, the ANNC ANNTERMS value is adjusted accordingly against the value in NUMTERMS. For upgrades from SN06 to SN07, the ANNC option ANNTERMS value is simply transferred.

Interactions

Not applicable.

Applicable customer facing sections

Fault Management

Logs _____N/A

Alarms _____N/A

Configuration

Data Schema _____X

User Interface _____N/A

Element Management _____N/A

Security _____N/A

Service Order _____N/A

Office Parameters _____N/A

Accounting (includes AMA billing) _____N/A

Performance (includes operational measurements) _____N/A

Glossary

Term	Description
GWC	Gateway Controller

Configuration for A00006483

Hardware and Software Requirements

Multiple Universal Audio Servers (UAS) or Audiocodes Media Servers (AMS) or some other packet-based announcement resource equivalent must be networked to provide the announcement resources. The announcement resource devices must be capable of being configured and networked to meet the announcement port demands.

Initial Configuration

Table SERVINV must be datafilled with a gateway controller (GWC) to be used as an Audio Controller GWC that will have subtending announcement resource devices.

Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable.

Upgrade Impact

Dump and Restore

Prior to SN06, the ANNC option did not exist. When the Core is upgraded to SN06, the reformat procedure for table SERVSINV assigns by default the ANNC option. The default value specified for the ANNTERMS field is 300 if no other options (i.e. 3PORT or 6PORT) are datafilled. The default value will not change in SN07. If 3PORT or 6PORT is datafilled, the ANNC ANNTERMS value is adjusted accordingly against the value in NUMTERMS. For upgrades from SN06 to SN07, the ANNC option ANNTERMS value is simply transferred.

Element Management Upgrade

Not applicable.

Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
SERVSINV	CHANGED	UNCHANGED

Table/MIB/Remote Database Schema information

Name: SERVSINV

Server Subtending Node Inventory Table

Functional description

Table SERVSINV contains the names of the server subtending nodes and their associated gateways. The subtending node relevant to this activity is the audio server node(AUD).

Usage sequence and implications (CM Only)

Current datafill order unchanged.

Size

Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SERVSINV	0	256	Protected

Fields/OIDs

The following table lists fields/OIDs for SERVSINV.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SRVSNAME	Not Changed		see subfields	<i>Server Subtending Name key.</i> This field contains subfields XPMTYPE and XPMNO. Specifies the logical subtending node off the GWC
	Not changed	XPMTYPE	PM_TYPE	<i>XPM Type.</i> For an audio server node, enter AUD.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
	Not changed	XPMNO	0 to 255	<i>XPM Number.</i> Enter the XPM number for the peripheral.
SRVRNAME	Not changed		see subfields	<i>Server Name.</i> This field contains subfields XPMTYPE and XPMNO. Specifies the associated gateway controller of the subtending node.
	Not changed	XPMTYPE	PM_TYPE	<i>XPM Type.</i> Enter GWC.
	Not changed	XPMNO	0 to 255	<i>XPM Number.</i> Enter the corresponding GWC node number found in table SERVINV.
NUMTERMS	Not changed		1024, 2048, or 4095	<i>Number of Terminals.</i> For AUD node, it is recommended that 4095 be used.
OPTIONS	Not changed		see subfield	<i>Options.</i> This field contains subfields for 3PORT, 6PORT, and/or ANNC for conferencing and announcement resources.
OPTIONS	Not changed		ANNC	<i>ANNC OPTION.</i> The subfield ANNC is used for announcement terminal allocation and to indicate the number of simultaneous announcements. The field contains the subfield ANNTERMS.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
	Changed	ANNTERMS	1 to 1280	Announcement terminals. Enter value up to 1280.

Datafill example

The following example shows sample datafill for table SERVSINV :

Example of table SERVSINV

```
>table servsinv
TABLE: SERVSINV
>list all
TOP
```

SRVSNAME		SRVRNAME		NUMTERMS	OPTIONS
AUD	1	GWC	1	4095	(ANNC 1280)\$
AUD	4	GWC	2	4095	(3PORT 300) (6PORT 120) (ANNC 300)\$

Table release history update

The following information was added: The ANNTERMS maximum value for the ANNC option of the OPTIONS field has increased from 300 to 1280.

Supplementary information

The ANNC option has a maximum ANNTERMS value of 1280 because of a GWC limitation.

Translation verification other tools

SERVSINV does not use translation verification tools.

Service Orders (SO) (CM & SESM)

Not applicable

Software optionality control (SOC)

Not applicable.

Element Management

Not applicable.

Command interface changes

Not applicable.

Security

Not applicable.

Configuration Walkthrough

Not applicable.

Product = CS 2000**A00006693 -- XA-Core IO Capacity Monitoring Toolset (Succession on DMS)*****Functional Description***

The IO Capacity monitoring toolset (IOCAP) provide the customer telemetry for messaging over HIOP and HCMIC.

XA-Core counts messages and bytes for each service. Software on the XA-Core accesses the measurements, calculates the messaging occupancy level, and displays the results on the IOCAP MAPCI level and the IOCAP OM group.

This feature will cause no more than 3% capacity degradation to IO capacity.

IOCAP MAPCI display

Following is a prototype of the IOCAP MAPCI display, which will subtend from the CAPACITY level. The display will be updated once per minute.

CATMP/HR	SMS/HR	VLR_UPD/HR	CAP	ENGBHCA	CCOVRD	CMICOVRD	PESC
303001	180	398700	128	233643	OFF	OFF	NO

Service	IOUTIL%	TxMsg/s	TxSize	RxMsg/s	RxSize
ETHR	64	15324	107	13234	91
CMIC	17	4102	202	1254	102
AMDI	0	0	0	0	0

The Service column identifies the type of IO service (Ethernet, CMIC, or AMDI). IOUTIL is the calculated percentage utilization of the available system messaging capacity, based on the known IO system capacity, the average rate through other services on the same card, and the throughput on other cards. TxMsg/s, TxSize, RxMsg/s and RxSize report average transmit and receive message rates and sizes through that service. Because the MAPCI display is updated once per minute, high water mark information will not be displayed.

IOCAPCI tool

The information in the MAP display is also available through the IOCAPCI tool, in addition to the following tools:

- one month's history of hourly high water mark percent utilization for each service (Ethernet, CMIC, and AMDI), similar to DMSMON HIGHCAP.
- one month's history of hourly average percent utilization for each service.
- current hour and last hour utilization and throughput for each service

An example of the CMIC high water mark data follows. A similar output will be available for each service.

```
> iomax cmic
Maximum CMIC Utilization
```

Date	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21
2/2	8	7	9	10	4	5	9	12	16	21	27	29	39	49	53	43	51	56	57	61	57	41	29	18
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/29	8	7	8	10	8	9	7																	
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21

IO capacity OM

The information displayed in the IOCAP MAP command is also recorded in the IOCAP operational measurement, as shown below.

IOCAP

CLASS: HOLDING

START:2003/12/03 09:30:00 WED; STOP: 2003/12/03 09:45:00 WED;
SLOWSAMPLES: 9 ; FASTSAMPLES: 90 ;

INFO (IO_SERVICE_TYPE)

	IOUTIL RXMSG/S	IOHWM RXSIZE	TXMSG/S IOTHRESH	TXSIZE
1 ETHR	64 13234	72 84	15204 0	105
2 CMIC	17 1254	18 63	1254 0	102
3 AMDI	0 0	0 0	0 0	0

The IOCAP OM provides measurements of messaging rates and sizes for each service. The IO_SERVICE_TYPE indicates the service provided. IOUTIL refers to percentage utilization of the services on the switch. IOHWM refers to the highest level that the corresponding utilization has reached in the sample period. TxMSG/S, TxSIZE, RxMSG/S and RxSIZE report the average transmit and receive message rates and sizes through the service. The IOTHRESH register is pegged every time the service average utilization for one minute exceeds the value of new OFCENG office parameter IO_WARNING_THRESHOLD. This register is intended to give the customer a flexible warning that they are approaching the need to upgrade their IO system.

Office parameter

A new office parameter in table OFCENG, IO_WARNING_THRESHOLD, indicates the minimum IO service utilization at which the IOTHRESH register in the IOCAP OM will be pegged.

Hardware Requirements or Dependencies

This feature is unavailable for CMIC, Ethernet and AMDI packets (NTLX05AB, NTLX09AA, NTLX05BA respectively).

This feature is supported on all versions of NTLX04 HIOP cards and NTLX17 HCMIC cards.

Software Requirements or Dependencies

None.

Limitations and restrictions

This feature will be submitted into CSP21 and patched back to CSP20.

When the system is in transition from IOP to HIOP, the utilization of all IO services are not be available.

Interactions

The MAPCI level display will subtend from the CAPACITY MAP level. It will be shown as an option from that level.

Applicable customer facing sections

Fault Management

Logs ☐ NA ☐

Alarms ☐ NA ☐

Configuration

Data Schema ☐ NA ☐

User Interface ☒ X ☐

Element Management ☐ NA ☐

Security ☐ NA ☐

Service Order ☐ NA ☐

Office Parameters ☒ X ☐

Accounting (includes AMA billing) ☐ NA ☐

Performance (includes operational measurements) ☒ X ☐

Glossary

Term	Description
New term	Definition

Configuration Management for A00006693

Hardware and Software Requirements

Not applicable.

Initial Configuration

Not applicable.

Office/Subnet parameters (OP/SP) (CM & SESM)

New/modified office/subnet parameters

New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management)
OFCENG	IO_WARNING_THRESHOLD	NEW	XA-Core

Parameter information

IO_WARNING_THRESHOLD

IO_WARNING_THRESHOLD

Functional description

This parameter defines a utilization warning threshold for all IO service types (CMIC, ETHR, AMDI) in the system. The IOCAP monitoring toolset uses the value of this parameter to peg the IOTHRESH register of the IOCAP OM whenever the IO utilization level of any IO service has exceeded this threshold on the switch.

Provisioning rules

There is no formula for provisioning this office parameter. However, this office parameter should be set by the customer in such a manner that will allow sufficient advance warning time for their maintenance personnel to upgrade or reconfigure their IO devices in case the condition reoccurs often.

Range information

Range Information

Minimum	Maximum	Default
1	100	100

Activation

Any change activation for this office parameter is immediate.

Dependencies

Not applicable.

Consequences

If this office parameter is set low, the IOTHRESH register might be in pegged more often than necessary. If this office parameter is set high, the customer may not have enough advance notice to upgrade their IO configuration.

Verification

To verify, users can modify and display the value of IO_WARNING_THRESHOLD on table OFCENG via table control.

Memory requirements

No memory impact.

Units per memory block = <10>

Words per memory block = <510>

If the parameter value = <25>

words required = (((parameter value - 1)/units per block) + 1) * words per block = <>

Parameter release history update

New office parameter in CSP20.

Upgrade Impact

Not applicable.

Data schema (DS) (CM, MIBS, RDB)

Not applicable.

Service Orders (SO) (CM & SESM)

Not applicable.

Software optionality control (SOC)

Not applicable.

Element Management

Not applicable.

Command interface changes

The following new directories will be provided in this feature.

Directory: CAPACITY

This existing CAPACITY MAPCI level will be modified to provide a new IOCAP MAPCI level in XA-Core only. The new IOCAP level will provide IO utilization and IO messaging throughput information for HCMIC and HIOP IO cards.

Directory description

This new IOCAP MAPCI level will be giving the IO utilization values and messaging throughput information for each IO service type (CMIC, ETHR and AMDI). The information on this new MAPCI level will be updated once every minute.

Accessing directory: CAPACITY**Access to directory or MAP level and return to CI**

To access this directory, type:

> MAPCI; MTC; CAPACITY

To return to the CI environment, type:

> QUIT ALL

Command: IOCAP

This is a new command available under the CAPACITY MAPCI level in XA-Core only.

Command type: Listed MENU

Command target: XA-Core only

Command availability: RES**Command description**

This new IOCAP MAPCI level will be giving the IO utilization values and messaging throughput information for each IO service type (CMIC, ETHR and AMDI). The information on this new MAPCI level will be updated once every minute.

Command syntax**IOCAP command parameters and variables**

Command	Parameters and variables
IOCAP	none
Parameters and variables	Description

Qualifications and warnings

Not applicable.

Responses

IOCAP response

MAP outputs with associated meanings and actions

Command
Service: The type of IO service of the values shown on the same line is captured. Meaning: Possible IO service types are CMIC, ETHR and AMDI. System or user actions: Not applicable
IOUTIL%: The average utilization of all active links in the system captured in the previous minute. Meaning: The value is given as a percent of total system and can take up to 3 digit. System or user actions: Not applicable
TxMsg/s: The average number of transmitted messages captured in the last minute for this IO service type. Meaning: The unit is number of transmitted messages per second. System or user actions: Not applicable
TxSize: The average size (in bytes) of all transmitted messages in the last minute. Meaning: The unit is in bytes. System or user actions: Not applicable
RxMsg/s: The average number of received messages captured in the last minute for this IO service type. Meaning: The value unit is the number of received messages per second. System or user actions: Not applicable
RxSize: The average size (in bytes) of all received messages in the last minute. Meaning: The unit is in bytes. System or user actions: Not applicable

This MAPCI level can be used for monitoring current IO throughput. Under normal condition, there is no response required from maintenance personnel. The descriptions of all fields displayed under this level are given above. These responses are seen in XA-core only.

Example

Usage examples for IOCAP command

Description of task:	This new IOCAP MAPCI level will be giving the IO utilization values and messaging throughput information for each IO service type (CMIC, ETHR and AMDI). The information on this new MAPCI level will be updated once every minute.
Command: MAP response:	MAPCI; MTC; CAPACITY; IOCAP See example output below.

An example output of this new MAPCI level is given below.

IOCAP MAPCI Level

XACM	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.	.	.	.	.	.	.
IOCAP									
0 Quit	CATMP/HR	UTIL	ENGCATMP	MAXCATMP	ENGLLEVEL	CCOVRD	CMICOVRD	PESC	
2	120000	75	160000	200000	BELOW	OFF	OFF	NO	
3									
4	Service	IOUTIL%	TxMsg/s	TxSize	RxMsg/s	RxSize			
5									
6	AMDI	64	15324	107	13234	91			
7	CMIC	17	4102	202	1254	102			
8	ETHR	10	8967	123	3456	123			
9									
10	IOCAP:								
11									
12									
13									
14									
15									
16									
17									
18									
XMAP0									
Time 14:12 >									

Command: QUIT

This command will allow the user to exit IOCAP MAPCI level and to return to IOCAP higher MAPCI level (CAPACITY MAPCI level).

Command type: Listed MENU

This QUIT command is listed in IOCAP menu.

Command target: XA-Core only

This new IOCAP QUIT command is available in XA-Core only.

Command availability: RES**Command description**

This command will allow the user to exit IOCAP MAPCI level and to return to IOCAP higher MAPCI level (CAPACITY MAPCI level).

Command syntax**QUIT command parameters and variables**

Command	Parameters and variables
QUIT	none

Qualifications and warnings

Not applicable.

Responses**QUIT****MAP outputs with associated meanings and actions**

Command
If QUIT is issued, the user will be returned to one MAPCI level higher than their current MAPCI level. If QUIT ALL is issued, the user will be returned to CI level. Meaning: Not applicable. System or user actions: Not applicable. Meaning: The IOCAP MAPCI level is exited and user is returned to one MAPCI level higher or to CI level. System or user actions: Not applicable.

Example**Usage examples for QUIT command**

Description of task:	
Description of task	Exit the IOCAP MAPCI level and return the user to CI level or one MAPCI level higher..
Command: MAP response:	Example: QUIT ALL Example: >

Directory: IOCAPCI

Directory description

This new IOCAPCI is provided to allow customers to display the IO utilization history data.

Accessing directory: IOCAPCI

Access to directory or MAP level and return to CI

To access this directory type:

> IOCAPCI

To return to CI environment, type:

> QUIT

Command: IOMAX

Command type: NON-MENU

Command target: XA-Core only

Command availability: RES

Command description

This command displays the hourly high watermark value captured for each IO service type (CMIC, ETHR or AMDI). The value is captured every hour of day for the last 31 days. The data survives all types of restarts (warm, cold and reload).

The date of the month will be in sequence. For every hour in the future (there is no data collected yet), a blank character will be displayed.

Command syntax

The command syntax for this command is as follows.

```
> q iomax
Display IO high watermark report.
Parms: <service> {CMIC,
                  ETHR,
                  ATM,
                  ALL}
```

IOMAX command parameters and variables

Command	Parameters and variables
IOMAX	service
IOMAX	<Service> (CMIC, ETHR, AMDI, ALL)

IOMAX command parameters and variables

Command	Parameters and variables
Parameters and variables	Description
Service	Possible values are CMIC, ETHR, AMDI or ALL
CMIC	Displays only CMIC hourly max history data
ETHR	Displays only ETHR hourly max history data
AMDI	Displays only AMDI hourly max history data
All	Displays all hourly.max history data for CMIC, ETHR, and AMDI.

Qualifications and warnings

Not applicable.

Responses**IOMAX response**

The following is the response if IOMAX CMIC is issued.

CMAF outputs with associated meanings and actions

Command
IOMAX CMIC: history data of CMIC hourly maximum utilization are displayed. Meaning: CMIC hourly maximum history data are displayed. System or user actions: Not applicable.
IOMAX ETHR: history data of ETHR hourly maximum utilization are displayed. Meaning: history data of ETHR hourly maximum utilization are displayed. System or user actions: Not applicable.
IOMAX AMDI: history data of AMDI hourly maximum utilization are displayed. Meaning: history data of AMDI hourly maximum utilization are displayed. System or user actions: Not applicable.
IOMAX ALL: history data of CMIC, ETHR, AMDI hourly maximum utilization are displayed. Meaning: history data of CMIC, ETHR, AMDI hourly maximum utilization are displayed. System or user actions: Not applicable.

Example

Usage examples for IOMAX command

Description of task	Display the history data of IO hourly max utilization.																							
Command: MAP response:	Example: IOMAX CMIC																							
	Example:																							
	Maximum CMIC Utilization																							
		Hour																						
Date	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/29	8	7	8	10	8	9	7																	
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21

Usage examples for IOMAX command

Command: MAP response:	Example: IOMAX ETHR																										
	Example: Maximum ETHR Utilization																										
	Date	0	1	2	3	4	5	6	7	8	9	10	11	Hour		12	13	14	15	16	17	18	19	20	21	22	23
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21			
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/29	8	7	8	10	8	9	7																				
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14			
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21			

Command: MAP response:	Example: IOMAX AMDI																										
	Example: Maximum AMDI Utilization																										
	Date	0	1	2	3	4	5	6	7	8	9	10	11	Hour		12	13	14	15	16	17	18	19	20	21	22	23
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21			
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/29	8	7																									

Usage examples for IOMAX command

Command: MAP response:	Example: IOMAX ALL																								
	Example: Maximum CMIC Utilization																								
	Hour																								
	Date	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
	2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21
	2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
	2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
	2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
	2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
	2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
	2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
	2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
	2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
	2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
	2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
	2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
	2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
	2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
	2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
	2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
	2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
	2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
	2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
	2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
	2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/29	8	7	8	10	8	9	7																		
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14	
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21	
Maximum ETHR Utilization																									
Hour																									
Date	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21	
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/29	8	7	8	10	8	9	7																		
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14	
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21	

Usage examples for IOMAX command

	Maximum AMDI Utilization																								
	Date	Hour																							
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21	
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
2/29	8	7	8	10	8	9	7																		
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14	
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21	

Command: IOAVG**Command type: NON-MENU****Command target: XA-Core only****Command availability: RES****Command description**

This command displays the hourly average value captured for each IO service type (CMIC, ETHR or AMDI). The value is captured every hour of day for the last 31 days. The data survives all types of restarts (warm, cold and reload).

The date of the month will be in sequence. For every hour in the future (there is no data collected yet), a blank character will be displayed.

Command syntax

The command syntax for this command is as follows.

```
> q ioavg
Display IO average report.
Parms: <service> {CMIC,
                  ETHR,
                  ATM,
                  ALL}
```

CIOAVG command parameters and variables

Command	Parameters and variables
IOAVG	service
IOAVG	<Service> (CMIC, ETHR, AMDI, ALL)
Parameters and variables	Description
Service	Possible values are CMIC, ETHR, AMDI or ALL
CMIC	Displays only CMIC hourly average history data
ETHR	Displays only ETHR hourly average history data
AMDI	Displays only AMDI hourly average history data
All	Displays all hourly average history data for CMIC, ETHR, and AMDI.

Qualifications and warnings

Not applicable.

Responses**IOAVG response**

The following is the response if IOAVG CMIC is issued.

MAP outputs with associated meanings and actions

Command
IOAVG CMIC: history data of CMIC hourly average utilization are displayed. Meaning: CMIC hourly average history data are displayed. System or user actions: Not applicable.
IOAVG ETHR: history data of ETHR hourly average utilization are displayed. Meaning: history data of ETHR hourly average utilization are displayed. System or user actions: Not applicable.
IOAVG AMDI: history data of AMDI hourly average utilization are displayed. Meaning: history data of AMDI hourly average utilization are displayed. System or user actions: Not applicable.

MAP outputs with associated meanings and actions

Command
IOAVG ALL: history data of CMIC, ETHR, AMDI hourly average utilization are displayed.
Meaning: history data of CMIC, ETHR, AMDI hourly average utilization are displayed.
System or user actions: Not applicable.

Example**Usage examples for IOAVG command**

Description of task	Display the history data of IO hourly average utilization.																								
Command: MAP response:	Example: IOAVG CMIC																								
	Example: Average CMIC Utilization																								
	Date	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21	18
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	14
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	14
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	14
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	14
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	14
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	14
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	14
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	14
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	14
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	14
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	14
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	14
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	14
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	14
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	14
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	14
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	14
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	14
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	14
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	14
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	14
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	14
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	14
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	14
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	14
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	14
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	14
2/29	8	7	8	10	8	9	7																		
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14	14
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21	14

Usage examples for IOAVG command

Command: MAP response:	Example: IOAVG ETHR																										
	Example: Average ETHR Utilization																										
	Date	0	1	2	3	4	5	6	7	8	9	10	11	Hour		12	13	14	15	16	17	18	19	20	21	22	23
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21			
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/29	8	7	8	10	8	9	7																				
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14			
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21			

Command: MAP response:	Example: IOAVG AMDI																										
	Example: Average AMDI Utilization																										
	Date	0	1	2	3	4	5	6	7	8	9	10	11	Hour		12	13	14	15	16	17	18	19	20	21	22	23
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21			
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21			
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14			
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18			
2/29	8	7	8																								

Usage examples for IOAVG command

Command: MAP response:	Example: IOAVG ALL																									
	Example: Average CMIC Utilization																									
		Hour																								
	Date	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	
	2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21	
	2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
	2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
	2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14	
	2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18	
	2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21	
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/29	8	7	8	10	8	9	7																			
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14		
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21		
	Average ETHR Utilization																									
	Hour																									
Date	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23		
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21		
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21		
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14		
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18		
2/29	8	7	8	10	8	9	7																			
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14		
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21		

Usage examples for IOAVG command

	Average AMDI Utilization																							
	Date	Hour																						
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
2/1	9	7	8	6	5	7	8	11	17	22	28	30	40	55	50	47	61	57	59	62	59	39	31	21
2/2	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/3	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/4	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/5	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/6	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/7	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/8	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/9	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/10	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/11	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/12	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/13	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/14	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/15	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/16	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/17	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/18	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/19	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/20	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/21	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/22	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/23	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/24	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/25	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/26	5	7	9	8	7	8	9	8	15	23	21	29	39	53	49	42	59	51	55	57	53	47	31	21
2/27	3	8	7	6	9	8	4	7	11	19	27	31	38	51	47	45	55	53	57	56	51	49	29	14
2/28	9	9	8	7	7	7	8	7	18	28	18	29	37	48	55	48	58	48	59	59	57	48	27	18
2/29	8	7	8	10	8	9	7																	
1/30	3	8	7	6	9	8	4	12	16	21	27	29	39	49	47	45	55	53	57	56	51	49	29	14
1/31	8	6	5	7	8	7	6	9	11	19	27	31	39	49	53	43	51	55	53	57	56	51	31	21

Command: DISP**Command type: NON-MENU****Command target: XA-Core only****Command availability: RES****Command description**

This DISP command displays the utilization and messaging throughput values of each IO service type of the last 60 minutes with option CURR (for example when a command is issued at 2:35, displayed data is from 1:34 to 2:34) or previous full hour with option PREV (for example when a command is issued at 2:35, displayed data is from 1:00 to 2:00). This information survives all types of restarts (warm, cold and reload).

Command syntax

The command syntax for this command is as follows.

```
> q disp
Display table of IO utilization.
Parms: <when> {CURR,
              PREV}
        <service> {CMIC,
                   ETHR,
                   ATM,
```

ALL}

DISP command parameters and variables

Command	Parameters and variables
DISP	<when> <service>
DISP	<when> (CURR, PREV) <service> (CMIC, ETHR, AMDI, ALL)
Parameters and variables	Description
When	Possible values are CURR or PREV
CURR	Displays the last 60 minutes utilization and messaging throughput of the specified IO service type
PREV	Displays the previous full hour utilization and messaging throughput of the specified IO service type
Service	Possible values are CMIC, ETHR, AMDI or ALL
CMIC	Displays only CMIC utilization and messaging throughput
ETHR	Displays only ETHR utilization and messaging throughput
AMDI	Displays only AMDI utilization and messaging throughput
ALL	Displays utilization and messaging throughput for CMIC, ETHR, and AMDI.

Qualifications and warnings

Not applicable.

Responses**DISP response**

The following is the response if DISP CURR CMIC is issued.

MAP outputs with associated meanings and actions

Command
DISP CURR CMIC: last 60 minutes of CMIC utilization and messaging throughput are displayed. Meaning: last 60 minutes data for CMIC utilization and messaging throughput are displayed. System or user actions: Not applicable.

MAP outputs with associated meanings and actions

Command
DISP CURR ETHR: last 60 minutes of ETHR utilization and messaging throughput are displayed. Meaning: last 60 minutes of ETHR utilization and messaging throughput are displayed. System or user actions: Not applicable.
DISP CURR AMDI: last 60 minutes of AMDI utilization and messaging throughput are displayed. Meaning: last 60 minutes of AMDI utilization and messaging throughput are displayed. System or user actions: Not applicable.
DISP CURR ALL: last 60 minutes of CMIC, ETHR, AMDI utilization are displayed. Meaning: last 60 minutes of CMIC, ETHR, AMDI utilization are displayed. System or user actions: Not applicable.

Example**Usage examples for DISP command**

Description of task	Display the last 60 minutes of IO utilization and messaging throughput.
Command: MAP response:	Example: DISP CURR CMIC Example: <pre> Time IOUTIL% TxMsg/s TxSize RxMsg/s RxSize 16:17 45 23421 34 23421 34 16:18 39 22119 31 21228 32 16:19 38 21228 32 22119 31 16:20 39 23421 31 21221 31 17:14 41 20023 32 20019 33 17:15 39 21221 31 21228 32 17:16 38 20019 33 23421 34 </pre>
Command: MAP response:	Example: DISP CURR ETHR Example: <pre> Time IOUTIL% TxMsg/s TxSize RxMsg/s RxSize 16:17 45 23421 34 23421 34 16:18 39 22119 31 21228 32 16:19 38 21228 32 22119 31 16:20 39 23421 31 21221 31 17:14 41 20023 32 20019 33 17:15 39 21221 31 21228 32 17:16 38 20019 33 23421 34 </pre>
Command: MAP response:	Example: DISP CURR AMDI Example: <pre> Time IOUTIL% TxMsg/s TxSize RxMsg/s RxSize 16:17 45 23421 34 23421 34 16:18 39 22119 31 21228 32 16:19 38 21228 32 22119 31 16:20 39 23421 31 21221 31 17:14 41 20023 32 20019 33 17:15 39 21221 31 21228 32 17:16 38 20019 33 23421 34 </pre>

Usage examples for DISP command

Command: MAP response:	Example: DISP CURR ALL Example: Time CMICUTIL ETHRUTIL AMDIUTIL 16:17 45 21 34 16:18 39 19 31 16:19 38 18 32 16:20 39 21 31 17:14 41 23 32 17:15 39 21 31 17:16 38 19 33

Command: STATUS**Command type: NON-MENU****Command target: XA-Core only****Command availability: RES****Command description**

This command displays all status information including current version of IOCAPCI tool, timestamp in terms of hour and minute, the current IO utilization values of all IO services (CMIC, ETHR, AMDI), the current value of the IO_WARNING_THRESHOLD office parm.

Command syntax

The command syntax for this command is as follows.

```
> q STATUS
Display current IOCAP status.
```

STATUS command parameters and variables

Command	Parameters and variables
STATUS	no parameter

Qualifications and warnings

Not applicable.

Responses**STATUS response**

The following is the response if STATUS is issued.

MAP outputs with associated meanings and actions

Command
STATUS: Status information such as IOCAPCI version, current utilizations and IO_WARNING_THRESHOLD office parm are displayed. Meaning: Status information such as IOCAPCI version, current utilizations and IO_WARNING_THRESHOLD office parm are displayed. System or user actions: Not applicable.

Example**Usage examples for STATUS command**

Description of task	Display status information such as IOCAPCI version, current utilizations and IO_WARNING_THRESHOLD office parm.
Command: MAP response:	Example: DISP CURR CMIC Example: <pre>> status IOCAP Version 1.0 Time CMICUTIL ETHRUTIL AMDIUTIL 17:16 32 29 15 IO_WARNING_THRESHOLD office parm is set to 100.</pre>

Security

Not applicable.

Configuration Walkthrough

Not applicable.

Performance Management for A00006693**Performance management strategy****Performance management tools and utilities**

The new OM group can be displayed and collected via OMSHOW interface regularly by Telcos to monitor system IO throughput.

Performance Measurements (PM), Operational Measurements (OM), and stats

This feature will provide a new OM group IOCAP.

PM, OM, and stats format

OM Group template (applies only to DMS)

New OM group IOCAP provides information on IO capacity such as utilization and utilization high watermark and IO throughput information on a per IO service type (CMIC, ETHR and AMDI).

OM description

OM group IOCAP provides one tuple per IO service type available in the office. Possible IO service types are CMIC, ETHR and AMDI.

Key field: IO_SERVICE.

Info field: none.

Release history update

The OM group is being created in CSP21 and will be patched backed to CSP20.

Registers

OM group registers display on the MAP terminal as follows:

OM Group Display

IO_SERVICE	IOUTIL	IOHWM	TXMSGPS	TXSIZE	RXMSGPS
RXSIZE	IOTHRESH				

Group structure

OM group provides one tuple for each IO service type. There are 3 possible IO service types (CMIC, ETHR, AMDI).

Key field: IO_SERVICE indicates the IO service type the information is captured. Possible IO service types are CMIC, ETHR, and AMDI. The service type is displayed as 4 character string (CMIC, ETHR, AMDI).

Info field: None.

Associated OM groups

Not applicable.

Associated functional groups

The following functional groups are associated with OM group: none

OM group registers logic flow chart

Not applicable.

Register (applies only to DMS)

IOHWM

Register description

IOHWM is a high watermark register holding the highest utilization value of the specified IO service type over the OM transfer period.

Register release history update

Register is being created in CSP21 and patched back to CSP20.

Associated registers

None.

Associated logs

None.

Register (applies only to DMS)

IOTHRESH

Register description

IOTHRESH is a peg register holding the number of one minute interval in the transfer period the IO utilization has exceeded the value of the IO_WARNING_THRESHOLD office parm.

Register release history update

Register is being created in CSP21 and patched back to CSP20.

Associated registers

None.

Associated logs

None.

Register (applies only to DMS)

IOUTIL

Register description

IOUTIL is a usage register holding the average utilization value of the specified IO service type. This value is accumulated every minute and the average is calculated for every OM transfer period.

Register release history update

Register is being created in CSP21 and patched back to CSP20.

Associated registers

None.

Associated logs

None.

Register (applies only to DMS)

RXMSGPS

Register description

RXMSGPS is a usage register holding the average total system number of received messages of the specified IO service type. This value is accumulated every minute and the average is calculated for every OM transfer period. The unit is number of messages per second.

Register release history update

Register is being created in CSP21 and patched back to CSP20.

Associated registers

None.

Associated logs

None.

Register (applies only to DMS)

RXSIZE

Register description

RXSIZE is a usage register holding the average incoming message size of the specified IO service type. This value is accumulated every minute and the average is calculated for every OM transfer period. The message size unit is in bytes.

Register release history update

Register is being created in CSP21 and patched back to CSP20.

Associated registers

None.

Associated logs

None.

Register (applies only to DMS)

TXMSGPS

Register description

TXMSGPS is a usage register holding the average total number of outgoing messages of the specified IO service type. This value is accumulated once every minute and the average is calculated for every OM transfer period. The unit is in number of messages per second.

Register release history update

Register is being created in CSP21 and patched back to CSP20.

Associated registers

None.

Associated logs

None.

Register (applies only to DMS)

TXSIZE

Register description

TXSIZE is a usage register holding the value of average size of outgoing messages of the specified IO service type. This value is accumulated once every minute and the average is calculated for every transfer period. The value unit is in bytes.

Register release history update

Register is being created in CSP21 and patched back to CSP20.

Associated registers

None.

Associated logs

None.

Product = CS 2000

A00008902 -- SAM21 Log Changes (PT-IP, UA-IP)

This feature add two lines at the end of the alarm detail entry, based on the digits of the alarm ID, for example, SCU310. The system will divide the three digits into two groups: the first digit stands for the alarm's category, and the last two digits stand for the alarm's cause. The system uses the mapping table that follows to find the appropriate text strings for the alarm category and the alarm cause, and it then appends those two text strings to the end of the alarm detail.

Example

OFC_NAME *** SCU310 JUL30 17:48:52 5000 FLT Alarm Raised

Location: sam21 1:CSAM01-02:shelf 1:slot 9:card 1

Time: Thu Jul 30 17:48:45 EST 2002

Reason: CPU load high. One Minute Load is 19.11

Category: processingError

Cause: cpuCyclesLimitExceeded

Mapping Tables

Problem Category mapped to integers

communications	(1)
qualityOfService	(2)
processingError	(3)
equipment	(4)
environmental	(5)

Probable Cause Values mapped to integers

ITU-T X.733 probable causes	
adapterError	(1)
applicationSubsystemFailure	(2)
bandwidthReduced	(3)
callEstablishmentError	(4)
communicationsProtocolError	(5)
communicationsSubsystemFailure	(6)
configurationOrCustomizationError	(7)
congestion	(8)
corruptData	(9)
cpuCyclesLimitExceeded	(10)
dataSetOrModemError	(11)
degradedSignal	(12)
dteDCEInterfaceError	(13)

Probable Cause Values mapped to integers

enclosureDoorOpen	(14)
equipmentMalfunction	(15)
excessiveVibration	(16)
fileError	(17)
fireDetected	(18)
floodDetected	(19)
framingError	(20)
heatingOrVentilationOrCoolingSystemProblem	(21)
humidityUnacceptable	(22)
inputOutputDeviceError	(23)
inputDeviceError	(24)
IANError	(25)
leakDetected	(26)
localNodeTransmissionError	(27)
lossOfFrame	(28)
lossOfSignal	(29)
materialSupplyExhausted	(30)
multiplexerProblem	(31)
outOfMemory	(32)
ouputDeviceError	(33)
performanceDegraded	(34)
powerProblem	(35)
pressureUnacceptable	(36)
processorProblem	(37)
pumpFailure	(38)
queueSizeExceeded	(39)
receiveFailure	(40)
receiverFailure	(41)
remoteNodeTransmissionError	(42)

Probable Cause Values mapped to integers

resourceAtOrNearingCapacity	(43)
responseTimeExcessive	(44)
retransmissionRateExcessive	(45)
softwareError	(46)
softwareProgramAbnormallyTerminated	(47)
softwareProgramError	(48)
storageCapacityProblem	(49)
temperatureUnacceptable	(50)
thresholdCrossed	(51)
timingProblem	(52)
toxicLeakDetected	(53)
transmitFailure	(54)
transmitterFailure	(55)
underlyingResourceUnavailable	(56)
versionMismatch	(57)
Probable Cause values 58-100 are currently unused.	
ITU-T X.736 probable causes	
authenticationFailure	(101)
breachOfConfidentiality	(102)
cableTamper	(103)
delayedInformation	(104)
denialOfService	(105)
duplicateInformation	(106)
informationMissing	(107)
informationModificationDetected	(108)
informationOutOfSequence	(109)
intrusionDetection	(110)
keyExpired	(111)
nonRepudiationFailure	(112)

Probable Cause Values mapped to integers

outOfHoursActivity	(113)
outOfService	(114)
proceduralError	(115)
unauthorizedAccessAttempt	(116)
unexpectedInformation	(117)
unspecifiedReason	(118)

Product = CS 2000**A59039138 -- (Visual) Message Waiting Indicator (V)MWI/CFX (IAC)**

Note: This feature was developed in SN05 and SN06 but was not activated for those releases in the North American market. It is now active and available in the North American market for SN07.

Description**Overview**

This activity provides the following functionality in SN05 for the Integrated Access Cable IP Solution:

- CMWI (Class Message Waiting Indicator) for CEPT and Bellcore lines on Succession.
- Announcement as an optional replacement for the MWT stuttered dial tone indications for MWT suboptions CMWI and STD.

Background Information

Message Waiting allows a user to have a list of messages stored against their station. When a message is queued for a station, the MWI (Message Waiting Indicator) associated with the line is activated. When the last message is retrieved, the MWI is deactivated.

The MWT option has several sub options (STD, MWL, CMWI, PRN, MWL_STD). This activity focuses on STD and CMWI suboptions.

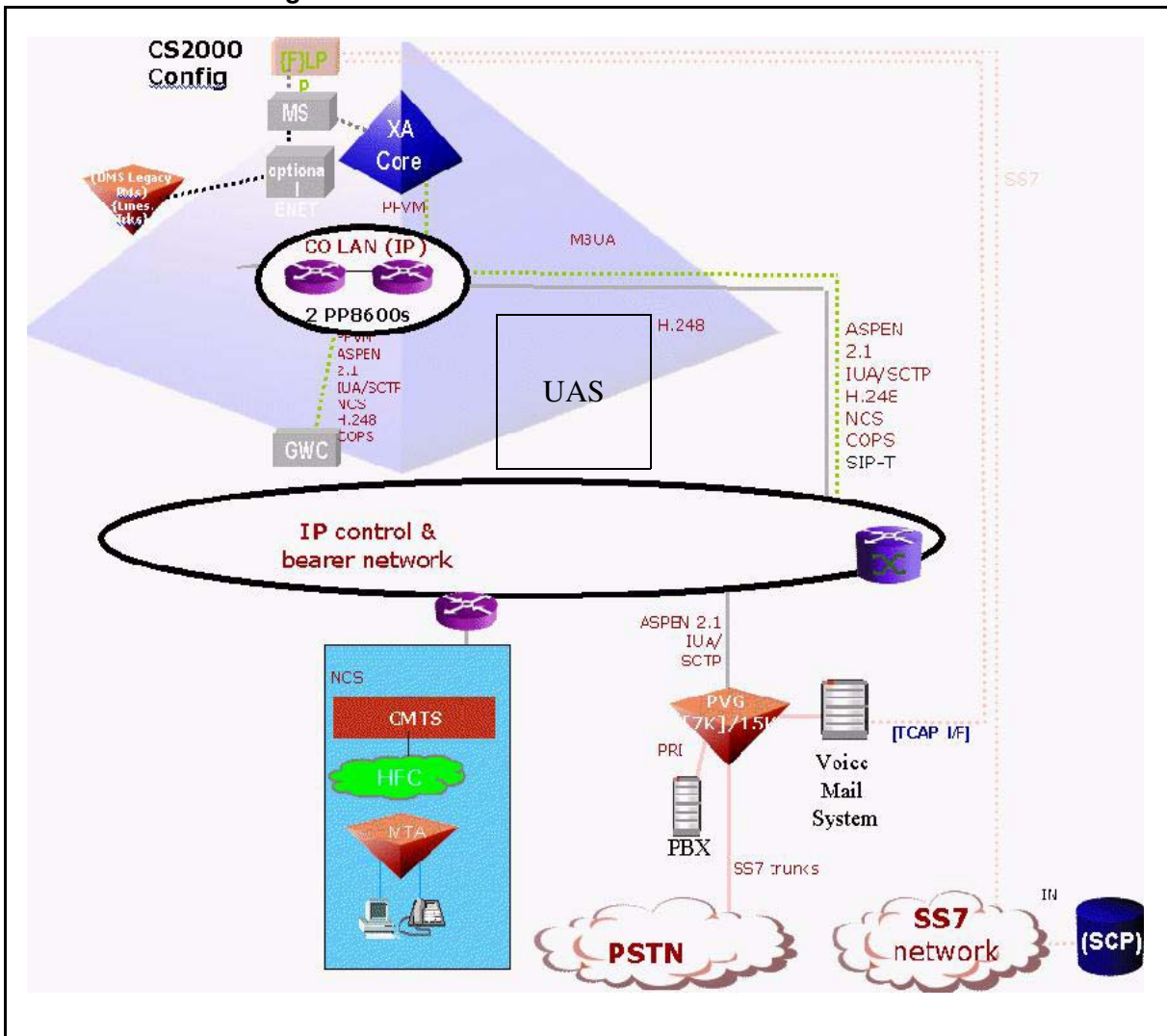
- CMWI (Class Message Waiting)¹ is used for sets which are capable of displaying a MWI request in a display or as a flashing lamp. In addition it

1. AG1954 'CLASS: VISUAL MESSAGE WAITING INDICATOR'

provides audible (stuttered dial tone) or ring splash notification. The last can be activated and deactivated by dialing an activation code.

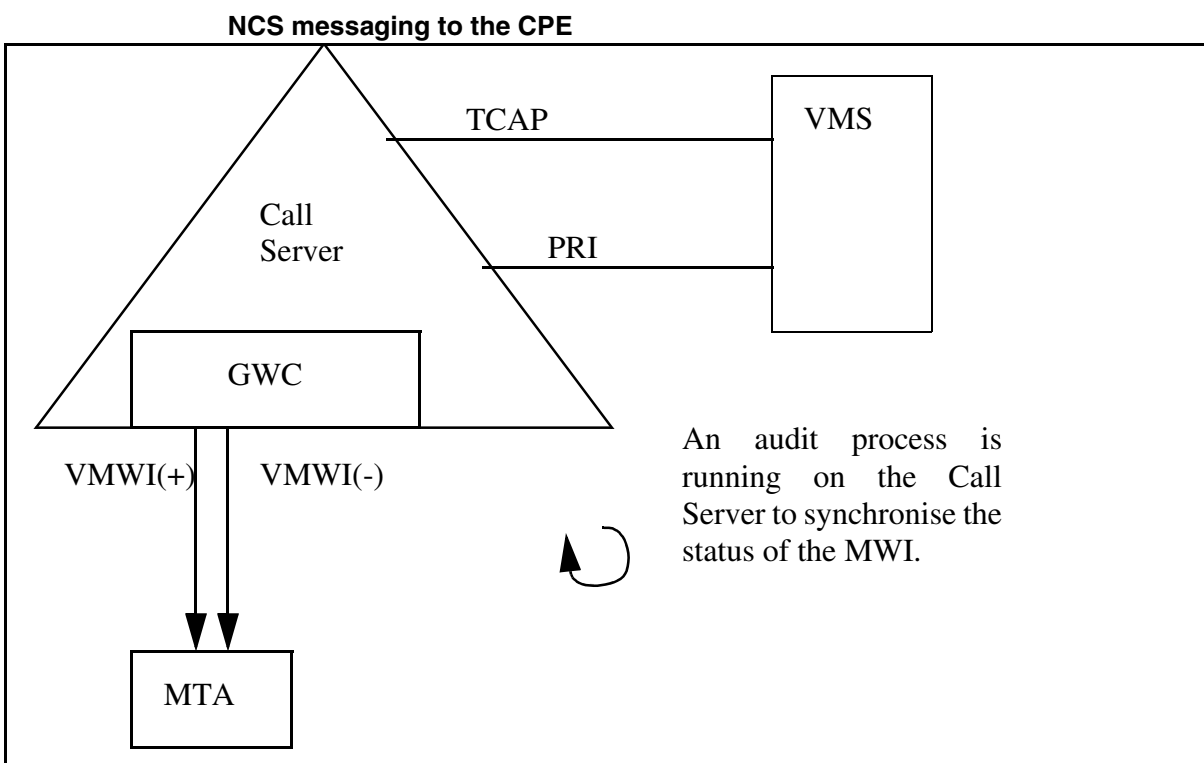
- STD (Stuttered Dial Tone) This is only used for applying a stuttered dial tone if a message is waiting.

Configuration VMWI



On MMP the Visual Message Waiting was signalled to the user by a special Line Class Tone. For Integrated Access Cable Media an NCS² message is used. For activating the MWI a VMWI(+) message is sent. For deactivation a VMWI(-).

In addition to this the Call Server should periodically refresh the CPE's (Customer Premise Equipment) visual indicator (Audit).



Agent Interworking

The Controlling user is a VMS (Voice Mail System) connected over

- PRI (PVG, PDTC)
- TCAP (LPP, USP)

to the Call Server.

The receiving user can be an IBN line connected via

- GWC - hosted on Motorola CG4500E MTA
- PLGC

Provisioning of the MWT service

The message waiting service can be provisioned with the following options: {**STD**,**MWL**,**CMWI**,**PRN**,**MWL_STD**}.

When the MWTANN announcement option is selected for MWT, datafill is required for the announcement. The CLLI for this announcement must be MWT. The CLLI can not be changed by the telco.

Below is sample datafill from a lab switch for the MWTANN feature:

```
> table clli
TABLE: CLLI
>pos mwt
MWT 433 5 TEST
>quit
CI:
>table anns
TABLE: ANNS
>pos mwt
MWT ALL 1 1 1 STND N 59 60
>quit
CI:
>table annmems
TABLE: ANNMEMS
>pos mwt 1
MWT 1
DRAM DRA
( 0 DTM 7 3)$
>quit
CI:
>table annphlst
TABLE: ANNPHLST
>pos mwt 0
MWT 0
( HAVE_MSG)$
>quit

***Create the announcement using DRAMREC***
> DRAMREC
> connect the HSET to a DRAM with available space.....
>Record have_msg 3 nopad 8 3 12
> QUIT
```

****This in turn creates a tuple in table dramphrs in a SN06 and beyond load. ****

```
>table dramphrs
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: DRAMPHRS
>pos 8 have_msg
8 HAVE_MSG 12 4 3 Y N 4
```

Table IBNFEAT

This feature adds the new announcement field MWT_ANNOUNCEMENT to the MWT feature in table IBNFEAT. A datafill example follows.

```
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
```

```
>y
LEN:
>HOST 01 0 07 00
DNNO:
>0
DF:
>mwt
FEATURE:
>mwt
NOTICE:
>std
MWT_ANNOUNCEMENT: N
>y
CAR:
>n
CRX: N
>n
TUPLE TO BE ADDED:
HOST 01 0 07 00
          0      MWT      MWT      STD      Y      N      N
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
JOURNAL FILE INACTIVE
>
```

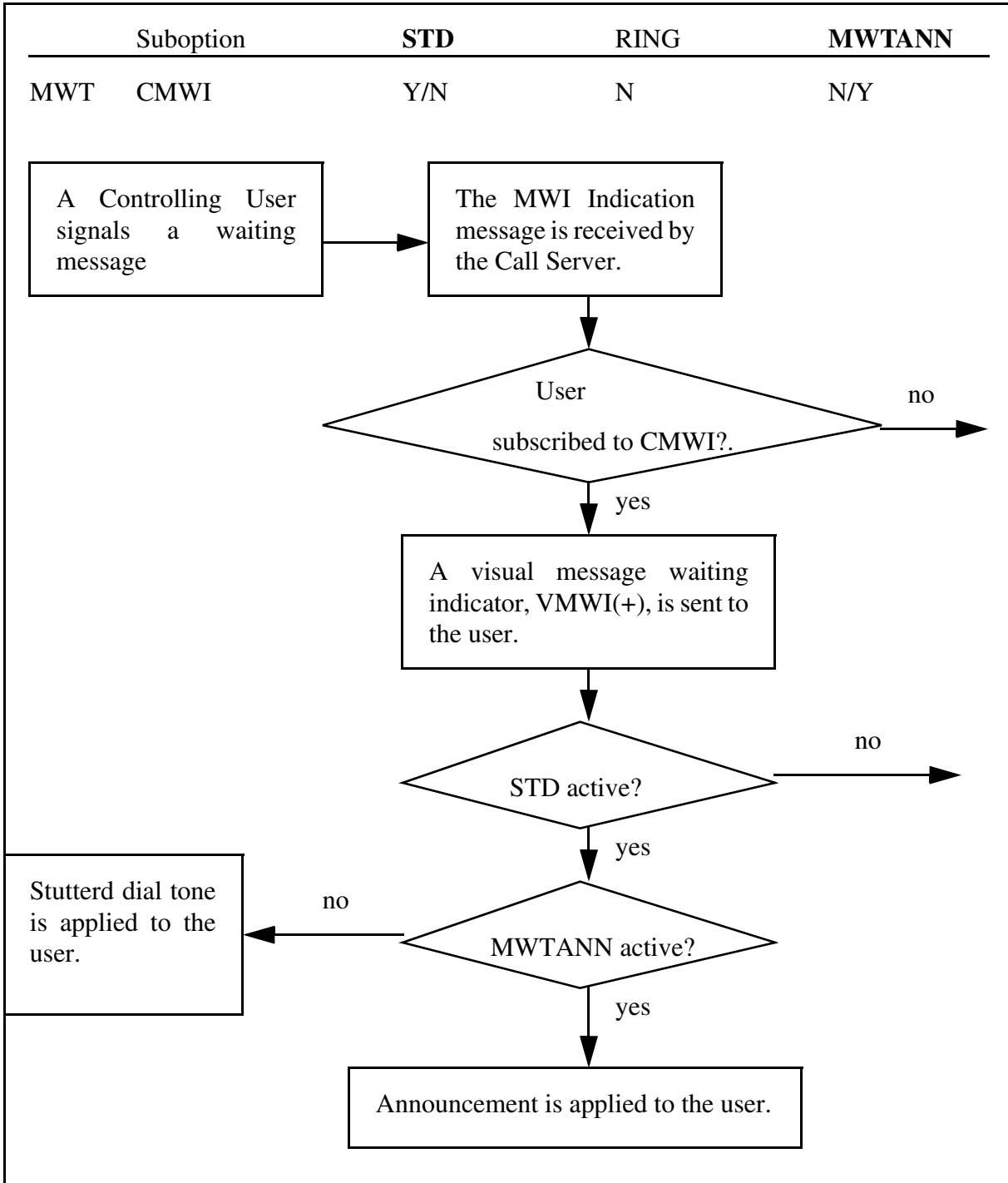
Overview of the CMWI Service

CLASS Message Waiting Indicator (CMWI) was developed under feature AG1954. The CMWI allows a subscriber to combine the visual message waiting indicator with audible indication types.

- **STD - Stuttered Dial Tone**
On active message waiting a stuttered dial tone is applied when the user goes off-hook
- **Ring Splash**
On active message waiting a ring burst is applied to the users' phone
- **MWTANN - Announcement**
On active message waiting an announcement is applied to the user.

For the Integrated Access Cable IP solution the signaling to the end user was shown in [“NCS messaging to the CPE” on page 1969](#).

Figure [“CMWI Overview” on page 1972](#) shows a functional overview on how the different indication components work together.

CMWI Overview

The provisioning for the CMWI service looks as follows:

SERVORD example for CMWI

```
>DN_OR_LEN:
>8838441020

OPTION:
>mwT

NOTICE:
>cmwi

CMWISTD:
>Y

MWT_ANNOUNCEMENT:

>Y

CMWIRING:
>Y

STATUS:
>act

CAR:
>Y

CRRCFW:
>all

CRX:
>n

OPTION:
>$

COMMAND AS ENTERED:

ADO NOW 1 12 4 AM 8838441020 ( MWT CMWI Y Y Y ACT Y ALL N ) $

ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
```

The CMWI option must be activated in table RESOFC.

Table RESOFC

KEY	ENABLED	ACCESS	FEATDATA
CMWI	Y	SUBSCR CMWI	SINGLE 5

The datafill above shows an example of the CMWI entry where the feature is enabled, using the Single Data Message format and allows 5 retransmissions per activation/deactivation request.

STD suboption

The STD option enables a subscriber to hear a stuttered dial tone if a message is waiting for them.

SERVORD example for STD suboption

```
>DN_OR_LEN:
>8838441020

OPTION:
>mwT

NOTICE:
>STD

MWT_ANNOUNCEMENT:

>Y

OPTION:
>$

COMMAND AS ENTERED:

ADO NOW 1 12 4 AM 8838441020 ( MWT STD Y Y ALL N ) $

ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
```

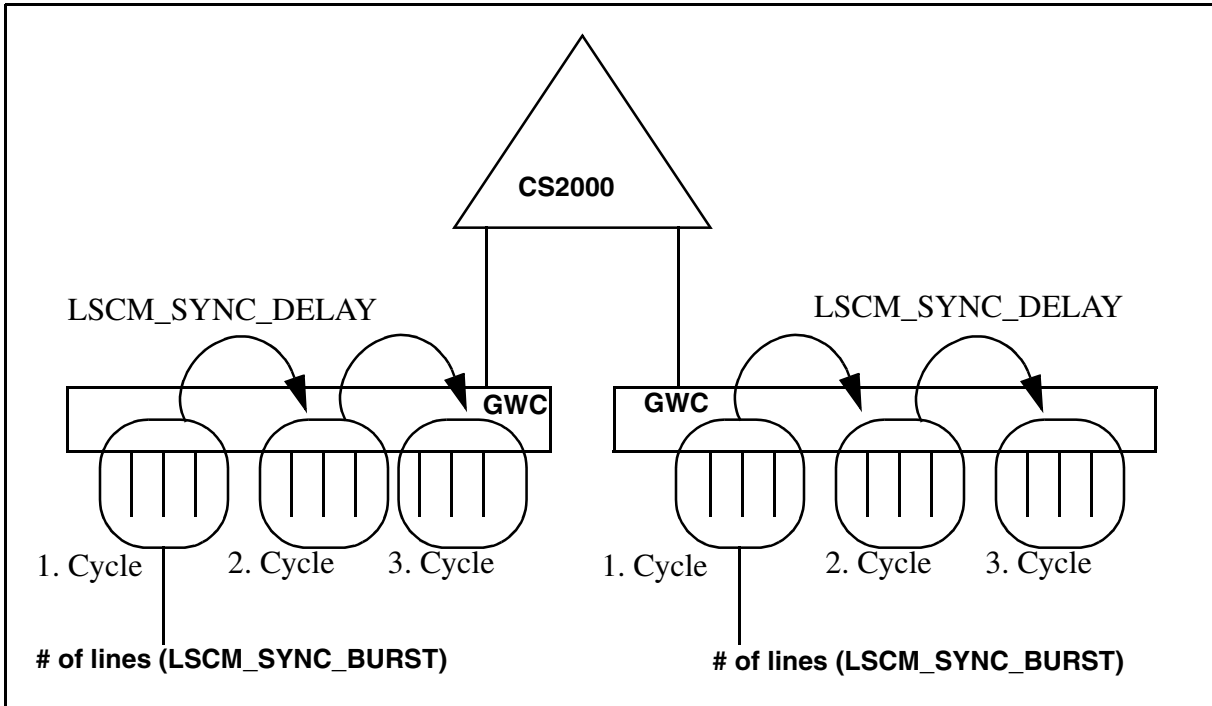
Datafilling the Audit for CMWI

In table OFCENG two tuples have to be datafilled in order to start the audit.

OFCENG - Audit

Tuple	Value
LSCM_SYNC_BURST	# of lines audited per peripheral in one cycle (0..10)
LSCM_SYNC_DELAY	delay between audit cycles (5 to 6000 s)

The next figure shows the how the audit based on the two datafillable parameters works. LSCM_SYNC_BURST gives the number of lines on an each peripheral which is audited by one cycle. The LSCM_SYNC_DELAY defines the time between the cycles.

Audit Process

Engineering information is provided below.

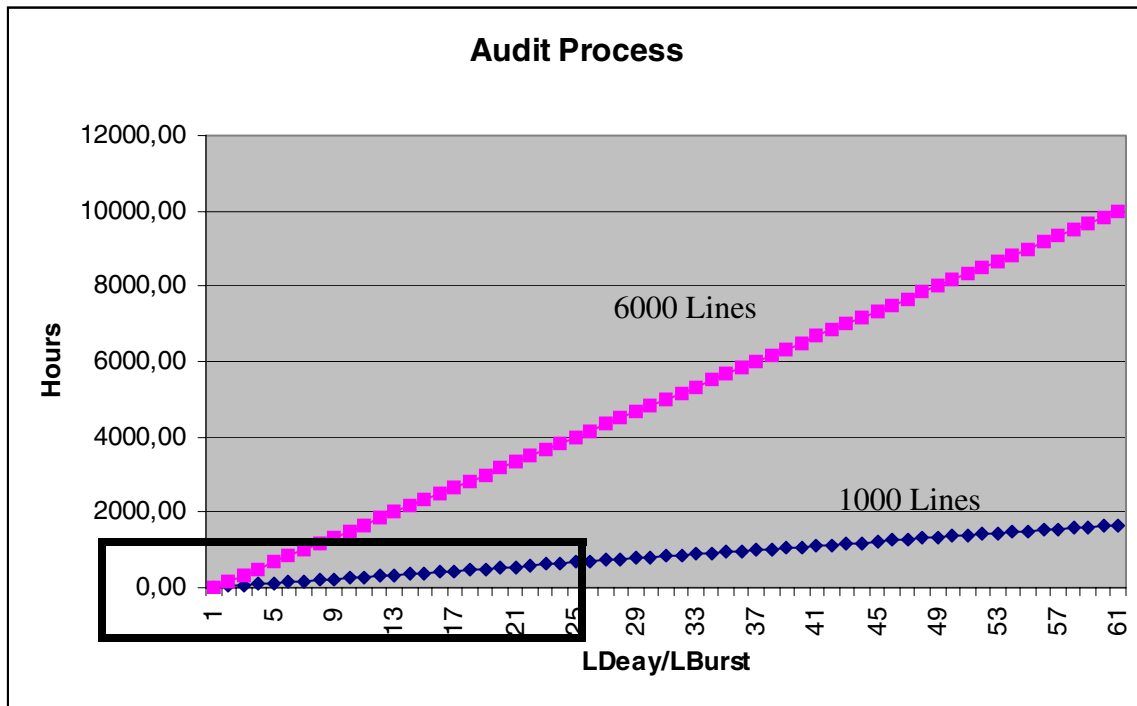
The following variables are defined:

- L_{Burst} (as datafilled)
- $L_{SyncDelay}$ (as datafilled)
- N_{all} (Number of all Lines connected to Peripherals)
- t_{circle} (Time for one complete Circle for all Lines)
- t_{c1} (Time for one circle)

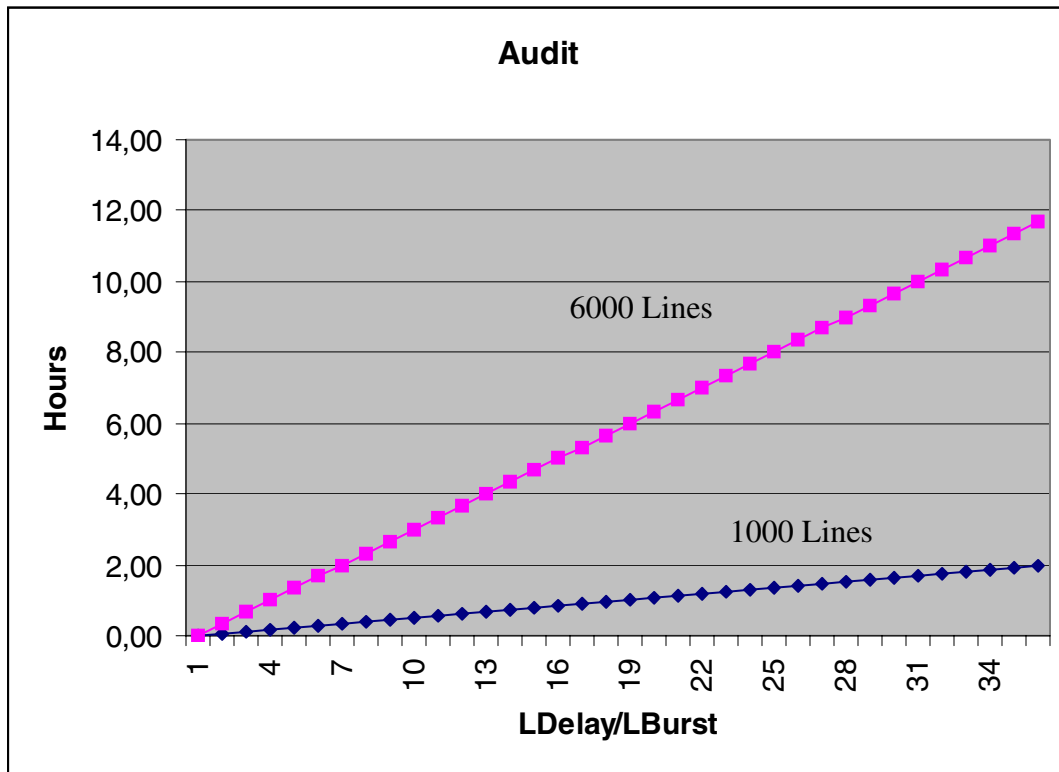
For the first calculation $t_{c1} \ll 1s$ and is not be considered.

$$\left(\frac{L_{Burst}}{L_{SyncDelay} \cdot N_{all}} \right)^{-1} = t_{circle}$$

Diagram for Audit Process



A detailed view of the marked area is shown in the next figure.

Diagram for Audit Process--detail

If t_{c1} is not considered to be small in comparison with the complete cycle time the equation will change into:

$$\left(\frac{L_{Burst}}{(L_{SyncDelay} + t_{c1}) \cdot N_{all}} \right)^{-1} = t_{circle}$$

t_{c1} is not only dependent on the time of the audit itself. Traffic and System Usage need to be considered.

Hardware Requirements or Dependencies

n/a

Software Requirements or Dependencies

n/a

Limitations and restrictions

- SMDI as a Controlling User is not included in this activity.
- No CEPT style user activation/deactivation for CMWI Ring Splash supported
- V5.2 Receiving Users are not covered by this activity.
- MWT_ANNOUNCEMENT will not be visible in KSETFEAT table for ISDN lines,
- Since MWT_ANNOUNCEMENT is not supported for ISDN lines, this field automatically set to FALSE, during addition of MWT option to ISDN lines.

Interactions

- CFIND: CFIND has precedence over MWI when Call Forwarding is active
- WML: The warm line timer is started after the announcement for MWT has finished playing.
- CEPT CFU (Call Forwarding Universal): CFU always gives a special dial tone to the user if CFU is active. If CFU and MWI are active and the user has the MWI announcement option, and first the announcement is played and then the user will hear the CEPT CFU tone.
- CEPT CFB/CFD: No interaction

Applicable customer facing sections

Fault Management

Logs	_____
Alarms	_____

Configuration

Data Schema	_____
User Interface	_____
Element Management	_____
Security	_____
Service Order	__X__
Office Parameters	_____

Accounting (includes AMA billing)	_____

Performance (includes operational measurements)	_____

Glossary

Term	Description
VMS	Voice Mail System
CMWI	Class Message Waiting Indicator
MWI	Message Waiting Indicator
PRI	Primary Rate Interface
CEPT	European Conference of Post and Telecommunications Administrations
CFx	Call Forwarding
CLASS	Custom Local Area Signalling Service

References

- PKT-SP-EC-MGCP-I02-991201 PacketCable Network-Based Call Signalling Protocol Specification

Product = CS 2000 Core Manager

A00002920 -- Support of Passport 8600 logs on SDM (Succession on DMS)

Excerpts from the Design Description

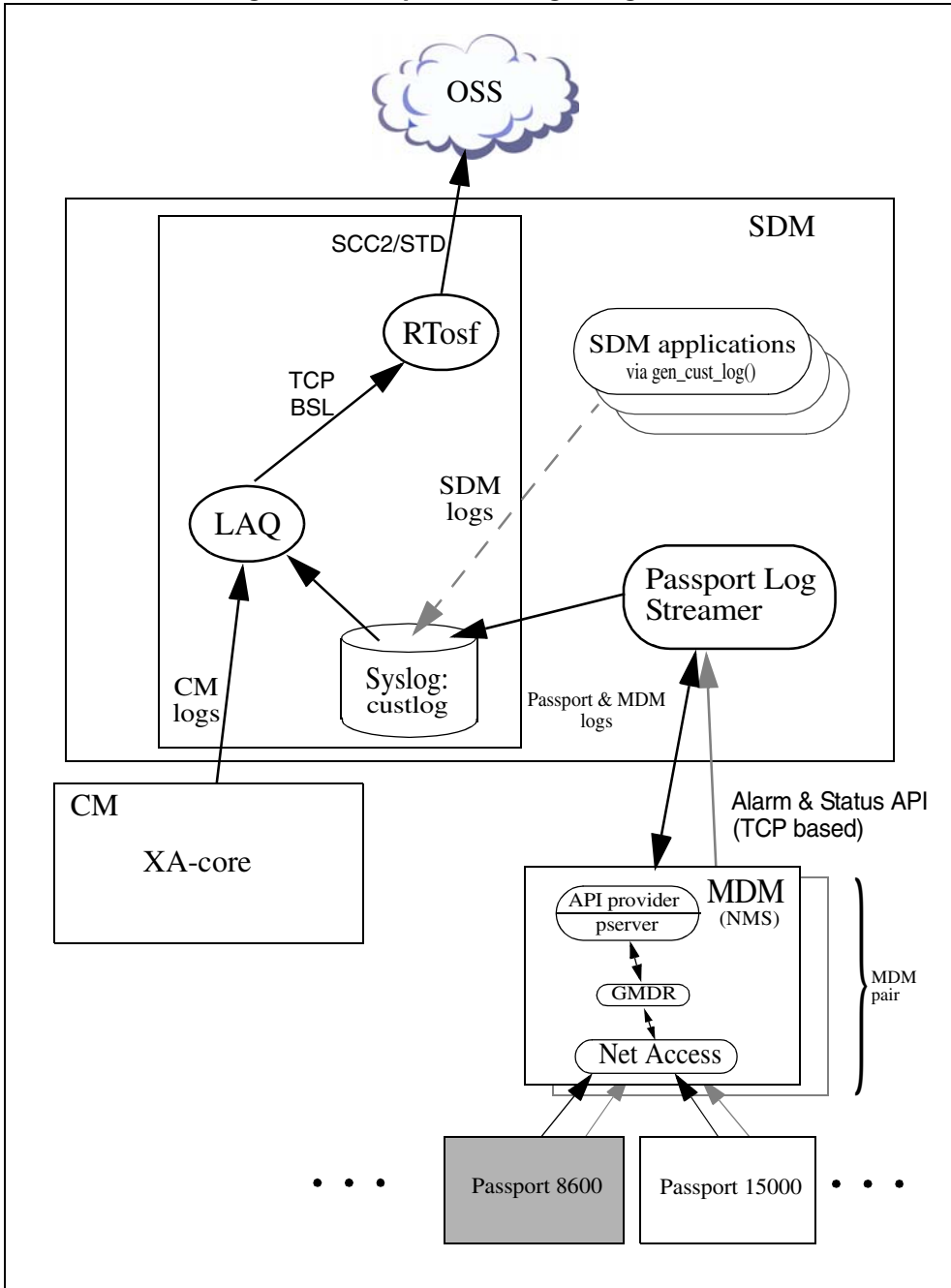
Purpose

The purpose of this feature is to support and generate Passport 8600 logs which are received by the PLS application.

Introduction

The following figure describes the configuration to generate passport logs.

High level component design diagram



Pserver : An application on MDM that allows programs running on separate workstation to communicate with each other by using stream sockets. Pserver allows the Alarm & Status API on MDM to export its output to the SDM Passport Log Streamer.

MDM Alarm & Status API is an ASCII based, local or remote interface capable of acquiring MDM state information as well as alarm (log) data. The

Passport Log Streamer application makes a registration request and thereafter can solicit or modify specific data (synchronous messages) or receive event notification (asynchronous messages). The Alarm & Status API interface also requires the instantiation of a 'psserver' server process on the MDM host.

Passport Log Streamer : The Passport Log Streamer application uses the MDM & Status API to acquire passport log data and then feeds the data stream into the syslog (custlog stream).

The alarms which are generated on Passport are received by the MDM and then sent to the SDM. The Passport Log Streamer application parses the data received from MDM and extracts the required fields needed to generate a customer log. These fields are

- time
- event
- compId
- Severity
- faultCode
- alarmType
- commentData

The above existing fields currently extracted by Passport Log Streamer application for Passport 15000 log from MDM API are also sufficient to generate the Passport 8600 log. The only difference lies in the values of the following fields.

- Log Name
- CompId
- faultcode
- commentData

Description of Fix

Support for Passport 8600 logs in Passport Log Streamer application.

Faultcode "C122XXXX" will be introduced into the "ReportNameMappingFile" file with a mapping to Log name "PPES". This will enable the Passport Log Streamer application to distinguish the logs which are generated by the Passport 8600 Network Element. The logs generated by the Passport 8600 Network Element will give a Report Name as "PPES".

ReportNameMappingFile

```
0000  CA
1100  INWP
3010  MDM
3011  MDM
7000  PPEM
7001  PPEM
7002  PPEM
7003  PPEM
7004  PPEM
---
---
C122  PPES
```

Selective filtering of logs from specific Passport 8600 network elements

The user will be provided the choice of filtering logs from specific passport 8600 network elements. Refer to the following example of the configuration interface.

Example of Configuration interface

Configuring Passport Log Streamer:

Enter the IP address for the first MDM[000.000.000.000]: 47.213.135.88

Enter the IP address for the second MDM[000.000.000.000]: 47.213.135.89

Enter the port number for the first MDM[3197]:

Enter the port number for the second MDM[3197]:

No previous MDM filters defined.

Do you want to receive MDM logs? [yln] :y

Enter MDM hostname 1 []: wcary2q5

Enter MDM hostname 2 []: wcary2q6

No previous Passport filters defined

Do you want to specify Passport 15000 filters? [yln] :y

How many Passport 15000 filters do you wish to specify? [3]:

Enter a Passport 15000 filter[]: PP15KA

Enter a Passport 15000 filter[]: PP15KB

Enter a Passport 15000 filter[]: PP15KN

Do you want to specify Passport 8600 filters?[yln] :y

How many Passport 8600 filters do you wish to specify? [3]:

Enter a Passport 8600 filter[]: PP86KA

Enter a Passport 8600 filter[]: PP86KB

Enter a Passport 8600 filter[]: PP86KN

Configuration selection summary:

MDM 1 IP Address: 47.213.135.88

MDM 2 IP Address: 47.213.135.89

MDM 1 Port: 3197

MDM 2 Port: 3197

MDM log reception: ON

MDM hostname 1: WCARY2Q5

MDM hostname 2: WCARY2Q6

The current defined Passport 15000 filters are:

Passport 15000 Filter 1 : PP15KA

Passport 15000 Filter 2 : PP15KB

Passport 15000 Filter 3 : PP15KN

The current defined Passport 8600 filters are:

Passport 8600 Filter 1 : PP86KA

Passport 8600 Filter 2 : PP86KB

Passport 8600 Filter 3 : PP86KN

Are the above configuration selections OK? [yln] :y

Generation of log for proxy alarm issued by MDM on behalf of Passport 8600.

When the proxy alarm with faultcode “09990013” is received, the Passport Log Streamer will generate a log with mapping to the Report Name of Passport 8600 (“PPES”).



SN07 Feature Deltas

Product = Centrex IP Client Manager (CICM)

A00003717 -- OSSGate - Centrex IP Flow-through Provisioning (IAW)

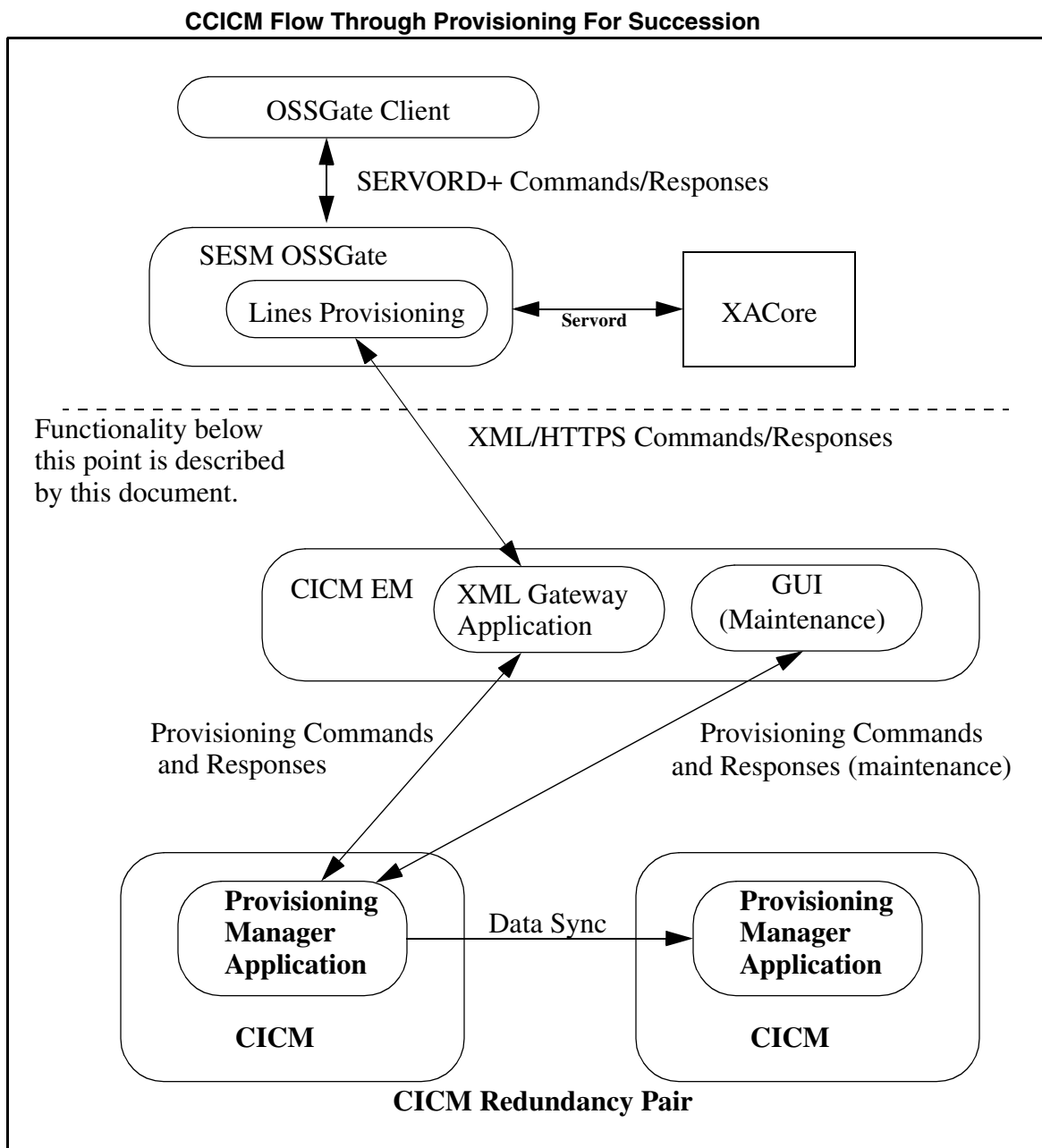
Description

This document describes the CICM component of new SUCCESSION functionality, providing support for the flow through of line and user provisioning data between the SESM OSSGate provisioning interface and the CICM platform.

Prior to the CICM 7.10 and SUCCESSION SN07 product releases, any provisioning requests targeted at the CICM platform would have been duplicated in 2 separate locations, the SESM OSSGate interface and subsequently the CICM Element Manager, so increasing the complexity of the provisioning operation and correspondingly increasing the possibility of service mismatches occurring due to human error.

As this document is specific to the CICM functionality, it is recommended that it be read with the corresponding SESM documentation, to gain a full understanding - please refer to cross references [1] and [2] on page 1999.

High Level Flow Through Provisioning Architecture



Support For Pre-Provisioned Lines

Changes will be made as part of this activity to support the introduction of pre-provisioned lines (feature key data). The modeling of feature key settings for the CICM lines is modified such that feature key settings are now stored against the line in question, as opposed to any user provisioned against that line. The modeling of lines at the SESM, CS2K and GWC components is also

updated by related features to introduce pre-provisioned line support for CICM.

These changes have the following functional implications:

- Line data fill always in existence at the SESM, CS2K and GWC platforms.
- Feature key settings being stored against the line, will survive any operations resulting in the deletion or replacement of a user entity, so allowing. This allows the CICM to remain in sync with the equivalent data fill present at the CS2K.

Feature Key Parameter Support

As the flow through provisioning activity requires that feature key settings are setup from the SESM OSSGate interface, this activity will ensure parity of support with provided at the CS2K. These changes involve the addition of missing feature key types, and the enforcement of equivalent rules at the flow through provisioning interface as are present at the CS2K.

Prior to this release, when setting up feature key options the options would need to be provisioned in two separate locations. Firstly from the OSSGate interface to provision the feature keys on the CM, and secondly from the CICM EM to ensure that the appropriate CICM node is aware of the feature key settings. With the previous release only a subset of the possible feature key settings were made known to the CICM EM, even though they represent functionality legally supported by the CICM nodes. This anomaly would be worked around by setting the appropriate feature key to the “Unknown” state indicating the presence of an unmappable feature key setting.

The flow through provisioning feature requires that CM feature key settings map correctly to those supported by the CICM EM and CICM. Hence those feature key settings missing from the earlier releases are added as part of this feature to ensure parity. These new mappings are represented by Table [“Feature Key Settings - CICM 7.10 Mappings Extensions” on page 1989](#) and Table [“Feature Key Settings - CICM 7.10 ACD DN Mapping Extensions” on page 1990](#). These do not represent new functionality, rather the correct modeling of existing functionality.

The following table describes the current feature key support. Where a CICM feature is shown with multiple SESM feature codes, this indicates multiple options applied against that key, with a single option being dominant from a CICM perspective.

Feature Key Settings - Existing Pre-CICM 7.10 Mappings

CICM Feature Code	SESM Feature Code	Description
Unassigned		No feature assigned to key
CFU	CFU	Call Forward

Feature Key Settings - Existing Pre-CICM 7.10 Mappings

CICM Feature Code	SESM Feature Code	Description
MWT	MWT	Message Waiting
CXR	CXR	Transfer
RAG	RAG	Ring Again
SCL	SCL	Speed Call
PDN	PDN	Primary DN
QTD	QTD	Time and date
AGN	INCALLS + DN	ACD Incalls (handled as INCALLS key)
DN	DN	Directory Number
ACDMSB	MSB	ACD make set busy
3WC	3WC	3 way call
DCPK	DCPK	Directed call
ACDNR	ACDNR	ACD not ready
ACDEMUR	EMR	ACD answer emergency
SPV	SUPR + DN	ACD incalls supervisor (handled as Supervisor key)
ACDCALLSUP	CLSUP + DN	ACD call supervisor
ACDEMURANS	AEMK + DN	ACD answer emergency
ACDAGNANS	AAK + DN	ACD answer agent
ACDAGNSTA	ASL	ACD agent status
ACDAGNOBS	OBS	ACD observe agent
C06	CNF	6 party conference
AUD	AUD	Auto dial
PRK	PRK	Non directed call
FXR	FXR	Fast transfer
CPU	CPU	Call pickup
ICM	ICM	Intercom (business sets)
CWT	CWT	Call waiting
QBS	QBS	Query busy station
DASK	DASK	ACD display agent summary
DQS	DQS	ACD display queue status
DQT	DQT	ACD display queue threshold

Feature Key Settings - Existing Pre-CICM 7.10 Mappings

CICM Feature Code	SESM Feature Code	Description
FAA	FAA	ACD forced agent availability
CIF	CIF	ACD Controlled interflow
NGTSRVCE	NGTSRVCE	ACD supervisor control of night service
LOB	LOB	ACD line of business
CAG	CAG + DN	ACD call agent
CALLFORCE	FORCING	ACD Call Agent with Call Forcing

The following table describes the additional feature key support for this release (excluding ACD DN related functionality).

Feature Key Settings - CICM 7.10 Mappings Extensions

CICM Feature Code	SESM Feature Code	Description
AAB	AAB	Automatic Answer Back
ACB	ACB	Automatic Callback
BLF	BLF	Busy lamp field
CCBS	CCBS	Call Completion To Busy Subscriber
CCV	CCV	Call Covering
COT	COT	Customer originated trace
CWD	CWD	Dial call waiting
EBO	EBO	Executive Busy Override
EMW	EMW	Executive message waiting
INSPECT	INSPECT	Calling Name Inspect Key
LVM	LVM	Leave message
MCH	MCH	Malicious call hold
MRFM	MRFM	Multiple Appearance DN Ring Forward
MSBI	MSBI	Make Set Busy Intragroup
MWIDC	MWIDC	Message Waiting Indication
MWQRY	MWQRY	Message waiting query
PRL	PRL	Privacy release
PRV	PRV	Privacy
SCS	SCS	Speed calling short list
SLQ	SLQ	Single line queuing

Feature Key Settings - CICM 7.10 Mappings Extensions

CICM Feature Code	SESM Feature Code	Description
UCDLG	UCDLG	Uniform call distribution login
GIAC	GIAC	Group intercom all calls
GIC	GIC	Group intercom
QCK	QCK	Quick conference key
SUBCOM	SUBCOM	Sub community route for emergency calls

The following table indicates those feature codes being added to support ACD DN type functionality. It is possible for multiple feature key settings to be provisioned against a line, and these options may be added or removed individually from the OSSGate interface, however a single dominant feature is always assumed to take precedence from a CICM perspective. The subordinate states are encoded so that CICM may correctly move between feature key settings on the individual options being added or removed.

Feature Key Settings - CICM 7.10 ACD DN Mapping Extensions

CICM Feature Code	SESM Feature Code	Description
SPVAGNDN	SUPR + INCALLS + DN	Supervisor key with subordinate INCALLS and DN options (Handled as Supervisor Key)
SPVAGNPDN	SUPR + INCALLS + PDN	Supervisor key with subordinate INCALLS and DN options (Handled as Supervisor key)
SPVPDN	SUPR + PDN	Supervisor key with subordinate PDN option (Handled as Supervisor key)
AGNPDN	INCALLS + PDN	Incalls key with subordinate PDN option (Handled as Incalls key)

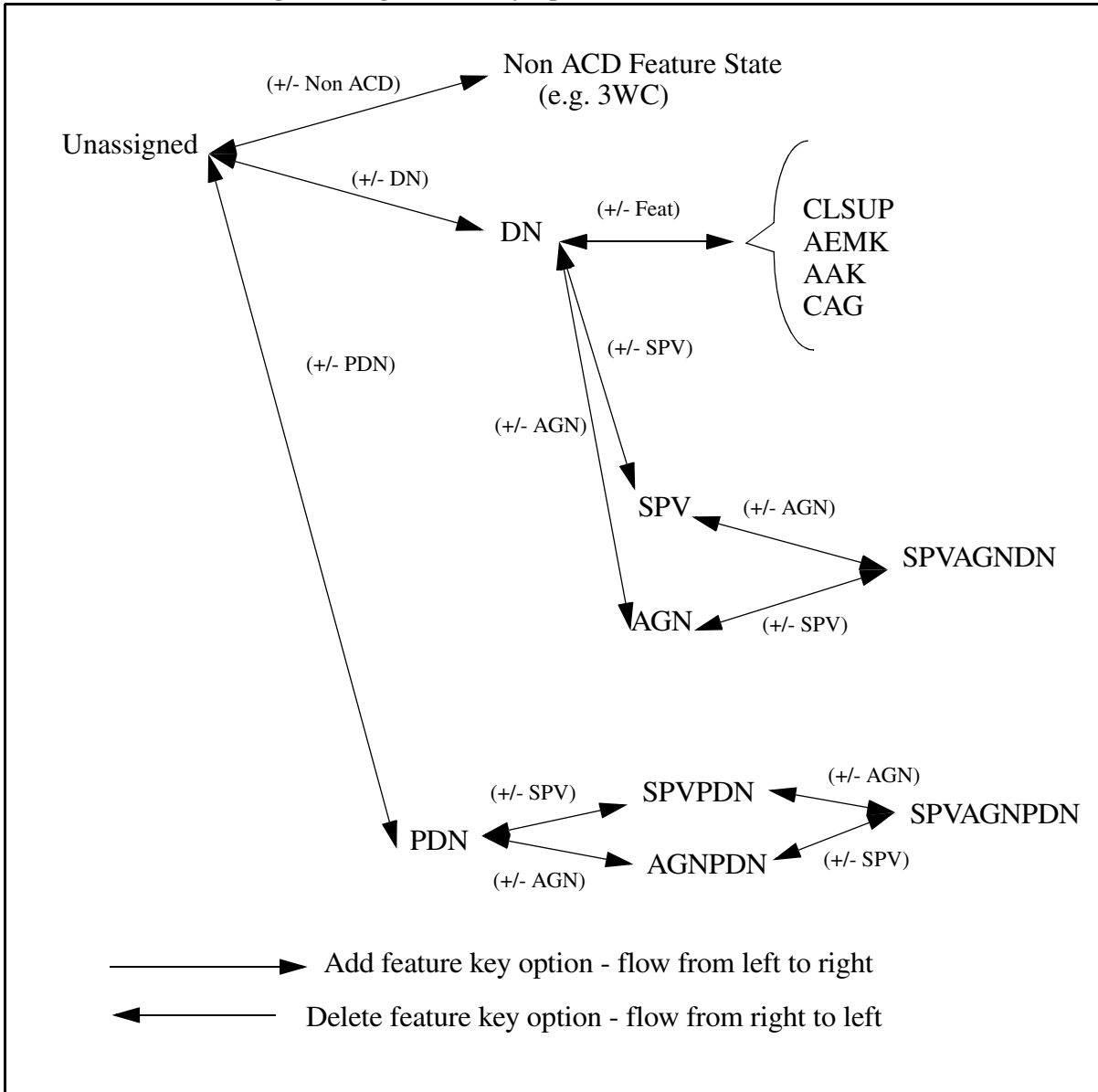
Note: Multiple SESM feature codes indicate that functionality is additive. Order of precedence runs from left to right, with that option listed first being dominant.

Flow Through Provisioning Interface Supported Operations

Flow Through Provisioning is driven on demand by SESM OSSGate. The usage of OSSGate is beyond the scope of this document, however what is documented in the following sections is a brief overview of the functionality provided on behalf of OSSGate. The relevant SESM documentation should be read to gain an understanding of how to drive that interface - see references [1] and [2] on page 1999.

The diagram in the following figure shows the valid transition states for adding and deleting feature key settings using the flow through addition and deletion functionality describes in earlier sections.

Adding / Deleting Feature Key Options



Feature Key Setting Addition

Feature key settings may be added incrementally against a valid CICM line feature key. The CICM platform will enforce the same rules that the CS2K applies when validating requests to add a feature to a feature key - specifically the translation from the original state to the new state must be valid.

Generically with the exception of ACD functionality this requires a feature key to move from the unassigned state to a new valid state.

Feature key addition will occur as a result of a OSSGate NEW or ADO command line option for ACD type functionality.

Feature Key Setting Deletion

Feature key settings may be deleted consecutively from a valid CICM line feature key. Performing a deletion will remove that option from the key in question, resulting the key moving into a new valid state. Typically this involves the key moving to the unassigned state - or potentially in the case of ACD functionality, to a new valid ACD state.

Feature key deletion will occur as a result of an OSSGate DEO command line option for ACD type functionality.

Feature Key Setting Updating

Feature key settings may be updated or overridden. This forces the feature key into a new state directly, regardless of any feature key setting previously in place. This allows the SESM OSSGate to directly set a feature key without needing to understand its previous state, which would impose additional overhead on the provisioning operation.

Feature key updating will occur as a result of an OSSGate NEW, ADO, DEO or CHF type operation for non ACD type functionality.

Line Outage

Flow through provisioning allows for a line to be reset to its original unassigned state. This has the immediate affect of deleting any user present on that line, and removing any provisioned feature key settings. This would occur if an OUT operation is invoked from OSSGate.

M522 Feature Key Extension Box Updating

Flow through provisioning allows the number of M522 extension boxes provisioned against a CICM line to be manipulated from OSSGate - so ensuring that an identical number of extension boxes are provisioned at the CICM and the CS2K, within the range 0 - 2 extension boxes.

User Creation

Flow through provisioning allows for CICM Users to be created on demand by the OSSGate interface. The presence of a valid User is a pre-requisite for a CICM line to become active as the data fill associated with the user is required for login purposes.

User Deletion

Flow through provisioning allows for the deletion of CICM users on demand by the OSSGate interface. Deletion of a CICM User effectively disables the line associated with that User as it will no longer be possible to log in.

User Updating

Flow through provisioning allows for the manipulation of selected parameters associated with a User. The users Password and/or Profile settings may be manipulated at the request of SESM OSSGate.

Flow Through Provisioning Order Of Data Fill

For the CICM 7.10 release, line feature key data fill and user data fill have been decoupled in-order to support pre-provisioned lines.

There is no imposed ordering to the order of data fill - feature keys may be setup against a line prior to a User entity being created or vice versa.

As the User entity is created on demand, the User password or profile settings may not be set in advance of creation.

Feature key settings will survive any deletion of an existing User, so allowing a new User to adopt the assigned settings for the line in question.

It is not possible for a line to go in service prior to the creation of a User entity as no mechanism exists for a handset to login exists without a valid User to associate against.

Provisioning Data Rollback

Flow Through Provisioning request from SESM OSSGate impact many functional components. As an example the setting of a group of feature keys in response to a Servord ADO command, results in provisioning requests being sent to both CICM and the XACORE. The potential exists for a request to fail either partially or completely at either the CICM or the XACORE.

Upon a failure being reported to SESM, the line provisioning application will request that all successful operations be rolled back to the previous state. This helps to maintain data consistency between the various SUCCESSION components.

Should it prove impossible to successfully perform a rollback of the CICM, the CICM EM GUI may be used to perform any manual corrections that are required.

Security And Access To Flow Through Provisioning

Access to the Flow Through Provisioning interface requires the presence of HTTPS security certificates at both the SESM and the CICM EM platforms.

These security certificates will be provided as part of the installation procedure, however should it be desired to provide alternative certificates, this will be supported.

Backwards Compatibility

Due to data fill changes required to support pre-provisioned CICM lines, the SESM platform will only provide Flow Through provisioning support for CICMs of vintage 7.10 or later. Any provisioning operation impacting a CICM running the 6.12 release or earlier must therefore be provisioned separately at the OSSGate interface and then subsequently at the CICM EM. This is due to there being no linkage between the SESM box and the CICM XML Gateway application.

This restriction is based on the vintage of the CICM box and not the managing CICM EM box, therefore the same restrictions apply to an installation running CICM EM release 7.10 with subtended CICM 6.12.

No support will be provided by the SESM OSSGate interface for TDM CICM installations.

Upgrade Considerations

Data fill changes at the CS2K XACore make it difficult to automate an upgrade between CICM 6.12 and CICM 7.10. No upgrade mechanism is therefore provided. Upgrading should be by means of a migration of service from a CICM running release 6.12 and CICM 7.10

The CS2K XACore load will support existing CICM 6.12 nodes and new CICM 7.10 nodes. Migration of service from CICM 6.12 to CICM 7.10 will be via means of the upgrade procedure described by reference [4] on page 2000.

User interface changes to the CICM EM GUI

Flow through provisioning changes the location of the feature key data from being held against a user, to being held against a line. This results in changes to the EM pages when managing a 7.10 (or higher) CICM. These changes are detailed in this section.

Editing line feature data

The existing browse users page is modified to provide a link to edit the data associated with a line. Note the additional hyperlink under the “Line No” column

Centrex IP Client Manager

CICM

status

configuration

terminals

users

maintenance

CICM-EM

status

synchronization

profiles

audio

enterprise

language

network

users on cicm cicm-001 (range 0-63 on vmc)

Line No	User	User Profile	Operation ?	Line No	User	User Profile	Operation
				0032			add
0001	000001		delete	0033			add
0002	000002		delete	0034			add
0003	000003		delete	0035			add
0004			add	0036			add
0005	000005		delete	0037			add
0006	000006		delete	0038			add
0007	000007		delete	0039			add
0008	000008		delete	0040			add

Clicking the hyperlink will load the page where the features can be corrected. In practise this page should not normally be used as the data should be provided by flow through provisioning. However should a mismatch occur, it can be corrected on this page.

Line Feature data entry page

On this page the user may enter the feature data filled against the Line.

ger

edit line 0001 on cicm-001

This page shows the features actually datafilled against the line on the CICM
During normal operation the data displayed by this page should NOT be altered.
Changes should be made only when a datafill mismatch between the CS2K and CICM has occurred

Feature Keys			
	Feature	User string	
Key 1	Primary DN	4162	Key 8
Key 2	Msg Wait		Key 9
Key 3	3 Way Call		Key 10
Key 4			Key 11
Key 5			Key 12
Key 6			Key 13
Key 7			Key 14

Extension Module 1 Keys

Changes to the user and profile pages

The feature key data is no longer stored within the profile or user override portions of the MIB, these page have been altered such that the feature key cannot be set. Instead for a user override the feature key from the line data is displayed along with the user override information. This can be seen in the next diagram. For profile pages no feature key data is displayed.

**trex IP
nt Manager**

CICM

status

configuration

terminals

users

maintenance

CICM-EM

status

synchronization

profiles

audio

enterprise

language

network

user

feature

diagnostics

diagnostics

Terminal Type	i2004			
Handset Transducer		db (Decibels)		
Headset Transducer		db (Decibels)		
Handsfree Transducer		db (Decibels)		

Feature Keys

	Feature	User string	AutoScroll	Inbox key		Feature	User string
Key 1	Primary DN	4162			Key 8		
Key 2	Msg Wait	Voice Mail			Key 9		
Key 3	3Way Call	Conf			Key 10		
Key 4					Key 11		
Key 5					Key 12		
Key 6					Key 13		
Key 7					Key 14		

Extension Module 1 Keys

Hardware Requirements or Dependencies

Hardware requirements as per a standard CICM installation. No special requirements exist for this functionality.

Software Requirements or Dependencies

Software must be aligned at the SN07 release at all SUCCESSION components.

Specifically:

- CS2K XACORE - CS2M0007 FCS
- CS2K SESM - SESM_7 FCS
- GWC - GN070 FCS
- CICM EM - 7.10 FCS

- CICM - 7.10 FCS

Limitations and restrictions

The following functional restrictions are imposed by the SESM platform:

- No mechanism to audit the CICM data fill against the SESM and CS2K XACORE.
- No mechanism to query CICM specific data fill from the SESM OSSGate interface (QLEN, QDN and related query operations). However CICM line data can be queried from the CS2K XACore via OSSGate.
- Provisioning requests that require SESM interaction with the CS2K XACORE will not flow through to the CICM. For example the provisioning of Hunt Groups.
- No support for CICM Release 6.12 or earlier.
- No support for TDM CICM releases as this is a SUCCESSION only delivery.

Note: Lack of Hunt Group provisioning flow through may result in a feature key assignment mismatch for those lines forming part of a hunt group. As the CS2K XACore data fill will be correct, this will manifest itself as a labelling mismatch. The outcome of selecting a mismatched feature key will be correct. The CICM EM GUI may be used to correct any mismatches, should this be desired.

Interactions

Flow through provisioning will interact with the SESM CICM OSSGate interface. This will manifest itself as an extension to the functionality available from OSSGate.

Applicable customer facing sections

Fault Management

Logs	___N/A___
Alarms	___N/A___

Configuration

Data Schema	___N/A___
User Interface	___X___
Element Management	___N/A___
Security	___X___
Service Order	___N/A___
Office Parameters	___N/A___

Accounting (includes AMA billing) _____N/A_____

Performance (includes operational measurements) _____N/A_____

Glossary

Term	Description
ACD	Call centre (administrative center) feature key functionality
ADO	Add Option (OSSGate / Servord)
CHF	Change Feature (OSSGate / Servord)
CICM	Centrex IP Client Manager
CICM EM	CICM Element Manager
CS2K	Nortel VoIP switch core (XACore)
DN	Directory Number
DEO	Delete Option (OSSGate / Servord)
FCS	Final Compile Ship
GWC	Gateway controller
HUNT Group	Grouping of 1 or more LENs / DN's into a functional group
LEN	Line Entity
NEW	Create new line (OSSGate / Servord)
OSSGate	SESM Northbound OSS interface for Line Provisioning
OUT	Remove line (OSSGate / Servord)
QDN	Query DN (OSSGate / Servord)
QLEN	Query Line Entity (OSSGate / Servord)
SERVORD	XACore line provisioning interface
SESM	Succession Element and Sub Element Manager
XACORE	Nortel switch core - CS2K

Cross References

[1] A00003717, Centrex IP Flow-Through Provisioning FN, SESM Component.

[2] A00001935, SESM Provisioning Support For Centrex IP Nodes And Lines

[3] A00003950, CICM Security Support

[4] CICM 6.12 To 7.10 Upgrade Procedure, David Tubb.

Product = Centrex IP Client Manager (CICM)

A00003718 & A00003719 -- Alarms, Logs & Performance for Centrex IP Client Manager (IAW)

Functional Description

This document contains the functional description for the Alarms, Logs and Performance feature for the SN07 release of the Centrex IP Client Manager (CICM). Fault and performance management is an important component of any Network Element in Succession. The ability for operators to detect, monitor and correct erroneous behavior and hardware outages is key to maintaining Quality of Service in a Succession network.

This feature will revisit the existing fault generation, logging and performance management capability of the CICM system. A new interface has been introduced to the Succession network that will manage the output used by external OSSs to monitor the network element and, for example, detect alarm conditions. This new interface is called the Integrated Element Manager System (IEMS). The IEMS can be accessed using a Graphical User Interface which will give access to the alarms and logs for a network element. This will also interact with the Element Manager GUI.

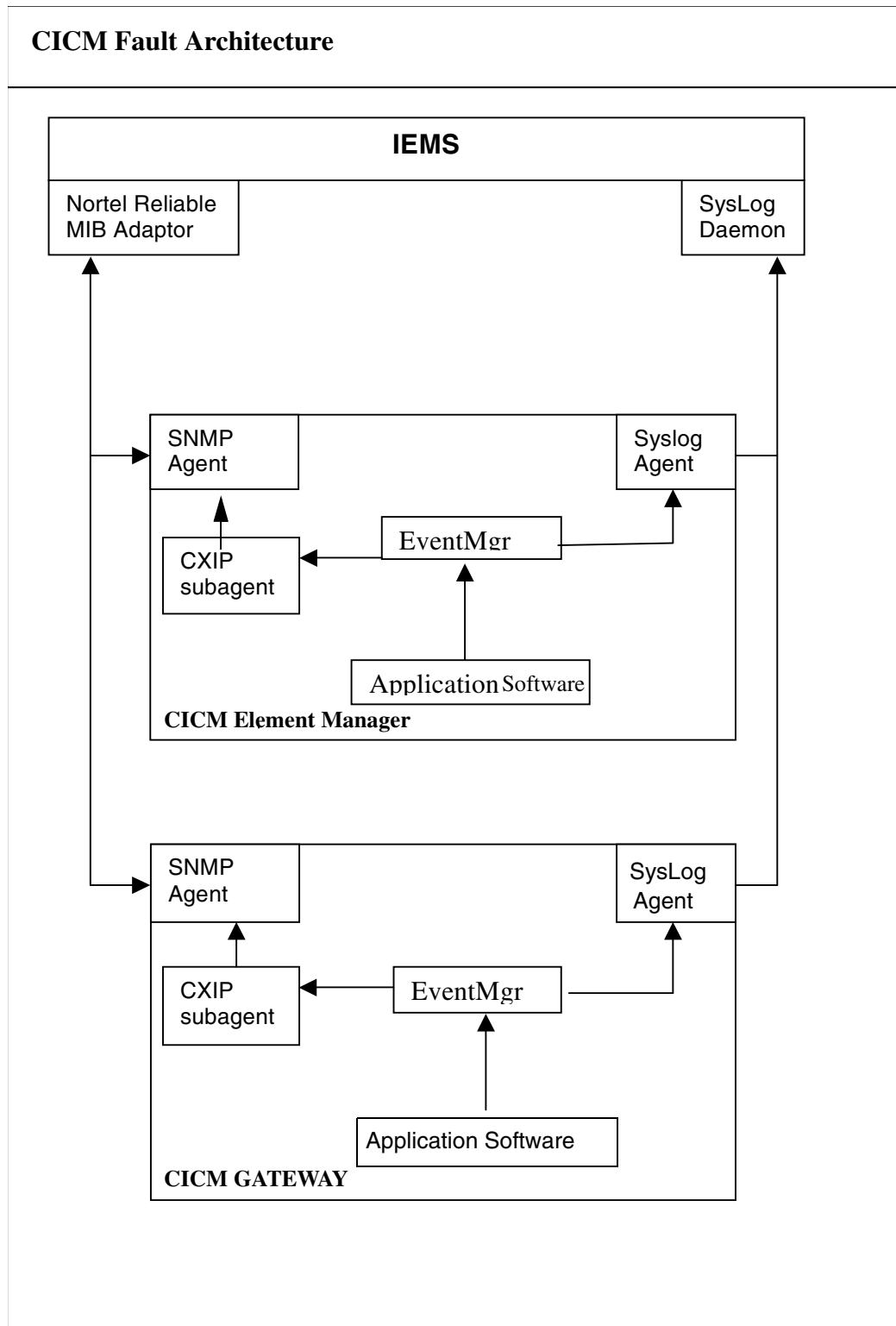
The CICM must integrate with the IEMS. Work needs to be done in this feature to raise alarms, logs and performance metrics in a suitable format that the IEMS can read.

There are two parts of the CICM system that can raise alarms and faults to the IEMS namely the CICM and the CICM Element Manager. The Element manager will raise alarms associated with the Element Manager Platform (e.g. memory shortage) and communication with the CICMs that it manages and will not have knowledge of the alarms and faults generated by the CICM. The CICM will send alarms as SNMP traps directly to the IEMS.

Logs are currently stored locally in debug and event Log files. Pertinent Event Logs must be sent to the OSS using Syslog formatted in the Custlog Format to aid debugging of alarms.

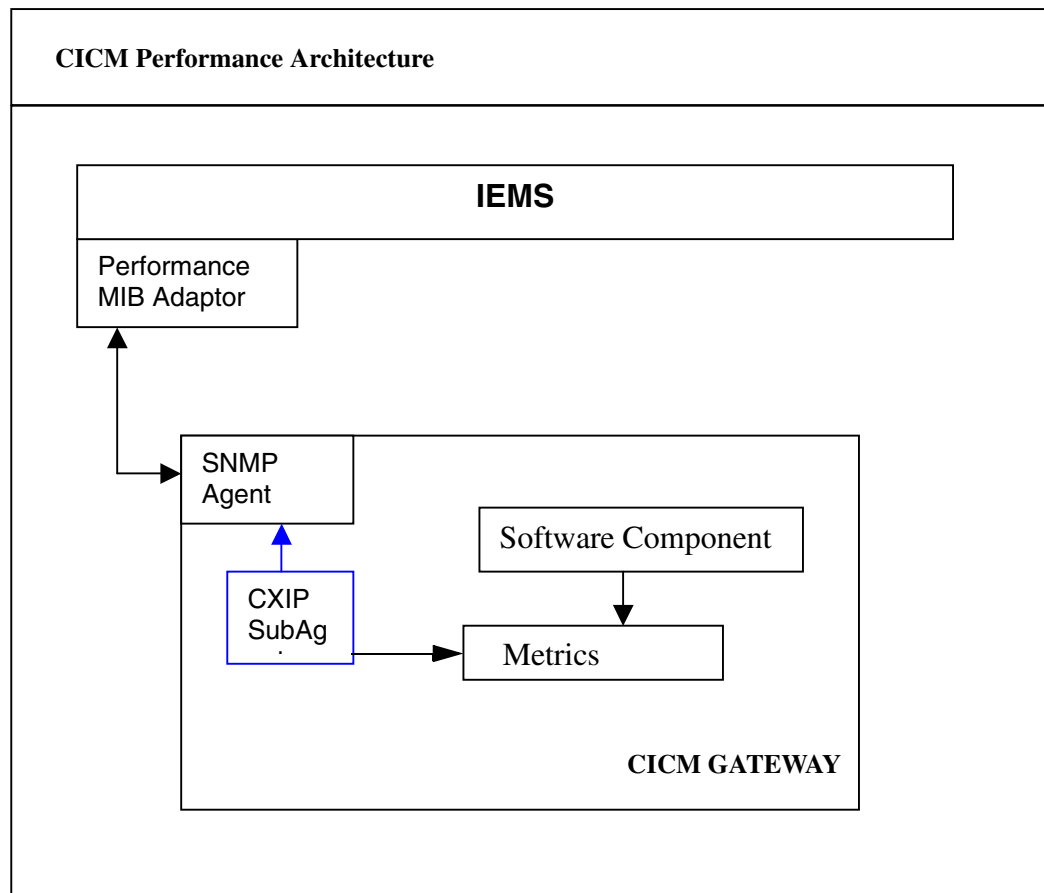
The following figure shows the overall intended system architecture for Faults and Logs.

CICM Fault Architecture



Performance management is a required part of any Succession system. A network element must be able to gather and provide statistical performance data to enable customers to evaluate the system and gauge where improvements would be most beneficial.

The following figure shows the overall intended Architecture for the Performance system.



It should be noted that there is no TDM support in this feature. Additional work will be required in order to support TDM within the new architecture. The nature of this extra work is to define and integrate the TDM specific cards into the architecture.

Applicable customer facing sections

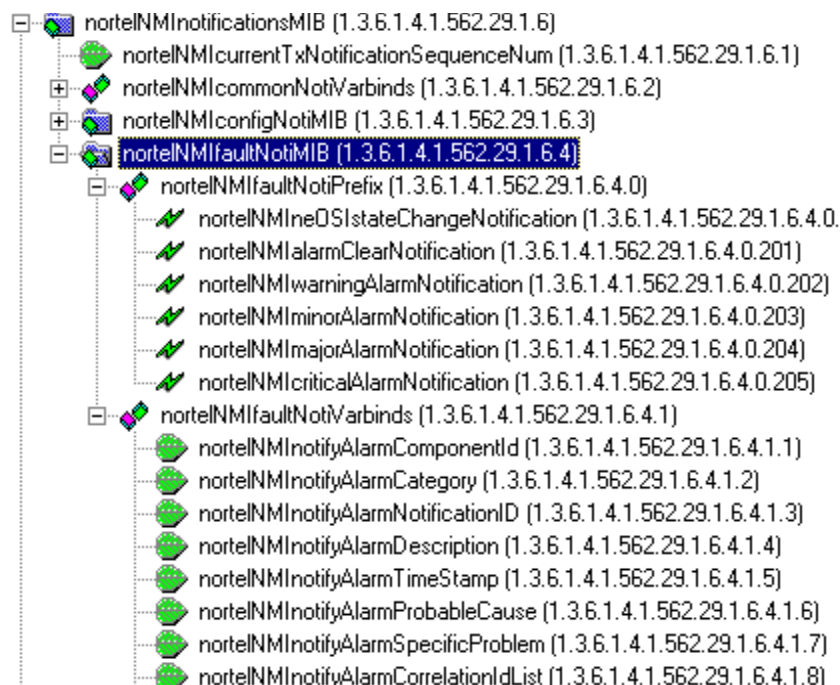
Alarms

All alarms are sent to the IEMS as an SNMP trap (to the Nortel Notifications MIB within the Nortel Reliable MIB, see Figure , on page 2004 . The CICM will store a copy of the trap information in the debug log. Each trap sent from the gateway will incorporate the following details:

- Sequence number.
- Severity indicator (see Table).
- Component ID – The distinguished name ID of the component in the Network element that the alarm was raised against.
- Category – The category of the Alarm (communications, quality of service, processing error, equipment or environment).
- Notification ID – Unique ID generated from the process number and sequence number combined.
- Description – The description text of the particular alarm.
- Time Stamp – The time the alarm was raised in UTC time.
- Probable Cause – An enum representing one of the most likely causes of the fault as defined in ITU-T X733 & X736.
- Specific problem – A refinement of the probable cause.
- Correlation ID list – To link this alarm with previous alarms and effectively override (clear) those alarms.

Alarm severity

	Critical	Major	Minor	Warning
Service Affecting	Yes	Yes	No (or few affected)	No
Action required	Yes	Yes	Yes	No
Recommended Timeliness of Action	Immediately – drop everything	Rapidly – in next work shift	Soon – could be delayed until next day	Later – investigate if reoccurrence
Target Reporting Time	Within 2 Sec	Within 30 Sec	Within 2 Min	Within 5 Min

Nortel Notifications MIB

Refer to the following table for a list of supported alarms.

Alarms

Object	Severity	probable cause
Element Manager		
failure to contact gateway	Major	eLanError
Authority server not available	Major	eOutOfService
CICM node		
GWC connection loss	Critical	eRemoteNodeTransmissionError
network messaging threshold reached	Major	eResourceAtOrNearingCapacity
network max connections reached	Major	eResourceAtOrNearingCapacity
terminal firmware update failure	Warning	eTransmitFailure
terminal max no of connections reached	Major	eThresholdCrossed
Windows Restart	Critical	eApplicationSubsystemFailure
Audit Mate Node Down	Warning	eUnspecifiedReason
Component failure : shutdown	Critical	eSoftwareProgramAbnormallyTerminated

Bad transition on mate node	Warning	eUnspecifiedReason
Audit: Mate Node Failed	Warning	eUnspecifiedReason
Chassis Failure	Major	eEquipmentMalfunction
No Message Received From B	Major	eLANError
Chassis Card State Change	Major	eUnspecifiedReason
ChassisStateChange	Major	eUnspecifiedReason
Major Red LED	Major	eEquipmentMalfunction
Minor Red LED	Minor	eEquipmentMalfunction
CPU A High Temp	Minor	eTemperatureUnacceptable
CPU B High Temp	Minor	eTemperatureUnacceptable
Cpu Card State Change	Major	eUnspecifiedReason
card OOS	Critical	eOutOfService
Card Alarm	Minor	eEquipmentMalfunction
Card Maintenance	Minor	eEquipmentMalfunction
chassis fan failure	Major	eheatingorventilationorcoolingsystemproblem
Platform		
mate node communication loss	Major	eOutOfService
SW version mismatch between nodes	Minor	eVersionMismatch
Syslog communication failure	Major	eCommunicationsSubsystemFailure
Critical Network Connection Not Responding	Critical	eLANError
Major Network Connection Not Responding	Major	eLANError
Process State Change	Critical	eApplicationSubSytemFailure
Service State Change	Major	eApplicationSubSytemFailure
host resources fault	Major	eResourceAtOrNearingCapacity
Max Rx Rate Exceeded	Minor	eRetransmissionRateExcessive
Max Creation Attempts	Minor	eRetransmissionRateExcessive
Backup Failure	Minor	eSoftwareProgramError
Fail Poll MG	Warning	eLANError

Component IDs

The CICM is divided into three objects for the purpose of reporting alarms, the CICM element manager, a CICM node and the platform which the EM and the CICM use. These objects contain sub-objects which appended together with the alarm type to form the Component Id.

Component IDs

Object	Sub Object	Component Id
CICM element manager	Node (CICM)	CICM=<CICM ID>;NODETYPE=cicmEm
CICM node	Terminal	CICM=<Cicm ID>;Nodetype=Cicm;Component=Terminals;terminal=<terminal ID>
	Cards	CICM=<Cicm ID>;Nodetype=Platform;Component=Card;Card=<card id>
CICM platform	Software Component	CICM=<Cicm ID>;Nodetype=Platform;SoftwareComponent=<component id >

Alarm Examples

Major Alarm Notification on Node A:

Component Id: CICM=CICM100A; Nodetype=CICM; User=000001

Category: 1 (communications)

Notification ID: 2

Description: Password Lockout

Probable cause: 101 (authentication Failure)

Specific Problem: user <userID> exceeded failed attempt threshold.

CorrelationId list: (list of alarms relating to other login attempt failures.)

Critical Alarm Notification on node B:

Component Id: CICM=CICM100B; Nodetype=Cicm; Component=chassis

Category: 4 (equipment)

Notification ID: 34

Description: Fan Overheating

Probable cause: 21– heatingOrCoolingOrVentilationProblem

Specific Problem:

CorrelationId list: (none)

Minor Alarm Notification on Node B:

Component Id:

Cicm=CICM100B; Nodetype=Cicm; Component=Card; CARD=<card number>

Category: 1 (communications)

Notification ID: 45

Description: Link OOS
Probable cause: 114 (out of Service)
Specific Problem:
CorrelationId list: (none)

Major Alarm Notification on node B:
Component Id: Cicm=CICM100B;Nodetype=Cicm;Component=CARD
Category: 1 (communications)
Notification ID: nnnn:nnnn
Description: Link group alarm - too many links OOS.
Probable cause: 51 (threshold exceeded)
Specific Problem:
CorrelationId list: (list of individual Link OOS alarms)

Alarm Throttling

The IEMS can receive logs at a maximum overall network rate. The CICM alarm generation rate must therefore keep within certain bounds in order to not exceed that IEMS rate. To solve this a throttling capability is required.

The alarm manager will meet this requirement by having separate buffers for each severity of alarm. This will enable the critical alarms to be sent immediately and for major, minor and warning alarms to be prioritized in order that they are sent within the required time periods as specified in Table , “Alarm severity,” on page 2003, but at a controllable rate. The rate of alarms being raised should be configured in the CICM registry MIB.

Alarm Provisioning

The CICM must be provisioned with the data it requires to determine whether it is to send traps and logs to an IEMS. A number of provisioning steps have been added to the preboot provisioning sequence to allow this. These steps are executed when the CICM load is first installed.

The following questions are asked relating to Alarms:

A prompt is made for an SNMP V1 and/or an SNMP V2c Trap destination as before:

Next, specify the IP addresses of the SNMP management stations that should receive traps and (alarm) notifications from this system.

Enter [list of] SNMP V1 Trap receiver address[es]:

>

Enter [list of] SNMP V2C Notification receiver address[es]:

>

If an IEMS is to be used the ip address of the IEMS should be provisioned in one of the above.

The next question confirms whether the IEMS is to be used.

Are the Above IP addresses IEMS Destinations? [Y\N, default=Y]
>

The next question asks about the Log destination. See “Log Provisioning” on page 2015. There will be a further chance to verify that the correct information has been entered (and alter it if not) before it is committed at the end of this provisioning stage. Invalid IP addresses including 0.0.0.0 and 255.255.255.255 will not be allowed.

Logs

This section describes the changes in logging functionality for both the CISM and the CISM element manager. Both the element manager and the CISM will be responsible for sending its own logs to the IEMS. Logs will not be exchanged between the CISM and element manager. The desired behavior for Logs is that they are sent to the IEMS using CUSTLOG or security log formats via a syslog agent. Three log streams will be used to send logs to up to three different syslog daemons (i.e. IEMS). This is an enhancement of the current functionality where all logs are stored on the CISM. Logs will still be stored on the CISM and the CISM will, in addition, send logs to custlog, audit log and security log streams. Each log must be formatted correctly for that particular stream.

The CISM will produce logs in the custlog or security log formats. This information will then be stored in the IEMS.

For this section the term CISM applies to both the CISM network element and the CISM element manager.

Syslog Details

The CISM will use the syslog protocol to send the logs to the IEMS. The CISM and CISM element manager will both act as senders. They will only be able to create and send syslog messages, they will not be able to receive or relay syslog messages. The CISM will conform to RFC 3164 The BSD syslog protocol [1].

As with most syslog applications UDP port 514 (the syslog port) will be used to send the syslog messages to the IEMS. The source UDP port will also be 514. The total length of the entire packet must not be greater than 1024 bytes. The CISM will not create a log that will exceed this limit.

To successfully send syslog packets to the IEMS the CISM needs to correctly format a syslog packet. The syslog packet can be split into three parts. The

first, named the PRI is a number that contains the syslog facility and severity. This number is enclosed in less than and greater than symbols < >.

The syslog facility is used to identify which process is responsible for raising the log. Below are two tables which show the facility and severity values that will be used by the CICM.

List of possible syslog facilities.

Code	Facility	Log Stream
0	kernel messages	
1	user-level messages	
2	mail system	
3	system daemons	
4	security/authorization messages	
5	messages generated internally by syslogd	
6	line printer subsystem	
7	network news subsystem	
8	UUCP subsystem	
9	clock daemon	
10	security/authorization messages	
11	FTP daemon	
12	NTP subsystem	
13	log audit	
14	log alert	
15	clock daemon	
16	Local use 0	
17	Local use 1	Custlog
18	Local use 2	
19	Local use 3	Audit log
20	Local use 4	
21	Local use 5	
22	Local use 6	Security log

Syslog packet severities

Code	Severity	Mapping custlog values
0	Emergency: system is unusable	
1	Alert: action must be taken immediately	Critical
2	Critical: critical conditions	Major
3	Error: error conditions	Minor
4	Warning: warning conditions	Minor
5	Notice: normal but significant condition	No alarm
6	Information	
7	Debug	

All logs sent to the IEMS must have a severity of 5 – Notice to enable the IEMS to differentiate between the logs and alarms.

The facility and severity fields will be used by the IEMS or another SYSlog daemon to sort the different logs into different problem areas and to highlight significant issues quickly.

The remainder of the syslog message is the MSG part. The MSG part has two fields known as the TAG field and the CONTENT field. The value in the TAG field will be the name of the program which generated the message, i.e. CISM. The CONTENT field contains the log in one of the supported formats, please see below.

Example of a syslog PRI and header.

```
<34> CISM: Log contents  
PRI process
```

The CISM will send log file header information after a system restart or whenever connection is opened the IEMS.

Syslog failure

If the CISM detects that a log stream has collapsed for any reason a SNMP trap will be sent to the IEMS. If the CISM cannot send any logs they will be buffered up to a point until the stream is operational. Please see section on throttling for details of buffer restrictions. If a problem occurs with the IEMS the CISM will not detect this and continue to send logs. These logs may become lost. The CISM will still store a local copy, which can be accessed via the CISM element manager. The CISM offers no guarantee that the log will be seen by the IEMS.

Custlog details

The CICM will log the following events using the custlog format and output the logs to the custlog stream.

- Service affecting state changes
- Specific customer/blm requested events
- Data corruptions/data mismatches

The custlog will contain the following information.

Node id is the name of the network element reporting the log. In this case it will be the name of the CICM gateway or element manager, e.g. CICM-100.

Hostname is the name or IP address of the element reporting the problem. In this case it will be the name of the side of active gateway or element manager, e.g. CICM100A

Application name is the type of network element reporting the log. In this case CICM.

Sequence number is a number applied each time the log is outputted. It is incremented by one for each log sent out on a particular stream. It is this mechanism that allows the IEMS to detect if it has missed a log. Valid sequence numbers are from 0 to 9999. When 9999 has been reached the number will be reset.

Report Name is a 4 char string representing the application that the log is being generated for (not the application doing the logging), e.g. CICM

ReportNum is a 3-digit number which ranges specify certain log categories.

Applications that generate new log reports must use the following log numbering scheme. Do not use the range 100-299 unless the log category does not fit into one of the standard categories.

Log Categories

Log Category Log	Number Range:
Trouble	300 to 399
Service summary	400 to 499
State Change	500 to 599
Information	600 to 799
Threshold	800 to 899

Expert	900 to 999

Alarm Value is one of: NONE, WARNING, MINOR, MAJOR, CRITICAL

All logs will have the value of NONE.

Event Type is one of: CBSY, EXC, FAIL, FLT, INFO, INIT, LO, MANB, OFFL, PASS, PBSY, RTS, SUMM, SYSB, TBL, TRAN, TRAP, UNEQ, THR.

Label is a string indicating the type of the log (perhaps identifying a subsystem) Label must not be “instance specific” – i.e. it is the same for all occurrences of log, e.g. Login failure.

TextFormat is a string detailing the log information – can be no longer than 860 chars. The following subfields are included in the test format:-

Location is the identifier of the machine sending the log.

Time is the time the error occurred.

ComponentID is an identifier of the system component that is sending the log. For more details see the alarm section.

Description is used to further describe the problem.

Required Syslog message format

May 24 00:02:00 rtpssdm oamp:

| Date, time, hostname, & Application generated by Syslog |

V2~I=CICM-130~H=CICM-130A~A=CICM~S=0001~~

| Node id || Host Name || Application || Sequence Number |

CICM 675 NONE INFO SDM OM FILE RETENTION

| Report name || report no || alarm value || Event Type || Label |

Breakdown of text format sub components.

Location: CICM-130-A^M

| Location |

Time: Fri Jun 04 17:18:56 2004^M

| Time |

ComponentID: CICM=CICM-130-A;NodeType=Cicm;Component=Card;Card=7^M

| Component ID |

Description: terminal id:7 Card 7 is INSV.

| Description |

For further details on field ranges and log reporting guidelines see Appendix A of the DID or <http://sdm.ca.nortel.com/vr23/resources/iempg.af05.pdf>

The logs should be indented by 8 characters and should be a maximum of 1000 characters.

Security log details

The CICM will log the following events using the security log format and output the logs to the security log stream.

- Unsuccessful terminal logins
- Successful terminal logins
- Unsuccessful PAM authentication.
- Successful PAM authentication.

Security logs will begin with a field identifying the class of log. For security this field value is class_security.vers01.

A security log will contain the following information. Other optional fields are supported by the log format but are not used by the CICM in this feature.

DST This is the address of the destination, e.g. the IEMS

DOC The document (DOC) field is the name of an accessed resource, e.g. CICM100A.

STAT The STAT field describes the state or status of the designed process. Possible values for this field may include “Failure”, “Success”, “Start”, “End”.

MID The Message Identifier allows message text to change, for translation to other language or to fix a typo, without affecting analysis tools. Another benefit of this would be saving bandwidth by not having to send the message itself. The value MUST be a unique string. The MID values would be stored at each sender, and the actual message templates would be stored at the collectors. This means that each sender (product) must submit to the collector/analyzer, message template files defining its’ MIDs. Separate template files would be required for each language. The collectors would need

to be configured to a certain language. The format of these message template files is defined in Ref 3 Section 3.2, "MID Message Template Format".

This field is currently not supported by the CICM or the IEMS. A value of 0 will be used.

SRC.OFFEND

The offending source field is the address of the originating packet, which triggered a security audit event. For this feature it will be the IP address of the CICM. If omitted it implies it is the same as the source address.

Optional fields:

SRC.USR

User name or user id.

EVNT.TYPE

The event type field specifies the type or classification of the event, e.g. login.

HOST The name of the host issuing the log.

CMD

This field is used to supply a little more information on the security breach. For example in the case of a terminal login failure the field will include the terminal ID and the login the person used.

Audit logs

The following actions will be logged to the audit stream:

- Addition or removal of CICMs from a CICM EM.
- Addition or removal of a profile from either a CICM or a CICM EM (controlled from the EM web pages).
- Any action using flow through provisioning e.g adding/deleting a user.

The audit logs will be in the same format as the security logs.

Debug log

Debug logs are logs that are not of interest to Nortel customers., e.g. swerrs should be classed as a debug log. No work will be done to enhance the debug logs. Currently debug logs are viewed via the CICM EM. Debug logs will not be sent via syslog to the IEMS. Any log or notification that is sent to the IEMS will be copied into the debug stream.

Log Throttling

There is an overall maximum rate that the IEMS can receive logs. The CICM logging device will contribute to that overall log rate; so it must therefore keep

within certain bounds in order to meet that IEMS rate. To solve this problem a throttling capability is needed. The customer should be able to set the number of logs that can be sent over a specified time frame. When the rate of logs being produced exceeds the threshold the remaining logs will be buffered until a time when they can be sent. If logs are being buffered for an extended period of time it will be possible to fill the buffer. In this scenario logs will be lost. Each log stream will have its own log buffer.

Debug logs will not be throttled as they are simply output to a file and not transmitted to the IEMS. A copy all logs and notifications will be sent to the debug stream even though they may have been buffered and lost. Therefore it should always be possible to get copies of lost logs or notifications.

Log Viewing

The logs which are stored on the CICM will be viewable from a page on the CICM EM. The EM will request the log files from the CICM and display them using a web page. This functionality is not part of this activity.

Log Provisioning

The CICM must be provisioned with the data it requires to determine whether it is to send traps and logs to an IEMS. A number of provisioning steps have been added to the preboot provisioning sequence to allow this. These steps are executed when the CICM load is first installed.

The following questions are asked for provisioning Logs:

This step follows on from the provisioning of trap information.

The following questions are asked:

Are Logs to be sent to Syslog stream destinations? [Y\N, default=N]

>

Next the ip addresses of the three syslog destinations are required, A prompt is made for CustomerLog, SecurityLog and Audit Log destinations in turn.

Next, specify the IP addresses of the Syslog management stations that should receive Customer, Security and Audit logs from this system. Enter each IP addresses in dotted form.:

Enter the network address of the Syslog destination for Custlogs:

>

Enter the network address of the Syslog destination for Security Logs:

>

Enter the network address of the Syslog destination for Audit Logs:

>

This Question is followed by the Performance provisioning Step (see “Performance Metric Provisioning” on page 2017). There will be a further chance to verify that the correct information has been entered (and alter it if not) before it is committed at the end of this provisioning stage. Invalid IP addresses including 0.0.0.0 and 255.255.255.255 will not be allowed.

Performance

Performance management is an important component of any Network Element in Succession.

A network element must be able to gather and provide statistical performance data to enable third parties to evaluate the system and gauge where improvements would be most beneficial. The ability for operators to monitor behavior and trends is key to maintaining Quality of Service in a Succession network.

This feature will revisit the existing performance management capability of the CICM system. A new interface has been introduced to the Succession network that will manage the output used by external OSSs to monitor CICM network elements. This new interface is called the Integrated Element Manager System (IEMS).

The CICM and CICM-EM network elements must integrate with the IEMS. Work will be done in this feature to make available performance metrics in a suitable format that the IEMS can read.

Currently a number of performance metrics are gathered in the CICM System and are logged and recorded.

The Performance metrics currently gathered are:

- Percentage Memory usage
- Number of Active Users
- Number of Active connections
- Percentage CPU Usage

Additional metrics that will be gathered include the following:

- Number of Busy hour call attempts
- Number of logged in users
- Number of Logs sent
- Transmitted bytes/sec
- Received bytes/sec.

Each of these metrics will be collected, averaged over a specific time interval and stored in the MIB.

Within the CICM software an audit function will collect each metric after a specified time interval has elapsed.

Some measurements (those relating to call traffic) will be taken every 5 minutes. Other measurements will be collected and averaged over either 15 or 30 minute intervals. There are no 5 minute interval metrics planned in the CICM. The 15 or 30 minute interval will be configured in the registry MIB. On installation of a new load the user will be prompted to select either a 15 or 30 minute interval for collection of data for all metrics, given the number of metrics provided this will be the only method of configuration. The interval selected will apply to all metrics.

The metrics will be stored in the performance MIB and will be collected at intervals by the IEMS.

Performance Metric Provisioning

The CICM must be provisioned with the data it requires to determine the interval over which performance metrics are to be collected. A provisioning step has been added to the preboot provisioning sequence to allow this. This step is executed when the CICM load is first installed.

The following question is asked for provisioning performance metrics: This step follows on from the provisioning of log information.

The following question is asked:

Enter the time interval over which performance metrics will be measured [15/30]:
>

There will be a further chance to verify that the correct information has been entered (and alter it if not) before it is committed at the end of this provisioning stage.

Data schema (DS)

A new MIB has been created as the key for this feature. There is a CICM MIB which makes performance data available to registered Trap listeners. This interface will be unaffected in the SN07 release. The performance data will still be made available via the existing interface for TDM implementations.

The new MIB interface has been created to integrate with the concept of a Nortel standard Performance MIB. The performance MIB has a number of fields for each performance Metric as follows:

- index - unique numeric key for each metric on a CICM basis
- metric name – text describing the name of the metric
- metric value type (counter or gauge)
- metric range - max & min
- metric gauge usage (average or peak)
- metric value holding registers (4 registers)
- metric current value - or
- metric current value OID - if the current value is kept in another MIB.

At the time of writing the MIB interface definition has not been completed, but will be finished in time for this development.

Hardware Requirements or Dependencies

The following is a list of the minimum hardware required for this feature:

- One CS2K
- One GWC with a CICM profile
- One CICM-EM
- One CICM
- Ccm Ethersets
- One IEMS platform

Software Requirements or Dependencies

Integrated Element Manager System (IEMS) Software is the recommended tool to be used in order to be able to access the output of this feature.
(loadname and firmware load)

Limitations and restrictions

The CICM will not guarantee that the IEMS will receive and logs or traps that it sent.

Each CICM can only datafill three log streams. It is possible to create a stream to three different IEMS.

This feature does not support TDM platforms for this release. Only the succession platform is supported. The existing TDM implementation will function as before however this feature is not intended for a TDM release and the necessary TDM components are not supported.

Changing the severity of an alarm, once set, is not supported.

Interactions

Glossary

Term	Description
CICM	CentrexIP Client Manager
CICM EM	CentrexIP Client Element manager
MIB	Managed information Base
VoIP	Voice over IP
XPM	eXtended Peripheral Module

References

- [1] The BSD syslog Protocol RFC 3164
- [2] Log Strategy for non-core Succession NEs v4.8
- [3] OA&M Security Audit Log Format SRD Issue 1.1.doc

Product = MG 4000

A00003650 -- MG4K-IP Logs (PT-IP, UA-IP)

Functional Description (FN)

This feature provides logs for the MG4K-IP product in SN07. The log series MG4I is introduced by this activity. The following logs are supported:

- MG4I 501 - Stream Control Transmission Protocol (SCTP) IP Control Connection Maintenance (CCMT) Core connection state change
- MG4I 502 - SCTP IPCCM Peer connection state change
- MG4I 300 - Media Integrity Failure
- MG4I 301 - Gigabit Ethernet Audit Subnet mismatch

The MG4I 501 and 502 logs are used by the IPCCM subsystem to generate logs to track the state transitions of SCTP connections from the MG4K-IP node to the core and peer nodes. The MG4I 300 and 301 logs are generated for problems reported by the corresponding subsystem in the CEM/GEM on the MG4K-IP node. However, the changes required in the CEM/GEM for these logs is to be implemented in SN08.

SCTP IP CCMT connection state change

The MG4I 501 log is generated for state change of the SCTP connection between the call server and the MG4K-IP node.

```
RTPH MG4I502 MAY02 22:04:48 800 INFO SCTP Peer Connection State Change
  From Node : MG4K 6 (47.108.11.3:5050; Associd: 10)
  To Node : MG4K 5 (47.142.211.1:5050)
  State Change From: ESTABLISHED To: CLOSED
  Reason : FAR END DISCONNECTED
  Location: SPM 6 Type: SMG4 Fabric: IP
```

The MG4I 502 log is generated for state change of the SCTP connection between an MG4K-IP node and its peer node.

```
RTPH MG4I502 MAY02 22:04:48 800 INFO SCTP Peer Connection State Change
  From Node : MG4K 6 (47.108.11.3:5050; Associd: 10)
  To Node : MG4K 5 (47.142.211.1:5050)
  State Change From: ESTABLISHED To: CLOSED
  Reason : FAR END DISCONNECTED
  Location: SPM 6 Type: SMG4 Fabric: IP
```

Media Integrity Failure

The MG4I 300 log is generated for any integrity failure detected in the media path for a call.

```
RTPH MG4I300 SEP04 03:41:44 2801 TBL Media Integrity Failure
  Call Type: G711
  Src IP: 47.108.11.3:5050 Dest IP:47.142.211.1:5050
  Description: RTCP Media Integrity Timer Expired
  Location: SPM 1 Type: SMG4 Fabric: IP
```

GigE Audit Failure

The MG4I 301 log is generated when GigE Audit has detected a problem in the subnet between the active and inactive GEM cards.

```
RTPH MG4I301 SEP04 03:41:44 2801 TBL GigE Audit Failure
  RM: GEM 0 in slot 1
  Description: Subnet Audit Mismatch
  Gateway IP: 47.108.11.3 GEM IP: 206.136.134.24
  Location: SPM 1 Type: SMG4 Fabric: IP
```

Hardware Requirements or Dependencies

This feature is specific to the MG4K-IP product line with associated hardware.

Software Requirements or Dependencies

No new software dependencies are introduced by this activity.

The MG4I 300 and 301 logs are generated for problems reported by the corresponding subsystem in the CEM/GEM on the MG4K-IP node. However, the changes required in the CEM/GEM for these logs is to be implemented in SN08.

Limitations and restrictions

None.

Interactions

These logs are accessible through the LOGUTIL CI interface in SOS. The craftsperson can access the MG4K-IP specific logs as follows:

```
>logutil  
>open MG4I  
>back all
```

Applicable customer facing sections

Fault Management

Logs	<u> X </u>
Alarms	<u> N/A </u>

Configuration

Data Schema	<u> N/A </u>
User Interface	<u> N/A </u>
Element Management	<u> N/A </u>
Security	<u> N/A </u>
Service Order	<u> N/A </u>
Office Parameters	<u> N/A </u>

Accounting (includes AMA billing)	<u> N/A </u>

Performance (includes operational measurements)	<u> N/A </u>

Indicate with an X if you are completing the sections of the DDOC listed below. Indicate with “N/A” if these sections do not apply to this functionality.

Realtime	<u> N/A </u>

Engineering Information	<u> N/A </u>

Glossary

Term	Description
SCTP	Stream Control Transfer Protocol
CCMT	Control Connection Maintenance
IP	Internet Protocol
GEM	Gigabit Ethernet Module
CEM	Common Equipment Module
IPCCM	Internet Protocol Control Connection Maintenance
CI	Command Interface

Fault Management for A00003650

Fault management strategy

This feature provides logs for the MG4K-IP product in SN07. The log series MG4I is introduced by this activity. The following logs are supported:

- MG4I 501 - Stream Control Transmission Protocol (SCTP) IP Control Connection Maintenance (CCMT) Core connection state change
- MG4I 502 - SCTP IPCCM Peer connection state change
- MG4I 300 - Media Integrity Failure
- MG4I 301 - Gigabit Ethernet Audit Subnet mismatch

These logs provide the craftperson with the capability to detect fault conditions and configuration issues.

Fault management tools and utilities

The logs can be viewed and reporting can be controlled using the existing LOGUTIL CI.

MG4I 501 Log

Log Title/Log ID: SCTP Core Connection State Change - MG4I 501

Formats

The format for MG4I 501 log report is as follows:

```
<Alarm Sev.> MG4I501 <date> INFO SCTP Core Connection State Change
  From Node : CORE (<Core IP addr>:<port>; Associd: <SCTP assoc id>)
    To Node : MG4K <SPM no:> (<MG4K IP addr>:<port>)
    State Change From: <SCTP From State> To: <SCTP To State>
    Reason : <State Change Reason>
    Location: SPM <SPM no:> Type: <DMSCP, IW, SMG4, DPT > Fabric: <IP,
ATM, UNK>
```

Example:

```
*** MG4I501 MAY02 22:04:48 800 INFO SCTP Core Connection State
Change
  From Node : CORE (47.108.11.3:5050; Associd: 10)
    To Node : MG4K 6 (47.142.211.1:5050)
    State Change From: ESTABLISHED To: CLOSED
    Reason : FAR END DISCONNECTED
    Location: SPM 6 Type: SMG4 Fabric: IP
```

Explanation

Description: This INFO log is generated when the SCTP IPCCM Core Connection state changes for an MG4K-IP node. IPCCM maintains the SCTP connection for reliable messaging between the call server and the MG4K-IP node. The state change log from 'CLOSED' to 'ESTABLISHED' indicates that the connection is up. The state change log from 'ESTABLISHED' to 'CLOSED' indicates that the connection is down. The trunks will go down and no call processing is possible when the connection is down. This is indicated by log alarm severity of Critical.

Field descriptions

Field descriptions

Field	Value	Description
From Node	CORE (<Call Server IP addr in dotted decimal format>: <Port>; Associd: <Association id>)	Indicates the call server Sctp connection end point IP address, port and Sctp association id.
To Node	MG4K <SPM no: (0 to 85)> (<MG4K IP addr in dotted decimal format>:<Port>)	Indicates the MG4K IP node, Sctp connection end point IP address, port
From Sctp State	string of 12 char length {CLOSED, ESTABLISHED}	Indicates the old Sctp connection state.
To Sctp State	string of 12 char length {CLOSED, ESTABLISHED}	Indicates the new Sctp connection state.
State Change Reason	1 line of variable text of 60 characters	Indicates the reason for the Sctp connection state change
Location	SPM <SPM no: (0 to 85)>, Type: {DMSCP, IW, SMG4, DPT}, Fabric: {IP, ATM, UNK}	Indicates the SPM node location. It can only be an MG4K node with IP Fabric. The SPM node number is the same as that in 'To Node' field.

Action

If the Sctp state change is from 'ESTABLISHED' to 'CLOSED', check the state change reason and corresponding NODE and SPM logs to determine possible causes of Sctp connection failure and attempt to recover the Sctp connection.

Associated Operational Measurements or Performance Measurements

Not Applicable.

Additional information

Not Applicable.

MG4I 502 Log

Log Title/Log ID: SCTP Peer Connection State Change - MG4I 502

Formats

The format for MG4I 502 log report is as follows:

```
MG4I502 <date> INFO SCTP Peer Connection State Change
  From Node : MG4K <SPM no:> (<MG4K IP addr>:<port>; Associd:
<SCTP assoc id>)
    To Node : <MG4K, GWC> <Node no:> (<Node IP addr>:<port>)
              <MG4K, GWC> <Node no:> (<Node IP addr>:<port>)
              ....
              <list of up to 29 peer IP nodes>
  State Change From: <SCTP From State> To: <SCTP To State>
  Reason : <State Change Reason>
  Location: SPM <SPM no:> Type: <DMSCP, IW, SMG4, DPT > Fabric: <IP,
ATM, UNK>
```

Examples:

```
MG4I502 MAY02 22:04:48 800 INFO SCTP Peer Connection State Change
  From Node : MG4K 6 (47.108.11.3:5050; Associd: 10)
    To Node : MG4K 5 (47.142.211.1:5050)
  State Change From: ESTABLISHED To: CLOSED
  Reason : FAR END DISCONNECTED
  Location: SPM 6 Type: SMG4 Fabric: IP

MG4I502 MAY02 22:04:48 0800 INFO SCTP Peer Connection State Change
  From Node : MG4K 6 (47.108.11.3:*; Associd: *)
    To Node : MG4K 5 (47.142.211.1:5050)
              MG4K 7 (47.142.211.2:5050)
              MG4K 10 (47.142.211.23:5050)
              MG4K 22 (47.142.211.24:5050)
  State Change From: ESTABLISHED To: CLOSED
  Reason : REPORTED BY PERIPHERAL
  Location : SPM 6 Type: SMG4 Fabric: IP
```

Explanation

Description: This INFO log is generated when the SCTP IPCCM Peer Connection from an MG4K-IP node to a peer MG4K-IP node changes state. IPCCM maintains the SCTP connections for reliable messaging between the MG4K-IP node and all its peer MG4K-IP nodes for peer-peer signaling during call processing. The state change log from 'CLOSED' to 'ESTABLISHED' indicates that the connection is up. The state change log from 'ESTABLISHED' to 'CLOSED' indicates that the connection is down. The messages are bounced off the call server when the peer connection is down.

Field descriptions

Field descriptions

Field	Value	Description
From Node	MG4K <SPM no:(0 to 85)> (<MG4K IP addr in dotted decimal format>: <Port>; Associd: <Association id>	Indicates the MG4K IP node, SCTP connection end point IP address, port and SCTP association id.
To Node list	Up to 29 nodes MG4K <SPM no: (0 to 85)> (<MG4K IP addr in dotted decimal format>:<Port>)	Indicates the peer MG4K IP node, SCTP connection end point IP address and port for up to 29 peer SCTP connections undergoing state changes.
From SCTP State	string of 12 char length {CLOSED, ESTABLISHED}	Indicates the old SCTP connection state.
To SCTP State	string of 12 char length {CLOSED, ESTABLISHED}	Indicates the new SCTP connection state.
State Change Reason	1 line of variable text of 60 characters	Indicates the reason for the SCTP connection state change
Location	SPM <SPM no: (0 to 85)>, Type: {DMSCP, IW, SMG4, DPT}, Fabric: {IP, ATM, UNK}	Indicates the SPM node location. It can only be an MG4K node with IP Fabric. The SPM node number is the same as that in 'From Node' field.

Action

These logs do not indicate a service affecting change. If the SCTP state change is from 'ESTABLISHED' to 'CLOSED', check the state change reason and corresponding NODE and SPM logs to determine possible causes of SCTP connection failure.

Associated Operational Measurements or Performance Measurements

Not Applicable.

Additional information

In SN07, the peer IP nodes are only MG4K-IP nodes managed by the same call server. The peer nodes may include GWC in a future release.

MG4I 300 Log

Log Title/Log ID: Media Integrity Failure - MG4I 300

Formats

The format for MG4I 300 log report is as follows:

MG4I300 <date> TBL Media Integrity Failure
Call Type: <Call type string>
Src IP: <Src IP addr>:<port> Dest IP: <Dest IP addr>:<port>
Description : <Media Integrity Failure Reason>
Location: SPM <SPM no:> Type: <DMSCP, IW, SMG4, DPT > Fabric: <IP, ATM, UNK>

Example:

MG4I300 SEP04 03:41:44 2801 TBL Media Integrity Failure
Call Type: G711
Src IP: 47.108.11.3:5050 Dest IP:47.142.211.1:5050
Description: RTCP Media Integrity Timer Expired
Location: SPM 1 Type: SMG4 Fabric: IP

Explanation

Description: This TBL log is generated when a media integrity failure has been detected during a call. The corresponding call is taken down.

Field descriptions

Field descriptions

Field	Value	Description
Call Type	8 character string	Indicates the call type codec (G711, G729)
Src IP	<Src IP addr in dotted decimal format>:<Port>	Source IP address and port
Dest IP	<Dest IP addr in dotted decimal format>:<Port>	Destination IP address and port
Description	1 line of variable text of 50 characters	Indicates the reason for the media integrity failure
Location	SPM <SPM no: (0 to 85)>, Type: {DMSCP, IW, SMG4, DPT}, Fabric: {IP, ATM, UNK}	Indicates the SPM node location which reported this failure. It can only be an MG4K node with IP Fabric.

Action

Check the description and investigate the cause of integrity failure.

Associated Operational Measurements or Performance Measurements

Not Applicable.

Additional information

Not Applicable.

MG4I 301 Log

Log Title/Log ID: GigE Audit Failure - MG4I 301

Formats

The format for MG4I 301log report is as follows:

MG4I301 <date> TBL GigE Audit Failure
 RM: <RM type> <RM no> in slot <slot no:>
 Description: <GigE Audit Failure Reason>
 Gateway IP: <Gateway IP addr> GEM IP: <GEM IP addr>
 Location: SPM <SPM no:> Type: <DMSCP, IW, SMG4, DPT > Fabric: <IP, ATM, UNK>

Example:

MG4I301 SEP04 03:41:44 2801 TBL GigE Audit Failure
RM: GEM 0 in slot 1
Description: Subnet Audit Mismatch
Gateway IP: 47.108.11.3 GEM IP: 206.136.134.24
Location: SPM 1 Type: SMG4 Fabric: IP

Explanation

Description: This TBL log is generated when GigE Audit has detected a problem in the subnet between the active and inactive GEM cards. This is possibly due to the inactive GEM RM being added to an invalid router or network. The RM is unable to provide service.

Field descriptions**Field descriptions**

Field	Value	Description
RM	<RM type> <RM no:> in slot <slot no:>	Indicates the GEM RM which has the mismatch
Description	1 line of variable text of 50 characters	Indicates the mismatch detected
Gateway IP	<Gateway IP addr in dotted decimal format>	Router/Gateway IP address
GEM IP	<GEM IP addr in dotted decimal format>	IP address of GEM RM which has the mismatch
Location	SPM <SPM no: (0 to 85)>, Type: {DMSCP, IW, SMG4, DPT}, Fabric: {IP, ATM, UNK}	Indicates the SPM node location. It can only be an MG4K node with IP Fabric.

Action

Validate the datafill in table MNMGPIP for the GEM RM reporting the mismatch.

Associated Operational Measurements or Performance Measurements

Not Applicable.

Additional information

Not Applicable.

Alarms

Not Applicable.

Related documentation

Not Applicable.

Performance for A00003650

Performance management strategy

This feature provides several new logs for the SMG4-IP product line, which are used to indicate possible performance affecting issues. One of these new logs is used to indicate a counter overflow in the Operational Measurement pegs, the other logs are not Performance or OM related.

Performance management tools and utilities

The new logs are accessible via the common LOGUTIL access. The OM related log is MG4I320, indicating an OM Counter Overflow.

Performance Measurements (PM), Operational Measurements (OM), and stats

No new PM or OM counters are being added by this feature.

This feature adds a log indicating an overflow of OM counters in the SMG4-IP product.

Example:

MG4I320 SEP04 03:41:44 2801 TBL SMG4-IP OM Overflow

RM: GEM: 0

Description: OM Counter Overflow.

Location: SPM 1Type: SMG4 Fabric:

Product = MG 4000

A00003669 -- Media Gateway 4000 - Internet Protocol (MG4K-IP) (PT-IP)

Functional Description

MG4KIP Product to support following table control changes

- FABRIC field is included in table MNNODE
- It enforces restriction on RM datafill based on the FABRIC type in MNNODE.

- RM datafill restriction in table MNCKTPAK.
- signaling Address datafill in MNMGPIP for MG4K (and IW) tuples
- VLAN TCIs datafilled in MNMGPIP for Bearer and signaling paths on GEM RMs
- DIFFSERV codepoints for signaling and voice data added to table MNIPPARM
- Media Integrity Indicator added to table MNIPPARM

Note that the signaling address design description is described under feature A00003659.

Hardware Requirements or Dependencies

No new hardware requirements for this feature.

Software Requirements or Dependencies

This feature requires SN07 loads in the call server, MG420 loads in the MG4K CEMs and GEM20 in the GEM RMs.

Limitations and restrictions

- New SGFABRIC field is only for the MG4K SPMs. It is not part of the IW or DMSCP SPMs node datafill.
- SGFABRIC field change is restricted - certain conditions must be met before the tuple is allowed to change.
- signaling IP address changes are restricted on MG4K - GEM must be out of service because this would cause node isolation.
- signaling IP address cannot be enabled unless a valid signaling IP address has already been datafilled. Once enabled, the signaling IP address cannot be changed without disabling it first.
- VLAN TCI-VID for bearer is restricted to 255 on NTLZ20AA, BA, and CA cards due to Broadcom Calisto DSP specification.
- Media Integrity Indicator requires RTCP to be enabled prior to enabling MI.

Interactions

This feature interacts with functionality provided by A00003659, which did not include an FN or a CN section. All table changes are documented in this feature instead.

Applicable customer facing sections

Fault Management

Logs

n/a_____

Alarms	n/a_____
Configuration	
Data Schema	X_____
User Interface	n/a_____
Element Management	n/a_____
Security	n/a_____
Service Order	n/a_____
Office Parameters	n/a_____
Accounting (includes AMA billing)	n/a_____
Performance (includes operational measurements)	n/a_____

Glossary

Term	Description
VLAN TCI	Virtual Lan Tag Component Indicator
DIFFSERV	Differentiated Services, using codepoints to potentially assign priority to packets for different applications. See IETF document RFC3260

Configuration for A00003669

Hardware and Software Requirements

Standard MG4K SPM node with all the datafills and RMs.

Initial Configuration

Not Applicable.

Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable.

Upgrade Impact

Not Applicable.

Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
MNNODE	changed-New field SGFABRIC is added for SMG4 (MG4K) class SPM.	new
MNMGPIP	changed- New fields GEMSIGIP, SIGSUBMASK, SIGWIP, BEARERVLAN, SIGVLAN, SIGIPENABLED are added	new
MNIPPARM	changed - new fields DIFFSERV and MEDIA_INTEG are added	new

Table/MIB/Remote Database Schema information

Name: MNNODE

Management Network Node Table

Functional description

This feature adds a new **SGFABRIC** field to the MG4K class of SPM in table MNNODE. T. For ATM MG4K nodes, this new field, **SGFABRIC**, is set to 'ATM' and for IP MG4K nodes, it is set to 'IP'.

Usage sequence and implications (CM Only)

Current datafill order unchanged.

Size

It does not change.

Fields/OIDs

The following table gives the information about the new fields introduced in table MNNODE.

MNNODE Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SGFABRIC	New		ATM or IP	If the value is set to 'ATM', it indicates that the particular MG4K is of ATM framework. The value of 'IP' indicates that the MG4K node is of IP framework. The default value is set to 'ATM' after TABXFR from previous releases to release having this change.

Datafill example**MAP display for table MNNODE**

<pre> NODEKEY ALIAS NODEINFO ----- SPM 4 SPM_4 SMG4 0 SYNC LINE 50 (COT 60) (DTMF 60) (ECAN 60) (TONESYN 60) (MF 60) \$(SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT) (SYSBNA CR RPT) (MANBNA MJ RPT) (COTLOW MN RPT) (DTMFLOW MN RPT) (ECANLOW MN RPT) (TONESLOW MN RPT) (MFLOW MN RPT) (CMRLOW MN RPT) (SMG4CN MN RPT) (PATCHFAIL MJ RPT) (ATMBCN CR RPT) (ST3EHL MJ RPT) (ST3EHL24 CR RPT) (SMCHLD MJ RPT) (SMCHLD24 CR RPT) (SPMSRMNTD MN RPT) (LOCUR MJ RPT) (TSRCFAIL CR RPT) \$ \$ N 0 \$ N N ATM </pre>

Table release history update**SN07:**

New field **SGFABRIC** is added to the table for SMG4 variant of SPM. This field is defined as a signaling FABRIC type. If this field is set to 'ATM', then only ATM RMs can be datafilled in MNCKTPAK. If the field is set to IP then only GEM RMs can be datafilled in MNCKTPAK.

Supplementary information

The field **SGFABRIC** can be changed for a datafilled MG4K node. Node must be in OFFL state for SGFABRIC field change operation. Steps to be followed during MG4K-ATM to MG4K-IP are listed below.

- BSY/OFFL the RM and CEM on the MG4K-ATM
- Delete all the tuple entries in table ATMCONN for the desired node.
- Delete All entries for MG4K-ATM from table MNATMIF.

- BSY/OFFL all ATM carriers.
- Delete ATM Carriers from table MNHSCARR
- Delete ATM RM datafill from the table MNCKTPAK.
- Delete ATM_GRP from table MNPRTGRP
- Add GEM_GRP in table MNPRTGRP
- Add load info in table PMLOADS.
- Change SGFABRIC field value from ATM to IP in table MNNODE
- Datafill GEM RM in the table MNCKTPAK for the desired node.
- Datafill table MNMGPIP, with entries for newly added GEM RMs.
- Change entries in table MNIPPARM for fine tuning of IP parameters.
- BSY/RTS MG4K-IP CEM and RMs.

For MG4K-IP to MG4K-ATM similar steps are followed with little changes.

Error messages for MNNODE:

- Trying a SGFABRIC change when the node is MANB/INSV/ISTb state.

For ATM to IP change:

Error: Failed to change SGFABRIC from ATM to IP.
Please OFFL the node before attempting SGFABRIC change.

For IP to ATM change:

Error: Failed to change SGFABRIC from IP to ATM.
Please OFFL the node before attempting SGFABRIC change.

- SGFABRIC change fails to verify node update tuple due to internal error.

Error: Failed to change SGFABRIC due to internal error.

- SGFABRIC change from ATM to IP fails because table ATMCONN datafill related to node undergoing change is not deleted.

Error: Failed to change SGFABRIC from ATM to IP.
Delete all the tuples corresponding to
SPM 10 from table ATMCONN

- SGFABRIC change from IP to ATM fails because table MNMGPIP datafill related to node undergoing change is not deleted.

Error: Failed to change SGFABRIC from IP to ATM.
Delete all the tuples corresponding to
SPM 10 from table MNMGPIP

- SGFABRIC change verification passes for ATM to IP operation.

Warning: Verification passed for SGFABRIC change from ATM to IP.
Please ensure that MNMGPIP is datafilled.

- SGFABRIC change verification passes for IP to ATM operation.

Warning: Verification passed for SGFABRIC change from IP to ATM.
Please ensure that ATMCONN is datafilled.

Name: MNCKTPAK***Management Network Circuit Pack*****Functional description**

This feature adds datafill restrictions for slot 1, 2, 9 & 10 of shelf 1 for RMs.

Usage sequence and implications (CM Only)

Current datafill order unchanged.

Size

It does not change.

Fields/OIDs

No Change.

Datafill example

No Change.

Table release history update**SN07:**

New datafill restrictions are applicable only if the GEM RM is provisioned in the SPM.

Supplementary information

None.

Error messages in MNCKTPAK

- Block ATM RM addition in table MNCKTPAK if the sgfabric of the node is IP.

Error: ATM RM cannot be datafilled because the SGFABRIC field in table MNODE is set to IP. Only GEM RM can be datafilled.

- Block GEM RM addition in table MNCKTPAK if the fabric of the node is ATM.

Error: GEM RM cannot be datafilled because the SGFABRIC field in table MNODE is set to ATM. Only ATM RM can be datafilled.

- No CPKs are allowed to be datafilled in slots 1, 2, 9 & 10 of shelf 1 if GEM RM is datafilled in any of these slots of shelf 0 because of thermal dissipation.

Error: No CPKs are allowed to be datafilled in slots 1/2/9/10 of shelf 1 while GEM RM is already datafilled in the same slot on shelf 0 since thermal restrictions dictate that we leave the slot empty over a GEM RM.

- GEM RM is not allowed to be datafilled in slot 1, 2, 9 & 10 of shelf 0 if any other RM is already datafilled in any of these slots of shelf 1.

Error: GEM RM is not allowed to be datafilled in slots 1/2/9/10 of shelf 0 while any other RM is already datafilled in the same slot on shelf 1 since thermal restrictions dictate that we leave the slot empty over a GEM RM.

Name: MNMGPIP

Management Network Media Gateway Processor Internet Protocol

Functional description

This feature adds 6 fields to the MNMGPIP table: the signaling IP address, the signaling mask, the signaling enabled status, the signaling gateway, the VLAN TCI for the signaling interface, and VLAN TCI for the bearer interface.

Usage sequence and implications (CM Only)

Current datafill order unchanged.

Restrictions on VLAN TCI values:

- Upon ONP to SN07, the default value showing a 0 N 0 will be used
- For the Bearer VLAN TCI, changes to this field will not be allowed without BSYing or OFFLing the GEM RMs. For signaling VLAN TCI, the change can be made on the fly for the FIRST CHANGE ONLY - once the TCI has been set, then the GEMs will have to be BSY in order to change the value. This is because the IP interface is active when the GEM is INSV - changing these values requires re-provisioning the far-end switch for VLAN as well and this would cause an INSV GEM to go SYSB.
- If the default value of '0 N 0' is present for a VlanTCI in the table, that GEM interface will not perform VLAN tagging of outgoing packets but will instead fill that word with the NULL VLAN tag.

Restrictions on signaling address:

- GEMSIGIP and SIGSUBMASK default to 0.0.0.0 for an IW-SPM during an ONP to SN07; this ensures the signaling interface starts out disabled on the new load.

- SIGIPENABLED field defaults to N during an ONP to SN07. It can be changed to Y only after a valid address has been entered in SIGIPADDR and SIGSUBMASK. It can be changed back to N at any time to disable IP signaling on the GEM.
- On an IW-SPM, GEMSIGIP and SIGSUBMASK are allowed to change from 0.0.0.0 to any valid value and back to 0.0.0.0 while the GEM is INSV and the SIGIPENABLED boolean is FALSE. All other changes are blocked.
- In the future, an MG4K-IP SPM will be provisioned; for these nodes, the SIGIP fields must all contain valid values and are not allowed to change while the GEM is INSV.

Size

Table tuple limits unchanged.

Fields/OIDs

The following table lists fields/OIDs for MNMGPIP.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GEMSIGIP	new	none	0 0 0 0 to 255 255 255 255	The usual DMS-format IP Address range (no "dots" in the field) used as the address for signaling interface
SIGSUBMASK	new	none	0 0 0 0 to 255 255 255 255	The usual DMS-format IP Address range (no "dots" in the field) used as the mask for signaling interface
SIGWIP	new	none	0 0 0 0 to 255 255 255 255	The usual DMS-format IP Address range (no "dots" in the field) used as the mask for signaling interface
SIGIPENABLED	new	none	Y or N	Is
BEARVLAN	new	PRIORITY	0-7	User Priority
BEARVLAN	new	CFI	Y or N	Canonical Format Indicator - only N is supported

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
BEARVLAN	new	VID	0-4095 (*255 for Calisto-based GEM RMs)	VLAN ID - a unique number to identify the VLAN (* NTLZ20AA, BA, and CA boards are restricted to 255 due to Broadcom Calisto DSP implementation), and 1 & 4095 are reserved by spec and are not allowed to be entered.
SIGVLAN	new	PRIORITY	0-7	User Priority
SIGVLAN	new	CFI	Y or N	Canonical Format Indicator - only N is supported
SIGVLAN	new	VID	0-4095	VLAN ID - a unique number to identify the VLAN - 1 and 4095 are reserved by the spec and are not allowed to be entered.

Datafill example

The following example shows sample datafill for table MNMGPIP.

MAP display for table MNMGPIP

```

>table mnmgpip
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: MNMGPIP
>list all
TOP
      MGPKEY
      GEMMGPIP      SUBNMASK      BCASTIP      GWIP
      GEMBARIP      AUTONEG
      GEMSIGIP      SIGMASK      SIGGWIP      SIGIPENA
      BEARVLAN      SIGVLAN
-----
      SPM  0 0  9
172  16 121  2  255 255 255  0  172  16 121 255  172  16 121  1
172  16 121  4                                Y
172  16 121 11  255 255 255  0  172  16 121  1                                Y
      0 N 0                                0 N 0
      SPM  0 0 10
172  16 121  3  255 255 255  0  172  16 121 255  172  16 121  1
172  16 121  4                                Y
172  16 121 11  255 255 255  0  172  16 121  1                                Y
      0 N 0                                0 N 0

```

Table release history update**SN07:**

New fields are present and datafilled “benignly” so that their features are not enabled over an ONP. They must be manually enabled at the customers need.

Supplementary information

The “range” command from the switch, just in case anyone is interested:

```

1 MGPKEY          T_SMGPCT_KEY
2 GEMMGPIP        IP_ADDRESS
3 SUBNMASK        IP_ADDRESS
4 BCASTIP        T_SMGPDEF_IP_ADDRESS
5 GWIP           T_SMGPDEF_IP_ADDRESS
6 GEMBARIP        T_SMGPDEF_IP_ADDRESS
7 AUTONEG        BOOL
8 GEMSIGIP        IP_ADDRESS
9 SIGSUBMASK      IP_ADDRESS
10 SIGGWIP        IP_ADDRESS
11 SIGIPENABLED   BOOL
12 BEARERVLAN     T_VLAN_TCI
13 SIGVLAN        T_VLAN_TCI
LOGICAL TUPLE TYPE: T_SMGPCT_LT

```


Translation verification other tools

None

Name: MNIPPARM***Management Network Internet Protocol PARaMeters*****Functional description**

This feature adds 2 fields to the MNIPPARM table: the DIFFSERV codepoints and the Media Integrity Indicator.

Usage sequence and implications (CM Only)

Current datafill order unchanged.

Size

Table tuple limits unchanged.

Fields/OIDs

The following table lists fields/OIDs for MNIPPARM.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DIFFSERV	new	EF_CODEPOINT	6-bits as ASCII, prefixed by "CP" for CodePoint, i.e.: CP101110	The codepoint for voice band defaults to CP101110
DIFFSERV	new	EF_PRIORITY	0-7	The priority for voice defaults to 6
DIFFSERV	new	CS5_CODEPOINT	6-bits as ASCII, prefixed by "CP" for CodePoint, i.e.: CP101000	The codepoint for signaling data defaults to CP101000
DIFFSERV	new	CS5_PRIORITY	0-7	The priority for signaling defaults to 6

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
MEDIA_INTEG	new	MI_STATUS	ENABLE or DISABLE	Indicates the state of Media Integrity on this GEM card, defaults to DISABLE
MEDIA_INTEG	new	MI_ACTION	NONE, LOGONLY, TEARDOWN	Indicates the action to be taken when MI fails.
MEDIA_INTEG	new	MI_INTEGER	0 to 32767	Today, this is unused but will be required when MI functionality is fully defined.

Datafill example

The following example shows sample datafill for table MNIPPARM.

MAP display for table MNIPPARM

```

>table mnipparm
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: MNIPPARM
Mate>list all
TOP
MNKEY  DFCODEC PRFCODEC PKTRATE INGRESS EGRESS JITMIN JITMAX JITTARG
      ECAN   VOICE CMFNOISE      T38 RFC2833 RTCP      TONESET LOGINT
CRCERROR USIZEPKT OSIZEPKT FRAGMENT JABBER DROPEVNT BRDCAST  JITTER LATENCY
VPKTLOST MINLOG      OMPARMS      DIFFSERV
      MEDIA_INTEG
-----
-
IWSPM G711ULAW      NONE      10      0      0      0      100      0
      DISABLE      OFF  DISABLE  DISABLE  DISABLE  N  NORTHAMERICA      5
  20  10  20  10  20  10  20  10  20  10  20  10  20  10  20  10  20  10
  20  10      1000  50  1000  1000 CP101110 6 CP101000 6
      DISABLE

MG4K G711ULAW      NONE      10      0      0      0      100      0
      DISABLE      OFF  DISABLE  DISABLE  DISABLE  N  NORTHAMERICA      5
  20  10  20  10  20  10  20  10  20  10  20  10  20  10  20  10  20  10
  20  10      1000  50  1000  1000 CP101110 6 CP101000 6
      DISABLE

BOTTOM

```

Table release history update

SN07:

New fields are present and datafilled with their default values so that their features are not enabled over an ONP. They must be manually enabled at the customers need.

Supplementary information

Media Integrity requires that RTCP field be set to “Y” before it can be enabled.

Once MI is enabled, RTCP can no longer be set to “N” until MI is disabled once again.

The range commands from the switch, just in case anyone wants to see them:

```
30 DIFFSERV          DIFFSERV_TYPE
31 MEDIA_INTEG       MEDIA_INTEGRITY_STATUS_TYPE
LOGICAL TUPLE TYPE: T_MNPARM_LT
Mate>range 30
30 DIFFSERV          DIFFSERV_TYPE
TYPE IS DIFFSERV_TYPE MULTIPLE WITH
    EF_CODEPOINT     DIFFSERV_CODEPOINT
    EF_PRIORITY      {0 TO 7}
    CS5_CODEPOINT    DIFFSERV_CODEPOINT
    CS5_PRIORITY     {0 TO 7}
Mate>range 31
31 MEDIA_INTEG       MEDIA_INTEGRITY_STATUS_TYPE
TYPE IS MEDIA_INTEGRITY_STATUS_TYPE MULTIPLE WITH
    MI_STATUS        {ENABLE,DISABLE} REFINEMENTS:
    {DISABLE}        MI_DISABLE_ACTION_FIELD
    {ENABLE}         MULTIPLE WITH
        MI_ACTION     {NONE,LOGONLY,TEARDOWN}
        MI_INTEGER    {0 TO 32767}
```

Translation verification other tools

None

Service Orders (SO) (CM & SESM)

Not Applicable

Software optionality control (SOC).

Not Applicable.

Element Management

Not Applicable.

Command interface changes

Not Applicable

Security

Not Applicable

Configuration Walkthrough

N/A

Product = MG 4000

A00003672 -- GEM NTLZ20CA Core Definition (PT-IP)

Functional Description

This feature provides the software support for the new NTLZ20CA 1000bLX (1300 nm, single mode) w/ LC connector pec code for the IP MG4K/IW GEM card.

Hardware Requirements or Dependencies

There are no hardware requirements or dependencies being introduced by this feature. This is simply adding a new pec code to the existing list of supported pec codes for MG4K and IW SPMs.

Note: The actual new card hardware is NOT required for this pec code to be implemented as a supported pec code for MG4K.

Software Requirements or Dependencies

There are no software requirements or dependencies being introduced by this feature. This is simply adding a new pec code to the existing list of supported pec codes for MG4K and IW SPMs.

Limitations and restrictions

There are no limitation introduced by this feature. This is simply adding a new pec code to the existing list of supported pec codes for MG4K and IW SPMs.

Interactions

There are no interactions with other features introduced by this feature. This is simply adding a new pec code to the existing list of supported pec codes for MG4K and IW SPMs.

Applicable customer facing sections

Fault Management

Logs

N/A

Alarms

N/A

Configuration

Data Schema	_X__
User Interface	_N/A__
Element Management	_N/A__
Security	_N/A__
Service Order	_N/A__
Office Parameters	_N/A__
Accounting (includes AMA billing)	_N/A__
Performance (includes operational measurements)	_N/A__

Glossary

Term	Description
IP	Internet Protocol
GEM	Gigabit Ethernet Module

Configuration for A00003672

Note: All unnecessary sections have been deleted from this document section. If it has been deleted then the reader can assume it is not applicable.

Hardware and Software Requirements

None.

Upgrade Impact

None.

Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
MNCKTPAK	CHANGED	UNCHANGED

Table/MIB/Remote Database Schema information

Name: MNCKTPAK

MN (SPM) RM Circuit Pack Table

Functional description

This is an addition of a new value to an existing field:

Existing Field: PEC

New Value: NTLZ20CA

Existing Format:

```
TABLE: MNCKTPAK
>ran
  1 CPKKEY          T_SPMCKT_KEY
  2 CPKINFO         T_SPMCKT_CKTPAK
  3 PEC             T_SPMCKT_CPK_PEC
  4 RELEASE         T_CPK_RELEASE
  5 LOAD            EIGHT_CHAR_VECTOR
LOGICAL TUPLE TYPE: T_SPMCKT_LT
>ran 3
  3 PEC             T_SPMCKT_CPK_PEC
TYPE IS T_SPMCKT_CPK_PEC
NORTEL Product Engineering Code:
{NTLX63AA,NTLX65AA,NTLX66AA,NTLX71AA,
NTLX73AA,NTLX99AA,NTLX72AA,NTLX65BA,
NTLX66BA,NTLX73AB,NTLX73BA,NTLX82AA,
NTLX82AB,NTLX82BA,NTLX89DA,NTLX67AA,
NTLX99BA,NTLX73BB,NTLX72BA,NTLX89AA,
NTLX83AA,NTLX92AA,NTLX74AA,NTLX76AA,
NTLX44AA,NTLX82EA,NTLZ20BA}

Non-NORTEL Product Identification Code:
TABLE OF 8 CHARs
```

New Format:

```
TABLE: MNCKTPAK
>ran
  1 CPKKEY          T_SPMCKT_KEY
  2 CPKINFO         T_SPMCKT_CKTPAK
  3 PEC             T_SPMCKT_CPK_PEC
  4 RELEASE         T_CPK_RELEASE
  5 LOAD            EIGHT_CHAR_VECTOR
LOGICAL TUPLE TYPE: T_SPMCKT_LT
>ran 3
  3 PEC             T_SPMCKT_CPK_PEC
TYPE IS T_SPMCKT_CPK_PEC
NORTEL Product Engineering Code:
{NTLX63AA,NTLX65AA,NTLX66AA,NTLX71AA,
NTLX73AA,NTLX99AA,NTLX72AA,NTLX65BA,
NTLX66BA,NTLX73AB,NTLX73BA,NTLX82AA,
```

NTLX82AB, NTLX82BA, NTLX89DA, NTLX67AA,
 NTLX99BA, NTLX73BB, NTLX72BA, NTLX89AA,
 NTLX83AA, NTLX92AA, NTLX74AA, NTLX76AA,
 NTLX44AA, NTLX82EA, NTLZ20BA, **NTLZ20CA**}

Non-NORTEL Product Identification Code:
 TABLE OF 8 CHARs

Usage sequence and implications (CM Only)

Not within scope of this document.

Size

Size of tuples or number of allowed tuples are not changed by this design.

Fields/OIDs

The following table lists fields/OIDs for <abbreviated name of table/MIB>.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
PEC	CHANGED	None	new value to be added: NTLZ20CA	New circuit pack for the GEM MG4K RM.

Datafill example

The following example shows sample datafill for table MNCKTPAK for the GEM RM.

```
CPKKEY CPKINFO PEC RELEASE LOAD
```

```
-----  

SPM 0 0 1 GEM 0 1 WORKING (SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT)  

      (PROTFAIL CR RPT) (PATCHFAIL MJ RPT) $ NTLZ20CA 03 GEM20BO
```

Note: The above example may not have the correct slots or load file name.
 This example is solely meant to show the new value for the pec code field.

Table release history update

NA

Supplementary information

NA

Translation verification other tools

The following example shows the output from DDEDIT when it is used to verify the addition of the new field in table MNCKTPAK field PEC:

```
>ddedit
```

```
DDE:
>printtype T_SPMCKT_CPK_PEC
TYPE IS T_SPMCKT_CPK_PEC
    NORTEL Product Engineering Code:
    {NTLX63AA,NTLX65AA,NTLX66AA,NTLX71AA,
    NTLX73AA,NTLX99AA,NTLX72AA,NTLX65BA,
    NTLX66BA,NTLX73AB,NTLX73BA,NTLX82AA,
    NTLX82AB,NTLX82BA,NTLX89DA,NTLX67AA,
    NTLX99BA,NTLX73BB,NTLX72BA,NTLX89AA,
    NTLX83AA,NTLX92AA,NTLX74AA,NTLX76AA,
    NTLX44AA,NTLX82EA,NTLZ20BA,NTLZ20CA}

    Non-NORTEL Product Identification Code:
    TABLE OF 8 CHARs
```

Configuration Walkthrough

NA

Product = MG 4000

A00003773--OM for TRKQOS for MG4K IP (PT-IP)

Functional Description (FN)

The activity A89007725 in SN06, '*Trunk Group based QoS OM*' provided a new trunk group-based operational measurement group (TRKQOSOM) on the Succession Call Server. The operational measurement values record instances in which QOS threshold values have been exceeded for calls handled by GWC based TDM trunk group.

This feature A00003773 '*OM FOR TRKQOS FOR MG4K IP*', extends trunk group based QoS OM support to MG4K-IP. As part of this activity, the operational measurement values record instances in which QOS threshold values have been exceeded for calls handled by MG4K-IP based TDM trunk group.

The QOS statistics that are included in the OM for each MG4K-IP and GWC trunk group are packet loss, jitter, and delay (latency).

When MG4K-IP based trunk calls are released, the QOS statistics for that call are compared to the QOS OM threshold values. If a statistic for the call exceeds the QOS OM threshold value, the OM value for that statistic on the MG4K-IP based trunk group will be incremented.

The OM group will contain entries for each MG4K-IP based TDM trunk group datafilled on the Call Server. In order for the trunk group to appear in the OM

group at least one member of the trunk group must be datafilled to reside on a MG4K-IP node via table TRKMEM.

Each entry in the OM group will contain a CLI and threshold-crossing counters for packet loss, jitter, and delay (latency).

The active registers will contain data for the current reporting interval. The holding registers will contain data for the previous reporting period. The interval for OM peg count transfer from the active to holding registers is controlled by the OM system. Refer to the OM system documentation for details on the available intervals for active to holding transfer.

In SN06, the activity A89007725 introduced a new office parameter *PACKET_QOS_OM_THRESHOLDS* to define QOS OM threshold values for GWC. The same QOS OM threshold values (*PACKET_QOS_OM_THRESHOLDS*) defined in table OFCVAR will be applied to all MG4K-IP nodes datafilled on the Call Server. The values may be changed at any time without the need for Call Server/MG4K-IP restart.

The following table describes the range of values possible for each QOS OM threshold office parameter datafilled in table OFCVAR.

PACKET_QOS_OM_THRESHOLDS Office Parameter

Parameter	Field		Range	Units
PACKET_QOS_OM_THRESHOLDS	Enabled		Y/N	
	Jitter		0 TO 100	Milliseconds (ms)
	Delay		0 TO 500	Milliseconds (ms)
	Loss	Whole	0 TO 9	% packet loss range from 0 TO 9.999999%
		Fraction	0 TO 999999	

The threshold values may be set in table OFCVAR by positioning on and changing the appropriate threshold as shown in the following figure.

Commands to set threshold values in table OFCVAR

```

TABLE: OFCVAR
>pos packet_qos_om_thresholds
    PACKET_QOS_OM_THRESHOLDS                N 1 2 3 4
>change
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
    PARMVAL: N 1 2 3 4
>Y 10 30 4 5
TUPLE TO BE CHANGED:
    PACKET_QOS_OM_THRESHOLDS                Y 10 30 4 5
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
Jitter Threshold : 10 milliseconds
Delay Threshold : 30 milliseconds
Loss Threshold : 4.500000 %
TUPLE CHANGED
JOURNAL FILE INACTIVE

```

In the above example, the QOS OM threshold reporting was changed such that the reporting is active and the thresholds were set (jitter=10 ms, delay= 30 ms, Packet Loss= 4.5%).

The default values for the OM thresholds will be set to the maximums and the enabled value will be set to N (No).

In order to view the QOS OM threshold crossing data, access the TRKQOSOM group via OMSHOW as shown in Figure , "Commands to view the QOS OM threshold crossing data" follows:

Commands to view the QOS OM threshold crossing data

```

>omshow trkqosom active(or holding for previous interval)
TRKQOSOM

CLASS: ACTIV
START:2002/07/22 12:50:00 MON; STOP: 2002/07/22 12:53:44 MON;
SLOWSAMPLES: 3 ; FASTSAMPLES: 22 ;

KEY (COMMON_LANGUAGE_NAME)
    PKTLOSS  JITTER  DELAY

64 IP01S7ITW2
    0        1        0
65 COMPISUP_OG
    0        0        0
66 IPD1ITSIMTS7
    0        0        0

.....

```

The data presented will include an entry for each MG4K-IP based TDM trunk group datafilled on the Call Server. For each entry, the CLI will be presented with the PKTLOSS, JITTER, and DELAY threshold crossing data.

Definitions for Packet Loss, Delay and Jitter registers are as follows:

Packet loss rate is calculated in percentage as:

$$\frac{[\text{RtpCumulativeLostPackets} * 100]}{[\text{RtpPacketsReceived} + \text{RtpCumulativeLostPackets}]}$$

Where, RtpPacketsReceived - The number of the RTP packets received from the IP network.

RtpCumulativeLostPackets - The number of lost RTP packets in the receiving direction. The count represents the Cumulative Number of Packets Lost field that is inserted in to the RTCP reception blocks.

Interarrival time jitter is an estimate of the statistical variance of RTP data packet interarrival times. The Jitter value calculated as the smoothed mean absolute value of the difference between the sending interval at a source and the interarrival time at a receiver. It is a running filtered average, basically a low pass filter with a 1/16 contribution each sample.

$$\text{jitter}_{\text{new}} = \text{jitter}_{\text{old}} + [(\text{instantaneous jitter} - \text{jitter}_{\text{old}}) / 16]$$

Where, instantaneous jitter = $|\text{rec}_i - \text{rec}_{i-1}| - |\text{sent}_i - \text{sent}_{i-1}|$
 $\text{rec}_i / \text{sent}_i$ = Time when i^{th} data packet is received/sent.

The round-trip delay is calculated when a RTCP reception report is received. The Delay (latency) is smoothed as,
$$\text{delay}_{\text{new}} = \text{delay}_{\text{old}} + [(\text{instantaneous delay} - \text{delay}_{\text{old}}) / 16]$$

Where instantaneous delay = $|A - \text{LSR} - \text{DLSR}|$
A = time a source received this reception report
LSR = last Send Report timestamp received field
DLSR = delay since last Send Report field

Hardware Requirements or Dependencies

None

Software Requirements or Dependencies

This functionality requires SN07 load in the Call Server, and SN07.1 or higher load in the MG4K-IP CEM and GEM RM.

Limitations and Restrictions

The intent of this activity is to provide an indication of QOS on the Call Server for each MG4K-IP based trunk group. As such, the activity does not attempt to record every violation of the QOS OM threshold. Rather, for the trunk group as a whole, a general indication of QOS health will be provided.

OM peg counts stored in the MG4K-IP that have not been reported to the Call Server will not be maintained over MG4K-IP GEM Sparring and Restarts.

TRKQOSOM OM group shall not be supported for IW-IP nodes.

Interactions

None

Applicable customer facing sections

Fault Management

Logs	<u>N/A</u>

Alarms	<u>N/A</u>

Configuration

Data Schema	<u>N/A</u>

User Interface	<u>N/A</u>

Element Management	<u>N/A</u>

Security	<u>N/A</u>

Service Order	<u>N/A</u>

Office Parameters	<u>X</u>

Accounting (includes AMA billing)	<u>N/A</u>

Performance (includes operational measurements)	<u>X</u>

Glossary

Term	Description
MG4K-IP	Multi-Service Gateway 4000-Internet Protocol.
GWC	Gateway Controller
Jitter	The Jitter value calculated as the smoothed mean absolute value of the difference between the sending interval at a source and the interarrival time at a receiver.
Delay (Latency)	Total time difference between the time a packet is sent and the time a corresponding reply packet is received. This delay refers to network delay only and does not include packetization/codec delay etc.
Loss	This is the percentage of packets lost over duration of the call.
OM	Operational Measurement
DPT	Dynamic Packet Trunk
QOS	Quality Of Service
RTCP	Real Time Control Protocol

Configuration for A00003773

Hardware and Software Requirements

This functionality requires SN07 load in the Call Server, and SN07.1 or higher load in the MG4K-IP CEM and GEM RM.

Initial Configuration

Not Applicable

Office/Subnet parameters (OP/SP) (CM & SESM)

New/modified office/subnet parameters

Parm table	Parameter name	NEW/CHANGED/DELETED/REL	Domain (CM or Subnet Mgmt)
OFCVAR	PACKET_QOS_OM_THRE SHOLDS	UNCHANGED	CM

This office parameter is introduced by feature A89007725 in SN06. This is being reused by this activity and explained for better understanding.

Parameter information

PACKET_QOS_OM_THRESHOLDS

Packet Quality of Service Operational Measurement Thresholds

Functional description

In SN06 the activity A89007725 - '*Trunk Group based QoS OM*' introduced a new office parameter PACKET_QOS_OM_THRESHOLDS to define QOS OM threshold values for GWC.

This parameter defines the QOS thresholds values used for pegging QOS issues on GWC based trunk groups. In addition, it allows the QOS reporting threshold feature to be enabled or disabled.

The same QOS OM threshold values (PACKET_QOS_OM_THRESHOLDS) defined in table OFCVAR will be applied to all MG4K-IP nodes datafilled on the Call Server. These QOS thresholds values will be used for pegging QOS issues on MG4K-IP based TDM trunk groups.

The values may be changed at any time without the need for Call Server/MG4K-IP/GWC restart.

Provisioning rules

To activate the QOS OM pegging feature for GWC and MG4K-IP based TDM trunk groups, set the enabled value to Y and specify the desired thresholds for jitter, packet loss, and delay.

Range information

Range information

Parameter	Field		Range	Units
PACKET_QOS_OM_THRESHOLDS	Enabled		Y/N	
	Jitter		0 TO 100	Milliseconds (ms)
	Delay		0 TO 500	Milliseconds (ms)
	Loss	Whole	0 TO 9	% packet loss range from 0 TO 9.999999%
		Fraction	0 TO 999999	

Activation

Changes take effect immediately.

Dependencies

A new log - *MG4K-IP OM Failure log*, shall be introduced by feature A00003650 - '*MG4K-IP ECAN, SCTP and OM Failure logs*'. The QOS

measurements shall be pegged on the GEM card per CLI basis. The pegs are stored in 16 bit integers. If these overflow, then the MG4K-IP OM Failure log shall be generated with a reason. The reason code description for the log are Jitter peg overflow, Delay Peg Overflow, Packet Loss Peg Overflow. The pegs in the GEM shall be reset to 0 when this log is generated.

Consequences

None.

Verification

None.

Parameter release history update

In SN06, this parameter is created and used by GWC to peg the trunk group based QoS OMs. From SN07.1 the MG4K-IP nodes also uses these threshold to peg trunk group based QoS OMs.

Upgrade Impact**Dump and Restore**

No Impact.

Element Management Upgrade

No Impact.

Product = MG9000**A00001893 and A00001894--MG9K Imaging (UA-IP)*****Functional Description***

Currently, there is not a concept of imaging a Media Gateway 9000 (MG9K) device load from the Media Gateway 9000 Element Manager (MG9K EM) or any other application. This means that after a new load is loaded into a Supercore OC3, ITX, ITP, DS1, or ABI device, each device must then be patched up to date. This process can take hours, days and some times months depending on the size of the office, the number of patches and the maintenance window.

This feature will provide a means for the customer to upgrade an MG9K Device, patch the device up to date, image the MG9K Device load with the patches applied and then upgrade the rest of the devices in the office with the imaged load.

This feature will also provide a means for imaging to occur automatically so that after the upgrade, if more patches arrive to the site, the customer can continuously keep a stored, up-to-date, imaged load.

This feature introduces MG9K device imaging from the following Succession applications:

- MG9K Element Manager (MG9K EM)
- Network Patch Manager (NPM)

The MG9K EM will provide an interface for the user to image one MG9K Device at a time. The NPM will provide a mechanism for the user to image a device via a maintenance command through the NPM user interfaces as well as schedule an imaging task through the NPM scheduler.

Note: The NPM will provide a mechanism for the user to request images of multiple device loads, but the MG9K EM will only be able to image one device at time per Network Element.

Media Gateway 9000 Element Manager

This feature will change the MG9K Element Manager Graphical User Interface (GUI) at the card level as well as asking the user to provide additional information at start up time for the MG9K EM Server.

Security

This feature does not change any of the login procedures or security level access for the MG9K EM, however, this feature does require that the user have emsadm or emsrw level of security in order to execute the Software Image command. Otherwise the command will be greyed out indicating that the user does not have access to execute the command.

Logs

This feature will introduce a new Information log that will indicate a success or failure of an image as well as a new Audit log that will indicate user access of the image command.

However, it is not the responsibility of this document to discuss the log information as it will be provided in a separate log document for this feature. This information is being provided here so the reader of this document can be aware of the new logs.

MG9K EM Server Configuration

Configuration for the MG9K EM will change when a user executes the mg9kconfig.sh script from the /opt/nortel/mg9ksrv_xx/bin directory on the SSPFS platform.

When a user executes the mg9kconfig.sh script before start up of the MG9K Server, the user will be asked to provide the following information:

- Image Server - the load server where the load images will be stored
- Image Server User ID - the user id for the load server that has ftp access
- Image Server password - the password for the load server user id
- Supercore IMA Image Directory - directory where the image for this load type will be stored.
- SuperCore OC2 Image Directory - directory where the image for this load type will be stored.
- ITP Image Directory - directory where the image for this load type will be stored.
- ITX Image Directory - directory where the image for this load type will be stored.
- DS1 Image Directory - directory where the image for this load type will be stored.
- ABI Image Directory -directory where the image for this load type will be stored.

The mg9kconfig.sh script will provide a default Image Directory for the user that will be located at: /swd/mg9k.

The user can change this information by executing the ./mg9kserver config script located in /opt/nortel/mg9ksrv_xx/bin. This command can be executed after the MG9K server is running. This feature will provide a “*Change Imaging Server Settings*” Menu in this script so that the default software imaging parameters can be changed without executing the entire mg9kconfig.sh script again.

MG9K EM GUI

Refer to the Configuration section of this feature for a discussion of this GUI.

Network Patch Manager

Refer to the Configuration section of this feature for a discussion of NPM.

Hardware Requirements or Dependencies

None

Software Requirements or Dependencies

This feature requires the SN07 MG9K EM, NPM and MG9K Device Software.

Limitations and restrictions

The following items are listed here as limitations from this feature:

- SmartImage is dependant on the default information that is input at configuration time of the MG9K EM Server. If this information is not available, the user will not be able to SmartImage or auto image.
- SmartImage or auto imaging for the customer who does not *specialize* his office. It is for the customer who patches all devices with the same patches.
- The patching criteria looks at the levels of patches in a device load. Therefore if a user patches a device with 4 patches, images the device, then removes the patches and then applies 4 different patches; the level of patches since the last image has not changed and the device will not be imaged.
- Due to the fact that two MG9K EM Servers execute on the same SSPFS box at one time during upgrades; the customer must be aware that when the mg9kconfig.sh script asks for the image user id and image server password, they must be the same for both MG9K EM Servers executing. This is due to the fact that there will only be one secure password file for the imaging server per SSPFS platform. However, the additional information the user provides via the mg9kconfig.sh script can be different, including the image server IP and load image directories.
- The load server used must have FTP read/overwrite access.

Interactions

None

Applicable customer facing sections

Fault Management

Logs	<u> X </u>
Alarms	<u>NA </u>

Configuration

Data Schema	<u> NA </u>
User Interface	<u> X </u>
Element Management	<u> NA </u>
Security	<u> NA </u>
Service Order	<u> NA </u>
Office Parameters	<u> NA </u>

Accounting (includes AMA billing)	<u> NA </u>

Performance (includes operational measurements) _NA__

Glossary

MG9K EM - Media Gateway 9000 Element Manager

NPM - Network Patch Manager

GUI - Graphical User Interface

CLUI - Command Line User Interface

Fault Management for A00001893 and A00001894

No additional tools are implemented by this feature. Customer and Audit logs for this feature are generated via the existing log software in the MG9K Element Manager.

Fault management tools and utilities

This feature utilizes the fault management tools provided by the MG9K Element Manager application. Customer logs are generated by the Element Manager application and are based on the processing of node logs received from the MG9K gateway.

Audit logs are generated by the Element Manager and are based on maintenance actions performed by the craft person only at the Element Manager console.

Logs

New MGEM 714 Audit Log

This log is generated whenever a user attempts to image an MG9K device.

Format

The following table is an example of the new MGEM 714:

```
Oct  2 14:37:14 wnc0s00v MGEM:joeuser 714 Software  
Image Requested MG9K: U16 [16]
```

Field Description for the MGEM log

Field	Description	Example
Date/Time	Date and Time stamp of the log	Oct 2 14:37:14
Host Name	Host machine name	wnc0s00v

Field Description for the MGEM log

Field	Description	Example
Application Name	Specifies the application producing the log	MGEM
User Name	User name attempting the action	joeuser
Log Number	The log number	714
Log Text	Specifies the action attempted and any associated details.	Software Image Requested MG9K: U16[16]

Action

No action is required.

Associated Operational Measurements or Performance Measurements

None.

Additional Information

None.

New NE609 Software Image Log

This new log is generated whenever a user executes an image request.

Format

The following is an example of what the new log might look like:

NE609 OCT6 11:06:14 0029 INFO MG9K Software Image Event

Imaging: NE Number: 7 NE Name: PL7 Card Type: DS1

Image Type: Card Type

Image Action: Image

Image Status: Image Completed

Time: Thu Oct 02 18:17:11 EDT 2003

Action

If the Image Status field indicates a failure, the user may want to attempt to image the device again.

Associated Operational Measurements or Performance Measurements

None.

Additional Information

None.

Configuration for A00001893-1894**Hardware and Software Requirements**

This feature requires the SN07 Media Gateway 9000 Element Manager, the Network Patch Manager and Media Gateway 9000 Device Software as well as the SSPFS platform software.

Upgrade Impact

This feature impacts MG9K Device upgrades by allowing the craft person to upgrade an MG9K Device with a new load, patch the load with all available patches for the load and execute an image.

The execution of the image will create a device load with a “.tar” file extension (ex. SCOA07AA_GZ.tar). This image load will contain the software load *and* the patches.

The user will then have the ability to upgrade the remaining devices in the office with the newly imaged load.

The availability of the image command could potentially reduce the amount of time an upgrade takes significantly

Dump and Restore

N/A

Element Management Upgrade

This feature will create a “.tar” load file during the imaging process that can be used to upgrade MG9K Devices of the same load type.

Element Management

This feature adds new commands to the Media Gateway 9000 Element Manager Graphical User Interface and the Network Patch Manager Graphical User and Command Line User Interface.

Media Gateway 9000 Element Manager

This feature adds new commands to the Media Gateway 9000 Element Manager Graphical User Interface and the Network Patch Manager Graphical User and Command Line User Interface.

Initial MG9K Element Manager Configuration

This feature will change/update two configuration scripts for the MG9K EM Server; *mg9kconfig.sh* and *mg9kserver config*.

mg9kconfig.sh

Today, the mg9kconfig.sh script must be executed before the MG9K EM Server can be started. Therefore, this script will be modified to ask the user for the following information:

- Image Server - the load server where the load images will be stored
- Image Server User ID - the user id for the load server that has ftp access. **NOTE: the ftp user must have over write privileges on the server.**
- Image Server password - the password for the load server user id
- Supercore IMA Image Directory - directory where the image for this load type will be stored.
- SuperCore OC2 Image Directory - directory where the image for this load type will be stored.
- ITP Image Directory - directory where the image for this load type will be stored.
- ITX Image Directory - directory where the image for this load type will be stored.
- DS1 Image Directory - directory where the image for this load type will be stored.
- ABI Image Directory -directory where the image for this load type will be stored.

The mg9kconfig.sh script will provide a default Image Directory for the user that will be located at: /swd/mg9k.

The following figure shows the final output from the mg9kconfig.sh script that the user will see and verify before starting the MG9K EM Server.

Script output of the mg9kconfig.sh verification

```
Setup Server As           : MASTER
Master Server IP Address  : wnc0s00v
SESM IP Address           : 47.142.164.250
Security Authentication Host : 47.142.164.250
Oracle IP Address         : 47.142.164.250
Initialize Database       : YES
Maintenance Release Upgrade : NO
Image Server              : 47.142.164.250
Image Server User ID      : maint
SuperCore IMA Image Directory : /swd/mg9k/sci
SuperCore OC3 Image Directory : /swd/mg9k/sco
ITP Image Directory       : /swd/mg9k/itp
ITX Image Directory       : /swd/mg9k/itx
ABI Image Directory       : /swd/mg9k/abi
DS1 Image Directory       : /swd/mg9k/ds1
```

mg9kimpl

The mg9kimpl script exists today and is available so that the user can change information the MG9K EM Server utilizes. This script is accessed by typing **./mg9kserver config**. This feature will provide a “*Change Imaging Server Settings*” Menu in this script so that the default software imaging parameters can be changed without executing the entire mg9kconfig.sh script again. The following figures show how the menu is displayed.

Main Configuration Menu for the MG9K EM Server

Main Configuration Menu

- 1) Change Distribution Policy
 - 2) Change SESM IP Address
 - 3) Change Oracle IP Address
 - 4) Change Debug Level for logs
 - 5) Change Persistence settings
 - 6) Change ESA data download settings
 - 7) Change Imaging Server settings
 - 8) Display current settings
 - 9) Exit from Main Menu
- Please make a selection =>

Image Configuration Menu for the MG9K EM Server

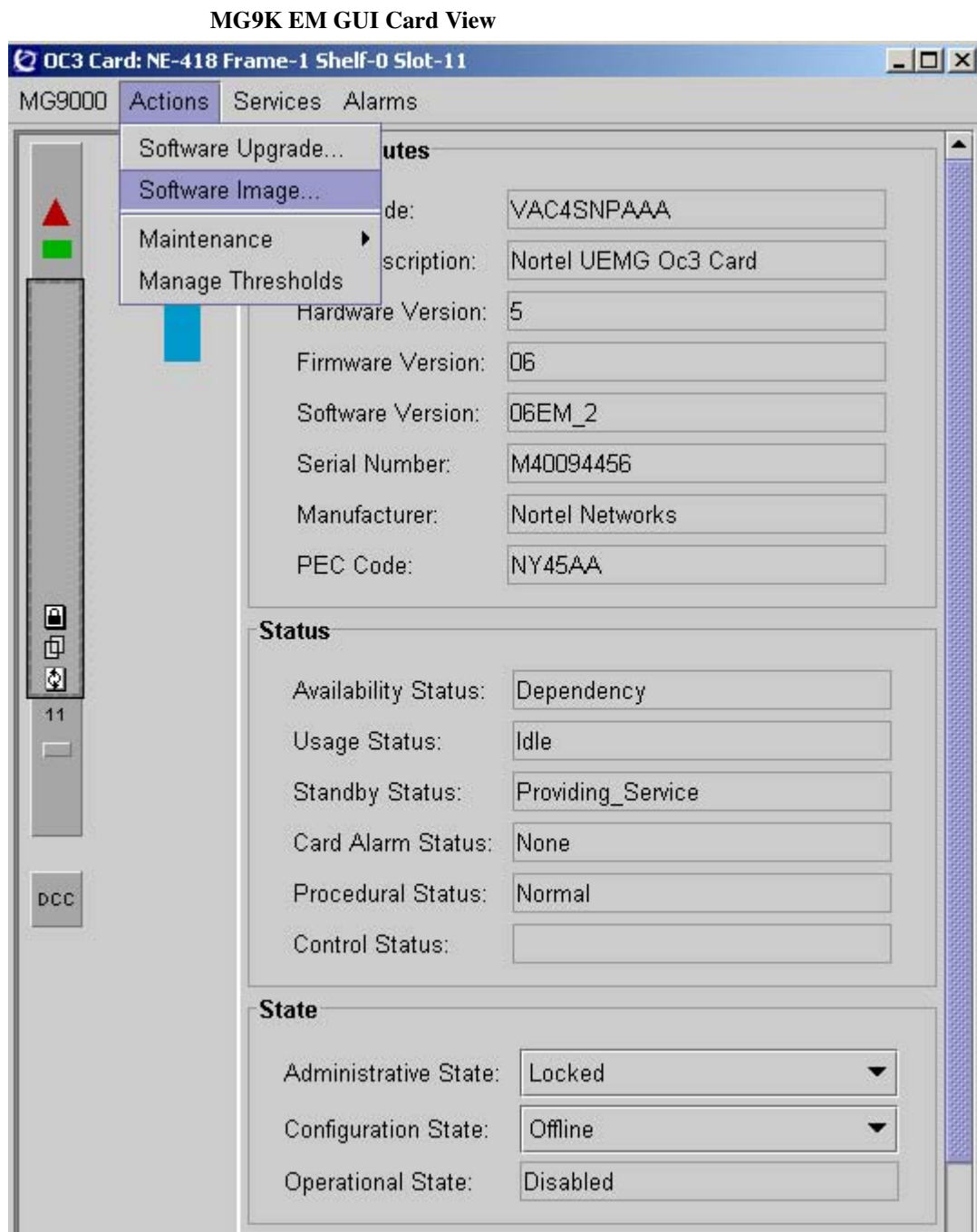
Image Configuration Menu

- 1) Change Image Server IP
 - 2) Change Image Server User ID and password
 - 3) Change Image Server default directories
 - 4) Exit to Main Menu
- Please make a selection =>

MG9K EM GUI

This feature changes the MG9K EM GUI at the card level only. An additional item named *Software Image* will be added to the *Actions* menu. The Software Image function is performed on a **per card basis** and is only available for the SuperCore OC3, SuperCore IMA, ITP, ITX, DS1 and ABI cards.

The following figures show the Software Imaging GUI interface for the MG9K EM.



After selecting the Software Image tab, the MG9K Image GUI appears. The next figure shows the message if the Floating IP has not been configured.

Floating IP Not configured

The screenshot shows a web browser window titled "voip33 [99]". The main content area is titled "MG 9000 Software Image Element: 99" and "MG9000". It contains several sections:

- Image Originator:**
 - MG 9000 Name: voip33 99
 - Originating View: OC3 Card: NE-99 Frame-1 Shelf-3 Slot-10
- Image State:**
 - Image Status: Waiting to image.
 - Image Action:
 - Image Type:
- Image Type Data:**
 - Imaging:
 - Load Server:
 - Load Server User Id:
 - Load:
- Image Instructions & Results:**

Need to add the floating IP address before the image is started.
Go to a card or frame view.
Invoke the menu Services -> Floating IP Address Manager.
Add a floating IP address.
Return to the Image view, then press Image to continue.

After the floating IP has been configured, the MG9K Image GUI can be re-entered and should look as follows:

MG9K EM Image GUI

The image shows a graphical user interface window titled "MG 9000 Software Image Element: 16". The window has a standard Windows-style title bar with minimize, maximize, and close buttons. Below the title bar, the text "MG9000" is displayed. The main content area is divided into several sections:

- Image Originator:** This section contains two text input fields. The first is labeled "MG 9000 Name:" and contains the text "UD16 16". The second is labeled "Originating View:" and contains the text "OC3 Card: NE-16 Frame-0 Shelf-2 Slot-10".
- Image State:** This section contains three text input fields. The first is labeled "Image Status:" and contains the text "Ready to image.". The second is labeled "Image Action:" and contains the text "Configure complete.". The third is labeled "Image Type:" and contains the text "Single Node".
- Image Type Data:** This section contains four text input fields. The first is labeled "Imaging:" and contains the text "OC3 Card: NE-16 Frame-0 Shelf-2 Slot-10". The second is labeled "Load Server:" and contains the text "47.142.164.250". The third is labeled "Load Server User Id:" and contains the text "maint". The fourth is labeled "Load:" and contains the text "/swd/mg9k/sco/SCOA06EM_2_GZ.tar".
- Image Instructions & Results:** This section contains a large text area with the following instructions:
Press Image to execute the image function with.
the default values provided. Or press configure
to enter an alternate load server and ftp user id
Or press Version List to see all the versions of the cards.
Or press History to see the results of previous images/upgrades.

At the bottom of the window, there is a row of six buttons: "History", "Configure", "Image", "Version List", "Abort", and "Close". The "Configure" button is highlighted with a blue border.

Notice from the preceding figure that there is a *Configure* button. If the user wishes to change the default server IP, server user ID, server password or directory, they can do so by clicking on the *Configure* button.

Note: *Configure* only changes these values for this session. It does not change the default values permanently.

The following two figures show the *Configure* menus.

Server Configure Menu



The Server User Identifier *must* be an FTP user that has overwrite access on the load server.

Server Directory Menu



As part of manual imaging, the MG9K EM will obtain patch information from the Network Patch Manager. This information will help the user to determine if there is any reason the device load should not be imaged. If the NPM determines any of the following conditions, a *Warning* message will be sent to the user:

- the device load contains obsolete patches
- the device load contains patches that are on hold
- the device itself is on hold
- the device load is at a lower patch level than the previously image load.

A *Failure* message will be sent to the user if communication with the NPM cannot be obtained. However, in all of these instances, the user will have the ability to override these conditions and continue with the image.

FTP User Configuration

This feature requires that the FTP server that is used for images have an FTP user configured that has read AND overwrite access to the server. After an image file is created once, every subsequent image of that load will be overwritten. NOTE: only the image file will be overwritten, not the original load file.

Image File

The imaged file name is pre-determined and **CANNOT** be configured. The imaged file name will be based on the name of the load file with a “.tar” extension. For example, if the file name of the load is SCOA07AA_GZ, the imaged load file name will be SCOA07AA_GZ.tar. This is the name of the load file that should be used when the user is ready to upgrade or re-load devices from disk.

The imaged load will be placed in the directory that the user specified during initial configuration of the MG9K EM Server or in the configuration entered via the Image Configuration Panels shown in [“Server Configure Menu” on page 2068](#) and [“Server Directory Menu” on page 2068](#).

Network Patch Manager

The NPM will offer the ability to image an MG9K Device via a new maintenance command; *SmartImage*. This new maintenance command will “look and feel” like the other maintenance commands in the NPM.

Unlike manual imaging from the MG9K EM, the *SmartImage* command utilizes a patching criteria that will determine if the devices that the user wishes to image *should* be imaged. The following sections discuss the patching criteria, NPM GUI and NPM CLUI changes as well as other changes to the NPM that will be necessary for this feature.

Security

This feature requires the user to have a security level of emsadm in order to execute the *SmartImage* command.

Logs

This feature will not add new log numbers for the SmartImage command. This feature will utilize the NPM maintenance log numbers that are currently available for maintenance commands.

NPM PreDefined Device Sets

This feature will introduce two new predefined device sets to the NPM:

- MG9KDevices
- GWCDevices

Each of these sets will include all of the devices of the device type they reference. For example, MG9K Devices will include all of the MG9K type devices; OC3, ITP, ITX, DS1, and ABI. It will be recommended that the user utilize these sets when executing the *SmartImage* command.

NPM Patching Criteria

Basically, the criteria for the SmartImage command boils down to which device(s) contains the highest patch content.

Because this is the “focus” of the criteria, it is essential that the user be aware of what they are doing when they image a device from the NPM. It is **highly** recommended that the user only use the “device sets” that will be provided as part of this feature. Otherwise, an image of a device could be taken that does not contain the highest patch content.

The tables below show an example of how the patching criteria will work for the SmartImage Command.

The following table shows a list of all the MG9K Devices, registered in the NPM, sorted by loadname.

Sorted devices and loads

Loadname	Device
SCOA07AB	UD16_16_62_OC3_0_2_10
	UD16_16_62_OC3_0_2_11
	UD17_17_72_OC3_0_2_10
	UD17_17_72_OC3_0_2_11

Loadname	Device
ITPA07AB	UD16_16_62_ITP_0_2_12
	UD16_16_62_ITP_0_2_13
	UD16_16_62_ITP_1_2_12
ITPA07AA	UD16_16_62_ITP_1_2_13
ITXA07AB	UD16_16_62_ITX_0_2_14
	UD16_16_62_ITX_0_2_15
	UD17_17_72_ITX_0_2_14
	UD17_17_72_ITX_0_2_15

Once all of the devices are sorted, the NPM looks at specific fields to determine if each device is a candidate for imaging. The following table shows the fields used and what impact they have on each device as it is evaluated.

Patching Criteria

Field	Description	Impact on Imaging
AppLevel	Contains an integer value to indicate the number of patches applied to the device.	If zero patches are applied, the device is not a candidate for imaging.
ActLevel	Contains an integer value to indicate the number of patches activated in the device.	If all the devices for a particular load are at the same applevel, this field is used as a "tie breaker" to determine if a device should be imaged.
Hold	Contains Y or N to indicate whether the device is on hold.	If the device is on hold (Y), the device is not a candidate for imaging.
Patches on Hold	Contains an integer to indicate how many patches are on hold.	If the device contains any patches that are on hold, the device is not a candidate for imaging.
Obsolete Patches	Contains an integer value to indicate how many obsolete patches.	If the device contains any patches that are obsolete, the device is not a candidate for imaging.

The following table shows an example the patching criteria field values for each device.

Patching Criteria Fields

Loadname	Device	App-Level	Act-Level	Patches on Hold	Obsolete Patches	Hold	Include
SCOA07AB	UD16_16_62_OC3_0_2_10	5	0	0	0	N	Y
	UD16_16_62_OC3_0_2_11	5	0	0	0	N	Y
	UD17_17_72_OC3_0_2_10	5	0	0	0	N	Y
	UD17_17_72_OC3_0_2_11	5	0	0	0	N	Y
ITPA07AB	UD16_16_62_ITP_0_2_12	3	0	0	0	N	Y
	UD16_16_62_ITP_0_2_13	2	0	0	0	N	Y
	UD16_16_62_ITP_1_2_12	5	0	0	0	Y	N
ITPA07AA	UD16_16_62_ITP_1_2_13	5	0	0	1	N	N
ITXA07AB	UD16_16_62_ITX_0_2_14	0	0	0	0	N	N
	UD16_16_62_ITX_0_2_15	0	0	0	0	N	N
	UD17_17_72_ITX_0_2_14	0	0	0	0	N	N
	UD17_17_72_ITX_0_2_15	0	0	0	0	N	N

From the Patching Criteria Fields table, let's evaluate which devices were chosen as candidates for imaging. We will look at the devices that were not chosen for imaging later in this section.

Candidates Devices for Imaging

Candidate Devices	
Group 1	UD16_16_62_OC3_0_2_10
	UD16_16_62_OC3_0_2_11
	UD17_17_72_OC3_0_2_10
	UD17_17_72_OC3_0_2_11
Group 2	UD16_16_62_ITP_0_2_12

The five devices from the previous table were chosen because they were not on hold and they had the highest level of patches applied to their load without any of the patches being obsolete or on hold.

Once the candidate device list is determined, the NPM then looks at the previously imaged AppLevel and ActLevel fields for each load.

If the AppLevel for the devices in a group are at a higher or lower level than the previously imaged levels, a device from the group will be chosen for imaging.

If the AppLevel is the same as the Previously Imaged AppLevel, the ActLevel will be used as a “tie breaker” to determine if an image should occur. If the ActLevel is the same, none of the devices will be imaged because the levels are the same level as the previous image.

NOTE: MG9K Devices do not currently support activation type patches, however, this patching criteria will continue to utilize this field as part to the criteria to determine the candidate device list, so that the patching criteria can be keep generic.

Chosen Devices for Imaging

Candidate Devices		Current AppLevel	Current Actlevel	Previous Imaged AppLevel	Previous Imaged ActLevel
Group 1	UD16_16_62_OC3_0_2_10	5	0	4	0
	UD16_16_62_OC3_0_2_11	5	0	4	0
	UD17_17_72_OC3_0_2_10	5	0	4	0
	UD17_17_72_OC3_0_2_11	5	0	4	0
Group 2	UD16_16_62_ITP_0_2_12	3	0	4	0

Once the NPM determines that a group of devices should be imaged, from this point on, the NPM views the devices in each group as “equals” and simply chooses the first device in the group to be imaged; as shown in Table 6.

Chosen Devices for Imaging

Chosen Devices	
1	UD16_16_62_OC3_0_2_10
2	UD16_16_62_ITP_0_2_12

Now that we know which devices will be chosen for imaging, let's take a closer look at why some of the devices were not chosen for imaging.

Devices NOT chosen for imaging

Loadname	Device	AppLevel	ActLevel	Patches on Hold	Obsolete Patches	Hold
ITPA07AB	UD16_16_62_ITP_0_2_13	2	0	0	0	N
	UD16_16_62_ITP_1_2_12	5	0	0	0	Y
ITPA07AA	UD16_16_62_ITP_1_2_13	5	0	0	1	N
ITXA07AB	UD16_16_62_ITX_0_2_14	0	0	0	0	N
	UD16_16_62_ITX_0_2_15	0	0	0	0	N
	UD17_17_72_ITX_0_2_14	0	0	0	0	N
	UD17_17_72_ITX_0_2_15	0	0	0	0	N

- Device UD16_16_62_ITP_0_2_13, was not chosen for imaging because it does not contain as high of a patch content as UD16_16_62_ITP_0_2_12.
- Device UD16_16_62_ITP_1_2_12, was not chosen for imaging because the device is on hold.
- Device UD16_16_62_ITP_1_2_13, was not chosen for imaging because the device load contains an obsolete patch.
- Device UD16_16_62_ITX_0_2_14, UD16_16_62_ITX_0_2_15, UD17_17_72_ITX_0_2_15 and UD17_17_72_ITX_0_2_15 were not chosen for imaging because there are not patches currently applied to either device.

NPM GUI

The following figures show example output of the *SmartImage* command and results. (Note the example output here, is not the example that is shown in the table example shown in the previous section.)

SmartImage Command from the Maintenance Panel;

Maintenance Task

Task List

Task: Apply

Apply
Remove
Audit
Activate
Deactivate
Restart
SmartImage

Patc
PEG01UEM

Filter
Select All
Deselect All
Reset

Device Selection

Filter
Select All
Deselect All
Reset

AUTORESTARTDEVICE
GWCDEVICES
MG9KDEVICES
OAMDEVICES
NPM
NTMG9KM_6_2_VWNCOSC
PSE_wnc0s00v
UD16_16_62_ITP_0_2_12
UD16_16_62_ITP_0_2_13
UD16_16_62_ITX_0_2_14
UD16_16_62_ITX_0_2_15

Save Task

Task Name:

Task Description:

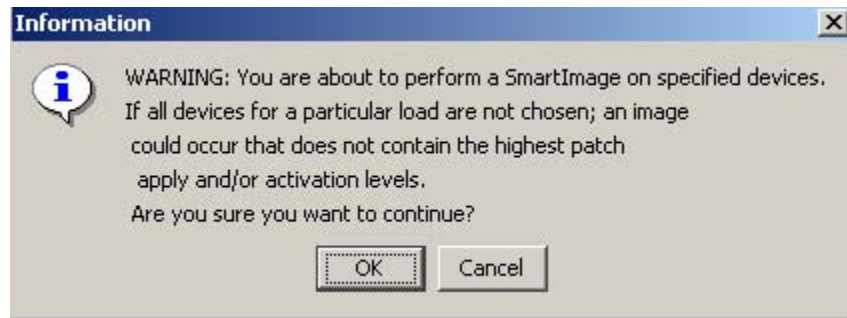
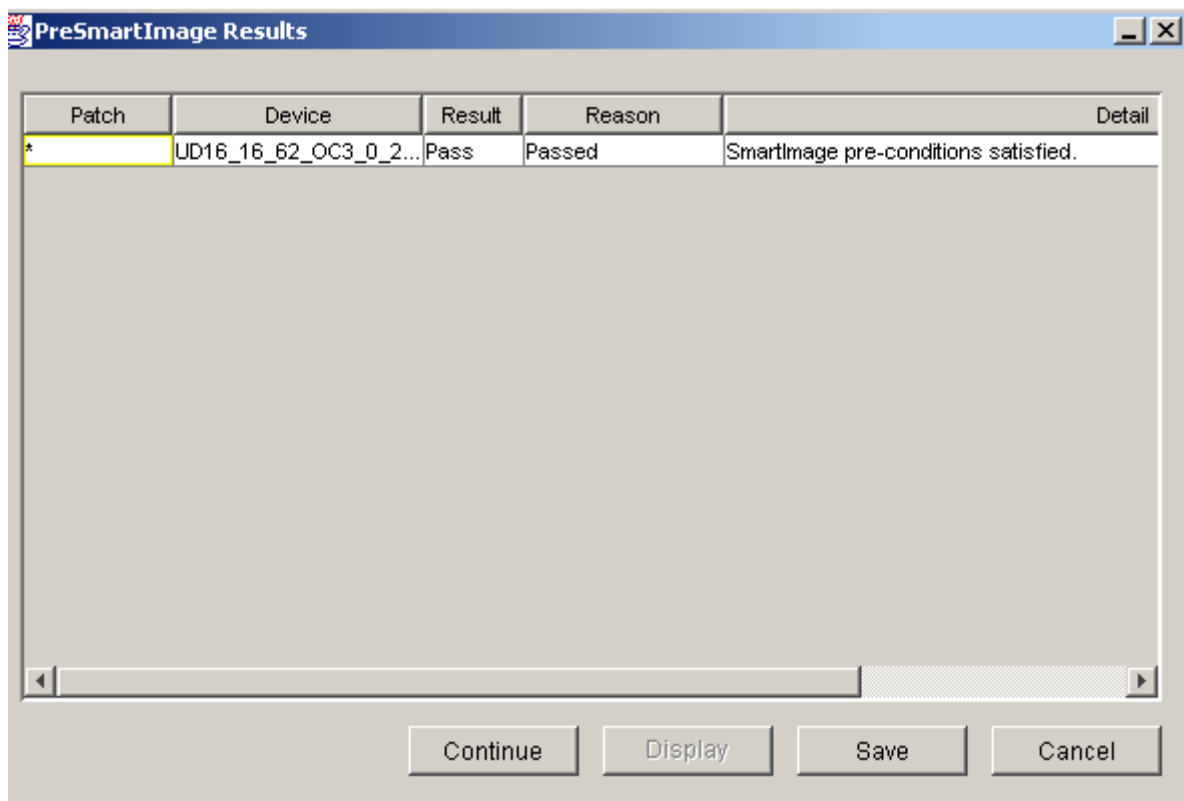
Save

Reset All

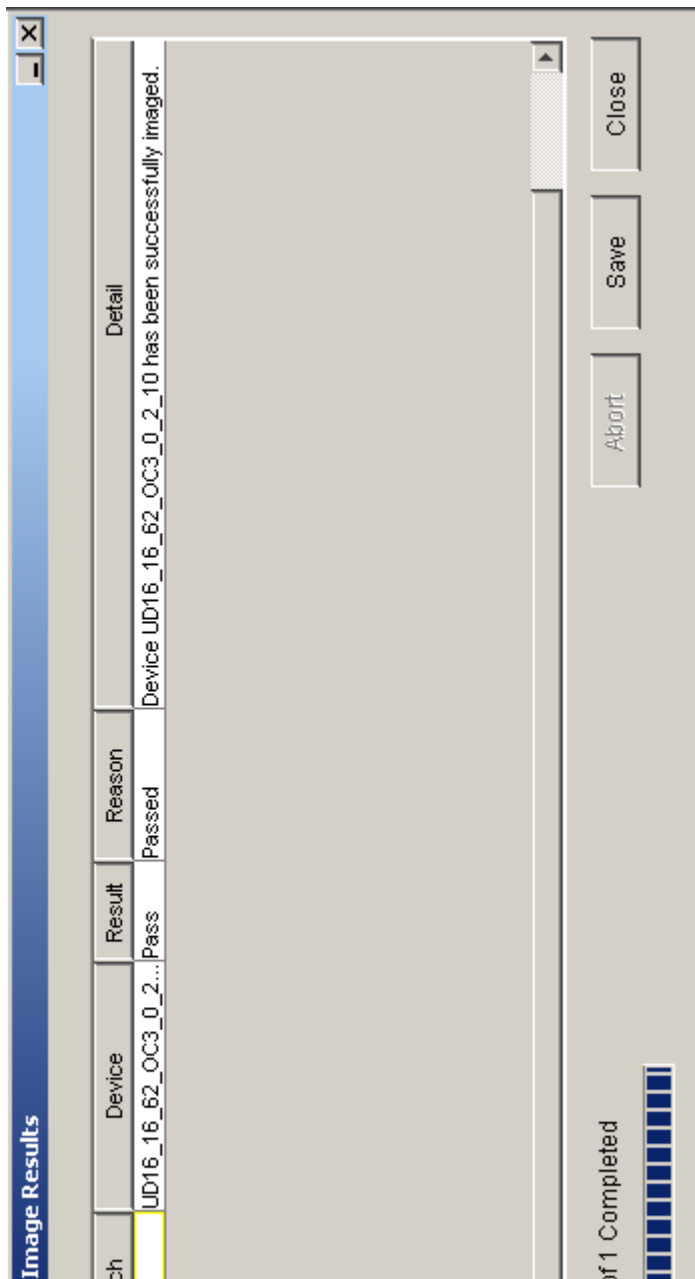
Execute

Close

After choosing the *SmartImage* Command and the selected devices, the user can click the *Execute* button. Once this button is clicked a warning message is displayed to the user to ensure that they agree that the devices chosen are the ones that they want evaluated.

Warning message for the SmartImage Command**Pre-results for the SmartImage Command**

Final results from the SmartImage Command



NPM CLUI

This feature changes the NPM CLUI by adding the new *SmartImage* command. The command will execute just as it does in the NPM GUI. The following is an example of the command and output.

NPM CLUI SmartImage Command Output

```
npm>smartimage SET MG9KDEVICES
```

WARNING: You are about to perform a smartimage on the specified devices.

Note that if all devices for a particular load are not chosen for imaging. A device may be chosen that does not contain the the highest patch content.

If you wish to continue with this maintenance request enter Yes (Y or y).

Otherwise, just enter return.

```
#y
```

```
Patch: *
```

```
Device: UD16_16_62_OC3_0_2_10
```

```
Result: true
```

```
Reason: Passed
```

```
Details: SmartImage pre-conditions satisfied.
```

If you wish to continue with this maintenance request enter Yes (Y or y).

Otherwise, just enter return.

```
#y
```

```
npm>
```

```
Patch: *
```

```
Device: UD16_16_62_OC3_0_2_10
```

```
Reason: Passed
```

```
Detail: Device UD16_16_62_OC3_0_2_10 has been successfully imaged.
```

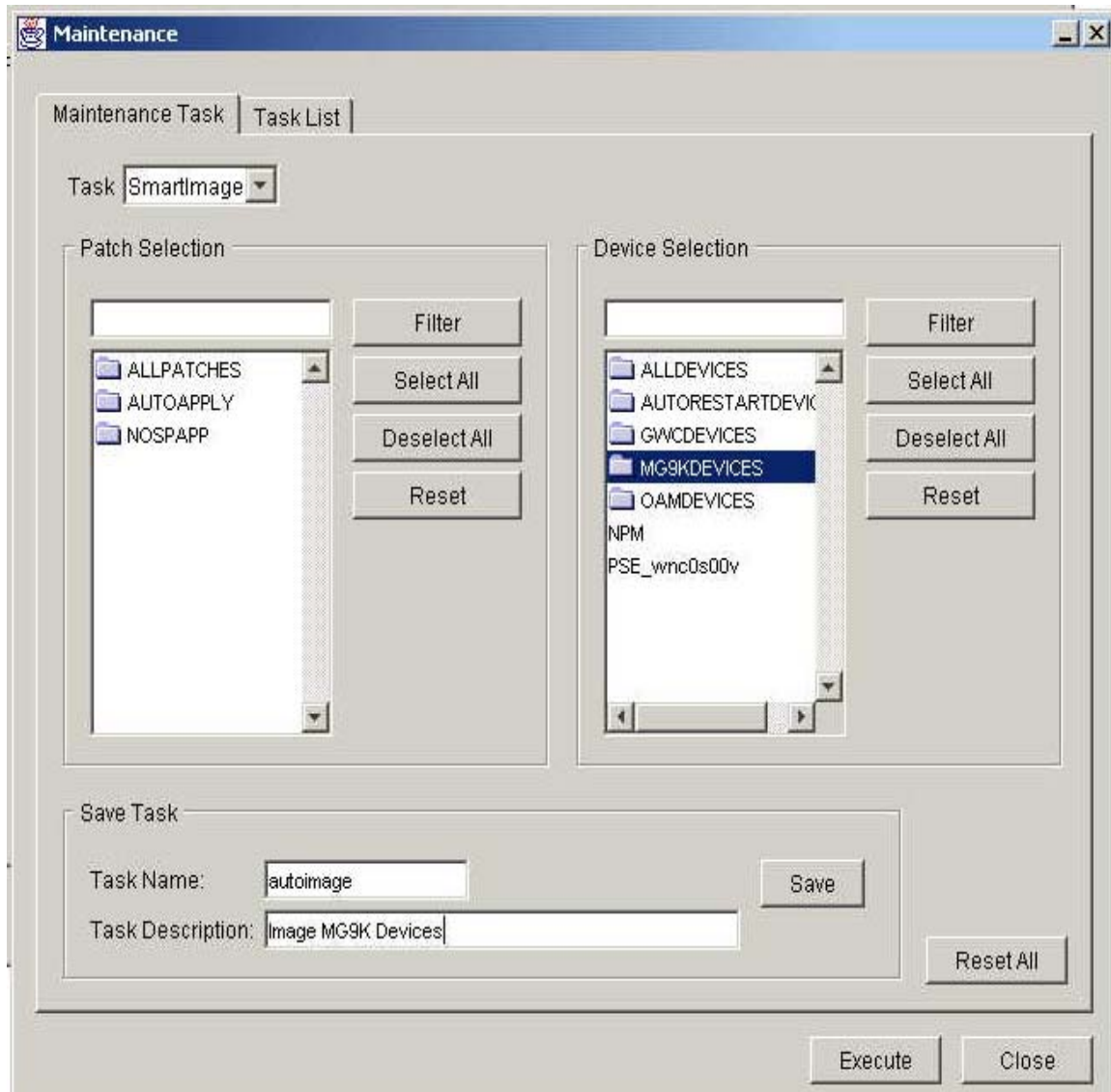
Scheduling SmartImage

The SmartImage command can be scheduled in the NPM via the NPM GUI or NPM CLUI and executed nightly, weekly or monthly. It is recommended that if SmartImage is scheduled on a nightly basis, that autoapply is also scheduled and executed before the SmartImage task is executed.

The following figures show some of the steps involved to schedule the SmartImage task.

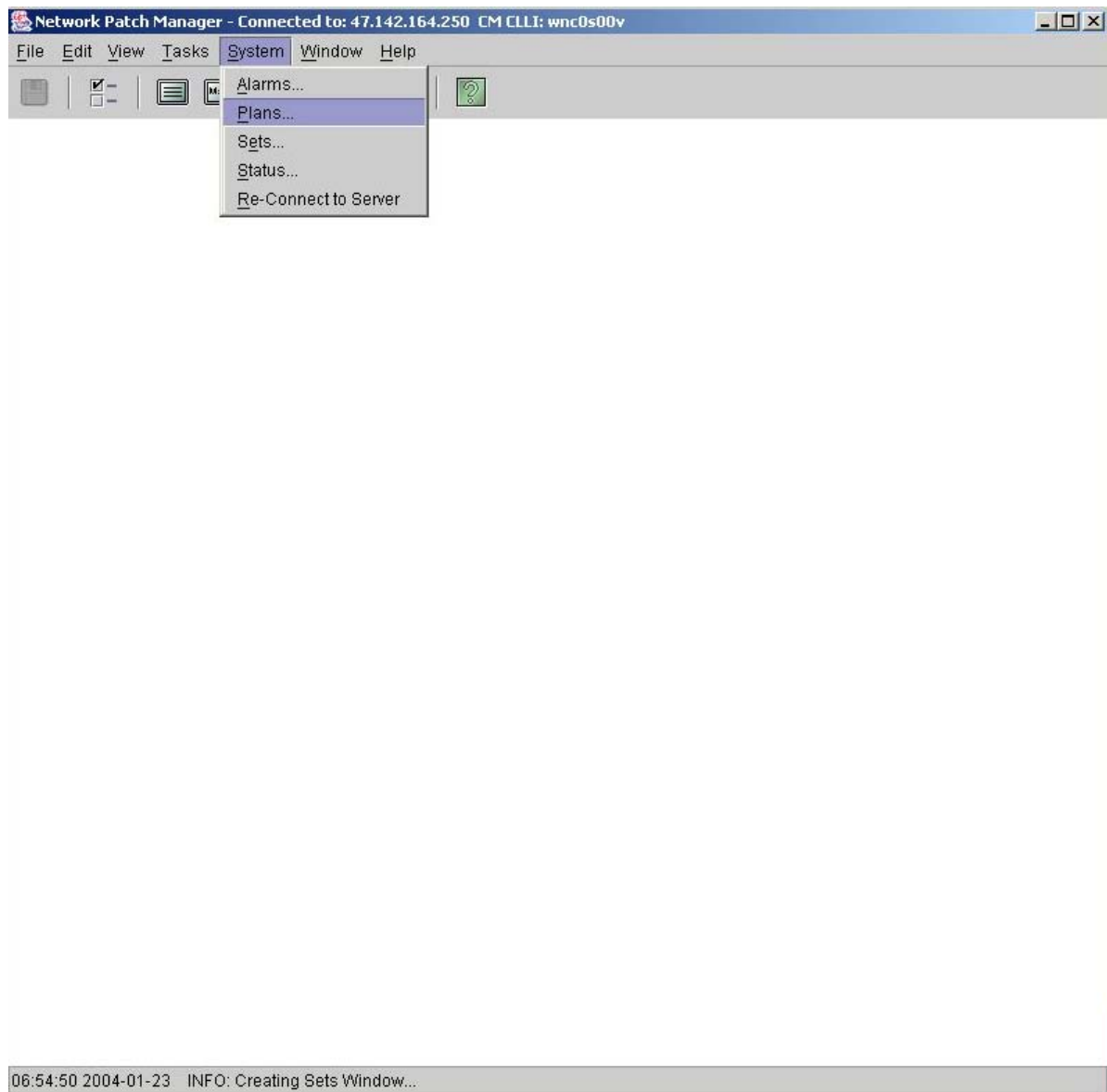
Scheduling a SmartImage from the NPM GUI

Saving the SmartImage Task

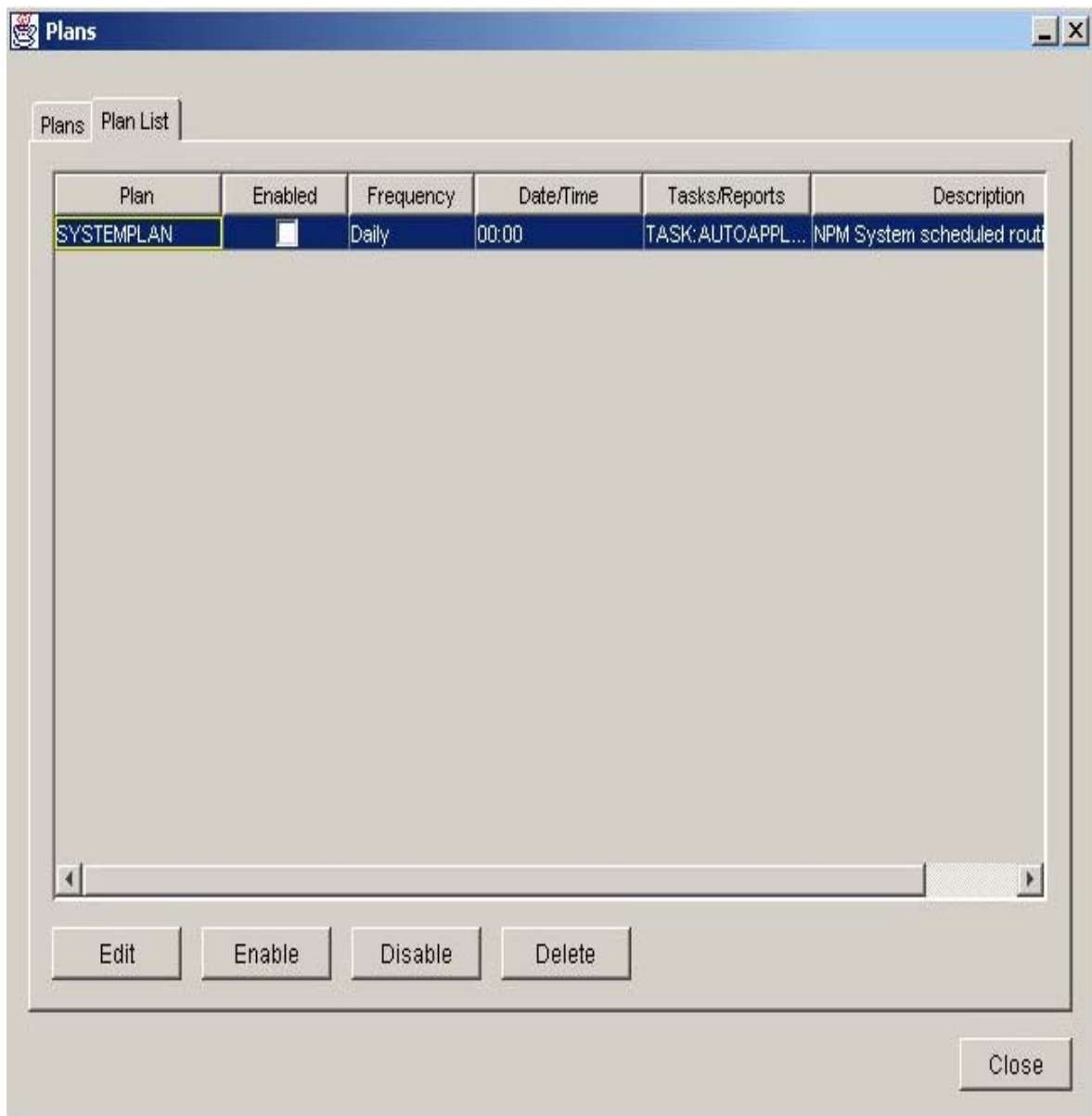


The preceding figure shows the SmartImage Task being saved and called *autoimage*.

After the task is saved it will show up as an available task to be scheduled in the NPM System Scheduler. The following figures show how to get to the NPM System plan and how to edit the plan to include the *autoimage* task.

Selection of the System Plans Menu

Selection of the System Plan for editing



List of Available Tasks

Plans

Plan Name: ☐ Enabled

Plan Description:

Task / Report Selection

Available Tasks/Reports

- Tasks
 - AUTOAPPLY
 - AUDIT
 - AUTORESTART
 - AUTOIMAGE
- Reports

Add >

< Remove

Reset

Selected Tasks/Reports

- Tasks
- Reports

Schedule

Frequency Time

Time Limit

Save Reset All

Close

The newly added *AUTOIMAGE* task can be added to the selected number of tasks to execute, as shown in [“Selection of the System Plan for editing” on page 2081](#).

Imaging added to the System Plan

The screenshot shows the 'Plans' window with the 'Plan List' tab selected. The 'Plan Name' is 'SYSTEMPLAN' and the 'Plan Description' is 'NPM System scheduled routine activities'. The 'Enabled' checkbox is unchecked. The 'Task / Report Selection' section shows two lists: 'Available Tasks/Reports' and 'Selected Tasks/Reports'. The 'Available' list contains 'Tasks' (with sub-items 'AUTOAPPLY', 'AUDIT', 'AUTORESTART', and 'AUTOIMAGE') and 'Reports'. The 'Selected' list contains 'Tasks' (with sub-items 'AUTOAPPLY', 'AUTORESTART', and 'AUTOIMAGE') and 'Reports'. The 'Add >' button is visible between the lists. The 'Schedule' section shows 'Frequency' set to 'Daily' and 'Time' set to '00:00'. The 'Time Limit' is set to 'No_Limit'. The 'Save' and 'Reset All' buttons are at the bottom left, and the 'Close' button is at the bottom right.

Plans Plan List

Plan Name: SYSTEMPLAN

Plan Description: NPM System scheduled routine activities

☐ Enabled

Task / Report Selection

Available Tasks/Reports

- Tasks
 - AUTOAPPLY
 - AUDIT
 - AUTORESTART
 - AUTOIMAGE
- Reports

Add >

< Remove

Reset

Selected Tasks/Reports

- Tasks
 - AUTOAPPLY
 - AUTORESTART
 - AUTOIMAGE
- Reports

Schedule

Frequency Time

Daily 00:00

Time Limit

No_Limit

Save Reset All

Close

Scheduling a SmartImage task from the NPM CLUI

The following figure shows how to save, add and schedule a *SmartImage* task from the NPM CLUI.

Scheduling SmartImage Task from NPM CLUI

```
npm>newtask MG9K_IMAGE_TASK SMARTIMAGETASK"MG9K AUTO IMAGING  
" MG9KDEVICES  
Task created successfully.
```

```
npm>sched SYSTEMPLAN TASK MG9K_IMAGE_TASK Add  
Done.
```

```
npm>updplan SYSTEMPLAN Daily"1-24-04 00:00 " No_Limit "Nightly Maintenance "  
Plan updated successfully.
```

```
npm>enableplan SYSTEMPLAN ON  
Done.
```

Hardware Requirements or Dependencies

None

Software Requirements or Dependencies

This feature requires the SN07 MG9K EM, NPM and MG9K Device Software.

Limitations and restrictions

Refer to the Limitations and Restrictions listed in the FN section of this feature.

Interactions

None



SN07 Feature Deltas

Product = MG 9000

A00003074 -- MG9000 Manager Capacity Increase (UA-IP)

Functional Description

In the SN07 release the MG9000 Manager will be required to support a maximum capacity of 110,000 H.248 native lines and 75 MG9000 network elements. The pre-SN07 maximum capacity for the MG9000 Manager is 55,000 lines and 60 MG9000 network elements. The recovery time for the 55,000 line configuration is 90 minutes per SN06 Engineering Guidelines. This feature by requirement will meet or exceed the current documented SN06 recovery time, under the new extended capacity requirements.

The reason for the long recovery times is that per the current software architecture, managed objects have to be instantiated within the EM to allow OAM&P. To achieve the SN07 requirements specific managed objects in the MG9000 Manager design will be collapsed. These objects will have their data persisted to the Oracle database and their business logic collapsed into a container class. This design simplifies the recovery of the “leaf nodes” in the system, which require the most memory footprint and instantiation resources during application startup.

Included as part of this design, all configurable MG9000 data will be persisted and restored from the Oracle database. There will also be work required to support maintenance release and major release upgrades.

Hardware Requirements or Dependencies

This feature will apply to all supported hardware platforms, per SN07 Succession Server Platform Foundation Software specification.

Software Requirements or Dependencies

None

Limitations and restrictions

MG9000 provisioning actions will not be accepted in the event of a loss of communication with the Oracle Database hosted on the CS2M host.

Interactions

None.

Applicable customer facing sections

Fault Management

Logs	__N/A__
Alarms	__N/A__

Configuration

Data Schema	__N/A__
User Interface	__X__
Element Management	__N/A__
Security	__N/A__
Service Order	__N/A__
Office Parameters	__N/A__

Accounting (includes AMA billing)	__N/A__

Performance (includes operational measurements)	__N/A__

Realtime	__X__

Engineering Information	__X__

Configuration for A00003074

Upgrade Impact

Dump and Restore

In order to upgrade to SN07.0, the customer must currently be running the SN06.0 release.

In order to bring the data from SN06.0 to SN07 during an SN06.0 to SN07 upgrade, the customer must export the SN06.0 data in the SN06.0 Subnet View for the individual gateway node and then import the gateway node into SN07. The export files from SN06.0 must be saved on another device if rollback of a

gateway is anticipated. The SN06.0 export data is used to repopulate the node in the SN07 Mg9k Element Manager.

Prior to performing a maintenance release (MR) upgrade (i.e. SN07 to SN07MR), the customer should backup the Oracle database on the CS2M machine. This is a normal backup of the oracle database on the CS2M machine.

Element Management Major Release Upgrade

Changes to the SN06.0 to SN07 upgrade are

- After upgrading to SN07, new hardware for SCO, SCI, ITX, ITP, and ABI can be upgraded.
- During the time when the DCC cards have been upgraded to SN07 but the NE resides in the SN06.X Subnet View, the SN06.X OM Collector will not collect any OMs due to security features added in the SN07 MG9k card software. The NE should be removed from the SN06.X OM Collector collection list.
- If attempting to rollback to SN06.0, the new SN07 boards have to be removed and replaced with the old hardware boards prior to downgrading the loads on the cards. Failure to do so could damage the hardware.
- When the user installs the MG9000 Master server software, the “pkgadd” command now performs an additional check. If two releases of the MG9000 server software are already installed, the installation fails and the user sees the following message:

The package cannot be installed. The following releases of the MG9000 EM Master server are already installed:

NTmg9ks_6_45.pkg

NTmg9ks_6_221_0.pkg

At most two releases of the MG9K EM Master server software should be installed on a given SSPFS at any time. Before installing the new package, you must remove one of the packages listed above. Please remove the package that is no longer being used. To remove a package, use the “pkgadd” command.

- When the user installs the MG9000 mid-tier server software, the “pkgadd” command now performs the same check. If two releases of the MG9000 mid-tier software are already installed, the installation fails and the user sees the following message:

The package cannot be installed. The following releases of the MG9000 EM mid-tier server are already installed:

NTmg9km_6_45.pkg

NTmg9km_6_221_0.pkg

At most two releases of the MG9K EM mid-tier server software should be installed on a given SSPFS at any time. Before installing the new package, you must remove one of the packages listed above. Please remove the package that is no longer being used. To remove a package, use the “pkgadd” command.

Element Management Maintenance Release (MR) Upgrade

Compared to previous releases, the SN07 maintenance release (MR) upgrade process has the following differences:

- Prior to the MR upgrade, the user should backup the entire Oracle database.
- The user does not export each NE prior to the upgrade.

The SN06.0 MR upgrade process is documented in section “Upgrading the MG 9000 Manager software to a maintenance release” of document NN10048-461 entitled “Upgrading the MG9000” (version SN07). Below is a summary of the MR upgrade process for SN07.

- Backup the entire Oracle database.
- Upgrade the hardware, if necessary. Ensure the connection from the MG 9000 Manager to the MG 9000 is up.
- Stop the GUI clients.
- Stop the mid-tier server.
- Stop the Performance Collector and Formatter (PCF) OM collection application.
- Stop the master server.
- Remove the old master server package.
- If required, perform an MR upgrade on the SSPFS software.
- Install, configure, and start the MR release master server. When you configure the master server, typically you should use the same settings from the previous installation of the master server. You will NOT be prompted with the questions “Is this an MR upgrade?” and “Do you want to initialize the database?”. The software knows the correct actions to take.
- Remove the old midtier server package.
- Install, configure, and start the MR release midtier server. When you configure the midtier server, typically you should use the same settings from the previous installation of the midtier server.
- Launch the new client. The client will display any NEs that were provisioned prior to the MR upgrade.
- Reconnect any third party application that retrieves alarms for delivery to Operations Support System (OSS) fault management systems.

- Install and start the MR release OM collection application.

OSS Changes

Prefix Changes

With SN07 the northbound interfaces need to change the prefix for event channel, and fault manager entries. In SN06.0, the prefix was Subnet_62. With the SN07 release the prefix for applicable CORBA Naming Service entries should be changed to Subnet_7.

Example ORB entry changes:

SN06.0

EventChannel = "Subnet_62.ec.Oss"

FaultServiceManager = "Subnet_62.Services.FaultServiceManager"

SN07

EventChannel = "Subnet_7.ec.Oss"

FaultServiceManager = "Subnet_7.Services.FaultServiceManager"

Customer Log Changes

New customer logs are added to inform users when data has not been saved in the database. These are cases where the data is provisioned successfully in all appropriate places except for the database. The logs indicate when this situation occurs for termination data, when an attempt to correct the database fails, and when the database is corrected. The MGEM logs apply to all components on the MG9K EM except for terminations and the VMG logs apply to termination data. The logs and examples are below:

- MGEM 704 - An attempt to correct the database has failed.

MGEM 704 Warning INFO

Database unavailable, correction failed

Failed database correction on VMG. The database will be corrected when it is available. Check the database for problems.

MGEM 704 Warning INFO

Database unavailable, correction failed

Failed database correction to MODIFY TERM ESA DATA on VMG LCE023-0-3, termination tp/04/01 with DN 9192234567. The database will be corrected when it is available. Check the database for problems.

- MGEM 705 - An attempt to correct the database has passed.

MGEM 705 Warning INFO

Database corrected

Data is corrected on VMG.

- VMG 600 - Termination data was successfully provisioned in all appropriate areas except for the database.

VMG 600 Warning INFO

Database unavailable, update failure

Failed database update to MODIFY TERM DN on VMG LCE023-0-3, termination tp/04/01 with DN 9192234567 and gateway ESA flag value of 0. The database will be corrected when it is available. Check the database for problems.

- VMG 601 - An attempt to correct termination data in the database has passed.

VMG 601 Warning INFO

Database corrected

Data is corrected for MODIFY TERM DN on VMG LCE023-0-3, termination tp/04/01 with DN 9192234567.

External Interface Changes

With SN07 the TL1 Adaptor for SN07 connects to 2363 port. Thus third party equipment should connect to port 2363 for SN07.

In SN07, the EM's SNMP listening port is 8002.

Element Management

New/modified GUIs

MG9000 Menu changes

In SN06.2 and earlier releases, the MG9000 menu tab in the subnet view has a menu item for ExportNE. However, as of SN07, the menu item for ExportNE no longer exists. When upgrading from SN07 to a later release, the user no longer exports the NE data.

New Status Icon

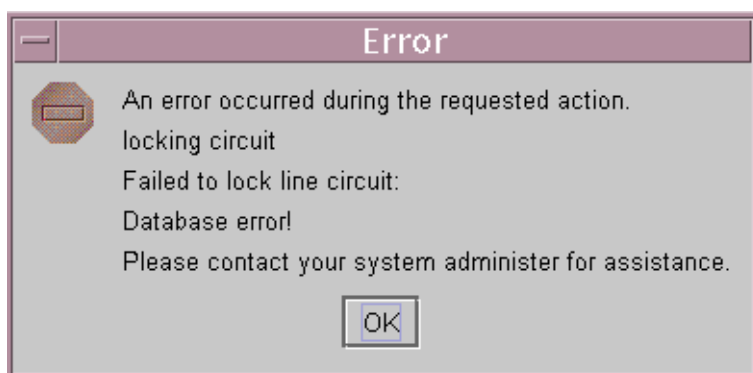
Consider a scenario in which an MG9K is upgraded from an EM running version SN06.0 to an EM running version SN07. After the upgrade, the SN06.0 version of the EM notices that the MG9K is reporting its traps to an IP address and port that is different from its own SNMP listening port. Essentially, the SN06.0 EM is no longer managing that MG9K.

When an EM has an MG9K provisioned but is no longer managing that MG9K, the EM's GUI should provide an indication to the user regarding the status of that MG9K. More specifically, in the GUI's subnet view, the following status icon will appear on top of the NE icon:



New database error

With this feature, some data that used to reside in memory will now be persisted in the database. If a database error is encountered during MG9000 EM GUI actions, an error message will be displayed to inform the user that the operation has failed due to a database error. The following GUI is an example of such an error message:



Product = MG 9000

A00003531 -- MG9K EM - Frame location enhancements (UA-IP)

Functional Description

This feature consists of following deliverables:

- 1** Office Frame number is displayed in MG9K EM Alarm browser, IEMS alarm browser and any other alarm browser/s provided by OSS.
- 2** Internal frame number is hard-coded to zero in VMG name, while provisioning VMG.
- 3** In MG9K-EM Frameview, frames are displayed without gap. However, any gap present between shelves will continue to be displayed.
- 4** With this change, MG9K-EM Frame view is displayed in a cleaner way. Some of the examples for this cleaner display are;
 - MG9K-EM Craft-person can see Master frame as and when he/she opens the Frame view, even when Master frame has two or more empty frames to its left side.
 - MG9K-EM Craft-person can see adjacent frames, without scrolling to right in Frameview, even when there is gap between the frames.
- 5** In MG9K-EM Frameview, Master frame is shown far left and all subtending frames are shown to the right of Master frame going by following logic.
 - Show Master frame far left.
 - Show other frames, whose frame number is higher than that of Master frame on right of Master frame, in increasing order of their Internal frame number (IFN).
 - And then, show other frames, whose IFN is lower than that of Master frame, in increasing order of their IFNs.

As a result of the deliverables #3 and #4, Frameview may not be a mirror reflection of actual line-up of frames in MG9K.

Note that, as in SN6.0, in MG9K-EM Frame view, Internal frame number is shown at the bottom of each frame and Office frame number is shown at the top of each frame. With this, Craft-person can map the MG9K-EM Frame view to actual line-up of frames in MG9K.

- 6 Office Frame number is used in place of Internal frame number in OMC CSV OM file (a stretch deliverable)
- 7 A *complete* flow through provisioning is supported for ITP VMGs. With this, Frame location information, which is specified in MG9K-EM while provisioning ITP VMGs, is sent to SESM. SESM in turn, updates XA-CORE table LGRPINV.
- 8 With these changes, Craft-person need not manually fill Frame location information in the table LGRPINV. Craft-person just need to provision Frame location information at MG9K-EM
- 9 A *partial* flow through provisioning is supported for ABI VMGs. With this, Frame location information, which is specified in MG9K-EM while provisioning ABI VMGs, is sent to SESM. However, SESM does not in turn updates XA-CORE table GWINV.
- 10 There is no impact on the way Craft-person handles ABI VMGs, because of these changes. i.e., he/she still needs to manually fill Frame location information in the table GWINV, apart from provisioning Frame location information at MG9K-EM.

Note: GWINV is a new table, which will be supported in SN07 through the Core feature A00003486 (Gateway location information).

MG9K-EM Frame view

This section gives example screen shots for the deliverable #3 and #4, which are explained in the beginning of this section. For this, two different scenarios are considered.

Scenario 1

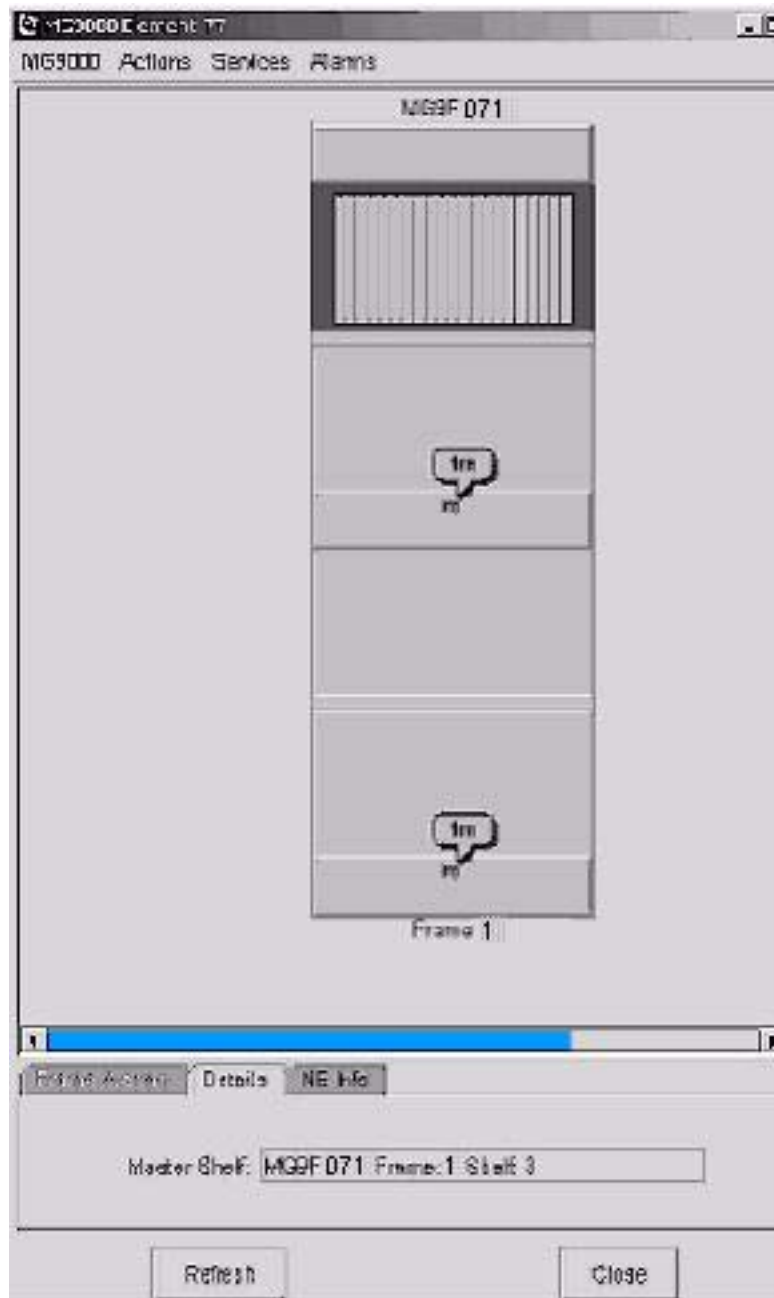
Let us consider a scenario wherein frames are lined-up from left to right as follows;

- 2 First frame is numbered as 1 and is Master frame
- 2 Second frame is numbered as 3 and is subtending frame

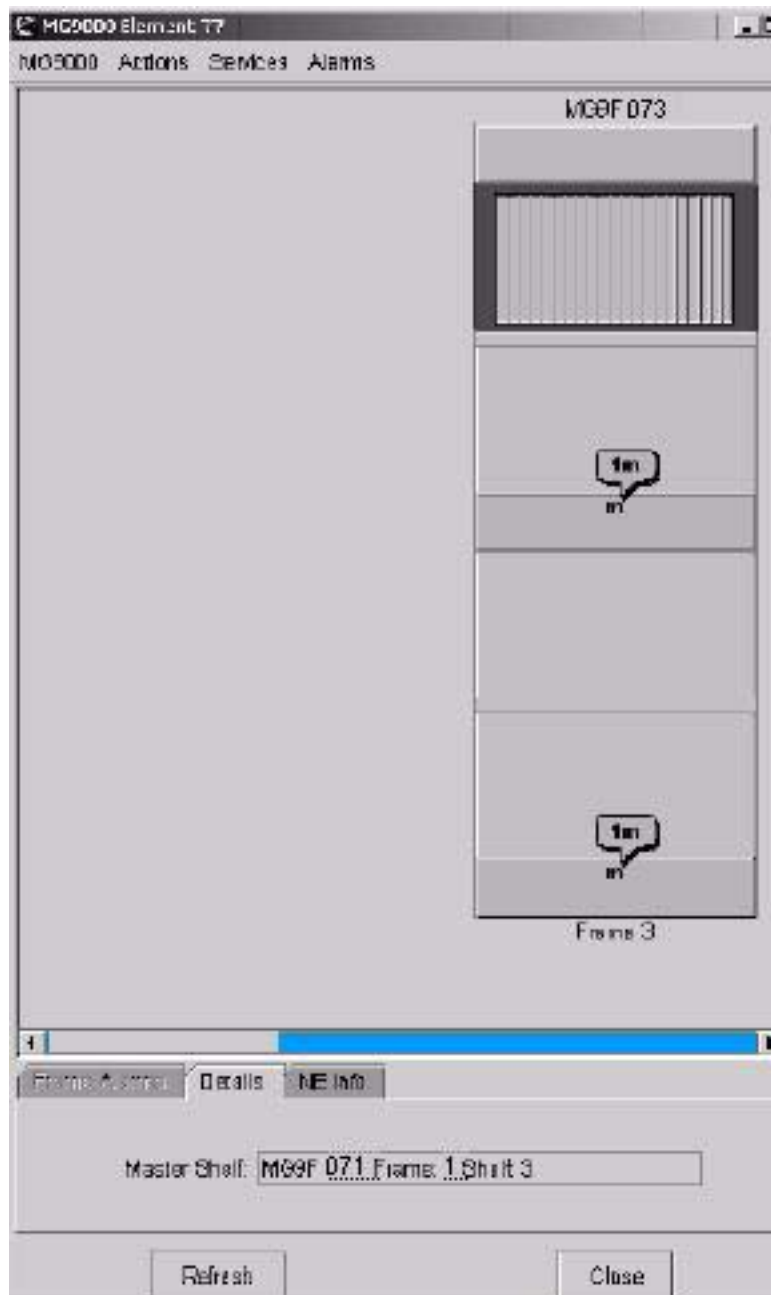
For this scenario, in SN06.0, craft-person need to use horizontal scroll bar to see the non-empty frames (frame #1 and frame #3) and MG9K-EM Frame view would look like figure “MG9K-EM Frame view in SN06.0 and prior – when Frame view comes up” on page 2094 and figure “MG9K-EM Frame view in SN06.0 and prior – Horizontally scrolled far right” on page 2095.

For this scenario, in SN07, craft-person see the non-empty frames as and when he/she opens the Frameview and MG9K-EM Frame view would look like figure “MG9K-EM Frame view in SN07” on page 2096.

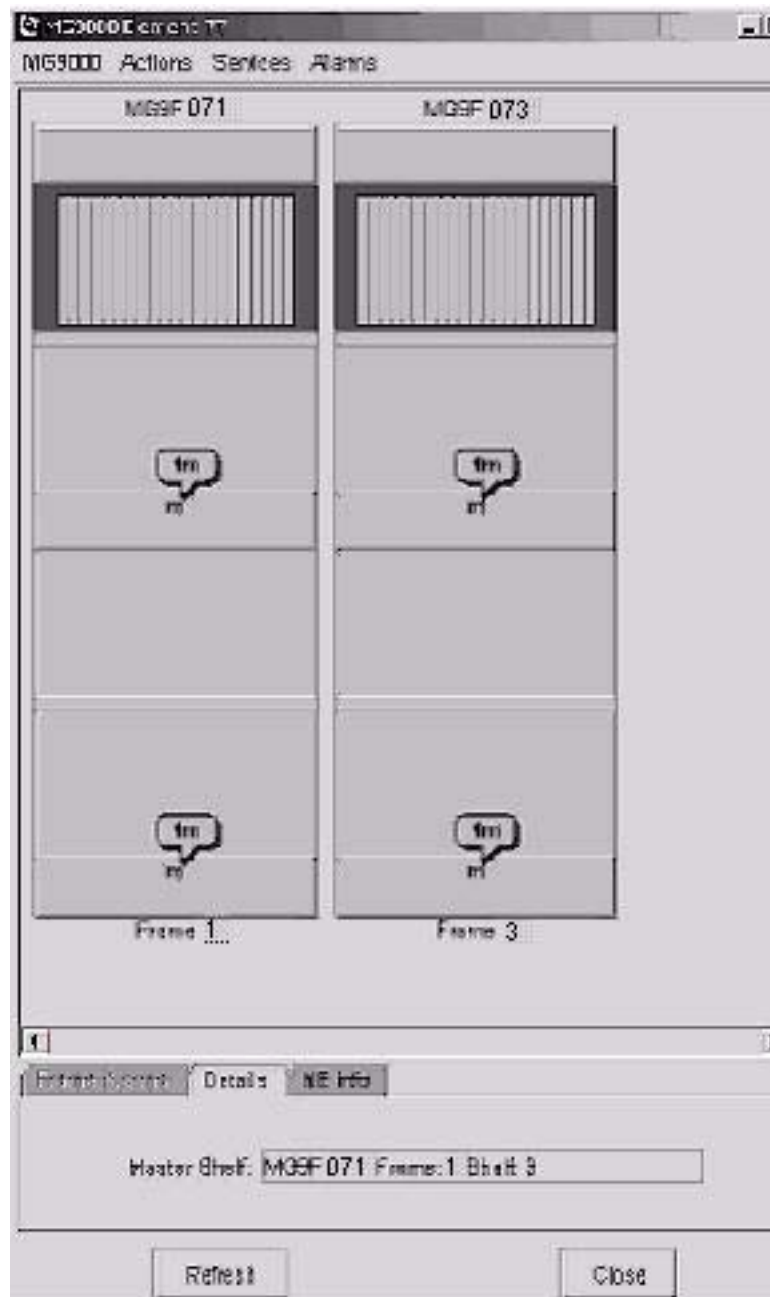
Even when frames are lined-up from right to left, in both SN06.0 and SN07, Frame view will look the same way as in left to right lineup.



MG9K-EM Frame view in SN06.0 and prior – when Frame view comes up



MG9K-EM Frame view in SN06.0 and prior – Horizontally scrolled far right

**MG9K-EM Frame view in SN07**

Scenario 2

Let us consider a scenario wherein frames are numbered as follows;

- ² First frame is numbered as 5 and is Master frame
- ² Subsequent three subtending frames are numbered as 7, 0 and 2.

For this scenario, in SN06.0, frames would be shown in increasing order of their Internal frame numbers. i.e, as [frame #0][frame #2][frame #5][frame #7]).

For this scenario, in SN07, frames would be shown as [frame #5][frame #7][frame #0][frame #2]); refer to the logic given in the beginning of this section, point #4.

MG9K-EM Alarm browser

The following figure “MG9K-EM Alarm browser GUI” is an example screen shot for the deliverable #1, which is explained in the beginning of this section. Note that, without Frame location information being provisioned, ‘Description’ field in the Alarm browser is shown with default filler ‘F’ in following format:

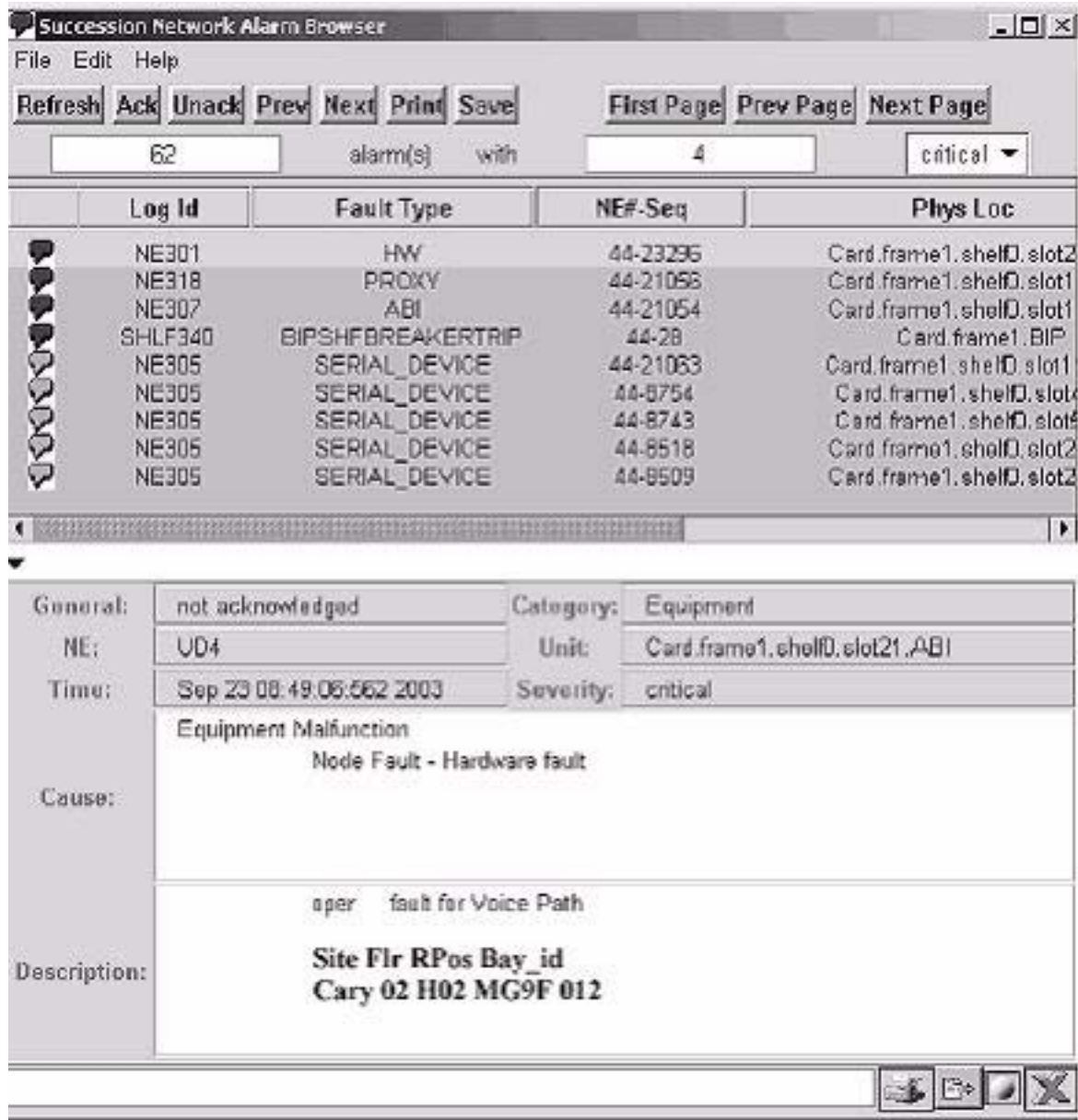
```
Site   Flr   RPos   Bay_id
FFFF   FF   FFFF   MG9F FFF
```

i.e.

```
<Site=FFFF><3 blank space><Flr=FF><2 blank
space><RPos=FFFF><3 blank space><Bay-id=MG9F FFF>
```

When Frame location information is (re)provisioned for a Master frame, all alarms (both Gateway alarms and EM alarms) reported on components in the frame are updated with latest frame location information.

When Frame location information is (re)provisioned for a subtending frame, only Gateway alarms reported on components in the frame are updated with latest frame location information.



MG9K-EM Alarm browser GUI

Hardware Requirements or Dependencies

None

Software Requirements or Dependencies

This feature depends on MG9K changes for the deliverable #5, mentioned in the beginning of this section.

Limitations and restrictions

- 1 VMGs which are provisioned in SN05/SN06+ with non-zero Internal frame number, continue to exist as they are. i.e., they continue to exist with non-zero Internal frame number.
- 2 Frame location information is sent from MG9K-EM to SESM only at VMG provisioning time. So, any changes done to Frame location information from MG9K-EM after VMG is provisioned, is not sent to SESM. Frame location information present at XACore can be changed, even after VMG is provisioned. Any mismatch, which is introduced as result of such changes, is not audited or corrected.
- 3 A complete flow through provisioning is not supported for ABI VMGs. Hence, for ABI VMGs, Craft-person need to manually enter Frame location information in XA-CORE table GWINV.

Interactions

This feature is an extension of the SN06.0 feature A00002704 and leverages the work of A00002704, to deliver the items 1 to 6 mentioned in the beginning of this section, which have impact on the end user.

Applicable customer facing sections

Fault Management:

Logs _N/A_

Alarms _X_

Configuration:

Data Schema _N/A_

User Interface _X¹_

Element Management _X_

Security _N/A_

Service Order _N/A_

Office Parameters _N/A_

Accounting (includes AMA billing) _NA_

1. Alarm browser GUI would show Frame location information.

Performance (includes operational measurements) X

Glossary

Term	Description
CSV	Comma separated values. One format of storing performance data
EM alarm	Alarm generated internally by MG9K EM. Ex; When communication from MG9K EM to MG9K goes down, MG9K-EM generates an alarm with specific problem "Comm Channel Down - Communication Lost to the NE".
Frame location information	It consists of frame type, floor position, row position, frame position, shelf position
Internal (logical) frame number	Frame number, which is unique within a MG9K
Gateway alarm	Alarm reported from gateway.
Master frame	It has the master shelf.
NE	Network element
Office frame number	Frame number, which is unique within an office
OM data	Operational Measurement data. A.k.a performance data
MG9K frame line-up	MG9K frames are lined-up either left to right or right to left. When frames are lined-up left to right, new frames are positioned/added to right of existing frames, as MG9K grows and frames are numbered from left to right. That means, Master frame will be the left-most frame in the NE. When frames are lined-up right to left, new frames are positioned/added to left of existing frames, as MG9K grows and frames are numbered from right to left. That means, Master frame will be the right-most frame in the NE.
Subtending frame	It has the subtending shelves of a MG9K
VMG	Virtual Media Gateway is a logical representation of a gateway

References

A00003486 Gateway location information FN

Configuration for A00003531

Hardware and Software Requirements

NA

Initial Configuration

NA

Office / Subnet parameters (OP/SP) (CM & SESM)

NA

Upgrade Impact

None

Data schema (DS) (CM, MIBS, RDB)

No new schemas, tables, or table columns are introduced by this feature. No existing external interfaces are changed.

Service Orders (SO) (CM & SESM)

None

Software optionality control (SOC)

NA

Element Management

New/modified GUIs

GUI Name	NEW, CHANGED or DELETED
MG9K-EM Frame-view	Changed
MG9K-EM "Provision a Virtual Media Gateway" GUI	Changed
MG9K-EM Alarm browser GUI	Changed

GUI information

GUI name: MG9K-EM Frame-view

Functional description

Following changes will be done in this GUI;

- a. Frames are displayed without gap.
- b. Master frame is shown on far left and all subtending frames to the right of Master frame.

With these changes, MG9K-EM Frame view is displayed in a cleaner way. Advantage of this cleaner display are;

- a. MG9K-EM Craft-person can see Master frame as and when he/she opens the Frame view, even when Master frame has two or more empty frames to its left side.
- b. MG9K-EM Craft-person can see adjacent frames, without scrolling to right in Frameview, even when there is gap between the frames.

As a result of these changes, Frameview may not be a mirror reflection of actual line-up of frames in MG9K. Note that, as in SN06.0, in MG9K-EM Frame view, Internal frame number is shown at the bottom of each frame and Office frame number is shown at the top of each frame. With this, Craft-person can map the MG9K-EM Frame view to actual line-up of frames in MG9K.

GUI Usage and implications

NA

GUI size

No changes in SN07.

GUI fields

No changes in SN07.

Usage example

Let us consider two scenarios.

Scenario 1:

Here, frames are lined-up from left to right as follows;

- frame-1 is the Master frame
- frame-0 and 2 are not cabled
- frame-3 is subtending frame

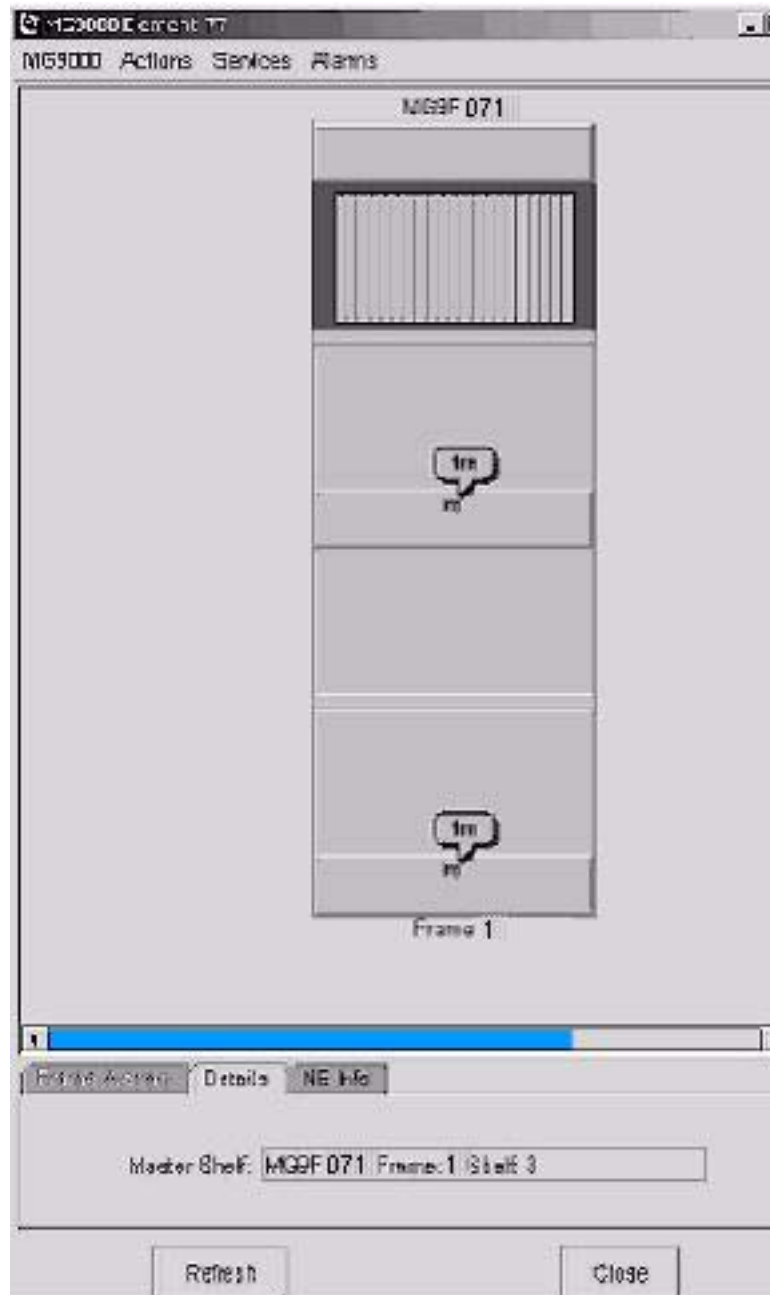
Scenario 2:

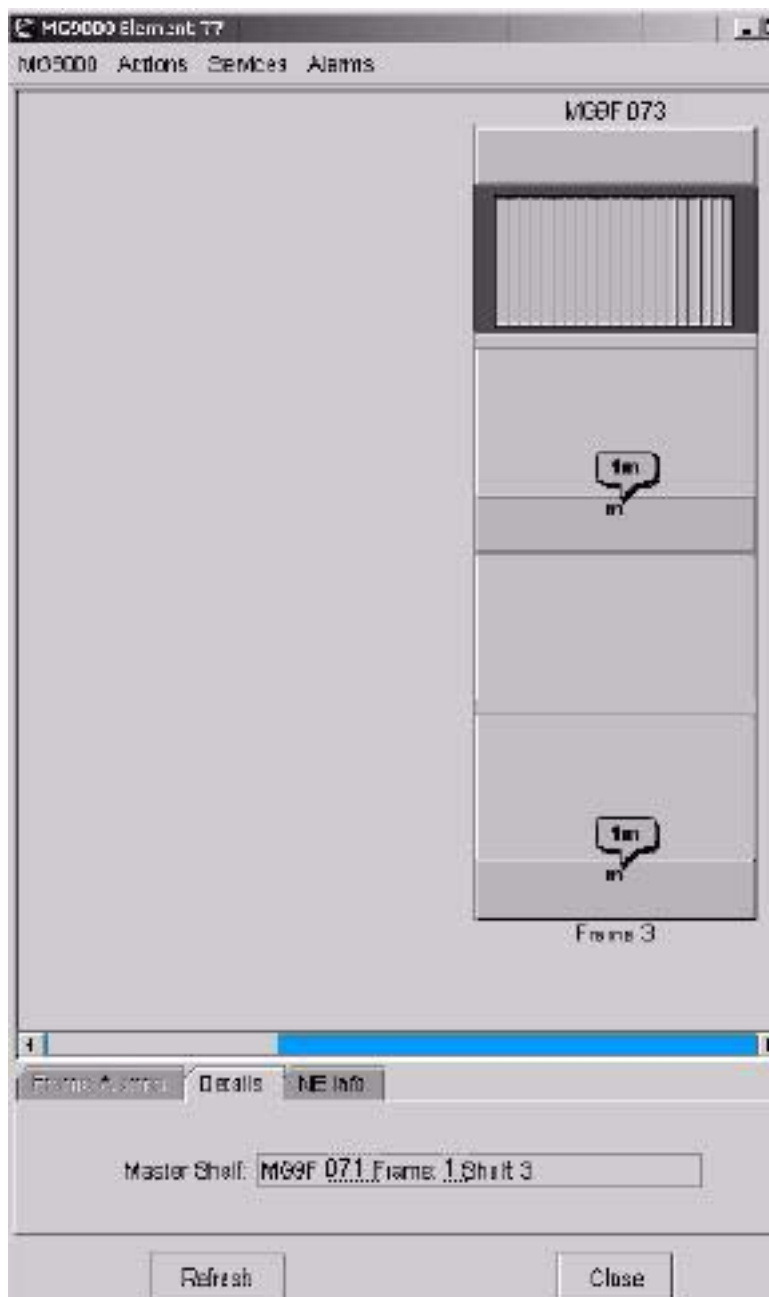
Here, frames are lined-up from right to left as follows (see explanation given for this type of line-up in 12.12);

- frame-1 is the Master frame
- frame-0 and 2 are not cabled
- frame-3 is subtending frame

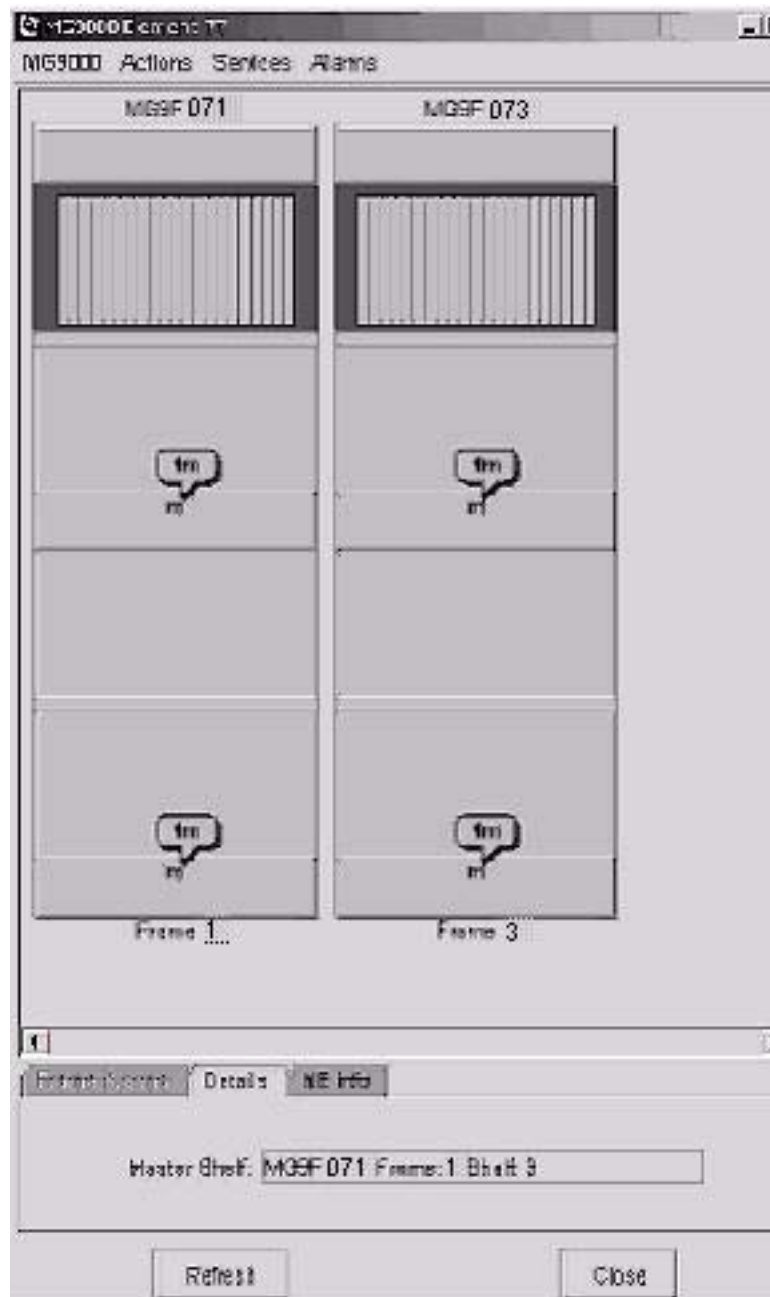
For both scenarios, in SN06.0, the craft-person needs to use horizontal scroll bar to see the non-empty frames (frame-1 and frame-3) and MG9K-EM Frame view would look like figures [“MG9K-EM Frame view in SN06.0 and prior when Frame view comes up”](#) on page 2104 and [“MG9K-EM Frame view in SN06.0 and prior when horizontally scrolled far right”](#) on page 2105.

For both scenarios, in SN07, the craft-person can see the non-empty frames as and when he/she opens the Frameview and MG9K-EM Frame view would look like figure [“MG9K-EM Frame view in SN07”](#) on page 2096.

MG9K-EM Frame view in SN06.0 and prior when Frame view comes up

MG9K-EM Frame view in SN06.0 and prior when horizontally scrolled far right

MG9K-EM Frame view in SN07



GUI release history update

SN07, following changes will be done to MG9K-EM Frameview GUI;

- a. frames are displayed without gap.
- b. Master frame is shown on far left and all subtending frames to the right of Master frame.

Supplementary information

None

CLUI Interface

NA

GUI name: MG9K-EM “Provision a Virtual Media Gateway” GUI**Functional description**

Following changes will be done in this GUI:

Internal frame number is hard-coded to zero in VMG name, while provisioning VMG. So, VMG name of a VMG which is provisioned in SN07, will be as follows;

<SITE_name><Office frame number><Internal frame number = 0><Shelf number>

An example VMG name is ‘SLOA007-0-1’.

GUI Usage and implications

No changes in SN07.

GUI size

No changes in SN07.

GUI fields

Following table describes fields of this GUI.

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Virtual Media Gateway Name	Changed	NA	No change in SN07	Internal frame number is hard-coded to zero in VMG name, while provisioning VMG.	No change in SN07

There is no change in SN07 for other GUI fields.

Usage example

The field "Virtual Media Gateway" is not configurable by MG9K-EM Craft-person. This field is populated based on value of the fields "Virtual Media Gateway type" and "Virtual Media Gateway physical location". Note that, in figure "MG9K-EM "Provision a Virtual Media Gateway" GUI in SN06.0 and prior", Internal frame number of 1 is used to construct VMG name and in figure "MG9K-EM "Provision a Virtual Media Gateway" GUI in SN07", Internal frame number is hard coded to zero while constructing VMG name.

MG9K-EM "Provision a Virtual Media Gateway" GUI in SN06.0 and prior

Provision a Virtual Media Gateway

Virtual Media Gateway type: ITP-IP

Virtual Media Gateway physical location: Frame: 1 Shelf: 3 Mated Slots: 12/13

Site Name: UAIP

Office Frame Number: 003

Virtual Media Gateway Name: UAIP003-1-3

Apply Clear Close

MG9K-EM "Provision a Virtual Media Gateway" GUI in SN07

Provision a Virtual Media Gateway

Virtual Media Gateway type: ITP-IP

Virtual Media Gateway physical location: Frame: 1 Shelf: 3 Mated Slots: 12/13

Site Name: UAIP

Office Frame Number: 003

Virtual Media Gateway Name: UAIP003-0-3

Apply Clear Close

GUI release history update

SN07, following changes will be done to MG9K-EM GUI:

- Internal frame number is hard-coded to zero in VMG name

Supplementary information

None

CLUI Interface

NA

GUI name: MG9K-EM Alarm browser GUI**Functional description**

In SN07, following changes will be done in “Description” field of this GUI;

- Once Frame location information is provisioned, for new alarms, Frame location detail is appended to the data which is shown in this field in SN06.0.
- If Frame location information is not provisioned, default filler F’s are appended in following format to the data which is shown in this field in SN06.0.

Site Flr RPos Bay_id

FFFF FF FFFF MG9F FFF

i.e., <Site=FFFF><3 blank space><Flr=FF><2 blank space><RPos=FFFF><3 blank space><Bay-id>

<Bay-id> = MG9F<One blank space><FFF>

GUI Usage and implications

As explained in the previous “Functional description” section, data shown in “Description” field of this GUI depends on whether Frame location information is provisioned or not.

GUI size

No changes in SN07.

GUI fields

Following table describes the fields of this GUI.

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Description	Changed	NA	No change in SN07	Refer to 12.8.2.3.1	No change in SN07

There is no change in SN07 for other GUI fields.

Usage example

After Frame location information is provisioned for frame 1, if an alarm is raised on an entity say card, which is present in frame 1, then in SN07, it will look as in the following figure.

MG9K-EM Alarm browser GUI in SN07 when Frame location information is provisioned for frame 1

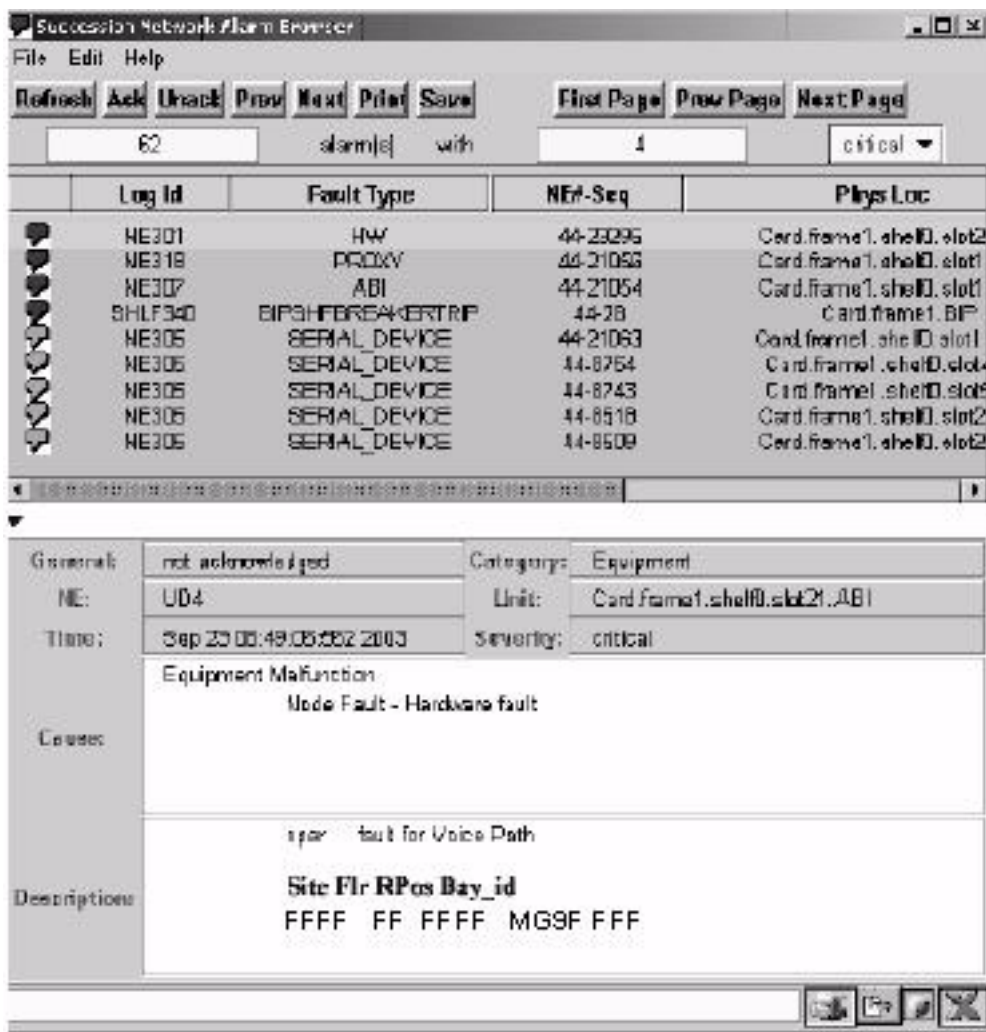
The screenshot displays the 'Succession Network Alarm Browser' window. The top menu bar includes 'File', 'Edit', and 'Help'. Below the menu is a toolbar with buttons: 'Refresh', 'Ack', 'Unack', 'Prev', 'Next', 'Print', 'Save', 'First Page', 'Prev Page', and 'Next Page'. A search filter is set to '62 alarm(s) with 4 critical'. The main table lists alarms with columns: Log Id, Fault Type, NE#-Seq, and Phys Loc. The bottom section provides details for a selected alarm.

Log Id	Fault Type	NE#-Seq	Phys Loc
NE301	HW	44-23295	Card.frame1.shelf0.slot2
NE318	PROXY	44-21056	Card.frame1.shelf0.slot1
NE307	ABI	44-21054	Card.frame1.shelf0.slot1
SHLF340	BIPSHFBREAKERTRIP	44-28	Card.frame1.BIP
NE305	SERIAL_DEVICE	44-21063	Card.frame1.shelf0.slot1
NE305	SERIAL_DEVICE	44-8754	Card.frame1.shelf0.slot4
NE305	SERIAL_DEVICE	44-8743	Card.frame1.shelf0.slot5
NE305	SERIAL_DEVICE	44-8518	Card.frame1.shelf0.slot2
NE305	SERIAL_DEVICE	44-8509	Card.frame1.shelf0.slot2

General:	not acknowledged	Category:	Equipment
NE:	UD4	Unit:	Card.frame1.shelf0.slot21.ABI
Time:	Sep 23 08:49:05:562 2003	Severity:	critical
Cause:	Equipment Malfunction Node Fault - Hardware fault		
Description:	oper fault for Voice Path Site Flr RPos Bay_id Cary 02 H02 MG9F 012		

If an alarm is raised on an entity say card, which is present in frame 1, for which Frame location information is not provisioned, then in SN07, it will look as in the following figure.

MG9K-EM Alarm browser GUI in SN07 when Frame location information is not provisioned for frame



GUI release history update

SN07, following changes will be done in Description field of this GUI;

- Once Frame location information is provisioned, for new alarms, Frame location detail is appended to the data which is shown in this field in SN06.0. If Frame location information is not provisioned, default fillers F's are appended to the data which is shown in this field in SN06.0.

Supplementary information

The frame location information within the alarm browser (and LOGs) will exist as a snapshot. If the frame location information is changed, the alarm browser will not be updated with the new frame location information. Also, Alarms which are generated/reported before corresponding frame is re-provisioned, are displayed in Alarm browsers without any change.

CLUI Interface

NA

Command interface changes

None

Security

None.

Note: Even though, MG9K OM Collector need access to MG9K EM Oracle database tables, DEM_APPS and FRAME_LOC, no changes need to be done in authentication.

Configuration Walkthrough

NA

Glossary

Term	Description
Frame location information	It consists of frame type, floor position, row position, frame position, shelf position
Internal (logical) frame number	Frame number, which is unique within a MG9K
MG9K frame line-up	MG9K frames are lined-up either left to right or right to left. When frames are lined-up left to right, new frames are positioned/added to right of existing frames, as MG9K grows and frames are numbered from left to right. That means, Master frame will be the left-most frame in the NE. When frames are lined-up right to left, new frames are positioned/added to left of existing frames, as MG9K grows and frames are numbered from right to left. That means, Master frame will be the right-most frame in the NE.

Term	Description
NE	Network Element. Each NE has a Master shelf and zero or more subtending shelves/s, whose ITP cards are connected to the ITX card present in Master shelf.
Office (External) frame number	Frame number, which is unique within an office
Subtending frame	It has the subtending shelves of a MG9K

References

A00003531_MG9000_Frame_Location_FN

A00003486 Gateway location information FN

Performance for A00003531

Performance management strategy

OM Collector (OMC) fetches performance data from MG9K through FTP, converts the performance data to CSV format and writes the converted data into a file. In subsequent sections of this document, this file is termed as “OMC CSV file”. OSSs which are present towards north bound interface of OMC, make use of these OMC CSV files.

Performance management tools and utilities

OMC CSV file contains data in the following format:

```
<ScalarTableName-1>  
<performance parameter name 1>, <performance parameter name 2>...  
Value1, Value2...
```

```
<NonScalarTableName-2>  
<performance parameter name 1>, <performance parameter name 2>...  
Source, Value1, Value2...
```

An example data in a SN06.0 OMC CSV file is as follows;

```
Miscellaneous  
snmpInvalidMsgs,snmpInBadCommunityNames,snmpInPkts  
0,0,1769
```

```
norCarrSonetMediumIntervalTable  
Source,norCarrSonetMedIntervalOpt,nnorCarrSonetMedIntervalLBC  
Frame2.Shelf0.Slot10.Port1,99,100  
Frame2.Shelf0.Slot11.Port401,100,100
```

Here, the table 'Miscellaneous' is a Scalar table. That means, it's Performance parameters are Scalar SNMP attributes. So, they are not identified by any 'source'. Whereas, the table norCarrSonetMediumIntervalTable is a non-scalar table. That means, it's Performance parameters are non-scalar SNMP attributes. So, they are identified by appropriate source, namely Frame number, Shelf number, Card number and Port number.

In SN06.0, OMC CSV file uses Internal frame number for values of Performance parameters of non-scalar table. In above example, number 2 shown next to 'Frame' is Internal frame number of the 'source' of the performance parameter.

In SN07, OMC CSV file will use Office frame number for values of Performance parameters of non-scalar table. So, if Frame location information is provisioned for frame-2, example data which is shown above, will be as follows in SN07.

```
Miscellaneous
snmpInvalidMsgs,snmpInBadCommunityNames,snmpInPkts
0,0,1769
```

```
norCarrSonetMediumIntervalTable
Source,norCarrSonetMedIntervalOpt,nnorCarrSonetMedIntervalLBC
Frame080.Shelf0.Slot10.Port1,99,100
Frame080.Shelf0.Slot11.Port401,100,100
```

In this SN07 example, number '080' shown next to 'Frame' is Office frame number.

If Frame location information is not provisioned for frame-2, example data which is shown above, will be as follows in SN07.

```
Miscellaneous
snmpInvalidMsgs,snmpInBadCommunityNames,snmpInPkts
0,0,1769
```

```
norCarrSonetMediumIntervalTable
Source,norCarrSonetMedIntervalOpt,nnorCarrSonetMedIntervalLBC
FrameFFF.Shelf0.Slot10.Port1,99,100
FrameFFF.Shelf0.Slot11.Port401,100,100
```

Performance Measurements (PM), Operational Measurements (OM), and stats

None

Product = MG 9000

A00003567 -- MG9000 Manager - ABI ESA Support (UA-IP)

Functional Description

In SN07, ESA capability will be introduced for ABI lines. ABI ESA provides the ability to support basic XPM calls within the MG9000. The MG9000 ABI cards will terminate CSide links of the extending XPMs and give them ESA capability if the MG9000 is out of communication with its assigned Gateway Controller (GWC).

The element manager will build on existing ITP ESA functionality for retrieving the ESA translation data from the core and pushing it to the MG9000. Data common to ITP and ABI VMGs will be handled as in SN06.0. Additionally, new data specific to ABI cards will be retrieved from the core and sent to the MG9000. This data will include, node, BNV and term type entries. This new data will allow the MG9000 to support the associated call processing features for ABI while in ESA mode.

As in SN06.0, this feature provide the following:

- Ability to retrieve the ESA data organized on a VMG basis from the core. This data will be retrieved through the SDM platform on a 24 hour basis. This data will also be retrievable from the SDM on a manual basis. Another manual command on the core will have to be used to generate the core ESA data, the MG9000 EM will not be able to invoke the core's ESA data build.
- The ability to push the required ESA data down to the MG9000 by formatting an XML data file and sending it via FTP to the associated VMGs ABI card using a floating IP address.
- Upgrades of ESA data.

Additionally, this feature will add support for secure FTP for the data transfer between the EM and the MG9000. Currently this transfer occurs over standard non-secure FTP. Functionality will be added to:

- Provide a means to set a password and/or username. This is currently proposed to be via a gui accessible via the EM server. (details TBD)
- Allow data transfer to and from the MG to take place via secure FTP. This change will be transparent to the user. Secure FTP will be used for the OM Collector utility and ESA data ftp to the MG9000.

Hardware Requirements or Dependencies

No additional ESA requirements are needed for this feature besides the standard CS2000 hardware, the MG9000 EM and the MG9000 Gateway.

Software Requirements or Dependencies

This feature is providing ABI ESA support capability for the MG9000 EM, as well as secure interface support. It has dependences on the following features:

- A00002380: ESA for ABI: MG9000, XPM and CM
- A00003737 - LCI Remote Access and Security

Limitations and restrictions

- The ESA data from the core will be downloaded to the MG9000 only once every 24 hours. This is the same manner in which the core handles loading the RSC with ESA data.
- The MG9000 EM will not allow the modification of any ESA data retrieved from the core.
- The MG9000 EM will not be providing a ESATVR test tool. This test tool will be supplied by the core.
- The MG9000 EM will provide a mechanism to manually pull the latest ESA data from the Core. This mechanism will not push the ESA data down to the MG9000. The craftsperson will have to manually push the ESA data down to the MG9000 for each VMG. This is to prevent overloading the MG9000 with new data. Also, this mechanize will only work provided that the craftsperson has used the Core command to generate the latest Core xml data file for the EM to retrieve, the EM does not have the ability to invoke this Core command.

Interactions

N/A

Applicable customer facing sections

Fault Management

Logs X

Alarms X

Configuration

Data Schema

User Interface

Element Management X

Security

Service Order	_____
Office Parameters	_____
Accounting (includes AMA billing)	_____
Performance (includes operational measurements)	_____

Glossary

Term	Description
XPM	Ex Peripheral Module
EM	Element Manager
ESA	Emergency Stand Alone
GUI	Graphical User Interface
GWC	Gateway Controller
MG9000	Media Gateway 9000
MIB	Managed Information Base
SNMP	Simple Network Management Protocol
VMG	Virtual Media Gateway

Fault Management for A00003567

Fault management strategy

This feature uses existing MG9KEM fault management structure.

Fault management tools and utilities

Alarm Browser - Reports alarms from registered events. When an alarm is generated, it is displayed in the Alarm Browser along with the date and time, the NE Id, the resource (where the alarm was generated), the severity and probable cause. Highlighting the alarm displays the description of the alarm in the text box at the bottom of the Alarm Browser.

Log Adaptor - Generates logs from registered events. The log names and numbers are predetermined and are matched with the incoming event. A log with the corresponding name and number which contains the date, time, physical location, severity and any other pertinent information is generated and placed into a separate file.

Logs and Alarms

A new alarm (nnESADownloadFault) will be added to indicate a failure to download ESA data to given VMG. This alarm will only be generated for autonomous download attempts. This was indicated by a log in previous releases. This alarm is EM generated and will be problems such as failure to setup the FTP connection to gateway or failure to login. It is different than the inconsistent data (nnESAFault) alarm generated by the hardware while the file transfer is in progress.

The alarm will be cleared by the EM when a successful download takes place.

The new alarm will be displayed at the Alarm Browser at the subnet as well as the well as the alarm browser for each corresponding network element. A log is also generated.

In addition, all the alarms and logs generated for the ITP ESA also apply to ABI ESA.

Explanation

nnESADownloadFault

Title: nnESADownloadFault

Name: ESA

Description: This log is generated when the EM is unable to download ESA data to a VMG.

Severity: Critical

Event type: ESA data download failure

Format

The Log Delivery application for this feature generates logs in the Number 2 Switch Control Center (SCC2) format and the NT standard (STD) format.

nnESADownloadFault

```
***ESA302 Tue Jul 09 14:50:26 EDT 2003 TBL
NnESADOWNLOADFAULT
NE Number: 8 NE Name: co8
State: not acknowledged
Type: Equipment
Cause: Failed to set up FTP connection: login failure!
```

Time: Jul 09 14:50:26:616 2003

Severity: critical

Mo: Card.f0.s2.113.1TP

Description: EM failed to push ESA to VMG

Field descriptions

nnESADownloadFault

Field descriptions ESA302

Field	Value	Description
office identification	String	Identifies the switch that generates the log. This field is optional. The maximum length of this field is 12 characters.
alarm	***, **, *, or blank	Indicates the alarm type of the log report. ***=critical, **=major, *=minor, blank = no alarms/warning
threshold	+ or blank	Indicates if a threshold is set for the log report. Plus (+) sign indicates that a threshold was set; if a blank, a threshold was not set.
report identification	AAAA nnn	Identifies the log subsystem that generates the report. This field uses 2-4 alphabetical characters and the number 100-999 of the log report in this subsystem. For this log AAAA= MGC and nnn=600.
day	String	Identifies the day of the week.
mmmmdd	January-December (01-31)	Identifies the month and date the report generates.
hh:mm:ss	00-23 00-59 00-59	Identifies the hour, the minute, and the second the report generates.

Field descriptions ESA302

Field	Value	Description
zone	PST, EST, MST, CST, AST	Identifies the time zone.
yyyy	0000-9999	Year
ssdd	0000-9999	Defines a different sequence number for each log report generated.
event type	TBL, INFO, etc	Trouble, Service Summary, State Change, Information, Threshold and Expert. TBL for this log.
event id	String	The Log Title.
NE Number	integer	Number of the NE
NE Name	string	Name of the NE
nnESA Fault Type	string	The type of the fault: ESA data download failed
nnUemgEventTime	DateandTime	The Date and Time the event occurred in the following format: day mmmdd hh:mm:ss zone yyyy
nnUemgAlarmSeverity	String	Warning
MediaGatewayName	string	The name of the Media Gateway control group which found ESA data inconsistent
Description	string	ESA data download failed

Action**nnESADownloadFault:**

Check failure cause in alarm or log text and perform manual downloading actions from the corresponding VMG view. The alarm will be cleared by the EM when the download is successful.

Associated Operational Measurements or Performance Measurements

None.

Configuration for A00003567

Hardware and Software Requirements

This functionality is for MG9000 EM that has SN07 or higher software version.

Initial Configuration

No changes to the initial configuration.

Upgrade Impact

Dump and Restore
N/A

Element Management Upgrade

ABI ESA functionality is only applicable if the MG9000 is at a software release of SN07 or higher.

Element Management

GUI information

New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
ESA Configuration View	Changed
Subnet View	Changed

ESA Configuration View

Functional description

In release SN07, this view will be enabled for ABI as well as ITP VMGs. For the ABI VMGs only enhanced ESA capability will be supported.

GUI usage and implications

From MG9kEMS software UE9000 MG Element Manager View, when you click Services submenu 'Switched Line Services Manager', this action invokes Switched Line Services for MG9000 Element View. The ESA Config Panel View which is displayed when the "ESA Config" tab is selected.

GUI size

Not Applicable

GUI fields

The following table lists the new fields in the ESA Config View:

GUI field descriptions

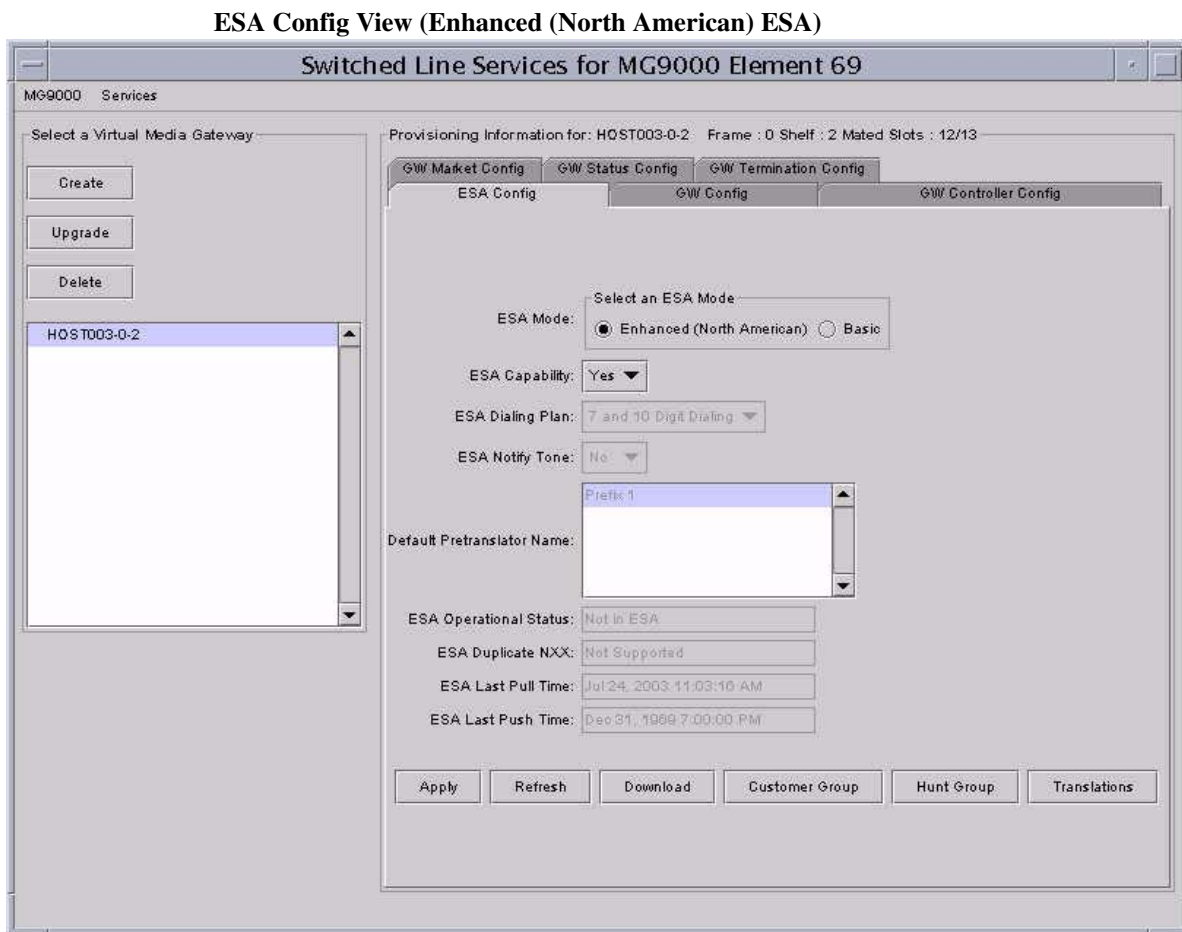
Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
ESA Mode	Changed	N/A	“Enhanced (North American)” or “Basic”	The “Enhanced” will use the ESA data provided by the Core. This will be used by both ABI and ITP VMGs The “Basic” will work in the same manner that ESA is configured in SN06 using the MG9000 EM for ITP VMGs but will not be supported for ABI VMGs.	None
ESA Capability	Not Changed	N/A	“Yes” or “No”	“Yes” means that the selected VMG is capable of going into ESA. “No” means that the VMG is not capable of going into ESA.	nnEsaConfigAdmin Status
ESA Dialing Plan	Not Changed	N/A	add “7 and 10 Digit Dialing”	7 and 10 digit dialing is supported in SN06.0. It is supported only for “Enhanced” ESA mode. It will be disabled.	nnEsaConfigDialing Plan
ESA Notify Tone	Not Changed	N/A	“Yes” or “No”	“Yes” means that a notify tone is given to alert user that in ESA mode. “No” means that there is no indication to the user that in ESA mode. It will be disabled if “Enhanced” is selected.	nnEsaConfigNotifyTone

GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Default Pretranslator Name	Not Changed	N/A	Default Pretranslator name which is from Core	This field is the Default Pretranslator name that is associated with the selected VMG. It will be disabled if "Enhanced" is selected.	nnEsaConfigDefPret ranslationId
ESA Operational Status	Not Changed	N/A	"Not in ESA" or "In ESA"	"Not in ESA" means that the VMG is not in ESA mode. "In ESA" means that the VMG is in ESA mode.	nnEsaConfigOperSt atus
Download	Not Changed	N/A	N/A	When user clicks on this button, it will perform a manual downloading the EM ESA data to Gateway in order to resync the MG9000 with EM latest Core data for selected VMG. The button will be disabled if "Basic" is selected.	None
Customer Group	Not Changed	N/A	N/A	Click on this button, "ESA Customer Group List" View will be displayed. It will be disabled if "Basic" is selected.	None
Hunt Group	Not Changed	N/A	N/A	Click on this button, "ESA Hunt Group List" View will be displayed. It will be disabled if "Basic" is selected.	None
Translations	Not changed	N/A	N/A	Click on this button, "ESA Translation List" View will be displayed. It will be disabled if "Basic" is selected.	None

Usage example

The following example shows sample datafill in ESA Config View:



Subnet View

Functional description

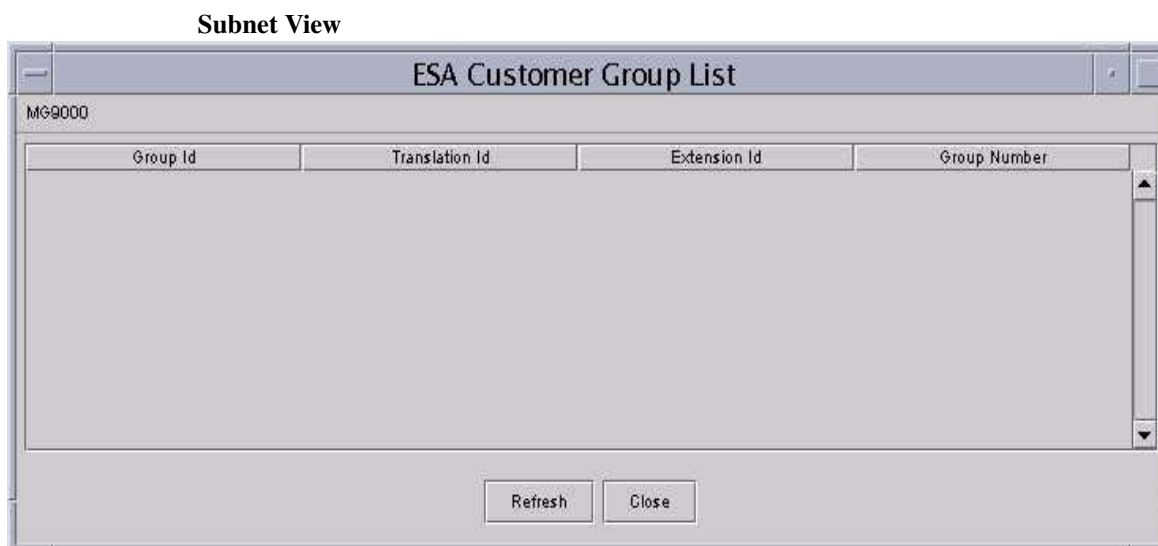
GUI usage and implications

GUI size

Not Applicable

Usage example

The following screenshot shows the additions to the subnet view.

**Usage example**

The following figure shows the sample datafill in GW Termination Config View:

GUI release history update

MG9000 EM Update: The ESA config GUI is modified to support ABI ESA, for enhanced ESA only. Subnet view changed to show DMS icon and subtending nodes.

Supplementary information

None.

CLUI Interface

N/A

Supplementary information

None.

CLUI Interface

N/A

Security

N/A

Configuration Walkthrough**SDM Configuration:**

Please ensure that the SDM has the latest available fileset as part of the CS2E06 SDM load, for the package SDM_BASE.fts for the application 'File Transfer Service'.

MG9K EM Configuration:

Set up the SSH authentication

This feature requires a key exchange between the MG9K EM server and the SDM for downloading the ESA data.

Procedure

1. Configure the SDM IP and SDM USER for this system. Log in to the MG9K EM server as 'root' and run the command:

```
$ cli
```

Select "Configuration", then select "OAMP Application Configuration", then select "Configure SDM IP and User" and set the SDM IP to the correct IP address of the SDM.

Set the SDM user name to be "esauser"

2. For the user, 'mgems' on the MG9K EM server, generate the ssh key pair needed for data transmission between the MG9K EM and the SDM. As the 'root' user, execute the following commands:

```
# su - mgems
```

```
$ ssh-keygen -t rsa
```

Accept the default location and enter an empty passphrase. This will create the following key file:

```
/export/home/mgems/.ssh/id_rsa.pub
```

3. The key information contained in the file
/export/home/mgems/.ssh/id_rsa.pub must be placed in the following file on the SDM:

```
/home/esauser/.ssh/authorized_keys2
```

— Secure copy the id_rsa.pub file to the SDM, using the command

```
$ scp /export/home/mgems/.ssh/id_rsa.pub  
root@$SDM_IP:/home/esauser/tempkey
```

Answer "yes" to the prompt "Are you sure you want to continue connecting (yes/no)?", then enter the password of the 'root' SDM user.

— Secure append the public key to the authorized keys list on the SDM, using the command

```
$ ssh root@$SDM_IP 'cat /home/esauser/tempkey >>  
/home/esauser/.ssh/authorized_keys2'
```

Enter the password of the 'root' SDM user when prompted for it.

Once completed, the MG9K EM will have the required access to the SDM for downloading the ESA data.

Set up ESA data download properties

ESA properties must be set up appropriately to download the right ESA data file from the Core at the right time. The Core will have an office parm configured to a specific time to start the collection of ESA data on the Core daily. The download of the ESA data is a nightly process and the corresponding time on the EM must be configured such that there is at least half an hour delay between this time and the Core configured time.

There are 3 ESA data download properties that need to be properly configured. These include the time that will be used for nightly downloads, the name of the device on the Core where the ESA data file will be stored and the name of the ESA data file itself. These properties have the following default values:

ESA.DataDownloadTime=1:30 AM

ESA.DataDeviceName=/SFDEV

ESA.DataFileName=ESA_SYSTEM_SD\$XML

ESA.DataFileNameUnix=ESA_SYSTEM_SD.XML

Notes:

- The ESA.DataFileNameUnix property is not editable. This is dynamically derived from the ESA.DataFileName property by the MG9K EM software.
- The ESA.DataFileName on the core should adhere to the following naming conventions:
 - a. There can only be one '\$' sign in the name separating the 'name' part from the 'extension' part. (Please see the default value for an example).
 - b. No spaces are allowed in the file name.

Use the following procedure only if you need to change the default values of the ESA properties.

Procedure

Telnet into the MG9K EM server and launch the 'mg9kserver' script, located under the "bin" directory under the server where it is installed. The menu walk through is described as follows only to be used as an example:

```
# ./mg9kserver config
```

Main Configuration Menu

1) Change Distribution Policy

- 2) Change SESM IP Address
- 3) Change Oracle IP Address
- 4) Change Debug Level for logs
- 5) Change Persistence settings
- 6) Change ESA data download settings
- 7) Display current settings
- 8) Exit from Main Menu

Please make a selection => 6

ESA Configuration Menu

- 1) Change ESA data download time
- 2) Change ESA data device name
- 3) Change ESA data file name
- 4) Exit to Main Menu

Please make a selection => 1

Please enter the new ESA data nightly download time?

Default: [1:30 AM] => 5:30 PM

ESA Configuration Menu

- 1) Change ESA data download time
- 2) Change ESA data device name
- 3) Change ESA data file name
- 4) Exit to Main Menu

Please make a selection => 2

Please enter the new ESA data device name on the core?

Default: [/SFDEV] => /ESADEV

ESA Configuration Menu

- 1) Change ESA data download time
- 2) Change ESA data device name
- 3) Change ESA data file name
- 4) Exit to Main Menu

Please make a selection => 3

Please enter the new ESA data file name on the core?

Default: [ESA_SYSTEM_SD\$XML] => ESADATA\$XML

Name of the ESA data file on the EM: ESADATA.XML

ESA Configuration Menu

- 1) Change ESA data download time
- 2) Change ESA data device name
- 3) Change ESA data file name
- 4) Exit to Main Menu

Please make a selection => 4

Once completed, the new ESA data download properties will become effective on the future downloading of the ESA data.

Core Configuration:

Overview

ESA data file will be downloaded from the core using FTP. Hence, it is important to ensure that enough TCP connections are configured on the core for the FTP Server sessions.

The maximum number of FTP sessions is controlled by the “CM” tuple in TABLE IPHOST in the “CM”. The “CM” tuple is usually the first tuple in the table. This tuple contains the following fields:

NODENAME: Node name = CM.

CMINDEX: Index = 0.

TCPCONN: The total number of TCP connections allowed. This number must be greater than or equal to $(FTPCLCON + FTPSVCON) * 2$.

FTPCLCON: The maximum number of FTP client sessions allowed. SFT is not impacted by this value.

FTPSVCON: The maximum number of FTP server sessions allowed. SFT shares this resource with other CM FTP users.

Care must be taken when determining the value of *FTPSVCON*. Other telnet applications may have been configured and the value of *FTPSVCON* should be incremented taking this into account.

If *FTPSVCON* is incremented, ensure that *TCPCONN* is large enough to support the total of *FTPCLCON* and *FTPSVCON*. Each FTP session will consume 2 TCP connections. This will be enforced by the *IPHOST* table control.

Product = MG 9000

A00003571 -- MG9000 Manager - New MG9000 Card Support (UA-IP)

Functional Description

This activity supports the release of the following PECCODEs for ITP, ITX, ABI and SCO cards in the MG9000EM:

- Internet Telephony Processor (ITP): NTNY30CA (IP & AAL1 modes)
- Internet Telephony Extender (ITX): NTNY41BA
- Super Core OC3 (SCO): NTNY45CA
- Access Bridging Interface (ABI): NTNY43BA (IP & AAL1 modes)

The user interface for the ITP, ITX, SCO and ABI are not impacted by this feature.

The new VMG of type ABI-IP is added to the VMG provisioning creation. The areas for 'Silence Suppression (VoIP)' and 'QoS Threshold (VoIP Only)' will be un-gray for this new VMG type (same configuration rules as the current ITP-IP VMG type).

A new field 'Bearer Address' will be added in the GW Config panel. This field will be editable for ABI-IP Vmg type and it will be gray out for all other VMG types but it will display the same IP address use in the CIPOA Address field.

The 'CIPOA Address' label will be renamed 'Signalling Address'.

The OVLD alarm and logs format are used to report the failures of the 'Stream Control Transmission Protocol' (SCTP) reported by the ABI.

The MG9000 is reporting SCTP Operational measurements via a OM collector interface (please refer to A00003767 'IP ABI PPVM ROBUSTNESS & MSG LOSS' for more information on OM fields and data collected).

Hardware Requirements or Dependencies

This activity supports the following new card releases:

- Internet Telephony Processor (ITP): NTNY30CA (IP & AAL1 modes)
- Internet Telephony Extender (ITX): NTNY41BA
- Super Core OC3 (SCO): NTNY45CA
- Access Bridging Interface (ABI): NTNY43BA (IP & AAL1 modes)

Software Requirements or Dependencies

This activity is released in SN07 MG9000 Element manager and has the correspondent SN07 MG9000 gateway release features:

- A00004109: CALLP CHANGES TO SUPPORT NEW ITP
- A00003767: IP ABI PPVM ROBUSTNESS & MSG LOSS
- A00003729: IP ABI CALLP AND CONNECTIONS

Limitations and restrictions

The new release of ITP and ABI cards are ONLY supported in the SN07 or higher release for MG9000EM and MG9000.

Due to the change of MIBs the fields in the 'Silence Suppression (VoIP Only)' area: *Voice Activity Detection Mode* and *Confort Noise Generator Mode*, for upgrades to SN07 the values VAD and CNG in the MG9000EM will be downloaded to the GW after the NE audit has completed. Before the audit is executed the GW will have the defaults values.

Interactions

None

Applicable customer facing sections

Fault Management

Logs ☒

Alarms ☒

Configuration

Data Schema ☐

User Interface ☐

Element Management ☒

Security ☐

Service Order ☐

Office Parameters ☐

Accounting (includes AMA billing) ☐

Performance (includes operational measurements) ☐

Fault Management for A00003571

Fault management strategy

This Feature adds three new alarms and three new logs that report failures of the 'Stream Control Transmission Protocol' (SCTP) in the ABI cards to the MG9000 element manager. The correspondent software is developed in the MG9000 and in the LCI.

Fault management tools and utilities

No additional tools are developed by this feature. The customer logs are generated by the element manager when the alarm notification is received from the MG9000 gateway.

Logs

Explanation

Title: External Packet Network Reliable Messaging Link(s) Failed

Name: OVLD

ID:808

Description: An external messaging link has closed and cannot send/receive message

Severity: Critical

Event type: Threshold**Format**

*** OVLD808 Mar08 11:56:14 1052 THRESHOLD MG9K PM Fault
Location: 8-co8-Frame000.Shelf2.Slot4
Notification Id: 832
State: not acknowledged
Category: SCTP protocol Alarm
Cause: Equipment Malfunction
Time: Thu Jan 01 04:53:18 EST 1970
Component Id: Card.Frame0.Shelf2.slot4.ABI
Specific Problem: SCTP message association closed
Description: SCTP message link has closed
Site Flr EPos bay_id
Cary 03 H03 MG9F 012

OVLD808 Mar08 11:56:14 1052 THRESHOLD MG9K PM Fault
Location: 8-co8-Frame000.Shelf2.Slot4
Notification Id: 832
State: Cleared
Category: SCTP protocol Alarm
Cause: Equipment Malfunction
Time: Thu Jan 01 04:53:18 EST 1970
Component Id: Card.Frame0.Shelf2.slot4.ABI
Specific Problem: SCTP message association closed
Description: SCTP message link has closed
Site Flr EPos bay_id
Cary 03 H03 MG9F 012

Explanation

Title: External Packet Network Reliable Messaging Link(s) Severely Degraded

Name: OVLD

ID:809

Description: Message loss is high enough such that the message link is in a degraded service state. For ABI, this would mean that some calls are failing and perhaps maintenance actions are failing (e.g. static data download, etc.)

Severity: Major

Event type: Threshold

Format

** OVLD809 Mar08 11:56:14 1052 THRESHOLD MG9K PM Fault
Location: 8-co8-Frame000.Shelf2.Slot4

Notification Id: 830
State: not acknowledged
Category: SCTP protocol Alarm
Cause: Equipment Malfunction
Time: Thu Jan 01 04:53:18 EST 1970
Component Id: Card.Frame0.Shelf2.slot4.ABI
Specific Problem: SCTP message loss threshold crossed
Description: SCTP Message Loss
Site Flr EPos bay_id
Cary 03 H03 MG9F 012

OVLD809 Mar08 11:56:14 1052 THRESHOLD MG9K PM Fault
Location: 8-co8-Frame000.Shelf2.Slot4
Notification Id: 830
State: Cleared
Category: SCTP protocol Alarm
Cause: Equipment Malfunction
Time: Thu Jan 01 04:53:18 EST 1970
Component Id: Card.Frame0.Shelf2.slot4.ABI
Specific Problem: SCTP message loss threshold crossed
Description: SCTP Message Loss
Site Flr EPos bay_id
Cary 03 H03 MG9F 012

Explanation

Title: External Packet Network Reliable Messaging Link(s) Degraded
Degraded

Name: OVLD

ID:810

Description: Message retransmissions are high enough that system is starting to see performance degradation. Potentially, this could mean increased latency, reduced messaging through the system, buffer overflows and perhaps heading toward congestion.

Severity: Minor

Event type: Threshold

Format

* OVLD810 Mar08 11:56:14 1052 THRESHOLD MG9K PM Fault
Location: 8-co8-Frame000.Shelf2.Slot4
Notification Id: 834
State: not acknowledged
Category: SCTP protocol Alarm
Cause: Equipment Malfunction
Time: Thu Jan 01 04:53:18 EST 1970
Component Id: Card.Frame0.Shelf2.slot4.ABI

Specific Problem: SCTP retransmission messages crossed threshold.

Description: SCTP retransmission messages too high.

Site Flr EPos bay_id

Cary 03 H03 MG9F 012

OVLD810 Mar08 11:56:14 1052 THRESHOLD MG9K PM Fault

Location: 8-co8-Frame000.Shelf2.Slot4

Notification Id: 834

State: Cleared

Category: SCTP protocol Alarm

Cause: Equipment Malfunction

Time: Thu Jan 01 04:53:18 EST 1970

Component Id: Card.Frame0.Shelf2.slot4.ABI

Specific Problem: SCTP retransmission messages crossed threshold.

Description: SCTP retransmission messages too high.

Site Flr EPos bay_id

Cary 03 H03 MG9F 012

Field descriptions

For All three alarms.

Field descriptions

Field	Value	Description
event type	INFO,TBL, etc....	Describes event type
event id	string	Name of the log
Location	NE Number-NE Name-Physical Location	Gives the complete location of the orig
Notification Id	number	Alarm Id
State	string	Indicates state of alarm. Can be one of {not acknowledged, acknowledged, cleared}
Category	string	Indicates type of fault. In this case it will be "NorNodeFault"
Cause	string	Cause of failure: In this case it will be "Equipment Malfunction"
Time	string	Date/Time indicating when the condition occurred

Field descriptions

Component Id	string	Indicates the type of equipment having the fault.
Specific Problem	String	String indicating the specific problem that caused the fault
Description	string	Provides specific text for the fault (as provided by the MG)

Action

TBD.

Associated Operational Measurements or Performance Measurements

none

Additional information

none

Alarms

- “External Packet Network Reliable Messaging Link(s) Failed” - critical
 - General conditions: an external messaging link has closed and cannot send/receive message
 - SCTP triggers: reflected by the abnormal closing of an SCTP association (ABORT)
 - This alarm will be reported by OVLD 808 and log OVLD 808
- “External Packet Network Reliable Messaging Link(s) Severely Degraded” - major
 - General conditions: message loss is high enough such that the message link is in a degraded service state. For ABI, this would mean that some calls are failing and perhaps maintenance action are failing (e.g. static data download, etc.).
 - SCTP triggers: reflected by message loss over the predetermined message loss threshold.
 - This alarm will be reported by OVLD 809 and log OVLD 809
- “External Packet Network Reliable Messaging Link(s) Degraded” - minor
 - General conditions: message retransmissions are high enough that system is starting to see performance degradation. Potentially, this could mean increased latency, reduced messaging through the system, buffer overflows and perhaps heading toward congestion.
 - SCTP triggers: reflected by message retransmission over the predetermined message retransmission threshold.

— This alarm will be reported by OVLD 810 and log OVLD 810.

OVLD alarms for SCTP failures

Alarm ID	Alarm Description
OVLD 808	External Packet Network Reliable Messaging Link(s) Failed
OVLD 809	External Packet Network Reliable Messaging Link(s) Severely Degraded
OVLD 810	External Packet Network Reliable Messaging Link(s) Degraded

Related documentation

N/A

Product = MG 9000

A00003591--MG9000 OC3 Channelization support from EM (UA-IP)

Functional Description

This feature enables the user to view and modify (only the administrative and configuration status can be modified) the channelized carrier (OC3) configuration. This document discusses the changes in EM for this feature from the user perspective.

Hardware Requirements or Dependencies

No new requirements. This product runs on the same hardware as the existing MG9k Element Manager application.

Software Requirements or Dependencies

No new requirements. This activity is packaged with the existing MG9k EM software application.

This feature will be shipped as part of the SN07 stream for the MG9k EM.

Limitations and restrictions

None

Interactions

This feature introduces new screens and modifications to the existing GUI.

Carrier configuration Display

The screen remains unchanged for concatenated sonet and SDH carrier. The following figure shows the carrier configuration details for the concatenated sonet carrier.

OC3c Carrier details

OC3 Port: NE-9 Frame-0 Shelf-3 Slot-10 Port-0[Maintenance mode]

1G9000 Actions Services Alarms

Section/Line

Circuit identifier:

Line coding:

Line type:

Description:

Speed:

Status

Administrative status:

Configuration status:

Operational status:

Path

Description:

Speed:

OC3 Port Alarms **NE Info**

Critical: Minor:

Major: Warning:

If the carrier is in 'channelized mode', clicking on the OC3 Port icon in the OC3 card view will display the screen as shown in the following figure. This new screen shows totally three icons for STS1 path details. By default OC3

section/Line description/status is displayed in a tab as shown in the following figure. Double clicking on the STS1 path will display STS1 path information and its status as shown in “[STS1 path description and status](#)” on page 2141. The user will be able to lock/unlock and online/offline the OC3 section/Line and all the 3 STS1 paths individually.

Section/Line Configuration details for channelized carrier

The screenshot shows a web-based configuration interface for an STS1 Port. The title bar reads "STS1 Port: NE-406 Frame-0 Shelf-3 Slot-10 Port-0". Below the title bar are tabs for "MG9000", "Actions", "Services", and "Alarms". The main content area is divided into two panes. The left pane shows a diagram of the OC3Port (a green box labeled '1') connected to three STS1Paths (blue boxes labeled '1', '2', and '3'). To the right of the STS1Paths, their respective descriptions are listed: "DS3CC/NETWORK" for path 1, and "DS3CC/NONE" for paths 2 and 3. The right pane has two tabs: "OC3 Attributes" and "STS1 Path". The "STS1 Path" tab is selected, showing the "Section/Line" configuration. Fields include: "Circuit identifier:" (empty), "Line coding:" (NRZ), "Line type:" (Short Single Mode), "Description:" (SONET Medium/Section/L), and "Speed:" (15552000). Below these is the "Status" section with three fields: "Administrative status:" (UNLOCKED), "Configuration status:" (OFFLINE), and "Operational status:" (Disabled). At the bottom of the window, there are tabs for "STS1 Port Alarms" and "NE Info". The "NE Info" tab is selected, showing four status counters: "Critical:" (2), "Minor:" (0), "Major:" (0), and "Warning:" (0).

OC3Port	STS1 Path	Description
1	1	DS3CC/NETWORK
	2	DS3CC/NONE
	3	DS3CC/NONE

Field	Value
Circuit identifier:	
Line coding:	NRZ
Line type:	Short Single Mode
Description:	SONET Medium/Section/L
Speed:	15552000
Administrative status:	UNLOCKED
Configuration status:	OFFLINE
Operational status:	Disabled

Category	Count
Critical	2
Minor	0
Major	0
Warning	0

The label next to the STS1 paths help the user to identify the network carrier and the payload on the paths. The payloads can be STS1, DS3CC and

DS3PLCP. If the payload is DS3PLCP, f or network carrier the label would be DS3PLCP/NETWORK and for inactive carrier it would be DS3PLCP/NONE.

The OC3 Section/Line can be locked only after locking all the 3 STS1 paths. When the user tries to lock OC3Section/Line, a warning message “The Network Path should be locked before locking OC3 Section/Line. Are you sure the network path is locked?” will be popped up to the user. If the network path is not locked, the user can cancel OC3Section/Line lock request and lock the network path, then attempt locking OC3Section/Line

For unlocking Network Carrier, the OC3 Section/Line should be unlocked first. When the user tries to unlock the network path, a warning message, “The OC3Section/Line should be unlocked before unlocking the network path. Are you sure the OC3Section/Line is unlocked?” will be displayed to the user. If the OC3Section/Line is not unlocked, the user can cancel network path unlock request and unlock the OC3Section/Line, then attempt unlocking network path

A non-network carrier can not be unlocked.

STS1 path description and status

STS1 Port: NE-406 Frame-0 Shelf-3 Slot-10 Port-0

MG9000 Actions Services Alarms

OC3Port STS1 Path

1 DS3CC/NETWORK
2 DS3CC/NONE
3 DS3CC/NONE

OC3 Attributes STS1 Path

Path

Description: SONET Path
Speed: 15552000
Destination: NETWORK

Status

Administrative status: UNLOCKED
Configuration status: ONLINE
Operational status: Disabled

STS1 Port Alarms NE Info

Critical: 2 Minor: 0
Major: 0 Warning: 0

The following figure shows the default screen if the carrier is not provisioned.

Default screen if the carrier is not provisioned

OC3 Port: NE-18 Frame-0 Shelf-3 Slot-11 Port-0

MG9000 Actions Services Alarms

Section/Line

Circuit identifier:

Line coding:

Line type:

Description:

Speed:

Status

Administrative status:

Configuration status:

Operational status:

Path

Description:

Speed:

OC3 Port Alarms NE Info

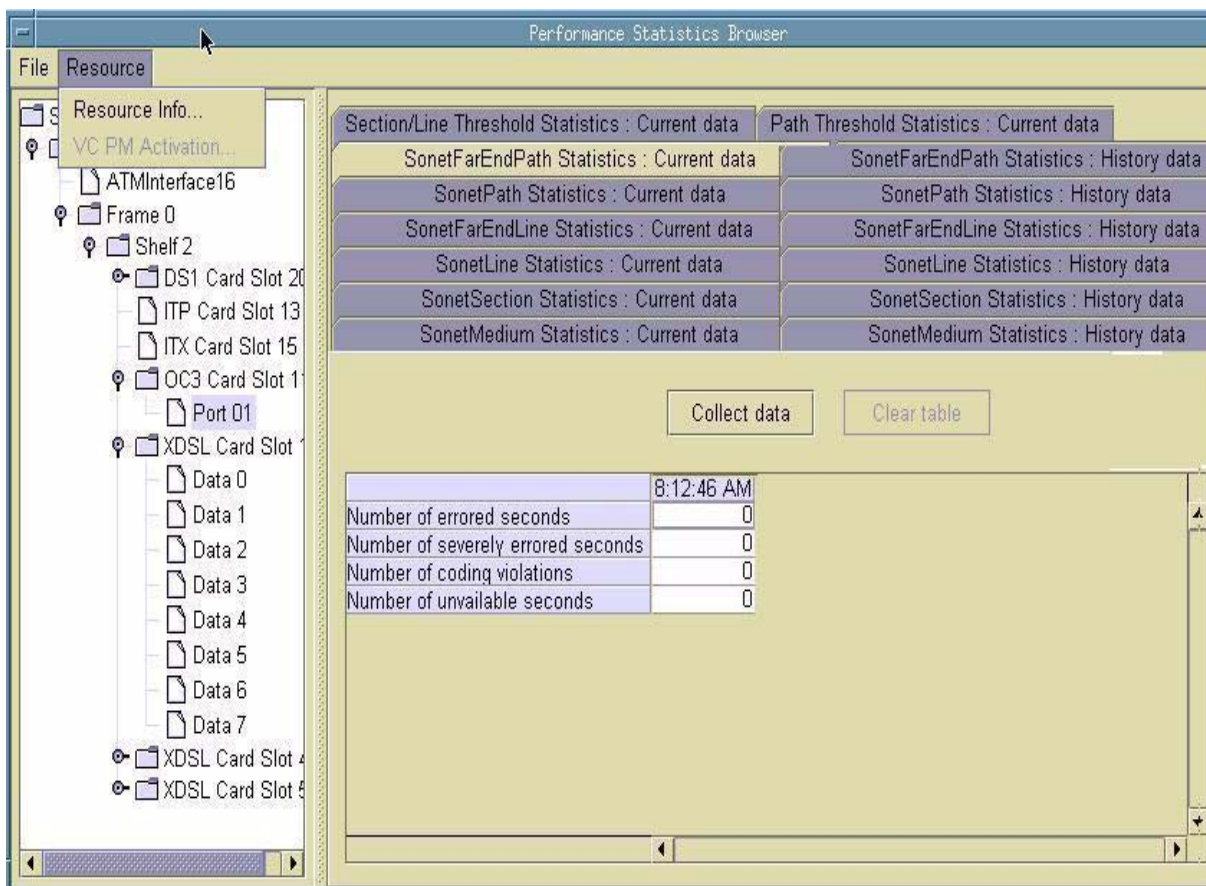
Critical: Minor:

Major: Warning:

Apply Refresh Close

Performance Parameters

If the carrier is configured in concatenated mode (Sonet or SDH), there is no change in the performance parameter screen.

OC3 section/Line, STS3 path performance parameters

If the carrier is in channelized mode, clicking on OC3 port will display OC3 section/Line information. Three STS1 subnodes will be displayed below Port for STS1 information. Clicking on each of STS1 will display its path performance details. DS3 path performance parameters will be displayed if DS3 is payload is supported on STS1. If the payload is STS1 the nodes label will be STS1-0x and if DS3 payload is selected on the STS1 path the nodes label will be STS1-DS3-0x. Refer to the following figure.

STS1 Path performance parameter

deepthip's X desktop (wnc1s0m5:3)

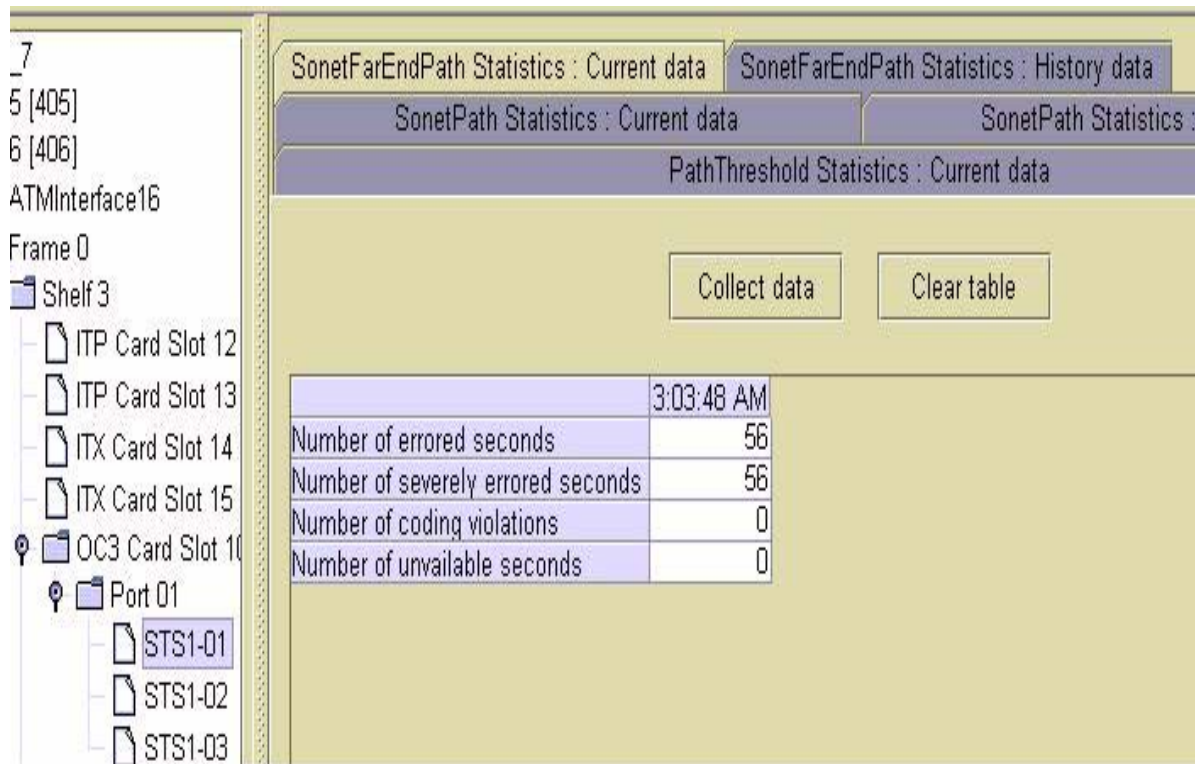
OC3 Card Slot 11
ProtectionSwitch
] Interface16
0
elf 3
ITP Card Slot 12
ITP Card Slot 13
ITX Card Slot 14
ITX Card Slot 15
OC3 Card Slot 10
Port 01
STS1-01
STS1-02
STS1-03

SonetFarEndPath Statistics : Current data SonetFarEndPath Statistics : History data
SonetPath Statistics : Current data SonetPath Statistics : History data
PathThreshold Statistics : Current data

Collect data Clear table

	3:01:31 AM
Number of errored seconds	0
Number of severely errored seconds	0
Number of coding violations	0
Number of unavailable seconds	0

The following figure shows STS1 FarEndPath Statistics.

STS1 FarEndPath Statistics

The following figure shows DS3 Path Performance parameters.

DS3 Path Performance parameters

2:49:49 AM	
P - bit number of errored seconds	0
P - bit number of severely errored seconds	0
Severely errored seconds	0
Number of unavailable seconds	0
P - bit number of coding violations	0
C - bit number of coding violations	0
C - bit number of errored seconds	0
C - bit number of severely errored seconds	0

The following figure shows DS3 FarEndPath performance parameters.

DS3 FarEndPath performance parameters

DS3 FarEndPath Statistics : Current data DS3 FarEndPath Statistics : History data

DS3 Path Statistics : Current data DS3 Path Statistics : History

SonetFarEndPath Statistics : Current data SonetFarEndPath Statistics : History

SonetPath Statistics : Current data SonetPath Statistics : History

PathThreshold Statistics : Current data

Collect data Clear table

	2:49:49 AM
P - bit number of errored seconds	0
P - bit number of severely errored seconds	0
Severely errored seconds	0
Number of unavailable seconds	0
P - bit number of coding violations	0
C - bit number of coding violations	0
C - bit number of errored seconds	0
C - bit number of severely errored seconds	0

STS1 and DS3 alarms

From the user perspective, the alarm display will not change. The alarms will be raised for both STS1 path and DS3 payload. Now the STS1 path and DS3 alarms will be included in the OC3 port alarm count. The DS3 alarms to expect at EM will be LOF, RAI and AIS. The alarm description will let the user know whether the alarm belongs to DS3 or STS1.

The following figure shows DS3 Alarm information

DS3 Alarm information

Refresh	Ack	Unack	Prev	Next	Print	Save	First Page	Prev Page	Next Page	Last Page	2	of 2	Goto Page
38			alarm(s)			with			1				
	Log Id	Fault Type	NE#-Seq	Phys Loc		Severity							
	MGCA334	ds3lof	405-361	Port.frame0.shelf2.slot10.OC3.oc3.sts1p...		major							
	MGCA333	ds3ais	405-368	Port.frame0.shelf2.slot10.OC3.oc3.sts1p...		major							
	MGCA335	ds3rai	405-376	Port.frame0.shelf2.slot10.OC3.oc3.sts1p...		minor							

General:	not acknowledged	Category:	Communication
NE:	c405	Unit:	Port.frame0.shelf2.slot10.OC3.oc3.sts1path1
Time:	Jan 01 02:33:51:885 1970	Severity:	major
Cause:	Loss Of Frame NorCarrFault - DS3 - Loss Of Frame (DS3) DS3 LOF Site: Elk River, Boulder		

Upgrade and Downgrade

The user should not try downgrading the MG9K when the carrier is channelized. The MG9K in SN07 has new hardware to support channelization, so SN06.2 and below load should not be used on this MG9k. If a SN06.2 MG9K has to be upgraded to SN07, it should have the new hardware.

Error scenarios

The SNMP set errors will be handled.

Glossary

STS1	Synchronous Transport Signal Level 1
STS3	Synchronous Transport Signal Level 3
EM	Element Manager
DS3	Digital Signal Type 3
OC3c	Concatenated carrier

OC3	Channelized carrier.
LOF	Loss Of Frame
RAI	Remote Alarm Indication
AIS	Alarm Indication Signal

Applicable customer facing sections

Fault Management

Logs	☒
Alarms	☒

Configuration

Data Schema	☒
User Interface	☒
Element Management	☒
Security	☐
Service Order	☐
Office Parameters	☐

Accounting (includes AMA billing) ☐

Performance (includes operational measurements) ☒

Fault Management for A00003591

Fault management strategy

The standard MG9K EM Fault Management strategy will apply to the new faults raised by this feature. Alarms will be displayed by the MG9K EM Alarm Browser, logged in NT standard format to the SSPFS CUST logs and forwarded to northbound OSS.

For the “A00003591 - OC3 Channelization” feature there will be new faults added when the payload selected DS3

Fault management tools and utilities

Alarm Browser - Reports alarms from registered events. When an alarm is generated, it is displayed in the Alarm Browser along with the date and time, the NE Id, the resource (where the alarm was generated), the severity and probable cause. Highlighting the alarm displays the description of the alarm in the text box at the bottom of the Alarm Browser.

Log Adaptor - Generates logs from registered events. The log names and numbers are predetermined and are matched with the incoming event. A log with the corresponding name and number which contains the date, time, physical location, severity and any other pertinent information is generated and placed into a separate file.

The DS3 alarms will be displayed here.

Faults, Alarms and Logs

There will be new faults generated and cleared by MG9000 when the carrier is channelized and payload selected on the STS1 path is DS3CC or DS3PLCP.

The alarms that can be generated for DS3 will be AIS, LOF and RAI. These faults will be generated when there is a Loss of Frame or some problem at the remote end.

Alarms

Explanation

AlarmIndicationSignal

Title: AlarmIndicationSignal

Name: ds3ais

Description: This log is generated when a AlarmIndicationSignal fault is received from the Gateway.

LossOfFrame

Title: Loss Of Frame

Name: ds3lof

Description: This log is generated when a LossOfFrame fault is received from the Gateway.

RemoteAlarmIndication

Title: RemoteAlarmIndication

Name: ds3rai

Description: This log is generated when a RemoteAlarmIndication fault is received from the Gateway.

Format

The Log Delivery application for this feature generates logs in the Number 2 Switch Control Center (SCC2) format and the NT standard (STD) format explained in the PLOA_SLOA_LOG_ALARMS DID.

STD Format

- **AlarmIndicationSignal**
MGCA333 MAR08 06:14:43 3409 TBL MG9K NorCarrFault
Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Channel01
Notification Id: 294
State: not acknowledged
Category: Communication Alarm
Cause: Communications Subsystem Failure
Time: Jan 01 05:39:05 1970
Component Id: Port.frame0.shelf3.slot10.OC3.oc3.sts1path1
Specific Problem: NorCarrFault - DS3 - Alarm Indication Signal - Check far-end carrier faults
Description: (DS3) DS3 AIS
Site Flr RPos Bay_id
FFFF FF FFFF MG9F FFF
- **LossOfFrame**
MGCA334 MAR08 06:12:43 8306 TBL MG9K NorCarrFault
Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Channel01
Notification Id: 292
State: not acknowledged
Category: Communication Alarm
Cause: Loss Of Frame
Time: Jan 01 05:37:08 1970
Component Id: Port.frame0.shelf3.slot10.OC3.oc3.sts1path1
Specific Problem: NorCarrFault - DS3 - Loss Of Frame
Description: (DS3) DS3 LOF
Site Flr RPos Bay_id
FFFF FF FFFF MG9F FFF
- **RemoteAlarmIndication**
MGCA335 MAR08 06:18:43 1111 TBL MG9K NorCarrFault
Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Channel01
Notification Id: 296
State: not acknowledged
Category: Communication Alarm
Cause: Communications Subsystem Failure
Time: Jan 01 05:43:02 1970
Component Id: Port.frame0.shelf3.slot10.OC3.oc3.sts1path1
Specific Problem: NorCarrFault - DS3 - Remote Indication Signal - Check far-end carrier faults

Description: (DS3) DS3 RAI
Site Flr RPos Bay_id
FFFF FF FFFF MG9F FFF

SCC2 Format

- **AlarmIndicationSignal**

MGCA333 5915 TBL MG9K NorCarrFault
Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Channel01
Notification Id: 300
State: not acknowledged
Category: Communication Alarm
Cause: Communications Subsystem Failure
Time: Jan 01 05:54:38 1970
Component Id: Port.frame0.shelf3.slot10.OC3.oc3.sts1path1
Specific Problem: NorCarrFault - DS3 - Alarm Indication Signal - Check
far-end carrier faults

Description: (DS3) DS3 AIS
Site Flr RPos Bay_id
FFFF FF FFFF MG9F FFF

- **LossOfFrame**

MGCA334 5013 TBL MG9K NorCarrFault
Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Channel01
Notification Id: 298
State: not acknowledged
Category: Communication Alarm
Cause: Loss Of Frame
Time: Jan 01 05:53:23 1970
Component Id: Port.frame0.shelf3.slot10.OC3.oc3.sts1path1
Specific Problem: NorCarrFault - DS3 - Loss Of Frame
Description: (DS3) DS3 LOF
Site Flr RPos Bay_id
FFFF FF FFFF MG9F FFF

- **RemoteAlarmIndication**

MGCA335 6016 TBL MG9K NorCarrFault
Location: 406-c406-FrameFFF.Shelf3.Slot10.Port00.Channel01
Notification Id: 301
State: not acknowledged
Category: Communication Alarm
Cause: Communications Subsystem Failure
Time: Jan 01 05:54:53 1970
Component Id: Port.frame0.shelf3.slot10.OC3.oc3.sts1path1
Specific Problem: NorCarrFault - DS3 - Remote Indication Signal -
Check far-end carrier faults

Description: (DS3) DS3 RAI
Site Flr RPos Bay_id

FFFF FF FFFF MG9F FFF

Action

AlarmIndicationSignal

This alarm will be cleared when an AlarmIndicationSignal with fault definition - clear is received.

LossOfFrame

This alarm will be cleared when an AlarmIndicationSignal with fault definition - clear is received.

RemoteAlarmIndication

This alarm will be cleared when an RemoteAlarmIndication with faultdefinition - clear is received.

Associated Operational Measurements or Performance Measurements

None.

Configuration for A00003591

Hardware and Software Requirements

NA

Initial Configuration

NA

Office/Subnet parameters (OP/SP) (CM & SESM)

NA

Upgrade Impact

NA

Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

This feature uses new MIBs - channelized carrier configuration details introduced by a Gateway feature A00003604

Service Orders (SO) (CM & SESM)

NA

Software optionality control (SOC)

NA

Element Management

The Element manager will display channelization carrier configuration details from SN07 release.

New/modified GUIs

GUI name	NEW, CHANGED, or DELETED
OC3STS1PortView	New
Performance browser	changed

GUI information

GUI name: Carrier configuration display

OC3STS1PortView

Functional description

If the carrier is channelized, the port view will display OC3 Section/Line and three STS1 path information. When the user clicks on the OC3 port on the OC3CardView, if the carrier is channelized, three ilog graphics will be displayed on the graphical panel in the portview for STS1 path information. The OC3Section/Line information is displayed by default in a tab. Double clicking on the ilogs will display STS1 path information in a separate tab.

The OC3 Section/Line details is unchanged for channelized carrier details. The STS1 path information displayed will be Description, speed, destination field and status of the STS1 path. The status includes administrative, operational and configuration status. The user can lock/unlock or online/offline the OC3 Section/Line and three STS1 path separately. To lock OC3 Section/Line, all the three STS1 paths should be locked first. To unlock network carrier the OC3 Section/Line should be unlocked. In the release SN07 traffic will be sent on only one STS1 path and that path is the network carrier. The STS1 label (next to STS1path ilog) will mention the payload type selected. The path description will be just "Sonet Path." For the network carrier, the destination will be NETWORK. For other STS1 paths the destination will be NONE. The STS1 path label will mention if DS3(plcp or clearchannel) payload is supported on STS1.

The carrier can be changed from OC3c to OC3 and vice versa dynamically from LCI. But a coldstart has to be sent to EM from Gateway after changing the carrier to EM know that the carrier has been modified

GUI size

New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
channelized OC3 carrier	3	3 per MG9000	NA

GUI fields

N/A

GUI release history update

None

Supplementary information

The carrier can be provisioned (concatenated/channelized) from LCI. The EM will display the carrier details. The EM user will be able to change only the administrative (lock/unlock) and configuration state. The user will not be able to provision the carrier from EM.

CLUI Interface

NA

Performance parameters for channelized carrier

GUI name: channelized carrier performance parameter

Performance browser

Functional Description

If the carrier is in channelized mode, the performance browser will display the OC3 Section/Line, STS1 path performance parameters and DS3 path information (if DS3 payload is selected). The information remains unchanged for OC3c.

In the performance browser, if the carrier is channelized, clicking on OC3 port will just display OC3 Section/Line performance parameters. Three nodes will be displayed under OC3 port for 3 STS1 paths information. Clicking on each of STS1 path will display STS1 path and DS3 performance parameters statistics. If DS3 payload is selected on the STS1 paths, the DS3 performance parameters will be displayed.

New Alarms

The STS1 and DS3 alarms will be handled at EM. The new alarms will be

LOP, UNEQ, PLM, AIS and RDI for STS1 and LOF, RAI and AIS for DS3.

Upgrade and Downgrade

To support channelization in SN07, the DCC card uses new hardware. So, SN06.0 and below, GW load should not be loaded on this card. A SN06.0 MG9K should have new hardware to be loaded with SN07 load.

Command interface changes

NA

Security

NA

Configuration Walkthrough

NA



SN07 Feature Deltas

Product = MG 9000

A00003737--LCI Remote Access, Enhancements and MG9000 Security (UA-IP)

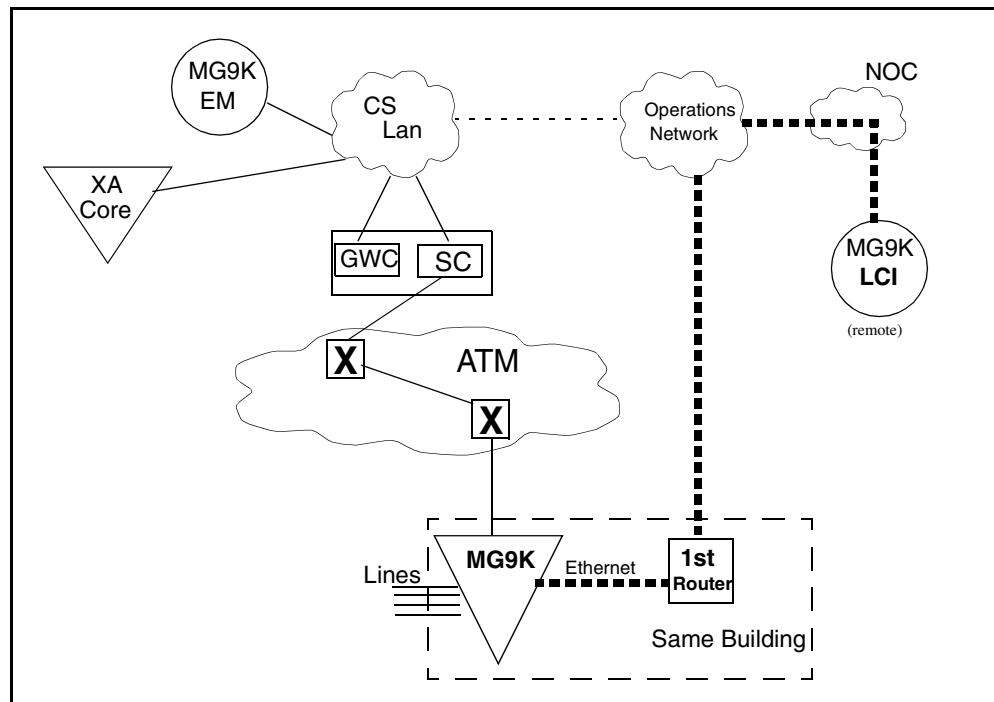
Functional Description

Feature A00003737 supplies the MG9K customer with a means for querying the ESA state and the SNMP alarm log history for a node that has lost Element Manager connectivity. The Element Manager remains as the master interface for maintaining the MG9000, with this newly added backup functionality being made available from the Local Craft Interface.

The customer requested remote access to the MG9000 LCI. Feature A00003737 provides this new functionality by allowing the ethernet addresses on the DCC cards to be provisionable. Thus, if they choose to support remote access, integrating the newly assigned address into their operations network.

As a result of adding remote access, interfaces (FTP, Telnet, Web Access) into the MG9k need to be secured using the Secure Sockets Layer.

The diagram below provides a simplified overview highlighting the location of the MG9k and its access points (atm/ethernet) within the Succession network.



Hardware Requirements or Dependencies

NA

Software Requirements or Dependencies

FTP, used for collecting Operational Measurement files and pushing down provisioning data for configuring ESA, has been replaced with Secure Shell FTP (SSH FTP). Any FTP requests into the MG9K will be required to use a Secure FTP client that supports the behavior as described by the IETF document “SSH File Transfer Protocol.”

Currently the web server running on the controller cards (DCC), uses HTTP (not secure) for the transmission of web content between the MG and a web client. Instead of HTTP, HTTPS will be used. This is the secure and encrypted transmission of the web content between the user’s client and the web server (DCC). The Local Craft Interface will use this protocol for all of its actions (commissioning, debug, password maintenance, dual homing management, ESA status’). All MG9K supported web browsers already include support for HTTPS - no customer change required.

FOR GNPS (support) ONLY:

Remote Telnet access has been disabled as a result of the Security portion of this feature. Instead, support groups are to use a Secure Shell client for

accessing Dsh. SSH works (from a users stand point) just like telnet. Run the SSH client command at the prompt on a computer that is connected to the same network as the node you are trying to access. All client-server communication is encrypted. Previously telnet allowed anonymous user access; SSH requires userid and password authentication. This is either the default password all MG9000 loads are shipped with, or a customer provisioned password. Once a user has ssh'd into the DCC card, they can telnet internally just as before. Also, SSH clients automatically try to connect to port 22 (default ssh port). The MG9K ssh server is running on port 24. This must be specified by the user of the client. Example (using openSSH client): `ssh -l admin -p 24 47.1.1.1`

Here we are attempting to ssh to "47.1.1.1" to port 24 as user "admin".

Limitations and restrictions

No new limitations/restrictions other than the secure client usage mentioned throughout the document.

Interactions

In previous releases, FTP and LCI communication was not secure. Now, using SSL, these data transmissions are secured. Regardless, the customer interface's look and feel remain unchanged. Required additional user-machine interactions are described in the subsequent sections.

Applicable customer facing sections

Fault Management

Logs __NA__

Alarms __NA__

Configuration

Data Schema __NA__

User Interface __NA__

Element Management __X__

Security __X__

Service Order __NA__

Office Parameters __NA__

Accounting (includes AMA billing) __NA__

Performance (includes operational measurements) __NA__

Glossary

Term	Description
SSL	Secure Socket Layer
HTTPS	Hypertext Transfer Protocol Secured
SSH	Secure Shell -an open protocol for securing network communications
SSH FTP	SSH File Transfer protocol - secured file transfers

Configuration for A00003737

Hardware and Software Requirements

Any FTP requests into the MG9K will be required to use a Secure FTP client that supports the behavior as described by the IETF document “SSH File Transfer Protocol.”

Initial Configuration

Ethernet

As part of the MG9000 initial commission steps, the user connects (ethernet) a laptop to the face plate (10.0.0.1) and will navigate via the LCI to the DCC card in which they wish to provision ethernet data. After selecting the specific card, the user will choose the “Provision Ethernet” item off the menu. Once the screen is displayed, any existing, if previously provisioned, data will be presented to the user. Otherwise, the desired IP address, subnet mask and default gateway may be entered and submitted.

Security

For all the newly secured interfaces (FTP, LCI, Ethernet), in order for secure communication to commence, a key (used for encrypting and decrypting data) exchange needs to occur. The user will be prompted with an inquiry of whether they accept the keys that were offered from the MG9k. These are accepted by simply entering “yes” or “no” at any of the various application client’s prompt.

ESA

In order to be able to query the ESA status of a node via the LCI, VMGs need to have been previously provisioned at the Element Manager.

Office/Subnet parameters (OP/SP) (CM & SESM)

NA

Upgrade Considerations

None

Data schema (DS) (CM, MIBS, RDB)

New/modified tables, MIBs, or Database Schema

The following MIB data has been added for Ethernet address retrieval via SNMP, however it is currently unused.

```
NorNodeDirectIpEntry ::= SEQUENCE
{
  norNodeDirectIpAddress IpAddress, -- rw
  norNodeDirectIpSubnetMask IpAddress, -- rw
  norNodeDirectIpDefGateway IpAddress, -- rw
}
norNodeDirectIpAddress OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-write
STATUS current
DESCRIPTION
"The actual direct IP address of the card."
::= { norNodeDirectIpEntry 1 }

norNodeDirectIpSubnetMask OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-write
STATUS current
DESCRIPTION
"The actual direct IP address of the card."
::= { norNodeDirectIpEntry 1 }

norNodeDirectDefGateway OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-write
STATUS current
DESCRIPTION
"The actual direct IP address of the card."
::= { norNodeDirectIpEntry 1 }
```

Service Orders (SO) (CM & SESM)

NA

Software optionality control (SOC)

NA

Element Management

LCI

Ethernet Provisioning screen (screen shot)

ESA Query Tool screen (screen shot)

SNMP Alarm Log screen (screen shot)

Password Provisioning screen (screen shot)

New/modified GUIs

GUI name	NEW, CHANGED, or DELETED
ESA Query Tool (LCI)	New
Ethernet Provisioning (LCI)	New
SNMP Alarm Log (LCI)	New
Password Change (LCI)	New

GUI information

GUI name: ESA Query Tool

Emergency Stand Alone Query Tool

Functional description

The esa query tool is a newly needed tool that will be integrated into the LCI. It's purpose is to inform the node owner whether a MG9K that has lost it's communication with the Element Manger is in ESA and still processing calls. An MG9K can contain multiple shelves, all of which are broken up into multiple VMGs, each of which may or may not be in ESA. Thus, the query tool needs to provide a list of all the VMGs for a node and the ESA status for each. A "yes" or "no" indication for whether a VMG is in ESA is not necessarily enough information for the node owner to know whether the VMG really needs to be in ESA. Example, an Element Manager communication loss doesn't always mean that MG9K and GWC communication is lost. i.e. cable cut beyond the Sam21. In this case the GWC will continue to control the MG9K and call processing will be unaffected. For this reason, 4 fields described below will be displayed from the esa query tool so the user has a better idea of what is actually going on.

A “query” button exists at the bottom of the screen. Query is used for

dsh> esaquerystatus				
VMG	ESA	ESA	Oper	Admin
Name		Capable	Status	Status
c411-1	No	Yes	Ins	Ins
c411-2	Yes	Yes	Ins	Ins
↑	↑	↑	↑	↑
NorLines VmgEntry	NnESAConfigEntry		MedGwyTerminationsEntry	

refreshing provisioned data from the MG9000, thus updating the screen.

GUI fields

VMG name - Virtual Media Gateway name that relates to all callp services on a specific frame and shelf

ESA - Emergency Stand Alone indicates whether specified VMG is presently in ESA

ESA Capable - indicates whether this particular VMG has been configured for ESA

Oper Status - Operational Status displays whether the VMG should be in a active and inservice state as specified by the VMG administrator

Admin Status - Administration Status indicates whether the VMG is presently active and inservice

GUI name: Ethernet IP Provisioning screen

Functional description

The purpose of this new screen is to allow the user to provision the ethernet ports to a specified IP address. This is so customers can gain remote access to the ethernet port for FTP and LCI management.

As part of the MG9000 initial commission steps, the user connects (ethernet) a laptop to the face plate (10.0.0.1) and will navigate via the LCI to the DCC card in which they wish to provision ethernet data. After selecting the specific

card, the user will choose the “Provision Ethernet” item off the menu. Once the screen is displayed, any existing, if previously provisioned, data will be presented to the user. Otherwise, the desired IP address, subnet mask and default gateway may be entered and submitted. Upon completion, the installer will connect the newly provisioned ethernet port to their network.

As with all LCI screens, a “submit” and a “query” button exists at the bottom of the screen. Submit is used for sending any data entered on the screen onto the MG9000 as a provisioning request. Results from the request are returned to the user and presented in the text area located at the bottom of the LCI GUI. Query is used for refreshing provisioned data from the MG9000, thus updating the screen.

GUI fields

IP Address - used to display previously provisioned address for the ethernet port on the selected card. Or allow a customer to specify a new address for the port.

Subnet Mask - subnet mask used by network administrators to indicate how they wish an IP address (host) to be interpreted

Default Gateway - defines the 1st hop in the routing of packets (i.e. the first hop being the initial router that the ethernet will be connected to).

Supplementary information

Aside from making the IP address assignable, the DCC cards will retain the address that they are shipped with, 10.0.0.1. This ensures that the DCC remains addressable if the users forget the IP address they provisioned to any given Controller card.

The LCI supports software downloading through the 10.0.0.1 interface. Software download will not be supported through the customer provisioned IP address in SN07.

Engineering rules:

1. The 1st router in the customer’s network must be configured to ignore/not route 10.0.0.x gratuitous ARPs since ALL DCCs on their network will have 10.0.0.1 as an IP address along with the IP address they provision.
2. The MG9k ethernet port must terminate to a router within the same building.

GUI name: SNMP Alarm Log screen

Functional description

The purpose of this new screen is to allow the user to query and display the SNMP alarm from the active DCC. This information provides the customer

with a history of all the major events that have occurred on a node. Helpful for debugging - all the events that took place to bring the node to its current state.

After the user navigates to this new screen, the data is automatically retrieved and displayed.

GUI fields

Data displayed on the screen will describe the events/faults that occurred, the associated timestamps, and the location from where they took place.

GUI name: Password Provisioning screen

Functional description

The purpose of this new screen is to allow the customer with a means for changing the default password that all MG9ks are shipped with. This password is used for LCI and SSH FTP authentication.

A “submit” button exists at the bottom of the screen. Submit is used for sending any data entered on the screen onto the MG9000 as a provisioning request. Results from the request are returned to the user and presented in the text area located at the bottom of the LCI GUI.

GUI fields

Password - the new desired password for the node

Retype Password - reentered password from above. If it is fat fingered, then an error message will be returned indicating so and the password change will not take affect.

Supplementary information

If the customer forgets the password they provisioned, one of the DCC card's will have to be pulled and have a serial dongle attached. (Customer should call GNPS for assistance) Once the card is plugged back in they will have access to Dsh where they can reset the password.

OSSGate Interface Changes

NA

Security

Network configuration

No additional information.

Key management

Keys are automatically generated when an intelligent card is plugged into a shelf and powered up. Keys are stored in flash memory after initial generation, thus persisting after card restarts. When persistent store on the MG9K is cleared, the key files are also cleared. Post restart, the keys will then be regenerated and stored.

Protocol

Standard SSL, SSH and HTTPS protocols.

Authentication

FTP, HTTP and Telnet are either secured or replaced by an equally functional, yet secured application using the Secure Sockets Layer. Any data transferred for any of the mentioned applications between the MG9k and a client in the network is encrypted. Access to these applications requires the user's to authenticate themselves via a valid userid and password prior to gaining access.

Product = MG 9000**A00004109--MG9K Hardware Upgrade and Call Processing Changes (UA-IP)**

Please refer to feature A00003571 for FN-related information. Only the Fault Management section of A00004109 appears here.

Fault Management for A00004109**Fault management strategy**

The overall fault management for the MG9K hasn't really been impacted by feature A00004109. Earlier documentation can be referenced for the overall fault management scope. This feature does introduce new functionality to support new ITP and ABI and as such, new alarms are used with these new cards.

Fault management implementation

It is perceived in the near future that sites will be supporting multiple platforms. For example, AAL1 and IP traffic. With the introduction of the new ITP/ABIs, this can be easier accomplished since these cards can support AAL1 and IP. With this new flexibility there is also a new risk however. In the event of a card needing replacing, it is possible that the ITP/ABI could be replaced with that of an older variety. For example, a NTNY3011CA (new ITP) could need to be replaced with NTNY3011BA (old IP-only ITP). However, with

multiple-platform sites, it is likely that multiple types of spare cards will be on hand (i.e. spare ATM-only ITPs, spare IP-only ITPs, and spare new-type ITPs). It is therefore conceivable that an incorrect replacement card could be used as the replacement.

If in fact, an incorrect card is used, an alarm will be sent to the EM and the card will be disabled (via failing BALdatasync). If this alarm is present, verify card type used for the replacement and replace the card. The required card type is given in the text of the alarm.

Alarms

If an incorrect ITP/ABI is paired with the active card application type (IP/ATM) a HW alarm will be present at the EM. This alarm defines the type of error and instructions on clearing the fault. The following figure shows a screen shot of the EM Alarm Browser GUI with the HW Mismatch alarm present (IP case). [“ATM ITP Mismatch Alarm” on page 2169](#) shows the same alarm but in the ATM case.

IP ITP Mismatch Alarm

Modular Alarm Browser: NL L

File Edit Help

Refresh Ack Unack Prev Next Print Save First Page Prev Page Next Page Last Page 1 of 1 Goto Page

1 alarm(s) with 1 critical

Log Id	Fault Type	NE# Seq	Phys Loc	Severity	Time
NE301	HW	1-2353	Card.frame0.slot0.slot12.ITP	critical	Mar 01 13:52:35 2004

General: not acknowledged Category: Equipment

NE: VOIPD Unit: Card.frame0.slot0.slot12.ITP

Time: Mar 01 13:52:35 2004 Severity: critical

Causes: Equipment Malfunction
Node Fault - Hardware fault

Description: oper fault for IP Not Supported. Replace With NTNY3011B4/C4/CB
Site Fir RPOe Bay_id
UAMP 00 ABB MGSF 000

ATM ITP Mismatch Alarm

File Edit Help

Refresh Ack Unack Prev Next Print Save First Page Prev Page Next Page Last Page 1 of 1 Goto Page

1 alarm(s) with 1 critical

Log Id	Fault Type	NE#-Seq	Phys Loc	Severity	Time
NE301	HW	1-2276	Card.frame0.slot12.1TP	critical	Mar 01 14:15:36 2004

General: not acknowledged Category: Equipment

ME: VOIPD Unit: Card.frame0.slot12.1TP

Time: Mar 01 14:15:36 2004 Severity: critical

Cause: Equipment Malfunction
Node Fault - Hardware fault

Description: oper fault for AAL1 Not Supported. Replace With NTN13011AB/CA/CB
SNA Fir RPos Bay_id
UAP 00 A99 MSGF000

Note: AAL1 is supported on all types of ABI cards. Therefore, there isn't an alarm that will state AAL1 is not supported. However, IP-ABI requires the use of "CA" or newer ABI cards.

Integrated Element Manager GUI Fields

The following table shows the relevant alarm fields for the DSP failure alarm.

Alarm Field descriptions

Field	Value
Severity	Critical
Category	Equipment
LogNumber	NE301
EventType	Equipment Malfunction
EventLabel	Node Fault-Hardware Fault
BodyText	Fault for <AAL1/IP> Not Supported. Replace Card with NTNYxxXX/XX.

For ABI:

xx = 43

XX/XX/XX = AB/BA/BB

For ITP:

xx = 3011

XX/XX/XX = AB/BA/CA/CB

Glossary

Term	Description
ABI	Access Bridge Interface
EM	Element Manager
HW	Hardware
ITP	Internet Telephony Processor
MG9000	Media Gateway 9000
SN07	Succession 07 Stream

Product = MG9000

A00005016 -- VMG Out of Service Alarms (UA-IP)***Functional Description***

This document provides the functional description for support of additional VMG alarms on the MG 9000 and Media Gateway 9000 Manager.

In SN06.2, there is only one alarm that is raised if a VMG has been provisioned that is in an Out of Service state. Unfortunately, the state of VMG Out of Service is symptomatic of many problems that could be occurring:

- missed steps in LCI commissioning
- bad IP address input during VMG provisioning
- mismatch provisioning between MG9000 EM and the core during ABI provisioning
- network router issues
- ITP/ABI is locked or disabled
- GWC locked
- card is still initializing

This feature addresses the problem that resolution of a single VMG OOSV alarm is too complex, especially at VMG provisioning time. Instead of the single fault raised in SN06.2 - VMG300 - VMG OOS, there will instead be a number of faults, each describing a different root cause for why the MG9K is not in service. Raising different alarms helps the user to narrow their resolution /debugging efforts to what is specifically broken.

In addition, because these different alarm reasons are logged, there will now be extra information in the logs when the VMG goes out of service as to why it did so (manually set to out of service vs. GWC unreachable vs. GWC not responding).

As a result of this feature, when a VMG goes out of service, the Alarm Browser will show the VMG300 alarm only in very unusual circumstances - instead, one or more of the following faults will be raised:

- rootTermStatusChange (1), -- generic reason
- vMGAdminStatusOutOfService (2), - VMG was administratively set to out of service
- cardLocked (3), -- card is locked
- cardDisabled (4), -- card is initializing
- cardInitializing (5), -- card is initializing
- lineMtceOnPairNotReady (8), -- Line maintenance is not ready
- megacoMtceOnPairNotReady (8), -- Megaco maintenance is not ready
- gWCUnreachable (53), -- pings to reach GWC failed
- noGWCREply (54), -- GWC didn't reply to ServiceChange

- aal1BearerSubsystemOnPairNotReady (56),
- ipBearerSubsystemOnPairNotReady (57),

All faults are cleared when a VMG goes to an In Service state.

While the VMG300 alarm was always critical in SN06.2, the following faults will be raised at a severity level of warning instead of critical to indicate that there was a (likely) user-initiated reason the VMG is out of service:

- Initializing - this fault will be raised during the initial period after an ITP/ABI card pair has been restarted or when the ITP/ABI is waiting for an initial registration response from the GWC, after which the VMG will either be in service (all faults cleared) or a different alarm will be raised.
- Card Locked - if the active ITP or ABI has been locked.
- VMG Admin Status Out Of Service - if the VMG has been set to out of service in the Gateway Status Config tab of the Switched Lines Services GUI.

All of the other faults will have a severity of critical.

The Switched Lines Services GUI will show what VMG alarms are currently raised against the VMG in a new field in the GW Status Config screen.

More information on the purpose and clearing procedures of the new faults is in the Fault Management section of this DDOC.

Applicable customer facing sections

Fault Management

Logs	☒
Alarms	☒

Configuration

Data Schema/MIBs	☐
User Interface	☒
GUI	☒
Element Management	☐
Security	☐
Service Order	☐
Office Parameters	☐
SOC	☐

Upgrades impact _____NA__

Accounting (includes AMA billing) _____NA__

Performance _____NA__

Hardware Requirements or Dependencies

N/A

Software Requirements or Dependencies

N/A

Limitations and restrictions

After SWACTs and card pair restarts, any alarms that had been raised against the VMG before the restart or SWACT are cleared and new faults are raised to match the present VMG fault state of the active card.

Interactions

N/A

Glossary

VMG Virtual Media Gateway

Fault Management for A00005016

Fault management strategy

The standard MG9K EM Fault Management strategy will apply to the new faults raised by this feature. Alarms will be displayed by the MG9K EM Alarm Browser, logged in NT standard format to the SSPFS CUST logs and forwarded to northbound OSS.

For the “New VMG Out of Service Alarms” feature there will be new faults added to more provide the reason why a VMG is out of service.

Fault management tools and utilities

Alarm Browser - Reports alarms from registered events. When an alarm is generated, it is displayed in the Alarm Browser along with the date and time, the NE Id, the resource (where the alarm was generated), the severity and probable cause. Highlighting the alarm displays the description of the alarm in the text box at the bottom of the Alarm Browser.

Log Adaptor - Generates logs from registered events. The log names and numbers are predetermined and are matched with the incoming event. A log with the corresponding name and number which contains the date, time,

physical location, severity and any other pertinent information is generated and placed into a separate file.

Gateway Status Config in Switched Lines Services GUI - The current list of VMG faults will also be displayed here.

Faults, Alarms and Logs

There will be new VMG Out Of Service faults raised and cleared by the MG9000 to indicate the specific reason the VMG is out of service.

Some of these faults will have a severity of WARNING. These faults will be raised for issues that are most likely caused by user intervention: locking cards, setting VMG administrative state to Out of Service and restarting cards.

All of the other faults raised must assume that there is a problem that is preventing the VMG from going into service and have a severity of CRITICAL, same as the existing VMG300 fault.

Alarms

Explanation

vmgAdminStatusOutOfService

LogID: VMG322

Title: vmgAdminStatusOutOfService

Name: VMG Admin State is OOS

Description: Admin State Out Of Service - Call Processing Out of Service

Severity: Warning

Event type: TBL (Trouble)

vmgInitializing

LogID: VMG325

Title: vmgInitializing

Name: VMG Initializing

Description: VMG Initializing - Call Processing Out of Service.

Severity: Warning

Event type: TBL (Trouble)

vmgOOSCardLocked

LogID: VMG323

Title: vmgOOSCardLocked

Name: VMG OOS-card locked

Description: Card Locked - Call Processing Out of Service.

Severity: Warning

Event type: TBL (Trouble)

vmgOOSCardDisabled

LogID: VMG324

Title: vmgOOSCardDisabled

Name: VMG OOS-card disabled

Description: Card Disabled - Call Processing Out of Service.

Severity: Critical

Event type: TBL (Trouble)

vmgOOSLineMtcNotReady

LogID: VMG328

Title: vmgOOSLineMtcNotReady

Name: VMG OOS- Line Maintenance is not Ready

Description: Line Maintenance Not Ready - Call Processing Out of Service.

Severity: Critical

Event type: TBL (Trouble)

vmgOOSMegacoMtcNotReady

LogID: VMG329

Title: vmgOOSMegacoMtcNotReady

Name: VMG OOS- Megaco Maintenance is not Ready

Description: Megaco Maintenance Not Ready - Call Processing Out of Service.

Severity: Critical

Event type: TBL (Trouble)

vmgOOSGWCUnreachable

LogID: VMG373

Title: vmgOOSGWCUnreachable

Name: VMG OOS- GWC is not reachable

Description: GWC Unreachable - Call Processing Out of Service.

Severity: Critical

Event type: TBL (Trouble)

vmgOOSNoReplyFromGWC

LogID: VMG374

Title: vmgOOSNoReplyFromGWC

Name: VMG OOS- no reply from GWC

Description: GWC Reachable But No Reply To Service Change - Check LGRP/GWC state - Call Processing Out of Service

Severity: Critical

Event type: TBL (Trouble)

vmgOOSAAL1BearerOnPairNotReady

LogID: VMG376

Title: vmgOOSAAL1BearerSubsystemOnPairNotReady

Name: VMG OOS- AAL1 bearer subsystem not ready

Description: AAL1 Bearer Not Ready - Call Processing Out of Service.

Severity: Critical

Event type: TBL (Trouble)

vmgOOSIPBearerOnPairNotReady

LogID: VMG377

Title: vmgOOSIPBearerSubsystemOnPairNotReady

Name: VMG OOS- IP bearer subsystem not ready

Description: IP Bearer Not Ready - Call Processing Out of Service.

Severity: Critical

Event type: TBL (Trouble)

Format

The Log Delivery application for this feature generates logs in the Number 2 Switch Control Center (SCC2) format and the NT standard (STD) format explained in the PLOA_SLOA_LOG_ALARMS DID.

The following sections show the STD format for each of the faults.

vmgAdminStatusOutOfService

```
250Q MG9K      *** VMG322 MAY18 10:44:31 4200 TBL MG9K NnMegacoFault
Location: 18-c418_sanity-Frame006.Shelf2.Slot12
Notification Id: 469
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 19:31:52 1970
Component Id: Card.frame1.shelf2.slot12.ITY
Specific Problem: NnMegacoFault - VMG Admin Status Out Of Service
Description: Admin State Out Of Service - Call Processing Out of Service
Site   Flr  RPos  Bay_id
HOST   03   A0    MG9F 006
```

vmgInitializing

```
250Q MG9K      *** VMG325 MAY18 10:44:31 4200 TBL MG9K NnMegacoFault
Location: 18-c418_sanity-Frame006.Shelf2.Slot12
Notification Id: 469
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 19:31:52 1970
Component Id: Card.frame1.shelf2.slot12.ITY
Specific Problem: NnMegacoFault - VMG is Initializing
Description: VMG Initializing - Call Processing Out of Service.
Site   Flr  RPos  Bay_id
HOST   03   A0    MG9F 006
```

vmgOOSCardLocked

```
250Q MG9K      *** VMG323 MAY18 10:44:31 4200 TBL MG9K NnMegacoFault
Location: 18-c418_sanity-Frame006.Shelf2.Slot12
Notification Id: 469
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 19:31:52 1970
Component Id: Card.frame1.shelf2.slot12.ITY
Specific Problem: NnMegacoFault - Card is Locked
Description: Card Locked - Call Processing Out of Service.
Site   Flr  RPos  Bay_id
```

HOST 03 A0 MG9F 006

vmgOOSCardDisabled

250Q MG9K *** VMG324 MAY18 10:44:31 4200 TBL MG9K NnMegacoFault
Location: 18-c418_sanity-Frame006.Shelf2.Slot12
Notification Id: 469
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 19:31:52 1970
Component Id: Card.frame1.shelf2.slot12.ITY
Specific Problem: NnMegacoFault - Card is Disabled
Description: Card Disabled - Call Processing Out of Service.
Site Flr RPos Bay_id
HOST 03 A0 MG9F 006

vmgOOSLineMtcNotReady

250Q MG9K *** VMG328 MAY18 10:44:31 4200 TBL MG9K NnMegacoFault
Location: 18-c418_sanity-Frame006.Shelf2.Slot12
Notification Id: 469
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 19:31:52 1970
Component Id: Card.frame1.shelf2.slot12.ITY
Specific Problem: Specific Problem: NnMegacoFault - Line Maintenance is not ready
Description: Line Maintenance Not Ready - Call Processing Out of Service
Site Flr RPos Bay_id
HOST 03 A0 MG9F 006

vmgOOSMegacoMtcNotReady

250Q MG9K *** VMG329 MAY18 10:44:31 4200 TBL MG9K NnMegacoFault
Location: 18-c418_sanity-Frame006.Shelf2.Slot12
Notification Id: 469
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 19:31:52 1970
Component Id: Card.frame1.shelf2.slot12.ITY
Specific Problem: NnMegacoFault - Megaco Maintenance is not ready
Description: Megaco Maintenance Not Ready - Call Processing Out of Service.
Site Flr RPos Bay_id
HOST 03 A0 MG9F 006

vmgOOSGWCUnreachable

250Q MG9K *** VMG373 MAY18 10:44:31 4200 TBL MG9K NnMegacoFault
Location: 18-c418_sanity-Frame006.Shelf2.Slot12
Notification Id: 469
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 19:31:52 1970
Component Id: Card.frame1.shelf2.slot12.ITY

Specific Problem: NnMegacoFault- Ping to reachGWC failed
Description: GWC Unreachable - Call Processing Out of Service.
Site Flr RPos Bay_id
HOST 03 A0 MG9F 006

vmgOOSNoReplyFromGWC

250Q MG9K *** VMG374 MAY18 10:44:31 4200 TBL MG9K NnMegacoFault
Location: 18-c418_sanity-Frame006.Shelf2.Slot12
Notification Id: 469
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 19:31:52 1970
Component Id: Card.frame1.shelf2.slot12.OTP
Specific Problem: NnMegacoFault - GWC did not reply to service change
Description: GWC Reachable But No Reply To Service Change - Check LGRP/GWC
state - Call Processing Out of Service.
Site Flr RPos Bay_id
HOST 03 A0 MG9F 006

vmgOOSAAL1BearerOnPairNotReady

250Q MG9K *** VMG376 MAY18 10:44:31 4200 TBL MG9K NnMegacoFault
Location: 18-c418_sanity-Frame006.Shelf2.Slot12
Notification Id: 469
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 19:31:52 1970
Component Id: Card.frame1.shelf2.slot12.OTP
Specific Problem: NnMegacoFault - AAL1 bearer subsystem not ready
Description: AAL1 Bearer Not Ready - Call Processing Out of Service.
Site Flr RPos Bay_id
HOST 03 A0 MG9F 006

vmgOOSIPBearerOnPairNotReady

250Q MG9K *** VMG377 MAY18 10:44:31 4200 TBL MG9K NnMegacoFault
Location: 18-c418_sanity-Frame006.Shelf2.Slot12
Notification Id: 469
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 19:31:52 1970
Component Id: Card.frame1.shelf2.slot12.OTP
Specific Problem: NnMegacoFault - IP bearer subsystem not ready
Description: IP Bearer Not Ready - Call Processing Out of Service.
Site Flr RPos Bay_id
HOST 03 A0 MG9F 006

Action

vmgAdminStatusOutOfService

To clear this, change the Admin status in the Gateway Status Config tab of the Switched Lines Services GUI to In Service

vmgInitializing

This alarm is raised at initial VMG creation, while waiting for a reply from the GWC when the VMG Admin status is changed to InService or as the active ABI/ITP is coming up out of a restart. There is no clearing procedure for this alarm. During a restart, this is raised as long as 15 minutes. During the first 15 minutes after a restart of an ITP pair, no other out of service VMG alarms are raised against the VMG, except the Card Locked and Admin State Out of Service faults. If the VMG is still Out of Service 15 minutes after the restart, the alarm will be cleared and replaced by the appropriate VMG fault indicating the fault condition at that time.

vmgOOSCardLocked

To clear this, unlock the active ITP or ABI.

vmgOOSCardDisabled

This alarm indicates the ITP or ABI card's status is disabled. The ITP or ABI card view or Alarm Browser will provide more information about what is preventing the card from going enabled. When the card's status goes to enabled, this alarm will be cleared.

vmgOOSLineMtcOnPairNotReady

This alarm indicates Line Maintenance on the ITP or ABI is not ready for call processing support. If this is raised when the card is enabled, then this is most likely a software error condition. If the ITP or ABI is disabled, the Line Maintenance fault is usually raised as well. Locking and unlocking the card might cause this condition to clear.

vmgOOSMegacoMtcOnPairNotReady

This fault would be raised because of a software error condition. Locking and unlocking the card might cause this condition to clear.

vmgOOSGWCUnreachable

This alarm indicates the GWC is not responding to pings from the ITP or ABI and either the VMG has never reached an Enabled state or ESA capability is not turned on for this VMG.

It could mean a number of things:

- If this VMG has never been in service, it could be because an invalid VMG IP address was provisioned. If the address is incorrect, then delete and re-add the VMG with the correct IP address
- It could be an issue with the network interface or edge router - most likely there will also be a Wanbuilder Heartbeat alarm - resolve the issue with that alarm

- If there is not a Wanbuilder Heartbeat alarm and Wanbuilder Heartbeat was turned on for the Call Control subnet (ITPs) or ABI subnet (ABIs) then this is likely a network issue - do pings/traceroutes to isolate the issue further
- Also verify that the pair of GWC cards is unlocked. If the active GWC is locked, it will not respond to pings.

vmgOOSNoReplyFromGWC

This alarm indicates the GWC is not responding to Megaco messages for this VMG and either the VMG has never reached an Enabled state or ESA capability is not turned on for this VMG.

It could mean a number of things, including:

- The LGRP for this VMG is not in a ready state. Check the LGRP state using MAPCI ; PM on the core.
- If this is a VMG for an ABI pair that has never been in service, it could mean that the core or MG9K EM is provisioned with the incorrect address for this VMG. Correct the VMG IP address in the datafill in the core or re-provision the VMG with the correct address in the MG9K EM.
- GWC pair has been set to man busy or has issues - check the GWC status in CS2M.

vmgOOSAAL1BearerOnPairNotReady

This usually indicates a software error situation on either the DCC or ITP. Lock and unlocking the ITP, ABI or DCC card(s) involved might clear this.

vmgOOSIPBearerOnPairNotReady

This is usually because the Call Control Subnet was not provisioned on the DCC. Go to LCI and provision the Call Control Subnet. As such, this fault is usually card to see if that clears the issue. If the Call Control Subnet has been provisioned and this fault does not clear, then this is likely a software error - lock and unlock the ITP/ABI card to see if that clears the issue.

VMG300

Most of the time, this alarm will be raised only for transient situations, and should either be cleared or replaced by a different alarm within 15 seconds. The two exceptions to this are:

- if the active card is at SN07 or greater, but the inactive card is on a pre-SN07 software release.
- the ITP or ABI pair is on SN07, but the DCC is on a pre-SN07 release

Until the inactive card and DCC are upgraded to SN07 or greater, the active card will raise only the VMG300 fault when the VMG is out of service. To clear this, follow the instructions for the various faults in this section until the alarm is cleared.

Associated Operational Measurements or Performance Measurements

None.

Related documentation***Configuration for A00005016*****Hardware and Software Requirements**

NA

Initial Configuration

NA

Office/Subnet parameters (OP/SP) (CM & SESM)

NA

Upgrade Impact

NA

Data schema (DS) (CM, MIBS, RDB)**New/modified tables, MIBs, or Database Schema**

As part of this feature the following modification was made to the UEMG Megaco Enterprise MIB:

The previous definition of nnMegacoFaultType had only one type in it:

```
nnMegacoFaultType OBJECT-TYPE
    SYNTAX      INTEGER
                {
                    rootTermStatusChange      (1)
                }
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Type of Megaco Fault"
 ::= { nnMegacoNotifObjects 1 }
```

This has been replaced by the following definition:

```
nnMegacoFaultType ::= TEXTUAL-CONVENTION
```

```

STATUS      current
DESCRIPTION
    "Enumeration of Fault Types Megaco Maintenance will throw."
SYNTAX      INTEGER
    {
        rootTermStatusChange      (1),          -- generic reason
        VMGAdminStatusOutOfService (2),  - VMG was administratively set to
out of service

        cardLocked (3),          -- card is locked
        cardDisabled (4),        -- card is disabled
        cardInitializing (5),      -- card is initializing
        nodeMtceOnPairNotReady (7), -- card is locked or disabled
        lineMtceOnPairNotReady (8), -- Line maintenance is not ready

        gwcLinkStatusDown (51), -- first hop layer 2 down
        edgeRouterUnreachable(52), -- pings to reach first hop failed
        gWCUnreachable (53),      -- pings to reach GWC failed
        noGWCReply (54),          -- GWC didn't reply to ServiceChange
        bearerSubsystemOnPairNotReady (55),
        aallBearerSubsystemOnPairNotReady (56),
        ipBearerSubsystemOnPairNotReady (57),
            --- skip 58
        carrier NotProvisioned (59), -- physical interface not provisioned
        carrierNotReady (60), -- physical interface not ready
        networkInterfaceNotProvisioned (61), -- layer 2 not provisioned
        networkInterfaceNotReady (62), -- layer 2 not ready
        messagingInterfaceNotProvisioned (63), -- call control not provisioned
        messagingInterfaceNotReady (64), -- call control not ready
            --- skip 65 and 66
        bearerInterfaceNotProvisioned (67), -- bearer subnet not provisioned
        bearerInterfaceNotReady (68), -- bearer subnet not ready
        .
        . (more types)
    }

```

The new MIB definition can be found at the following location:

<http://triweb/smg5000/mibDir/mibTxt/NORTEL-UEMG-MEGACO.mib>

Service Orders (SO) (CM & SESM)

NA

Software optionality control (SOC)

NA

Element Management

The Switched Line Services Screen will now have a new field on the GW Status Config tab “Fault status”. This field will show what, if any, faults have been raised against the VMG.

New/modified GUIs

GUI name	NEW, CHANGED, or DELETED
GW Status Config Tab under the Switched Line Services screen	CHANGED

GUI information

GUI name: GW Status Config

GateWay Status Configuration tab.

Functional description

A new field will be added to the Gateway Status Configuration tab to show what alarms have been raised against the VMG.

The status screen will in most cases automatically be updated when alarms are raised against the VMG. In addition, when the user presses the Refresh button, the correct fault status will be displayed, based on what VMG alarms have been raised to the EM.

GUI size

New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
GW Status Config	1	1 per MG9000	NA

GUI fields

The following table lists the new field for GUI GW Status Config.

GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
outOfServiceState	New	No	Fault Status for VMG	Displays the VMG faults raised for this VMG. If there are no faults, then this field will display "None."	None

Usage example

The screenshot displays the 'Switched Line Services for MG9000 Element 41' window. On the left, under 'Select a Virtual Media Gateway', 'UAIP004-0-1' is selected. The main area shows 'Provisioning Information for: UAIP004-0-1' with tabs for 'GW Market Config', 'GW Status Config', 'GW Termination Config', 'ESA Config', 'GW Config', and 'GW Controller Config'. The 'Administrative Status' is set to 'Out of Service' and the 'Operational Status' is 'Disabled'. The 'Disabled Cause' field is expanded, showing a 'Fault Description' of 'VMG322 : Admin State Out Of Service - Call Processing Out of Service.' At the bottom, there are 'Apply' and 'Refresh' buttons.

This example shows a VMG with Administrative Status Out of Service. In this state, the Disabled Cause field will show one alarm as show above.

The example below shows a VMG that is in an Enabled state.

Switched Line Services for MG9000 Element 41

MG9000 Services

Select a Virtual Media Gateway

Create

Delete

UAIP004-0-1

Provisioning Information for: UAIP004-0-1 Frame : 0 Shelf : 1 Mated Slots : 12/13

GW Market Config GW Status Config GW Termination Config

ESA Config GW Config GW Controller Config

Administrative Status: In Service

Operational Status: Enabled

Fault Description

None

Disabled Cause:

Apply Refresh

GUI release history update

None

Supplementary information

None

CLUI Interface

NA

Command interface changes

NA

Security

NA

Configuration Walkthrough

NA

Product = MG 9000

A00005375 -- New Shelf Discovery Alarms (UA-IP)

For this corrective CAF, only the Fault Management section is provided.

Fault Management

Fault management strategy

The standard MG9K EM Fault Management strategy will apply to the new faults raised by this feature. Alarms will be displayed by the MG9K EM Alarm Browser, logged in NT standard format to the SSPFS CUST logs and forwarded to northbound OSS.

For the “New Shelf Discovery Alarms” feature there will be new faults added to provide the reason when shelf discovery failed due to a particular card or due to an incompatible card.

Fault management tools and utilities

Alarm Browser - Reports alarms from registered events. When an alarm is generated, it is displayed in the Alarm Browser along with the date and time, the NE Id, the resource (where the alarm was generated), the severity and probable cause. Highlighting the alarm displays the description of the alarm in the text box at the bottom of the Alarm Browser.

Log Adaptor - Generates logs from registered events. The log names and numbers are predetermined and are matched with the incoming event. A log with the corresponding name and number which contains the date, time, physical location, severity and any other pertinent information is generated and placed into a separate file.

Faults, Alarms and Logs

There will be new Shelf faults raised and cleared by the MG9000 to indicate the specific reason the shelf discovery failed.

Alarms

Explanation

SHELFCOMPATIBILITY

Title: shelfCompatibility

Name: Incompatible Shelf

Description: This log is generated when a shelfCompatibility fault is received from the MG9kEM server.

CARDDISCOVERY

Title: cardDiscovery

Name: Card Discovery failure

Description: This log is generated when a cardDiscovery fault is received from the MG9kEM server.

CARDDISCPOWIO

Title: cardDiscPowIo

Name: Discovery failure for IO card

Description: This log is generated when a cardDiscPowIo fault is received from the MG9kEM server.

CARDDISPOWSIC

Title: cardDiscPowSic

Name: Discovery failure for SIC card

Description: This log is generated when a cardDiscPowSic fault is received from the MG9kEM server.

CARDDISCSLOT2

Title: cardDiscSlot2

Name: Discovery failure for card in Slot 2

Description: This log is generated when a cardDiscSlot2 fault is received from the MG9kEM server.

CARDDISCSLOT3

Title: cardDiscSlot2

Name: Discovery failure for card in Slot 3

Description: This log is generated when a cardDiscSlot3 fault is received from the MG9kEM server.

CARDDISCSLOT4

Title: cardDiscSlot4

Name: Discovery failure for card in Slot 4

Description: This log is generated when a cardDiscSlot4 fault is received from the MG9kEM server.

CARDDISCSLOT5

Title: cardDiscSlot5

Name: Discovery failure for card in Slot 5

Description: This log is generated when a cardDiscSlot5 fault is received from the MG9kEM server.

CARDDISCSLOT6

Title: cardDiscSlot6

Name: Discovery failure for card in Slot 6

Description: This log is generated when a cardDiscSlot6 fault is received from the MG9kEM server.

CARDDISCSLOT7

Title: cardDiscSlot7

Name: Discovery failure for card in Slot 7

Description: This log is generated when a cardDiscSlot7 fault is received from the MG9kEM server.

CARDDISCSLOT8

Title: cardDiscSlot8

Name: Discovery failure for card in Slot 8

Description: This log is generated when a cardDiscSlot8 fault is received from the MG9kEM server.

CARDDISCSLOT9

Title: cardDiscSlot9

Name: Discovery failure for card in Slot 9

Description: This log is generated when a cardDiscSlot9 fault is received from the MG9kEM server.

CARDDISCSLOT10

Title: cardDiscSlot10

Name: Discovery failure for card in Slot 10

Description: This log is generated when a cardDiscSlot10 fault is received from the MG9kEM server.

CARDDISCSLOT11

Title: cardDiscSlot11

Name: Discovery failure for card in Slot 11

Description: This log is generated when a cardDiscSlot11 fault is received from the MG9kEM server.

CARDDISCSLOT12

Title: cardDiscSlot12

Name: Discovery failure for card in Slot 12

Description: This log is generated when a cardDiscSlot12 fault is received from the MG9kEM server.

CARDDISCSLOT13

Title: cardDiscSlot13

Name: Discovery failure for card in Slot 13

Description: This log is generated when a cardDiscSlot13 fault is received from the MG9kEM server.

CARDDISCSLOT14

Title: cardDiscSlot14

Name: Discovery failure for card in Slot 14

Description: This log is generated when a cardDiscSlot14 fault is received from the MG9kEM server.

CARDDISCSLOT15

Title: cardDiscSlot15

Name: Discovery failure for card in Slot 15

Description: This log is generated when a cardDiscSlot15 fault is received from the MG9kEM server.

CARDDISCSLOT16

Title: cardDiscSlot16

Name: Discovery failure for card in Slot 16

Description: This log is generated when a cardDiscSlot16 fault is received from the MG9kEM server.

CARDDISCSLOT17

Title: cardDiscSlot17

Name: Discovery failure for card in Slot 17

Description: This log is generated when a cardDiscSlot17 fault is received from the MG9kEM server.

CARDDISCSLOT18

Title: cardDiscSlot18

Name: Discovery failure for card in Slot 18

Description: This log is generated when a cardDiscSlot18 fault is received from the MG9kEM server.

CARDDISCSLOT19

Title: cardDiscSlot19

Name: Discovery failure for card in Slot 19

Description: This log is generated when a cardDiscSlot19 fault is received from the MG9kEM server.

CARDDISCSLOT20

Title: cardDiscSlot20

Name: Discovery failure for card in Slot 20

Description: This log is generated when a cardDiscSlot20 fault is received from the MG9kEM server.

CARDDISCSLOT21

Title: cardDiscSlot21

Name: Discovery failure for card in Slot 21

Description: This log is generated when a cardDiscSlot21 fault is received from the MG9kEM server.

Format

The Log Delivery application for this feature generates logs in the Number 2 Switch Control Center (SCC2) format and the NT standard (STD) format explained in the PLOA_SLOA_LOG_ALARMS DID.

SHELFCOMPATIBILITY

- **STD Format:**

```
SHLF392 MAR08 04:58:42 8781 TBL MG9K NorShelfFault
  Location: 8-CO8-Frame123.Shelf2
  Notification Id: 125
  State: not acknowledged
  Category: Equipment Alarm
  Cause: Equipment Malfunction
  Time: Jan 01 03:05:03 1970
  Component Id: Shelf.frame0.shelf2
  Specific Problem: NorShelfFault - Shelf Compatibility
  Description: testing
  Site Flr RPos Bay_id
  HOST 00 A0 MG9F 123
```

- **SCC2 Format:**

```
SHLF392 8168 TBL MG9K NorShelfFault
  Location: 8-CO8-Frame123.Shelf2
  Notification Id: 3
  State: not acknowledged
  Category: Equipment Alarm
  Cause: Equipment Malfunction
  Time: Jan 01 02:30:17 1970
  Component Id: Shelf.frame0.shelf2
  Specific Problem: NorShelfFault - Shelf Compatibility
  Description: asf
  Site Flr RPos Bay_id
  HOST 00 A0 MG9F 123
```

CARDDISCOVERY

- **STD Format:**

```
SHLF393 MAR08 04:55:43 6680 TBL MG9K NorShelfFault
  Location: 8-CO8-Frame123.Shelf2
  Notification Id: 126
  State: not acknowledged
  Category: Equipment Alarm
  Cause: Equipment Malfunction
```


Time: Jan 01 02:40:06 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 6612 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 4
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:40:06 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

CARDDISCPOWIO

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 127
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Power IO
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 887 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 5
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:13 1970
Component Id: Shelf.frame0.shelf2

Specific Problem: NorShelfFault - Card Discovery Power IO
Description: asdf
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

CARDDISCPOWSIC

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 128
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Power SIC
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9279 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 6
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:31 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Power SIC
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

CARDDISCSLOT2

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 129
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2

Specific Problem: NorShelfFault - Card Discovery Slot 2

Description: testing

Site Flr RPos Bay_id

HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault

Location: 8-CO8-Frame123.Shelf2

Notification Id: 7

State: not acknowledged

Category: Equipment Alarm

Cause: Equipment Malfunction

Time: Jan 01 02:41:58 1970

Component Id: Shelf.frame0.shelf2

Specific Problem: NorShelfFault - Card Discovery Slot 2

Description: testing

Site Flr RPos Bay_id

HOST 00 A0 MG9F 123

CARDDISCSLOT3

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault

Location: 8-CO8-Frame123.Shelf2

Notification Id: 130

State: not acknowledged

Category: Equipment Alarm

Cause: Equipment Malfunction

Time: Jan 01 02:43:46 1970

Component Id: Shelf.frame0.shelf2

Specific Problem: NorShelfFault - Card Discovery Slot 3

Description: testing

Site Flr RPos Bay_id

HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault

Location: 8-CO8-Frame123.Shelf2

Notification Id: 8

State: not acknowledged

Category: Equipment Alarm

Cause: Equipment Malfunction

Time: Jan 01 02:41:58 1970

Component Id: Shelf.frame0.shelf2

Specific Problem: NorShelfFault - Card Discovery Slot 3

Description: testing

Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

CARDDISCSLOT4

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 131
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 4
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 9
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 4
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

CARDDISCSLOT5

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 132
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 5
Description: testing
Site Flr RPos Bay_id

HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 10
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 5
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

CARDDISCSLOT6

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 133
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 6
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 11
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 6
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

CARDDISCSLOT7**• STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 134
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 7
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

• SCC2 Format:

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 12
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 7
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

CARDDISCSLOT8**• STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 135
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 8
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

• SCC2 Format:

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 13
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 8
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

CARDDISCSLOT9

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 136
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 9
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 14
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 9
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

CARDDISCSLOT10

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 137
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 10
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 15
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 10
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

CARDDISCSLOT11

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 138
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 11
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2

Notification Id: 16
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 11
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

CARDDISCSLOT12

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 139
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 12
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 17
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 12
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

CARDDISCSLOT13

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 140

State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 13
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 18
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 13
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

CARDDISCSLOT14

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 141
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 14
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 19
State: not acknowledged
Category: Equipment Alarm

Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 14
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

CARDDISCSLOT15

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 142
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 15
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 20
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 15
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

CARDDISCSLOT16

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 143
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction

Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 16
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 21
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 16
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

CARDDISCSLOT17

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 144
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 17
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 22
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2

Specific Problem: NorShelfFault - Card Discovery Slot 17
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

CARDDISCSLOT18

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 145
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 18
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 23
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 18
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

CARDDISCSLOT19

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 146
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 19

Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 24
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 19
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

CARDDISCSLOT20

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 147
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 20
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 25
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 20
Description: testing
Site Flr RPos Bay_id

HOST 00 A0 MG9F 123

CARDDISCSLOT21

- **STD Format:**

SHLF393 MAR08 04:36:50 8513 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 148
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:43:46 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 21
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

- **SCC2 Format:**

SHLF393 9178 TBL MG9K NorShelfFault
Location: 8-CO8-Frame123.Shelf2
Notification Id: 26
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Jan 01 02:41:58 1970
Component Id: Shelf.frame0.shelf2
Specific Problem: NorShelfFault - Card Discovery Slot 21
Description: testing
Site Flr RPos Bay_id
HOST 00 A0 MG9F 123

Action

SHELFCOMPATIBILITY

To clear this, insert a compatible card in the slot. for example put a NY30AA card if the active mate card is a NY30AA

CARDDISCOVERY

Insert a good card

CARDDISCPOWIO

Insert a good IO card

CARDDISCPOWSIC

Insert a good SIC card.

CARDDISCSLOT2

Insert a good card in the slot.

CARDDISCSLOT3

Insert a good card in the slot.

CARDDISCSLOT4

Insert a good card in the slot.

CARDDISCSLOT5

Insert a good card in the slot.

CARDDISCSLOT6

Insert a good card in the slot.

CARDDISCSLOT7

Insert a good card in the slot.

CARDDISCSLOT8

Insert a good card in the slot.

CARDDISCSLOT9

Insert a good card in the slot.

CARDDISCSLOT10

Insert a good card in the slot.

CARDDISCSLOT11

Insert a good card in the slot.

CARDDISCSLOT12

Insert a good card in the slot.

CARDDISCSLOT13

Insert a good card in the slot.

CARDDISCSLOT14

Insert a good card in the slot.

CARDDISCSLOT15

Insert a good card in the slot.

CARDDISCSLOT16

Insert a good card in the slot.

CARDDISCSLOT17

Insert a good card in the slot.

CARDDISCSLOT18

Insert a good card in the slot.

CARDDISCSLOT19

Insert a good card in the slot.

CARDDISCSLOT20

Insert a good card in the slot.

CARDDISCSLOT21

Insert a good card in the slot.

Associated Operational Measurements or Performance Measurements

None.

Product = MG 9000**A00006639--MG9K Overload OM pegs (UA-IP)****Description**

When a Media Gateway 9000 (MG9K) begins to reach an overload threshold call connections request are denied. This condition can occur on an ITP, ABI or at the nodal level (DCC). A log is currently generated corresponding to the line or trunk which requested the connection.

Overload condition occurs when the MG9K has reached a threshold where subsequent calls with the exception of calls marked 'essential or emergency' must be denied to prevent further catastrophic degradation of the MG9K node.

In SN07 an Operational Measurement (OM) register will be incremented for every connection which is denied. A new OM group GWOVL0M will be defined and the register OVERLOAD will be incremented upon connection denial.

In SN07 feature 'A00004430 - SVC Failure OMs' introduced the ability to peg OMs for ATM switched virtual circuits call failures. It pegs the logical group of the MG9K for calls which involve lines hosted off the ITP boards and it pegs the hosting legacy XPM peripherals directly connected to the ABI DS512 pack for calls involving lines subtending the ABI board.

To be consistent in pegging OMs, this feature will follow the same model.

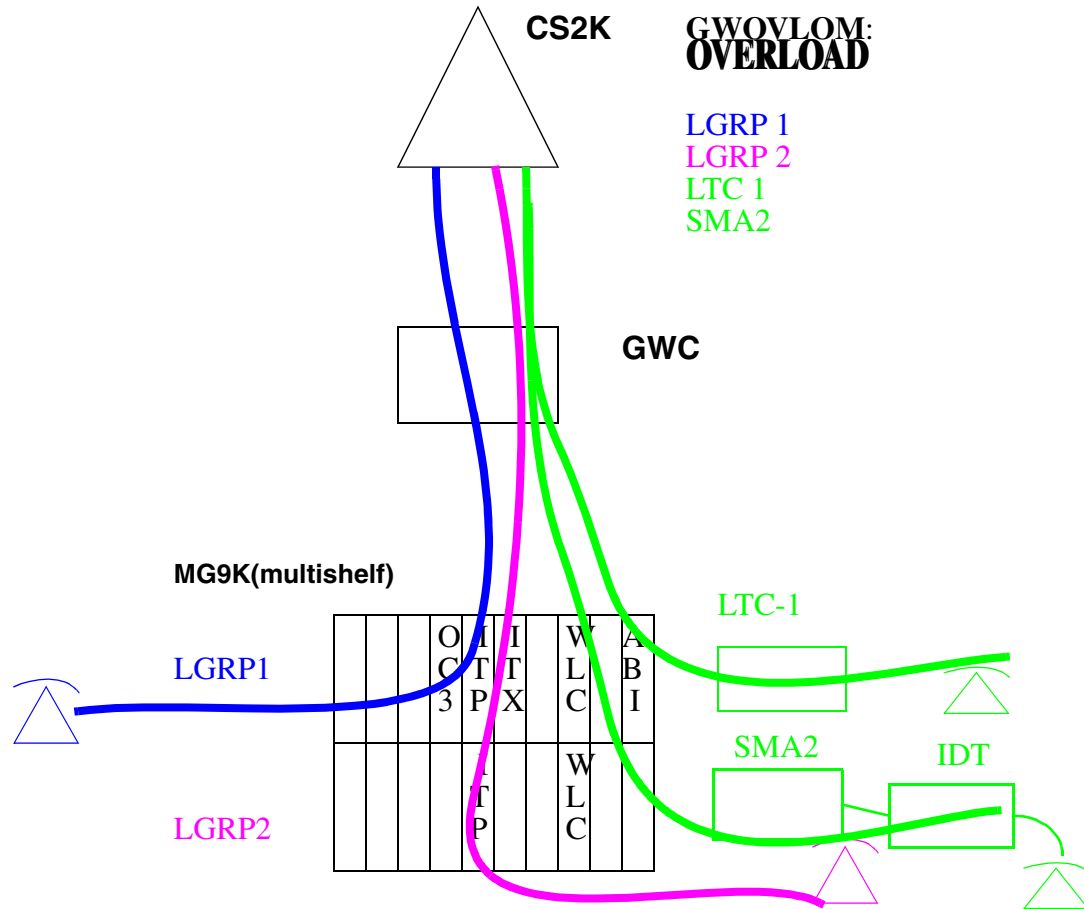
When a connection is denied for a call originated or terminated on an ITP board, i.e. a native MG9K call, the register associated with the logical group will be pegged. MG9Ks are identified as 'logical groups' because the CS2K is not aware of the MG9Ks on a nodal basis. In SN06.2 the feature 'A00002607 ABI XPMSITE and MG9K Location support on the Core' provided the first step towards recognizing ABI XPM and MG9K on a nodal basis. However currently only ABI 'nodes' are recognized in the CS2K.

If the connection is denied for a call which originates or terminates on an agent which is subtending an ABI board, the OM peg will occur on the hosting XPM which is directly connected to the DS512 pack on the ABI board. Currently the hosting XPMs which can be pegged are LTCs, SMA2s, LGCs.

For ABI connection failures line or RCC trunk could be rejected and pegging will be done for either one on the hosting XPM node.

The following figure shows the level where the OM register will be pegged.

CS2K Identification of MG9k and ABI lines Pegs



OM group GWOVLOM with OVERLOAD register

omshow gwovlom active
GWOVLOM

CLASS: ACTIVE

START:2004/03/05 13:30:00 FRI; STOP: 2004/03/05 13:56:48 FRI;

SLOWSAMPLES: 17 ; FASTSAMPLES: 161 ;

KEY (GWOVL_OM_PM_INFO1)

INFO (GWOVL_OM_TUPLE_DATA1)

OVERLOAD

68

MG9K ABI SMA2 1

0

73

MG9K ABI SMA2 0

0

87

MG9K ABI SMA2 2

0

89

MG9K ABI LTC 2

0

114

MG9K HOST 04 0

0

116

MG9K HOST 01 2

0

117

MG9K SLOA 31 3

0

Hardware Requirements or Dependencies

This feature has no hardware requirements or dependencies.

Software Requirements or Dependencies

This feature is no additional software dependencies.

Limitations and restrictions

There are no new limitations or restrictions introduced by this feature.

Interactions

No new interactions are introduced by this feature.

Applicable customer facing sections

Fault Management

Logs _N/A_

Alarms _N/A_

Configuration

Data Schema _N/A_

User Interface _N/A_

Element Management _N/A_

Security _N/A_

Service Order _N/A_

Office Parameters _N/A_

Accounting (includes AMA billing) _N/A_

Performance (includes operational measurements) X

Glossary

Term	Description
MG9K	Media Gateway 9000
ITP	Integrated Telephony Processor
DCC	Data Communication Card
OM	Operational Measurement
ATM	Asynchronous Transfer Mode

Product = MG 9000

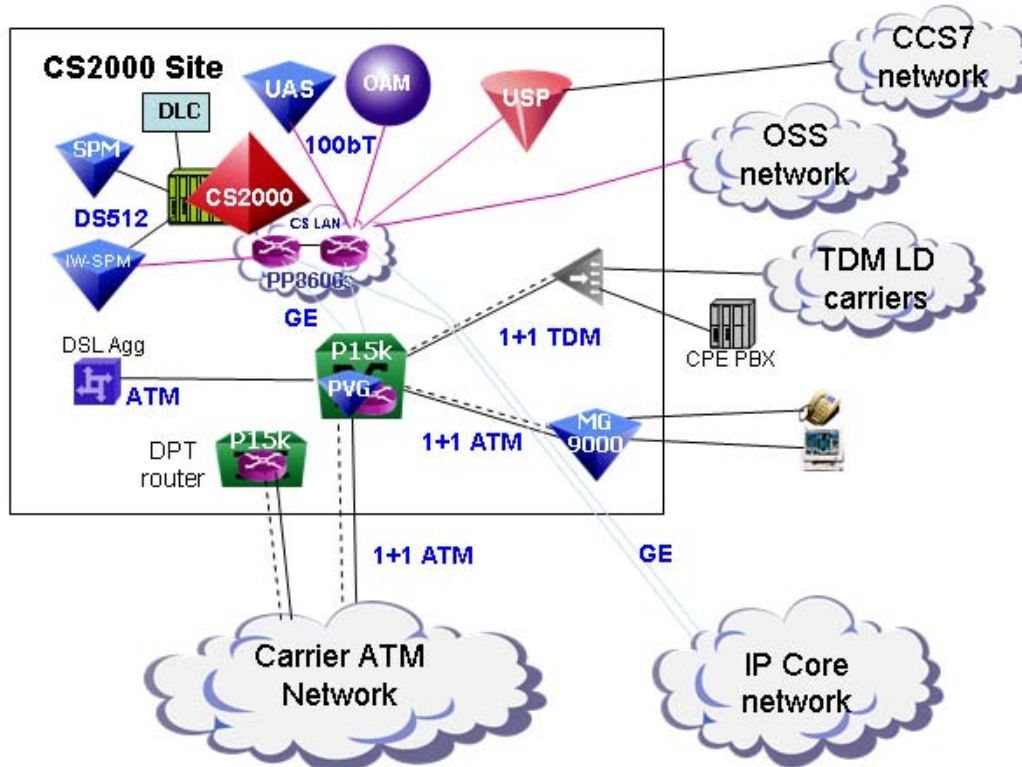
CD003593--MG9000 Aggregation on Passport 15000 and PVG (UA-IP)

The Succession ILEC-IP (UA-IP) Solution delivers an end-office solution (i.e. POTS and other access services) utilizing IP as the packet technology. Passport 15000 is positioned as the IP “aggregation” router of choice. In order to ensure the reliability, performance and capacity requirements of the Succession ILEC-IP solution are met, a standardized configuration is defined for the Passport 15000 and it is tested against the stated Succession generic requirements for ILEC-IP.

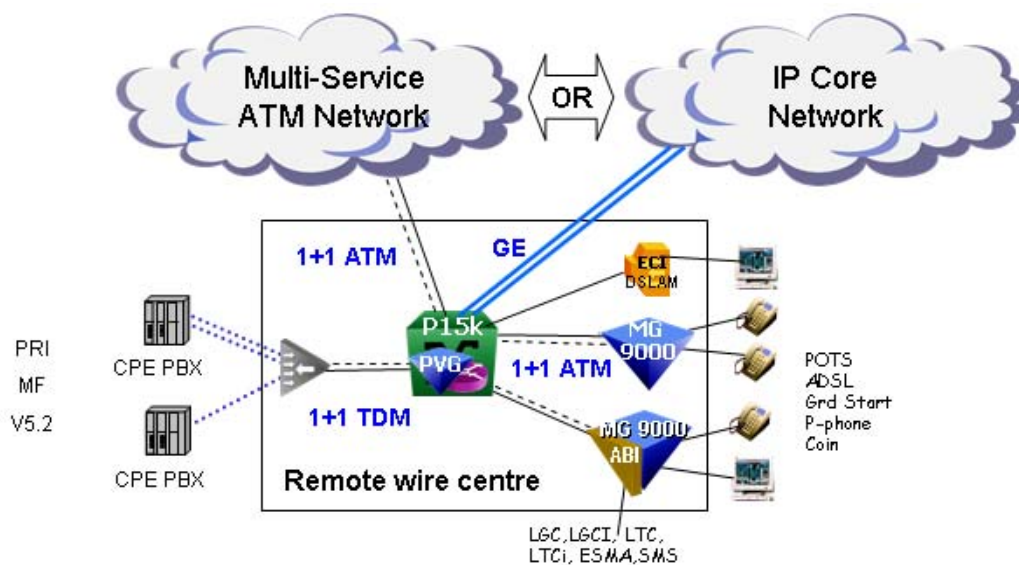
For reference, the following figures show the generic Succession UA-IP reference model, where a number of end-offices are replaced by “Remote” Passport 15000 shelves that aggregates IP traffic from a number of MG9000 line gateways and PRIs off of PVG cards. These Passport route traffic between each other and, as necessary, up to the CS2000 site (local tandem location), using either a multi-service ATM network or a Core IP network, where one or more Passports support PVG trunks to long distance companies or other tandems. Packets are also routed to the CS-LAN, particularly MG9000 and PVG control and OAM packets, but also voice packets for calls that need to inter-work with legacy TDM peripherals, through the IW-SPM platforms.

The Passport 15000 also aggregates DSL traffic from MG9000 gateways and DSLAMs, back to DSL aggregators, however this traffic is only carried as ATM traffic in the Passport 15000 switches.

Succession UA-IP Architecture (CS2000 site)



Succession UA-IP Architecture (remote site)



Deployment process development overview

Passport 15000 shelves deployed in the field are installed and configured by Nortel installation and Data Deployment. They configure the Passports

according to procedures define in Installation Methods, using MDM NP templates filled in with site specific information taken from Network Engineering Specification books.

Overview

The H/W configuration and CAS provisioning of a Passport 15000 acting as the aggregation router in a ILEC-IP solution is driven by requirements that we have categorized as follows:

- **Traffic Management:** the real-time datapath behavior, during steady state and during overload.
- **Reliability:** the overall availability of the system and the interruption to service as a result of different maintenance procedures or equipment failures.
- **Management:** overall service quality can be effected by how a Network Element is managed: Fault, Configuration, Performance and Security.

Background information

The Passport 15000 is aggregating VoIP traffic from four potential sources:

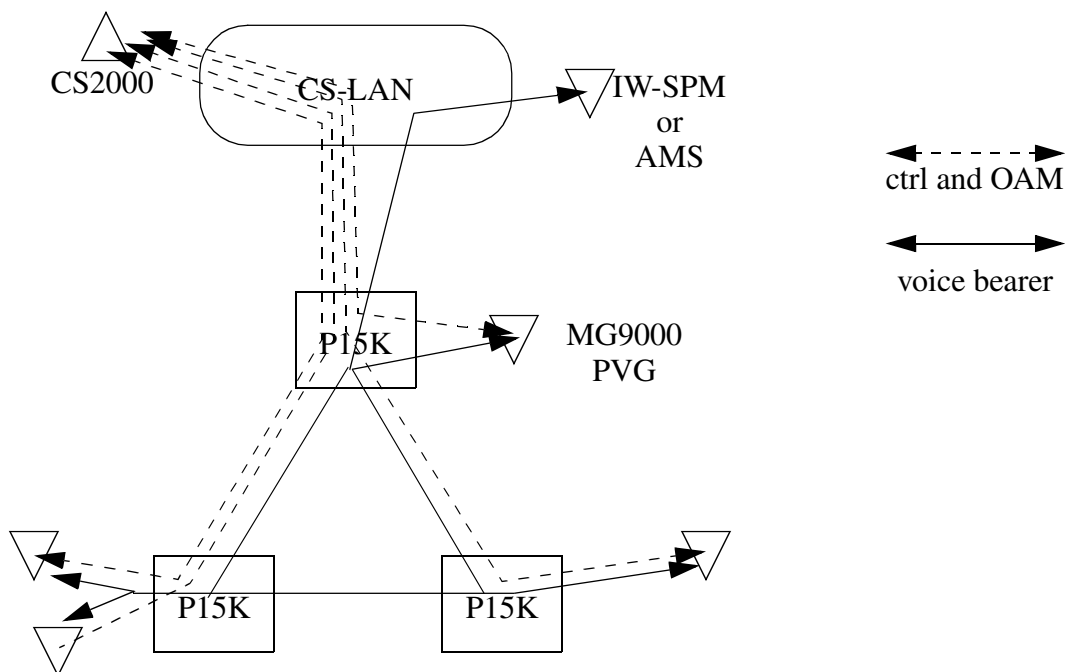
- **MG9000:** this line media gateway (MG) has one of a 1+1 APS OC-3, DS-3 or DS-1 IMA IP over ATM interfaces. IP traffic is carried to the VR over 2 or 3 Vccs: an rt-VBR Vcc carrying all the voice traffic plus the H.248 control traffic, an nrt-VBR Vcc for the OAM of the gateway and a third optional rt-VBR Vcc to carry other signalling (PPVM) and control traffic.
 - The voice+control Vcc requires a /27 subnet as there are up to 16 IP devices behind it, plus the Passport protocol port address.
 - The OAM Vcc requires a /29 subnet for three IP addresses; two IP addresses on the MG9000, plus the Passport protocol port address.
- **PVG VSP cards:** these trunk MG cards reside in the Passport 15000 shelf and connect to the VR via 2 or 3 “links”; one for the bearer traffic, one for H.248 control and a third optional one for PRI backhaul (signalling) traffic.
 - Each link requires a /30 subnet (the PVG application IP address plus the Passport protocol port address).
- **DSL:** ATM traffic can be aggregated from MG9000 gateways or DSLAMs, such as the ECI. This traffic is carried as UBR ATM traffic to a centrally located (e.g. CS2000 site) DSL aggregator, such as a Shasta BSN 5000.

- **CS-LAN:** consists of a pair of Passport 8600, connected to a Passport 15000 by a pair of GE or to a pair of Passport 15000 by two unprotected OC-12 links. Traffic is mostly H.248/PPVM control traffic between the MGs and the gateway controllers (GWC) in the CS2000, and OAM traffic between the MG9000 and the MG element managers. There is also some bearer traffic on these links. Ideally different traffic types would be separated into different VLANs.
 - The 8600s route all traffic sent to it by the Passport, so each link is part of a /30 subnet.
 - The amount of bearer traffic to the CS-LAN will vary, depending on the customer's deployment. In a very large office, the CS-LAN may also be used to tandem bearer traffic over GE links between a pair of co-located Passport 15000.

Data flow

This section describes the IP flows between the sources mentioned in the above section.

Data flow among the various Succession platforms



Bearer traffic

Any MG9000, PVG VSP card and the CS-LAN can be a source and sink of bearer traffic, i.e. voice, data or fax call. Hence for a bearer traffic subnet, all of these sources have to be IP reachable.

Note: Note: the MG9000 only supports the G.711 codec, with either 10 or 20 millisecond packets. Hence in a UA-IP network where PVGs need to inter-work with MG9000, G.711 must be used, even though the PVG supports the lower bandwidth G.729a codec.

Control traffic

All control traffic is between the CS2000 GWCs on the CS-LAN and the MG9000 or PVG VSP cards. MGs never exchange control traffic directly.

MG9000 OAM traffic

Like the MG9000 control traffic, the OAM traffic goes between a gateway and the MG9000 EMS on the CS-LAN. But unlike the control traffic, the OAM traffic is carried on a separate Vcc from the MG9000 interface, and hence can be carried as L2 (ATM) directly from the MG9000, whether it be at the CS2000 site or a remote site, to the VR on the CS2000 site Passport 15000. Advantages for this are discussed later in the Scalability section.

Passport 15000 (and PVG) OAM traffic

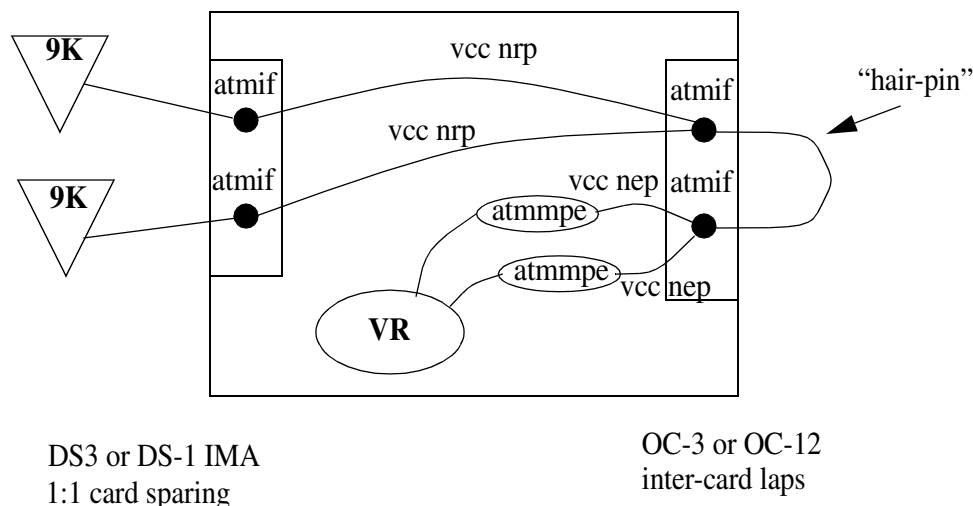
The Passport 15000/PVG are managed over IP by the Preside MDM server - typically connected to the CS-LAN or on some other customer management network that is. Since the Passport cannot be managed through GE links, the CP Ethernet ports are connected to the CS-LAN (Passport 8600s). Remote Passport 15000 are managed “in-band” as they are in Succession VoA, over the management VR (Vr/0).

MG9000 Electrical hair-pins

The MG9000 can also have either a DS-1 IMA or an STS-1 interface which terminates on the Passport as a DS-3.

As IP is not supported on the 4pDS3ChIMA card, and carrier grade IP is not supported on the 12pDS3ATM FP card, these cards can only terminate the ATM layer, and an optical “hair-pin” must be used for IP forwarding.

Electrical interface hair-pin IP connectivity



This optical hair-pin can be deployed on a pair of cards deployed expressly for this purpose, or it can be deployed on spare ports of an optical pair with spare capacity. For instance, a pair of 4pOC12 FP cards with only one OC12 trunk will have at least 1000 DS0s spare capacity, which can be used to support about 3 DS-3 MG9000.

References

For additional information, refer to the following publications.

- NN10225-512, Passport for Succession Configuration Attribute Summary Guide
- NN10028-111, PP15K and PMDM in Succession Networks Product & Technology Fundamentals for UA-AAL1 and UA-IP
- NN10114-511, PP15K and PMDM in Succession Networks Configuration Overview Guide
- NN10198-912, PP15K and PMDM in Succession Networks Fault Management Troubleshooting for UA-AAL1 and UA-IP

Product = MediaServer 2000

A00004873--MS2000 CLUI Enhancements (UA-IP, IAW)

Description

In SN06.0, the MS2000 (Media Server 2000) Series Node CLUI was introduced to configure the MS2010 device. The CLUI is delivered to the customer as part of the SESM load that is bundled as part of the CS2M load. The tool requires that the SESM server is in service.

The tool is launched with the command:
/opt/nortel/NTsesm/bin/ms2000.sh

The existing MS2000 Series Node CLUI will be enhanced in SN07 to handle configuration for the MS2020 ATM device. The following new functionality will be added to the MS2000 CLUI:

- 1) Ability to configure MS2020 device
- 2) Force Lock of a Device
- 3) Ability to change the SNMP Community Strings
- 4) Ability to change the MS2000 web interface user name and password.
- 5) Ability to configure the NTP (Network Time Protocol) settings for the MS2000 device.

Sample Usage

Forced Lock Menu change

Here is an example of logging into the device issuing a force lock command.

```
***** Media Server 2000 Series CLUI Main Menu *****
```

- 1) Display list of MS 2000 series nodes
- 2) Node Maintenance and Configuration
- 3) Backup INI file for all nodes
- 4) Copy a file to the SDM
- 5) Configure CLUI tool
- x) EXIT

```
Enter Selection (1 - 5, x)
```

```
> 2
```

```
Enter the IP address of the MS 2000 node
```

```
> 47.142.134.127
```

```
*** MS2020 Maintenance and Configuration Menu for Node : 47.142.134.127 ***
```

- 1) Display this nodes current configuration
- 2) Configure this node
- 3) Download load files to this node
- 4) Backup the INI file for this node
- 5) Perform a soft reset on this node
- 6) Lock or Unlock this node
- x) EXIT

```
Enter Selection (1 - 6, x)
```

```
> 6
```

```
*** MS2020 Lock Menu for node : 47.142.134.127 ***
```

```
*** Current State : unlocked(2)
1) Graceful Lock Node
2) Force Lock Node
3) Unlock Node
x) EXIT
Enter Selection (1 - 2, x)
> 2
```

*** WARNING ***

Performing a forced lock on the node will take it out of service immediately.
Active calls will be dropped!

Perform forced lock? (y/n)

> y

The MS2020 node has been locked.

Press <enter> to continue

Configuration menus for MS2020 devices

An example of logging into the box follows. The menu initially displays the name as MS2000 Series CLUI. Once we go to the configure level and enter in a device IP, the CLUI determines the device type and displays the menu specifically for the MS2020.

To be added later.

```
wnc0s0jm:/opt/nortel/NTsesm/bin> ./ms2000.sh
*****
**  Nortel Media Server 2000 Series Configuration Tool  **
**                               version 2.00                               **
*****
Enter user name > ptm
Enter password >
ORBWrapper orb initialized
```

***** Media Server 2000 Series CLUI Main Menu *****

- 1) Display list of MS 2000 series nodes
- 2) Node Maintenance and Configuration
- 3) Backup INI file for all nodes
- 4) Copy a file to the SDM
- 5) Configure CLUI tool
- x) EXIT

Enter Selection (1 - 5, x)

> 2

Enter the IP address of the MS 2000 node

> 47.142.147.134

*** MS2020 Maintenance and Configuration Menu for Node : 47.142.147.1 ***

- 1) Display this nodes current configuration
- 2) Configure this node
- 3) Download load files to this node
- 4) Backup the INI file for this node
- 5) Perform a soft reset on this node
- 6) Lock or Unlock this node
- x) EXIT

Enter Selection (1 - 6, x)

>

Here we choose to display this nodes configuration. The displayed data is identical to the MS2010 device but adds the 2 ATM parameters at the bottom.

*** MS2020 Maintenance and Configuration Menu for Node : 47.142.147.1 ***

- 1) Display this nodes current configuration
- 2) Configure this node
- 3) Download load files to this node
- 4) Backup the INI file for this node
- 5) Perform a soft reset on this node
- 6) Lock or Unlock this node
- x) EXIT

Enter Selection (1 - 6, x)

> 1

*** Current configuration for 47.142.147.1 ***

IP Address	: 47.142.144.1
SubNet Address	: 127.0.0.1
Default Gateway	: 127.0.0.1
MG Control Protocol	: controlProtocol-MGCP(1)
Software Version	: softwareVersion
Lock State	: shuttingDown(1)
Megaco Call Agent IP Address	: 1.2.3.4
Is Megaco Call Agent Used	: yes(1)
Number of Conference Ports	: 1
Number of TestTrunk Ports	: 1
Number of Lawful Intercept Ports	: 5
Number of Announcement Ports	: 5
APS IP Address	: 127.0.0.1
Primary Language	: amsLangCantonese(1)
Secondary Language	: amsLangCantonese(1)
AMS Profile	: enabled(1)
Syslog Server IP	: 127.0.0.1
SNMP Trap Manager IP	: 127.0.0.1
Is Trap Manager Used	: no(0)
ATM Default Application Type	: aal1(1)
Transmission mode	: sdh(0)

Press <enter> to continue

There are certain data tables that can be datafilled for AAL2 devices that are not available for AAL1. In this example we chose to configure the device and the CLUI determines it is an MS2020 AAL1 device.

*** MS2020 Maintenance and Configuration Menu for Node : 47.142.147.1 ***

- 1) Display this nodes current configuration
- 2) Configure this node
- 3) Download load files to this node
- 4) Backup the INI file for this node
- 5) Perform a soft reset on this node
- 6) Lock or Unlock this node
- x) EXIT

Enter Selection (1 - 6, x)

> 2

```
***** MS2020 AAL1 Configuration Menu *****
1) General node configuration
2) Configure ATM loopback table
x) EXIT
Enter Selection (1 - 2, x)
```

We now change the configuration to AAL2 by entering the General node configuration menu item.

```
***** MS2020 AAL1 Configuration Menu *****
1) General node configuration
2) Configure ATM loopback table
x) EXIT
Enter Selection (1 - 2, x)
> 1
*** Configuring MS2020 at 47.142.147.1 ***
```

Enter the desired value at the prompt. The current setting is displayed in brackets. To chose the default setting press Enter. Enter '?' for help with the format.

Megaco Call Agent IP Address [1.2.3.4]

```
>
Using current value 1.2.3.4
```

Number of Conference Ports [1]

```
>
Using current value 1
```

Number of TestTrunk Ports [1]

```
>
Using current value 1
```

Number of Lawful Intercept Ports [5]

```
>
Using current value 5
```

Number of Announcement Ports [5]

```
>
Using current value 5
```

APS IP Address [127.0.0.1]

```
>
Using current value 127.0.0.1
```

Primary Language [amsLangCantonese(1)]

```
>
Using current value amsLangCantonese(1)
```

Secondary Language [amsLangCantonese(1)]

```
>
Using current value amsLangCantonese(1)
```

AMS Profile [enabled(1)]

```
>
Using current value enabled(1)
```

Syslog Server IP [127.0.0.1]

```
>
Using current value 127.0.0.1
```

```
SNMP Trap Manager IP [127.0.0.1]
>
Using current value 127.0.0.1

Is Trap Manager Used [no(0)]
>
Using current value no(0)

ATM Default Application Type [aal1(1)]
> ?
SYNTAX: INTEGER { aal1 ( 1 ) , aal2-i-366-2 ( 2 ) , aal2-umts ( 3 ) }
*** NOTE ***
For enumerated types, enter the string value rather than the numeric value.
For example: For Primary Language, enter the string name "isoLangFrench".

> aal2-i-366-2
Value validated and set to aal2-i-366-2

Transmission mode [sdh(0)]
>
Using current value sdh(0)

Would you like to write these values to the MS2020 node? (y/n)
> y

***** MS2020 AAL2 Configuration Menu *****
1) General node configuration
2) Configure ATM loopback table
3) Configure ATM port table
4) Configure AAL2 PVC table
x) EXIT
Enter Selection (1 - 4, x)
>
```

As the example above shows, the ATM default application type was changed to AAL2. As a result of this change, new menu items appear in the Configuration menu. The user now has the option to configure the ATM port and AAL2 PVC tables.

Entering into the configuration for the port table we get another menu. In the following example we select to list the port table from the Configure Port Menu.

```
***** MS2020 AAL2 Configuration Menu *****
1) General node configuration
2) Configure ATM loopback table
3) Configure ATM port table
4) Configure AAL2 PVC table
x) EXIT
Enter Selection (1 - 4, x)
> 3

***** MS2020 ATM Port Configuration Menu *****
1) List current table
2) Add Port entry
```



```

3) Delete Port entry
x) EXIT
Enter Selection (1 - 3, x)
> 1

*** Port Table for MS2020 at 47.142.147.1 ***

Table Entry 0
*****
Port Number           : atmPortAdministrativeState.0:-->unlocked(2)
Administrative State   : atmPortOperationalState.0:-->enabled(1)
Operational State     : atmPortNumber.0:-->port0(0)
Port Address          : atmPortAddress.0:-->atmPortAddress
Alarm Status          : atmPortAlarmStatus.0:-->los(1)

Table Entry 1
*****
Port Number           : atmPortAdministrativeState.1:-->unlocked(2)
Administrative State   : atmPortOperationalState.1:-->enabled(1)
Operational State     : atmPortNumber.1:-->port1(1)
Port Address          : atmPortAddress.1:-->atmPortAddress
Alarm Status          : atmPortAlarmStatus.1:-->los(1)

Table Entry 2
*****
Port Number           : atmPortAdministrativeState.2:-->unlocked(2)
Administrative State   : atmPortOperationalState.2:-->enabled(1)
Operational State     : atmPortNumber.2:-->port2(2)
Port Address          : atmPortAddress.2:-->atmPortAddress
Alarm Status          : atmPortAlarmStatus.2:-->los(1)

***** MS2020 ATM Port Configuration Menu *****
1) List current table
2) Add Port entry
3) Delete Port entry
x) EXIT
Enter Selection (1 - 3, x)
>

```

Each of the configuration menus for the data tables behaves in the same manner. Adding entries will prompt for the needed data, deleting entries will prompt the user for the entry number to delete.

Setting Network Time Protocol

Do not have MIB from AudioCodes yet to implement this.

Setting SNMP Community Strings

Do not have MIB from AudioCodes yet to implement this.

Applicable customer facing sections

Fault Management

Not applicable

 X

Logs	☐
Alarms	☐
Configuration	
Not applicable	☐
Data Schema/MIBs	☐
User Interface	☒
GUI	☐
Element Management	☐
Security	☐
Service Order	☐
Office Parameters	☐
SOC	☐
Upgrades impact	☐
Accounting (includes AMA billing)	☐
Not Applicable	☒
Billing changes	☐
Performance	☒
Not Applicable	☐
Operational Measurements	☐
Performance Measurements	☐
Realtime	☐
Not applicable	☒
Engineering Information	☐
Not applicable	☒

Hardware Requirements or Dependencies

Software Requirements or Dependencies

Limitations and restrictions

Interactions

Glossary

Term	Description
MS2020	Media Server 2020, ATM Media Server

Product = Network Patch Manager

A00003560 -- Patching SSPFS, CBM, and IEMS via the NPM (UA-IP)

Functional Description

The Network Patch Manager is responsible for patching many Succession Network components previous to SN07. These components include:

- GWC cards
- MG9K-based cards
- SESM
- SAM21 EM
- NPM
- PSE
- QCA
- MG9K server
- MG9K midtier
- OM Collector

Beginning with this feature in SN07, the Network Patch Manager is used to patch additional components in Succession Networks as well as components in non-Succession configurations. These new components include the following:

- CBM - Core Billing Manager
- SSPFS platform
- IEMS - Integrated Element Management System

NPM Installation and Configuration

Prior to SN07, the NPM is always installed on the SSPFS machine that contains the CS2000 Management load. Beginning with this feature in SN07,

the NPM is delivered as part of the SSPFS platform and not the CS2000 Management load.

In existing customer sites where an NPM is moving from one physical box to another physical box, a migration process is required to ensure the new NPM contains any necessary previous data. This migration process includes the following:

- saving any customer-specific predefined reports that are stored in the NPM database
- saving all patch files from the golden directory
- movement of the data in the previous bullets from the old machine to the new machine
- re-datafilling of the predefined reports into the new NPM
- saving of the patch files in the golden directory on the new machine

In a given customer site, only one NPM should be installed. The SSPFS installation/upgrade/configuration scripts assist in identifying which SSPFS-based machine should have the NPM software installed. In general, the SSPFS-based machine that is to contain the IEMS application is the machine that should have the NPM installed. If an IEMS is not part of a customer site installation, the NPM should be installed on the same machine as the CBM application.

The various supported configurations are now discussed.

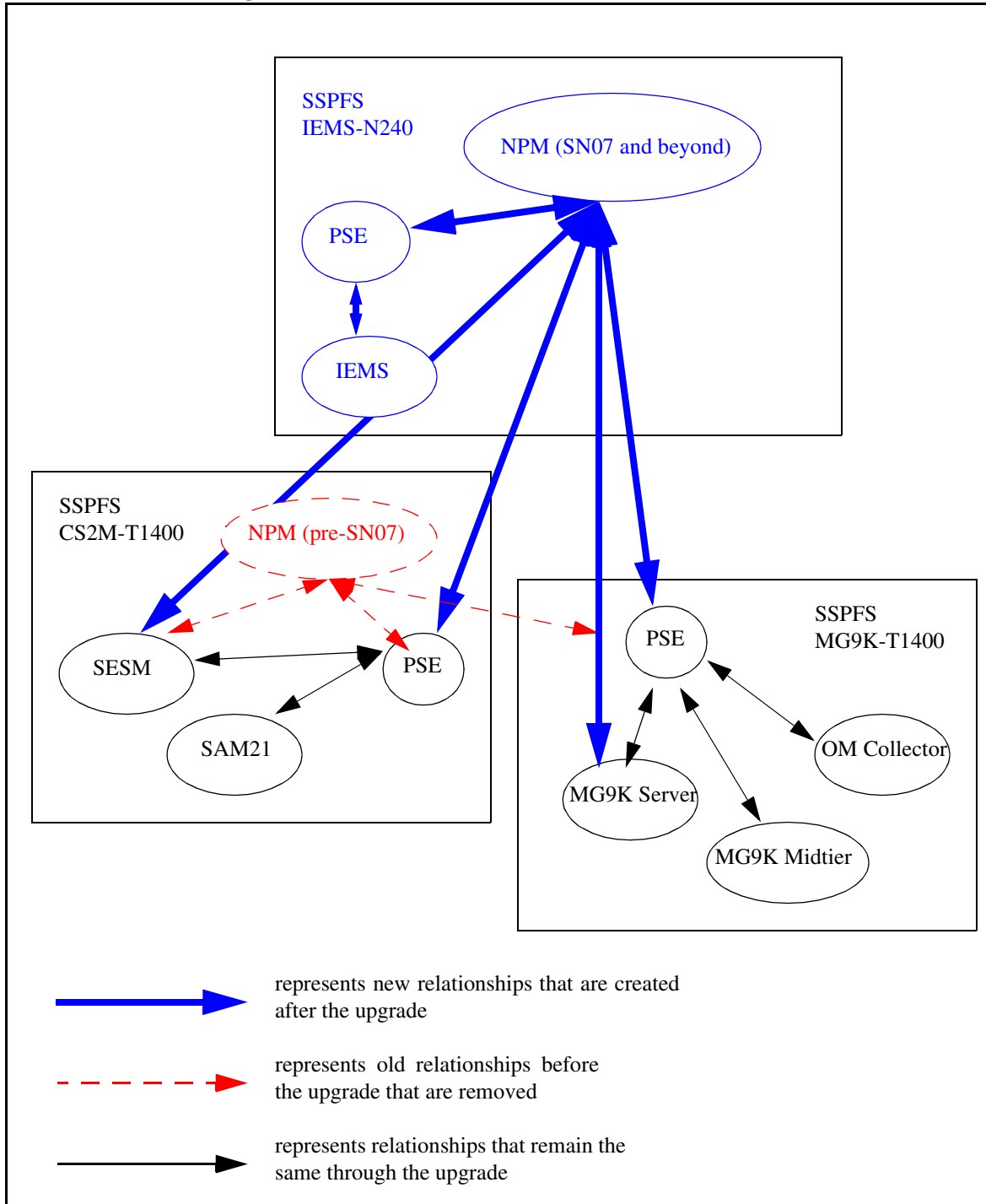
Existing CS2M on a T1400

In this configuration, an existing CS2000 customer site is being upgraded to SN07. The site has an existing T1400 SSPFS-based machine with NPM already installed and running with pre-SN07 software. Figure , on page 2229 shows this site with a new N240 being installed that contains the IEMS and NPM running SN07. After the upgrade, the CS2M-based T1400 continues to run in the customer site (with SN07 CS2M software) without the NPM since it would be installed on the new N240 machine. In addition if MG9K EM components are present, these SSPFS-based machines continue to run on T1400(s) with the new SN07 software.

It should be noted in the figure that other patchable components may exist but are not shown to reduce the complexity of the diagram. In addition, the MG9K EM components running on 1 T1400 in the figure may run on separate T1400s. The components not listed in the figure may include:

- optional QCA application running on the T1400 that communicates with the PSE local to the T1400
- the CBM component being introduced in SN07 may be installed on the N240 along with the NPM and IEMS

Existing CS2M with T1400

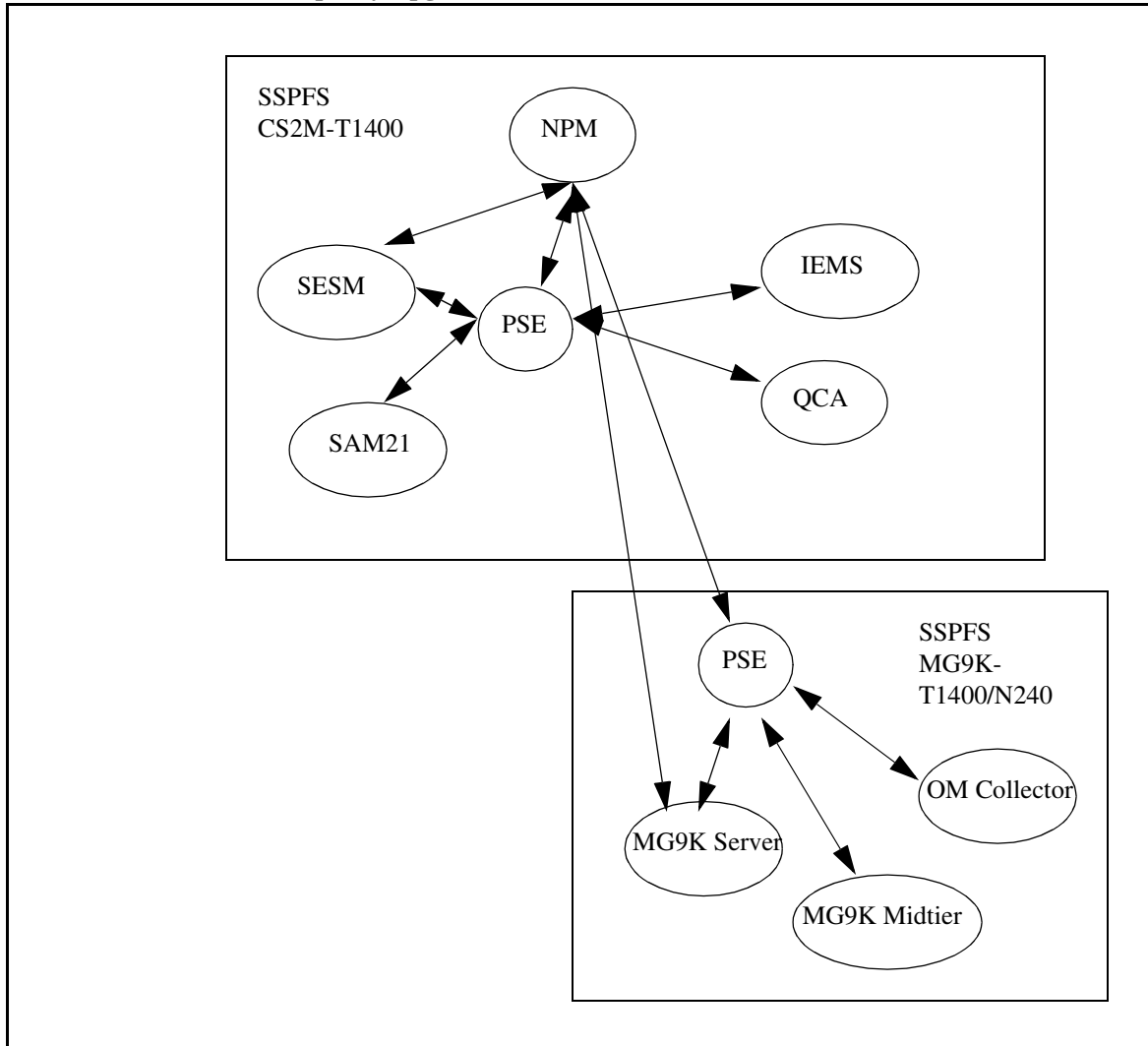


The following steps are required during the upgrade process in this configuration:

- the new N240 machine is commissioned with the SN07 versions of the IEMS and NPM installed on the machine
- the CS2M machine is upgraded to SN07, this process consists of the following:
 - the PSE on the CS2M T1400 machine is configured to look at the CORBA name service on the new N240 machine
 - the SESM application is upgraded, the EPM component within SESM now looks at the name service hostname associated with the local PSE to find the location of the NPM (this step ensures the GWCs associated with the EPM are registered with the new NPM)
 - the NPM is not upgraded in the CS2M T1400 machine (i.e. effectively it is uninstalled)
- the MG9K machine (if present) is upgraded to SN07, this process consists of the following:
 - the PSE on the MG9K-based T1400 machine(s) are configured to look at the CORBA name service on the new N240 machine
 - the MG9K components are upgraded, the EPM component within the MG9K-server component now looks at the name service hostname associated with the local PSE to find the location of the NPM (this step ensures the MG9K-based cards associated with the EPM(s) are registered with the new NPM)

Existing CS2M gets a Capacity Upgrade

In this configuration, an existing CS2000 customer site has software that is being upgraded from pre-SN07 software to SN07 software and also has hardware that is being upgraded from a T1400 to an SN240. With this scenario, the IEMS component is loaded into the existing CS2M machine. Hence, there is only one place where the NPM can reside. The following figure shows this configuration. Optionally shown in the figure is an MG9K-based machine that can run on a T1400 or N240 machine. Regardless of the number of MG9K-based machines or hardware, the NPM and PSEs are configured in the same way.

CS2M Capacity Upgrade

The following steps are required during the upgrade process in this configuration:

- the CS2M T1400 machine is upgraded to an N240 machine
- the SSPFS software on the N240 machine is upgraded to SN07
 - SSPFS software is upgraded
 - the PSE on this machine is upgraded to SN07 (since the NPM and PSE will co-reside on this box, no configuration of a CORBA name service host is necessary on this machine)
 - the old version of NPM is unloaded and the SN07 version is loaded
- IEMS is installed on the N240
- CBM is installed on the N240

- the remainder of the applications on the CS2M machine are upgraded to SN07
- the MG9K machine(s) (if present) are upgraded to SN07, from a patching perspective there are no modifications to the existing upgrade procedure

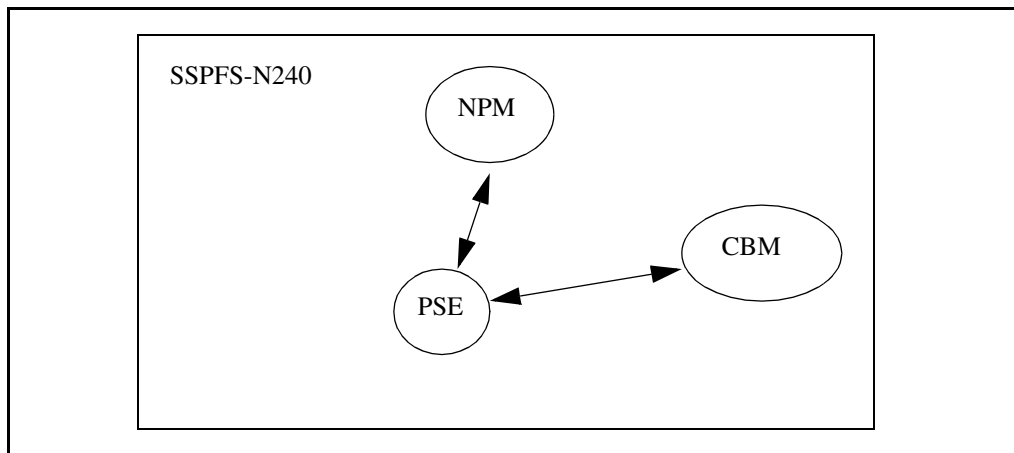
New CS2M Office gets an N240

This scenario is similar to the configuration in Figure , on page 2231 . The only difference is this scenario is a 'new install' instead of an upgrade. The following steps are required during this 'new install' process:

- the SSPFS SN07 software on the N240 machine is installed
 - SSPFS software is installed
 - the SN07 PSE on this machine is installed (since the NPM and PSE will co-reside on this box, no configuration of a CORBA name service host is necessary on this machine)
 - the SN07 NPM is installed
- IEMS is installed on the N240
- CBM is installed on the N240
- the remainder of the applications on the CS2M machine are installed with SN07 software
- the MG9K machine(s) (if present) are installed with SN07 software, from a patching perspective there are no modifications to the existing installation procedure

TDM/Wireless

Beginning in SN07, existing TDM/wireless customers will be receiving an N240 SSPFS-based machine to handle CBM (SDM in the AIX-based configuration) instead of the SDM (Supernode Data Manager). Since there is only one SSPFS-based machine in this configuration, the NPM can only reside on this machine. In SN07 the process of receiving the new N240 machine is treated as a new install from a patching software perspective since the NPM and PSE components did not exist in this configuration prior to SN07. The following figure shows this configuration.

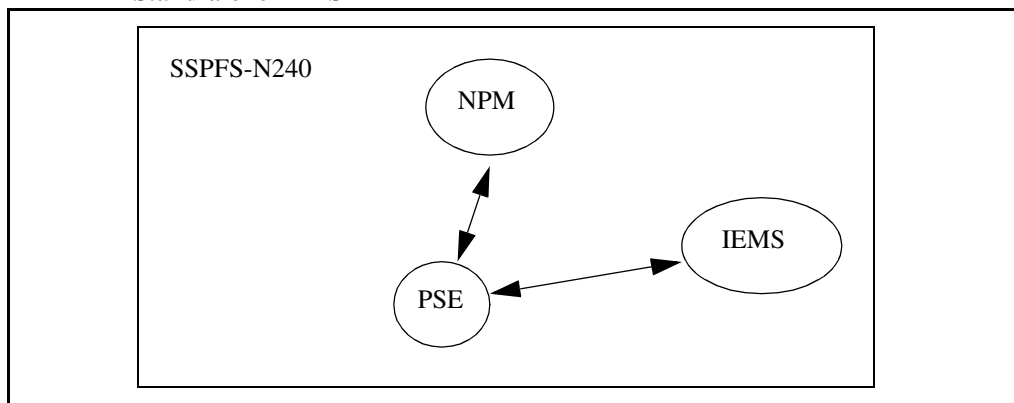
TDM/Wireless Installation

The following steps are required during this 'new install' process:

- the SSPFS SN07 software on the N240 machine is installed
 - SSPFS software is installed
 - the SN07 PSE on this machine is installed (since the NPM and PSE will co-reside on this box, no configuration of a CORBA name service host is necessary on this machine)
 - the SN07 NPM is installed
- CBM is installed on the N240

Stand-alone IEMS

Beginning in SN07, a stand-alone IEMS configuration is supported. This configuration is similar to section "TDM/Wireless" from a patching software perspective as it is a 'new install'. Since there is only one SSPFS-based machine in this configuration, the NPM can only reside on this machine. The following figure shows this configuration.

Stand-alone IEMS

The following steps are required during this 'new install' process:

- the SSPFS SN07 software on the N240 machine is installed
 - SSPFS software is installed
 - the SN07 PSE on this machine is installed (since the NPM and PSE will co-reside on this box, no configuration of a CORBA name service host is necessary on this machine)
 - the SN07 NPM is installed
- IEMS is installed on the N240

Only One NPM

There should only be one NPM server installed in each site. This feature attempts to ensure only one NPM is installed via the following ways.

- SSPFS profiles
No NPM should be installed on an MG9K-based machine. An NPM is preferred to be installed on the IEMS-based machine.
- verification of the PSE NS hostname when the NPM server is started
When the PSE is configured, the configuration step asks for the hostname/ip address of the NPM server location. This feature modifies the NPM server to look at that configuration value. If the value is ever different from the local machine, the NPM fails to start.

While these steps help prevent more than one NPM from being installed, it is not a guarantee that it will prevent the scenario from occurring.

Patching Maintenance

When the new NPM patchable applications are installed (CBM, SSPFS, and IEMS), the NPM automatically becomes aware of the components. These components appear in reports and the device list of the GUI. The following functions that exist for other targets in previous releases are now available for IEMS, CBM, and SSPFS.

- apply
- remove
- audit
- restart (IEMS only)
- set/report creation
- plans/automation
- alarms

IEMS

Similar to the existing OAM Java-based applications like SESM, SAM21EM, and MG9K EM components, the IEMS requires 2 steps for application and 2 steps for removal of patches.

application

- apply command from the NPM GUI or CLUI (sets patch to applied/disabled)
- restart command from the NPM GUI or CLUI on IEMS (sets patch to applied/enabled)

removal

- remove command from the NPM GUI or CLUI (sets patch to removed/enabled)
- restart command from the NPM GUI or CLUI on IEMS to disable the patch (sets patch to removed/disabled)

Beginning in SN06.0, the restart operation from the NPM GUI and CLUI can be automatically scheduled via NPM plans (autorestart). This capability is similar to the automatic application of patches.

SSPFS and CBM

Patches that are created and require application to the SSPFS and CBM components require one step from the NPM GUI or CLUI. Likewise for the removal operation. A single apply command or remove command from the NPM GUI or CLUI is sufficient for complete application or removal. If the associated application requires a restart or recreation of an existing process for application or removal, the 'restart' action is initiated during the single apply or remove request.

In some cases, an SSPFS or CBM patch may require additional action outside of the NPM GUI or CLUI for complete application or removal. In these cases, the patch is marked as non-autoapplicable and contains special application instructions that describes the extra actions that are required.

For application of these patches, the patch appears as applied/disabled after the NPM apply command from the NPM GUI/CLUI. The extra actions described in the special application instructions automatically trigger the patch to become applied/enabled when the actions have been successfully completed. This behavior is also applicable for the remove scenario.

Full Matrix

The following table shows a complete list of patchable applications/devices that are supported by the NPM in SN07. The table indicates the necessary

commands required to fully apply or remove patches and whether automation is supported.

Target/Command Matrix

	Full Application		Full Removal			
Target	Apply Cmd Required	Restart Cmd Required to enable	Remove Cmd Required	Restart Cmd Required to disable	autoapply supported	autorestart supported
MG9K Cards (OC3, SCI, SCO, ITP, ITX, DS1, ABI)	yes	no	yes	no	yes	n/a
GWC Cards	yes	no	yes	no	yes	n/a
SESM	yes	yes	yes	yes	yes	yes
SAM21 EM	yes	yes	yes	yes	yes	yes
NPM	yes	yes	yes	yes	yes	yes
PSE	yes	yes	yes	yes	yes	yes
QCA	yes	yes	yes	yes	yes	no
MG9K server	yes	yes	yes	yes	yes	yes
MG9K midtier	yes	yes	yes	yes	yes	yes
OM Collector	yes	yes	yes	yes	yes	yes
IEMS	yes	yes	yes	yes	yes	yes
SSPFS	yes	no ^a	yes	no ^a	yes	n/a
CBM	yes	no ^a	yes	no ^a	yes	n/a

a. In some cases SSPFS or CBM patches may require reboot of applications or machines. These patches are marked as non-autoapplicable and require human intervention.

Patch File Format Modifications

For the NPM to track different software with various behaviors, the patch file format is modified with this feature. While the specific details of the patch file format are not in this section, they can be found in the CN document associated with this feature.

Patch Calculation for CBM and SSPFS Patches

Prior to SN07, all NPM-based patching uses a loadname associated with a given device or application to perform patch calculation in determining what patches calculate for any given office. All previous SN07 patch types will continue to use the loadname for calculation purposes.

Beginning in SN07 with this feature, CBM and SSPFS patches that are tracked by the NPM use a new record in addition to the loadname. A functional component record (fc) is introduced into the patch file and the NPM database. This new record is tracked against CBM/SSPFS patches and CBM/SSPFS applications.

The NPM ‘getpatch’ command and ‘apply’ command are updated with this feature to check for the presence of functional component records in a patch file. If these records are present, the records are compared against the fc’s associated with the devices in the office in addition to the loadname. Both the loadname and functional component records must match for the given patch to calculate for the office.

QCA Patches with Autorestart=“n”

The optional QCA application became patchable via the NPM beginning in SN06.0. With this feature and the patch file format modifications, all QCA patches have the autorestart flag set to ‘n’ by default. This modification is necessary to ensure that the QCA application does not lose service by virtue of an NPM automated task triggering the action. As the QCA application tracks critical customer data, the prevention of unforeseen data is paramount.

Applicable customer facing sections

Fault Management

Not applicable	<u> X </u>
Logs	<u> N/A </u>
Alarms	<u> N/A </u>

Configuration

Not applicable	<u> </u>
Data Schema/MIBs	<u> X </u>
User Interface	<u> X </u>

GUI	<u> N/A </u>
Element Management	<u> N/A </u>
Security	<u> N/A </u>
Service Order	<u> N/A </u>
Office Parameters	<u> N/A </u>
SOC	<u> N/A </u>
Upgrades impact	<u> X </u>
Accounting (includes AMA billing)	<u> </u>
Not Applicable	<u> X </u>
Billing changes	<u> </u>
Performance	<u> </u>
Not Applicable	<u> X </u>
Operational Measurements	<u> </u>
Performance Measurements	<u> </u>

Hardware Requirements or Dependencies

None.

Software Requirements or Dependencies

None.

Limitations and restrictions

Please refer to “ Only One NPM” on page 2234 for limitations on preventing more than one NPM being installed in a site.

Interactions

A00003615 - SSPFS Patching
A00002133 - CBM Patching

Product = SAM21 Element Manager

A00003562--New Cards Support in SAM21 EM (UA-IP)

Functional Description

The SAM21 Element Manager now allows the user to:

- Provision CentrexIP Client Manager application (also known as “CICM”) on a given MCPN5385 card
- Provision CICM Element Manager application (also known as “CICM-EM”) on a given MCPN5385 card
- Enable Provisioning Gateway Controller application (also known as “GWC”) on a given Force695 card

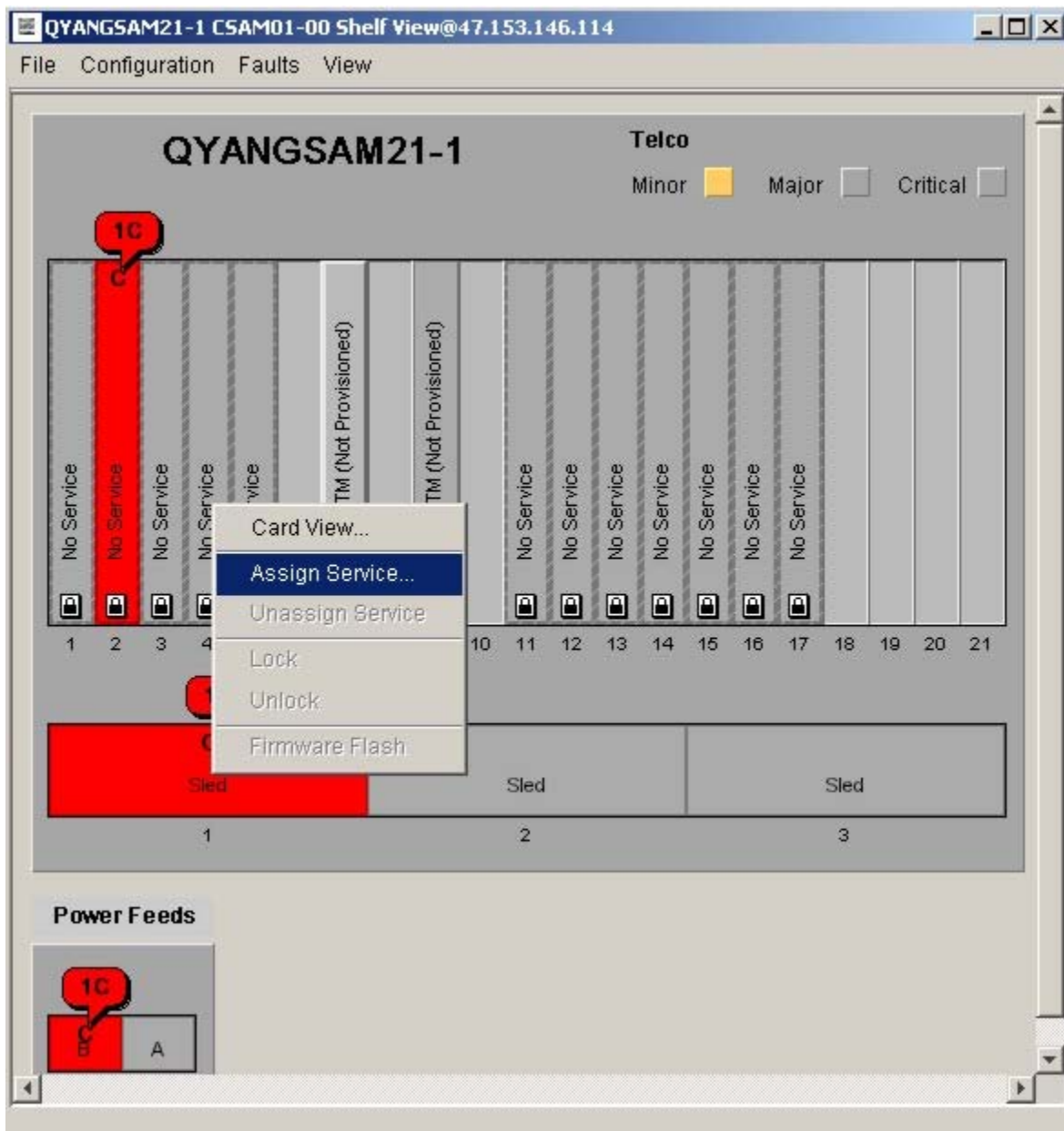
The SAM21 defines new provisioning panels for the new CICM and CICM-EM service respectively.

Before this writing, GWC application has been enabled provisioning on MCPN750 or MCPN750a card. And now they should also be supported on the Force695 card.

Provision CICM Service On a MCPN5385 card

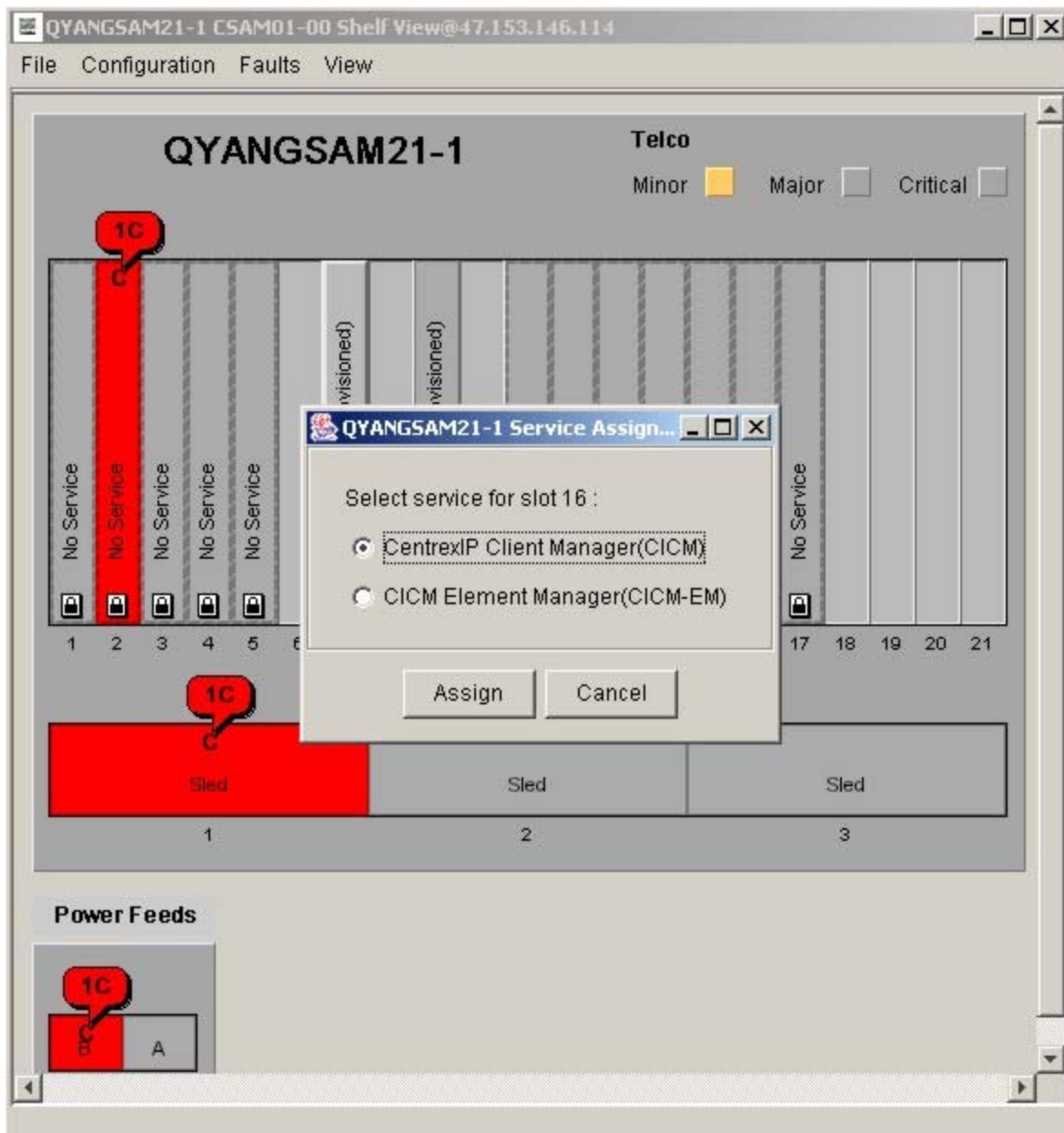
Assign Service

The SAM21 EM mechanism to provision service on a card has not changed. When displaying the shelf view, the user can right click on a card to view the Card Popup Menu. If the card currently is not assigned a service, the user can select “Assign Service ...” from this menu.



When the user selects “Assign Service...”, the SAM21 EM displays the Service Assignment popup window. Based on the card’s hardware (model type and memory), the SAM21 EM determines the set of services that can be assigned to the card and allows the user to choose one of them.

The CICM service can be assigned to a MCPN5385 card.



When the user selects the listed “CICM” service and then clicks “Assign”, the SAM21 EM displays a CICM service provisioning panel.

CICM Provisioning Panel

The CICM Provisioning Panel displays the following fields. Fields in *italics* are automatically filled in for the user. A picture of the CICM Provisioning Panel follows.

- **IP:** The IP address of the MCPN5385 card.
- **Router IP:** The IP address of the card's router.
- **Subnet Mask:** The card's subnet mask.
- **FW Version:** The card's firmware version, will be set to "Not reported" by shelf controller.
- **MAC Address:** The MAC addresses of the MCPN5385 card, need manual input.
- **Instance ID:** The instance integer identifier of the CICM card, and applies to both CICM and CICM-EM.
- **UNIT ID:** 'A' or 'B', identifies the two units of a CICM/CICM-EM pair.
- (Load Info) **Server IP:** The IP address of the server (SDM) containing the CICM software load.
- (Load Info) **Path:** The server's directory that contains the CICM software load.
- (Load Info) **Load:** The file name of the CICM software load.
- (Load Info) **Boot File:** The file name of the CICM Linux bootstrap, distributed with the boot server.
- **FW Flash Enable:** Check this box to enable firmware flash on the card. Now Disabled.
- **CICM-EM IP:** The IP address of the CICM-EM, for CICM only.

QYANG-1 Slot 16 CardView@47.153.146.202

File View

QYANG-1 : Slot 16

Alarms Equip States Provisioning

General

IP: 3.3.3.16 Router IP: 3.3.3.1

Subnet Mask: 255.255.255.0 FW Version: Not Reported

MAC Address: 123456789016 Instance ID: 5

Unit ID: A

CICM-EM

Host IP: 3.3.3.8

Load Info

Server IP: 3.3.3.9

Path: /swd/cicm1.0

Load: cicm.zip

Boot File: cicmlinuxbootstrap

☐ FW Flash Enable

Modify Save Clear Cancel Details... Help

Provisioning Rules

Two CICM/CICM-EM cards (card A and B) form a pair to provide redundancy. When provisioning a mated pair of CICM cards, the user can provision the cards in either order. For example, "CICM-110-A" and "CICM-110-B" form a CICM pair.

There is no existing relationship between the IP addresses of the CICM/CICM-EM pair. And there are no active and inactive IP addresses (like the GWC) for CICM card.

Some provision information, including load info, subnet, router, and EM address, should be the same between the CICM/CICM-EM pair. But it is not mandatory. If the craftsperson provides different datafill, the SAM21 EM will prompt a warning message for confirmation.

The CICM/CICM-EM Provisioning Panel verifies the following provisioning rules:

- At most two CICM/CICM-EM cards can be provisioned with the same instance ID, each CICM/CICM-EM pair has a unique instance ID.
- Each MAC address of a CICM/CICM-EM card must be unique among all the cards on SAM21 shelf.

When the user changes the datafill for an existing CICM card, the SAM21 EM performs the change and then displays the following message to the user: “The datafill for this CICM card has been changed. Please ensure that the card’s mate uses the same datafill.”

Maintenance Behavior

This section considers the behavior the user should see when the user attempts a maintenance action on a card provisioned with the CICM service.

- If the user attempts to lock the inactive CICM card, the SAM21 EM immediately attempts to lock the card.
- If the user attempts to lock the active CICM card, the SAM21 EM client displays the following message: “WARNING: This is the active CICM unit. Locking the active unit will cause a service outage. Contact next level NT support before continuing. Do you wish to proceed with the lock?” If the user clicks “Yes”, then the SAM21 EM immediately attempts to lock the card.
- If the user attempts to unassign service to an CICM card, the SAM21 EM client displays the following message: “WARNING: Unassigning service to the card in slot x decommissions one of the processor units of CICM node. Do you wish to proceed?”. If the user clicks “Yes”, then the SAM21 EM unassigns service.

Card Replacement

Firstly the user removes a CICM/CICM-EM card from SAM21 EM shelf. Then a card is inserted into the same slot, it will be auto-provisioned with the same provisioning data as the previous card in that slot, so the MAC address will be the old MAC.

Several scenarios are described here:

- If the craftsperson reseated the same card, he needn’t to take further action.
- If the craftsperson replaces the card with a different one, then he needs to reprovision its MAC address. If the craftsperson doesn’t reprovision the MAC address, the card will fail to boot.
- If the craftsperson exchanges two cards in the same shelf or from different shelves, for example, card A in slot 1, card B in slot 2. After exchange, card A is in slot 2, card B is in slot 1. Card A will be auto-provisioned as card

B, card B auto-provisioned as card A. If the user does not reprovision them accordingly, the two cards will not work properly after booted.

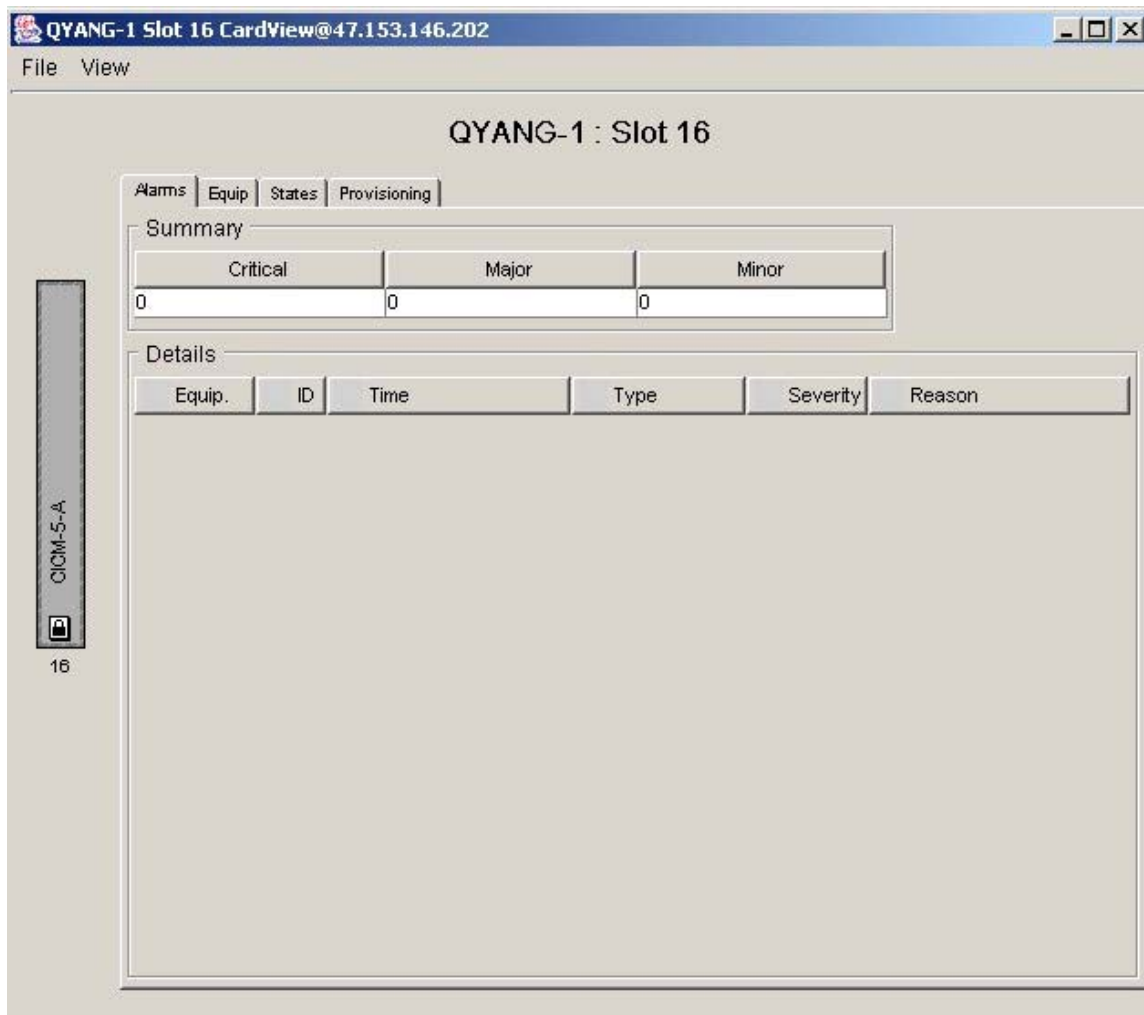
The craftsperson must reprovision the MAC address after card replacement. It is recommended that when replace the card with a different one the user unassigns service from CICM card before removal.

If the craftsperson wants to reinsert a CICM card into a different slot, he must reprovision its MAC address to a dummy one, such as “aaaaaaaaaaaa” before removal, then he can insert it into another slot. Otherwise, he will get an error message stating that the mac address has been reserved by the previous slot.

Card View

Out-of-Service Diagnostics (OOS Diags) for the CICM hardware is not supported in SN07. So the diagnostics tab will not appear on CICM card view.

A picture of the CICM Card View follows.



Popup Menu for CICM card

Firmware flash for the CICM hardware is not supported in SN07. When the user right-clicks on the CICM card item on the shelf view, a popup menu will appear, but the “firmware flash” menu item is disabled.

A picture of the CICM Card popup menu follows.



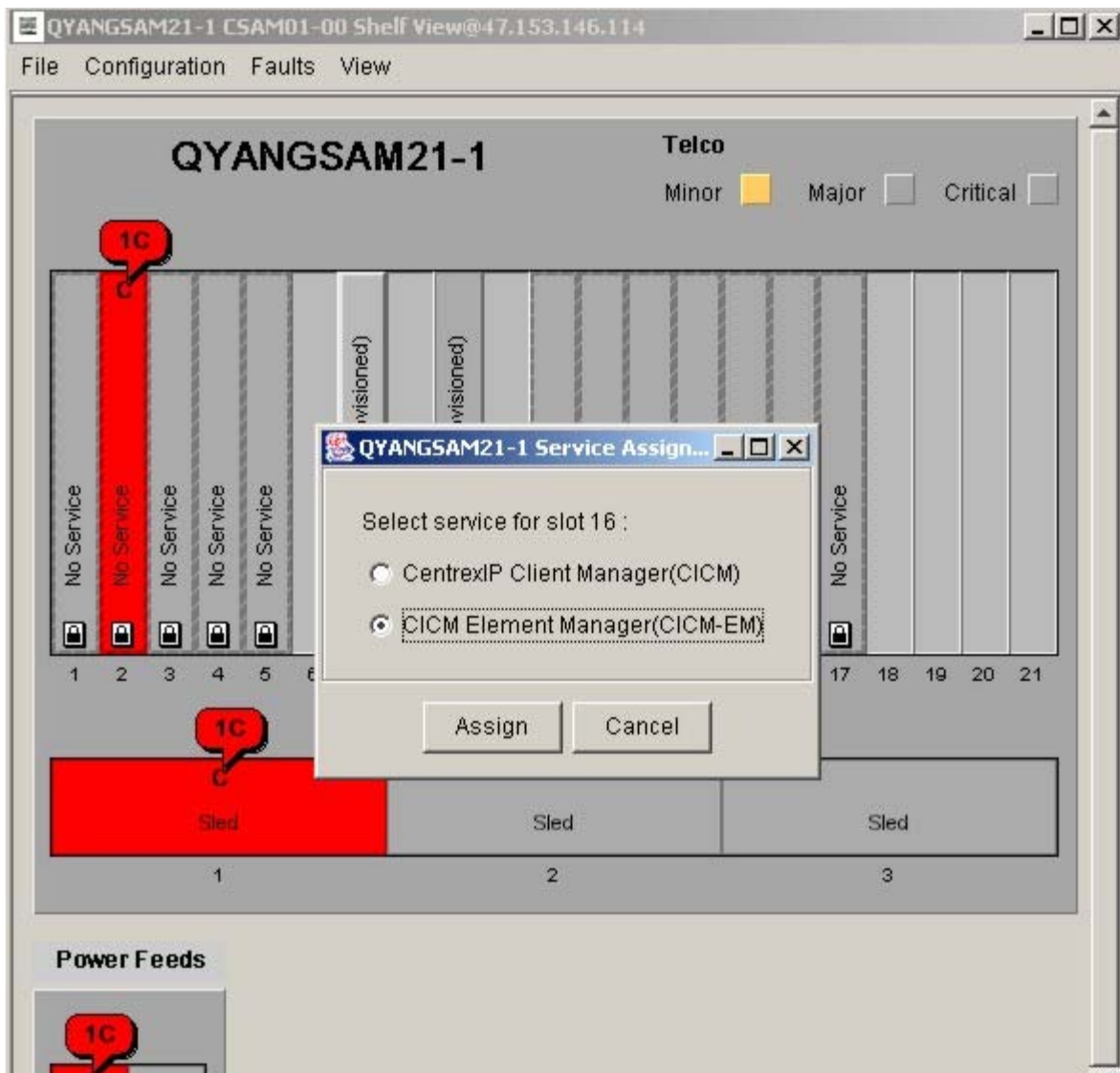
Provision CICM-EM Service On a MCPN5385 card

The CICM-EM is different from CICM card on its provisioning panel. The other aspects, such as maintenance, provisioning rules, etc., is the same as CICM card.

Assign Service

When the user selects “Assign Service...” on a MCPN5385 card, the SAM21 EM displays the Service Assignment popup window.

The CICM-EM service can be assigned to a MCPN5385 card.



When the user selects the listed “CICM-EM” service and then clicks “Assign”, the SAM21 EM displays a CICM-EM service provisioning panel.

CICM-EM Provisioning Panel

The CICM-EM Provisioning Panel displays the following fields. Fields in *italics* are automatically filled in for the user. A picture of the CICM-EM Provisioning Panel follows.

- **IP:** The IP address of the MCPN5385 card.
- **Router IP:** The IP address of the card’s router.
- **Subnet Mask:** The card’s subnet mask.

- **FW Version:** The card's firmware version, will be set to "Not reported" by shelf controller.
- **MAC Address:** The MAC addresses of the MCPN5385 card, need manual input.
- **Instance ID:** The instance integer identifier of the CICM-EM card
- **UNIT ID:** 'A' or 'B', identifies the two units of a CICM/CICM-EM pair.
- (Load Info) **Server IP:** The IP address of the server (SDM) containing the CICM-EM software load.
- (Load Info) **Path:** The server's directory that contains the CICM-EM software load.
- (Load Info) **Load:** The file name of the CICM-EM software load.
- (Load Info) **Boot File:** The file name of the CICM-EM Linux bootstrap, distributed with the boot server.
- **FW Flash Enable:** Check this box to enable firmware flash on the card. Now not supported.

The screenshot shows a web-based configuration interface for a Nortel device. The title bar reads "QYANG-1 Slot 13 CardView@47.153.146.202". The interface has a menu bar with "File" and "View". Below the menu bar, the title "QYANG-1 : Slot 13" is displayed. There are four tabs: "Alarms", "Equip", "States", and "Provisioning", with "Provisioning" being the active tab. On the left side, there is a vertical sidebar with a slot indicator showing "13" and a label "CICM-EM-5-B". The main content area is divided into two sections: "General" and "Load Info".

General

IP:	3.3.3.13	Router IP:	3.3.3.1
Subnet Mask:	255.255.255.0	FW Version:	Not Reported
MAC Address:	123456789112	Instance ID:	5
Unit ID:	B		

Load Info

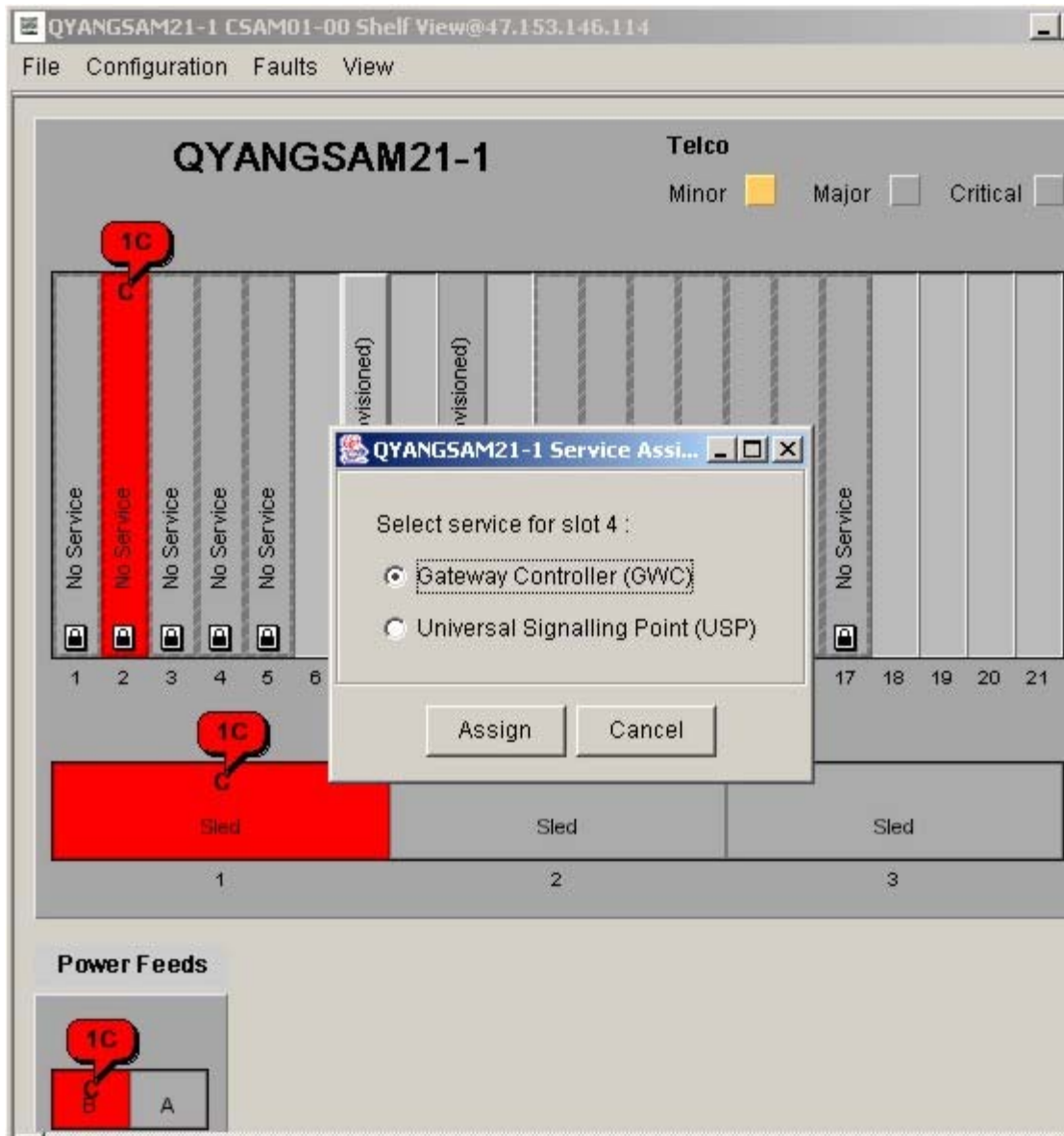
Server IP:	3.3.3.8
Path:	/swd/cicmem1.0
Load:	cicm-em.zip
Boot File:	cicmemlinuxbootstrap
☐ FW Flash Enable	

At the bottom of the main content area, there are six buttons: "Modify", "Save", "Clear", "Cancel", "Details...", and "Help".

Enable Provisioning GWC Service On a Force695 card

When the user selects "Assign Service..." on a Force695 card, the SAM21 EM displays the Service Assignment popup window.

The GWC service can be assigned to a Force695 card that reports 1GB of memory.



When the user selects the listed “GWC” service and then clicks “Assign”, the SAM21 EM displays a GWC service provisioning panel.

GWC Provisioning: QYANGSAM21-1 Slot 4

General

IP: 47.123.45.6 Gateway IP: 47.123.45.1

Subnet Mask: 255.255.255.0 FW Version: N

MAC Address: 0001af01ddde GWC Number: 67

NTP

Primary NTP: 47.140.160.111

Secondary NTP: 47.140.160.112

GWC-EM

Host IP: 47.153.146.114

Load Info

Server IP: 47.142.35.16

Path: /swd/gwc

Load: 9.000.01.1

☒ FW Flash Enable

Domain Servers

Primary: 0.0.0.0 1st Alt: 0.0.0.0

2nd Alt: 0.0.0.0

Because the existing GWC provisioning requirements are unchanged in this feature, they are not described in detail here.

Glossary

Acronym	Definition
EM	Element Manager
CICM	CentrexIP Client Manager
CICM-EM	CentrexIP Client Manager's Element Manager
SAM	Service Application Module

SC	Shelf Controller
SDM	Succession Data Manager
SSPFS	Succession Server Platform Foundation Software
GWC	Gateway Controller

Product = TOPS

A00002740 -- TOPS International DA Call Completion (Succession on DMS)

Functional Description

This feature allows DA calls with an international requested number to be completed using manual DA Call Completion (DACC) or Automated DACC (ADACC).

Overview

TOPS needs an international indicator to process a called number as international/overseas. When a call is signalled with an international called number, there is either a prefix or parameter to indicate international. When an international called number is entered by an operator at position, a functions key is first entered to indicate the number is international. Currently, when TOPS receives a requested number from the DA Service provider (DAS), it is assumed to be domestic (or local). This feature requires the DAS to provide a predetermined international indicator along with an international requested number. Thus, the **DAS must be upgraded** prior to activating this feature.

This feature enhances TOPS to look for the international prefix on requested numbers from the DAS. When found, TOPS will translate the requested number as international for call completion.

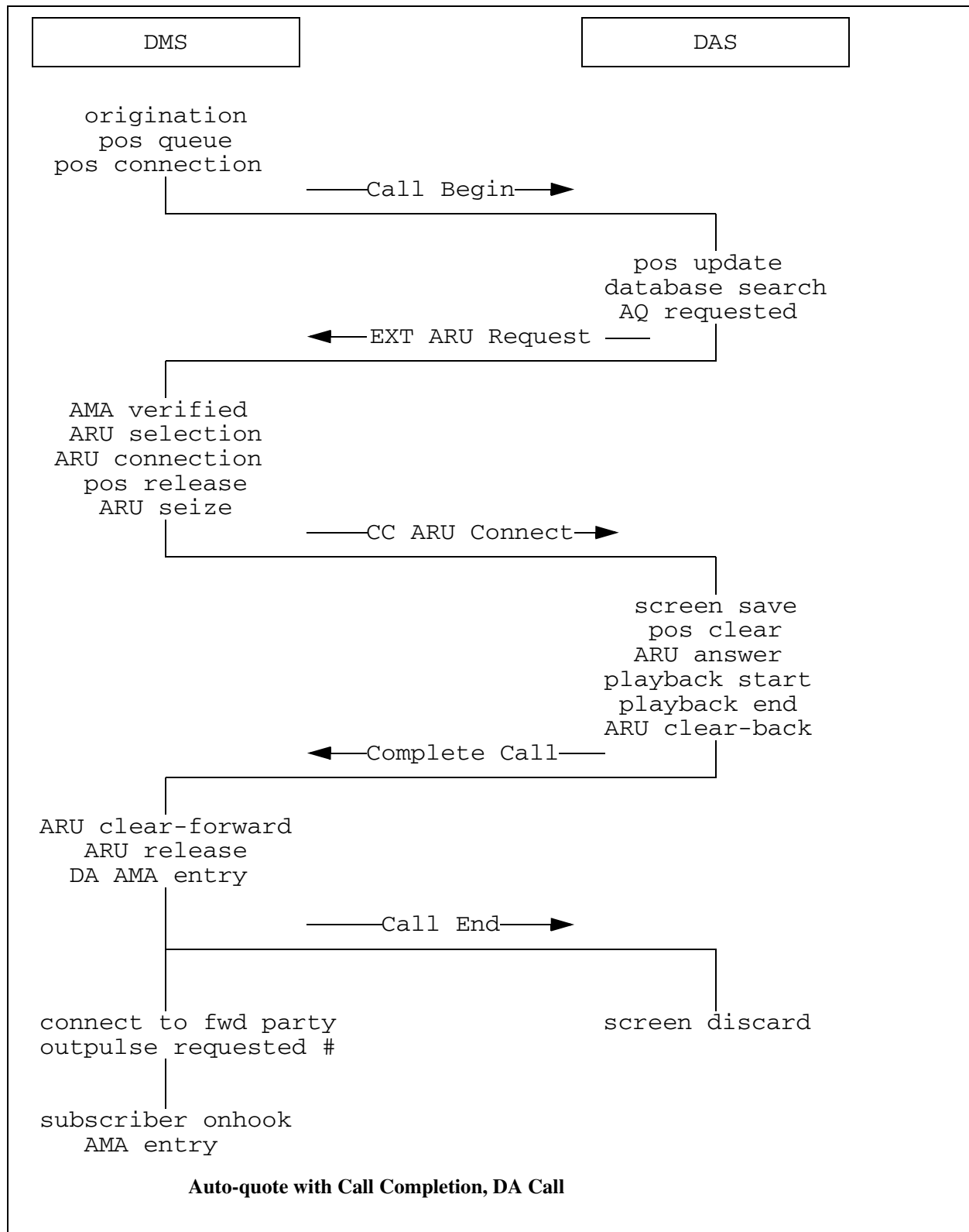
Since this feature is dependent upon DAS changes, there are a variety a scenarios which can or cannot be supported based on the level of DAS support. For full IDACC support, ensure the vendor supports the international prefix in all messages which contain the requested number.

The initial release of this feature only supported the ADACC scenario as documented in a00002740.aa01; these limitations have been reproduced in an appendix of this document. A second release (a00002740.aa02) added the ability to restrict overseas ADACC by adding it to table TDBDAOPT. This version captures the full functionality TOPS can provide for IDACC calls.

IDACC Callflow using ADACC

International listing numbers are supported via an international indicator prepended to the listing number. This international prefix indicator is datafillable via a new parameter in TOPSPARM, as described later in this document.

When TOPS receives a listing number from the DAS with the pre-determined international prefix, the listing is treated as an international number. The following callflow illustrates the ADACC scenario, and notes the IDACC specifics below.



In the EXT ARU Request message, the DAS sends the international indicator, the country code, and the listing number (prefix+CC+listing). TOPS recognizes the international prefix and records the listing number as international. The prefix is then removed from the listing to enable existing translations to be used.

When the Complete Call message is received, TOPS will generate a DA AMA record¹ with the requested number showing the country code and listing number. It will also contain an international indicator.

```
*HEX ID:AA  STRUCTURE CODE:40106C  CALL CODE:194C  SENSOR TYPE:036C
SENSOR ID:0000000C  REC OFFICE TYPE:036C  REC OFFICE ID:0000000C
DATE:30410C  TIMING IND:00000C  STUDY IND:0200000C  SERVICE OBSERVED:0C
SIG DIGITS NEXT FIELD:010C  ORIG OPEN DIGITS 1:01036321005C
ORIG OPEN DIGITS 2:FFFFFFFFF  ORIGINATING CHARGE INFO:FFFF
CONNECT TIME:0854090C  ELAPSED TIME:000000112C  SERVICE FEATURE:000C
STATION SIGNALING IND:9C  SCREENING CODE:000C  CALLED NUMBER INPUT:1C
CALLING NUMBER SOURCE:1C  MODULE CODE:042C
CALL RECORD SEQUENCE NUMBER:0000035C  MODULE CODE:311C  ORIG CALL TYPE:036C
MODULE CODE:032C  OPERATOR IDS:1050915009999C
ACC OPERATOR WORK TIME:00060C  MODULE CODE:037C  LINE NUMBER TYPE:001C
DOMESTIC/INTL INDICATOR:2C  SIG DIGITS NEXT FIELD:011C
TERM OPEN DIGITS 1:10123444444C  TERM OPEN DIGITS 2:FFFFFFFFF
MODULE CODE:310C  KEYING ACTIONS:111111111C  MODULE CODE:055C
SERVICE ID:001C  MEANS OF INFORMATION INPUT:1C  MEANS OF LSDB ACCESS:1C
LSDBS BOC ID:12138C  LSDB ACCESSES:FF  LISTING RESPONSE:1C
LISTING STATUS:999999900C  REQUEST COUNTER:001C  MODULE CODE:104C
TRUNK FACILITY ID:102950000C  MODULE CODE:000C
```

TOPS can then utilize ADACC to complete the call if all ADACC checks pass.

In addition to existing ADACC checks in tables DABILL, DATRKOPT, ADACCOPT and ICNTRY (for direct routes to country), table TDBDAOPT includes a new option for International/Overseas calls. Thus, for IDACC calls to complete using ADACC, the ADACCSRV field of TDBDAOPT must include the new option, OVERSEAS, or be set to ALL.

1. This AMA structure is not changed by this feature; however, DA AMA records can now include the international indicator and country code. Although the country code is included with the listing number in the 'TERM OPEN DIGITS' fields, the number of country code digits is not specified for open numbering dialling plans for this 'new' DA record (194) nor for the existing call completion record (192).

Note: Please ensure existing datafill for table TDBDAOPT field ADACCSRV which is set to 'ALL' should be completing International/Overseas calls.

Table DOMBILL still enforces billing restrictions for domestic calls and table OVSBILL is now used for billing restrictions for international calls.

Table VROPT has a parameter, DACC_LOCAL_TOLL_ACTIVATION, in which international/overseas calls are now part of the TOLL and ALL options for this parameter.

Auto-collect as sent from the DAS also includes a TOLL/ALL option in which now include international/overseas calls.

When ADACC processing can be applied to the IDACC call, existing translations are performed using the operator FOREIGN entry in table IOPRTRAN.

If outpulsing to a SS7 ISUP trunk (ANSI or ETSI), the NOA of the IAM will contain 'international' as shown below.

```
OUTGOING 10:25:30.038  NODE TYPE= LTC_NODE
S512: ENCAP MS_CARD= 6 MS_PORT= 3  NODE= 4123
N= 001D  TN= 01CC  MSGTAG= 00  ROUTE= 101B  ERROR= 00  LENGTH= 2A
GENT= CKT      T915TO95ETSI    1
F 01 00 01 00 0A 03 0A 10 01 00 01 02 03 00 01 00 06 04 10 01 21 43 45 0A 07
3 10 01 63 23 01 50 00
```

CCS7 MESSAGE TYPE: ISUP_IAM

DATA BYTES:

```
00 01 00 0A 03 0A 10 01 00 01
02 03 00 01 00 06 04 10 01 21
43 45 0A 07 03 10 01 63 23 01
50 00
```

NATURE OF CONNECTION: ISUP_NO_SATELLITE, NO_ISUP_CONT_CHK
ISUP_NO_HALF_ECHO_SUP

FORWARD CALL INDICATORS:

ISUP_Call Type:	ISUP_INTERNATIONAL_CALL
E_to_E_Method:	NO_E_TO_E_METHOD_AVAIL
ISUP_Interworking:	NO_INTERWORKING
E_to_E_Info_Check:	NO_E_TO_E_INFO
ISDN_UP_Ind:	NOT_ISUP_ALL_THE_WAY
ISDN_UP_Pref_Ind:	ISDN_UP_PREF_ALL_THE_WAY
ISDN_Access_Ind:	ACCESS_NON_ISDN
Trans_Called_Num_Ind:	NUMBER_NOT_TRANSLATED
Routing_Attempt_Ind:	NO_ROUTING_ATTEMPT

CALLING PARTY CATEGORY: #0A - ISUP_CPC_SUBSCRIBER_1

MAND.VARIABLE PART: Generic Base USI:

TRANSMISSION MEDIUM REQ:	TMR_NIL
INFORMATION TRANSFER CAP:	GEN_ITC_SPEECH
CODING STANDARD:	STD_CCITT
INFORMATION TRANSFER RATE:	ITR_64KB
TRANSFER MODE:	MODE_CIRCUIT
LAYER1 INFORMATION:	LAYER1_G711_ALAW
USER RATE:	USER_RATE_NIL
SYNCHRONIZATION:	SYNCHRONE
NEGOTIATION:	NEGOT_NOT_INBAND

MESSAGE PRIORITY: 1

CALLED PARTY:

EVEN_ODD_IND : EVEN_NUM_NIBBLES

NATURE_OF_ADD : #04 - INTERNAT_NUMBER

NUMBERING_PLAN : ISDN_TELEPHONY_NUM_PLAN

ADDRESS_INFORMATION = 10123444

INTERNAL_NET_NUMBER : ALLOWED

OPTIONAL PART:

CALLING PARTY:

EVEN_ODD_IND: EVEN_NUM_NIBBLES

NATURE_OF_ADD : UNIQUE_NATIONAL_SIG_NUMBER

ADDR_PRES_RESTRICTED_IND : PRESENTATION_ALLOWED

NUMBERING_PLAN : ISDN_TELEPHONY_NUM_PLAN

SCREENING_IND : USER_PROVIDED_NOT_SCREEN

CLG_PTY_INCOMPL_IND : CALLING_PARTY_COMPLETE

ADDRESS_INFORMATION = 1036321005

When the call ends, the call completion AMA record is generated as shown below. No changes were made to this AMA record.

*HEX ID:AA STRUCTURE CODE:40106C **CALL CODE:192C** SENSOR TYPE:036C
SENSOR ID:0000000C REC OFFICE TYPE:036C REC OFFICE ID:0000000C
DATE:30410C TIMING IND:00000C STUDY IND:0200000C SERVICE OBSERVED:0C
SIG DIGITS NEXT FIELD:010C ORIG OPEN DIGITS 1:01036321005C
ORIG OPEN DIGITS 2:FFFFFFFFF ORIGINATING CHARGE INFO:FFFF
CONNECT TIME:0854304C ELAPSED TIME:000000052C SERVICE FEATURE:000C
STATION SIGNALING IND:9C SCREENING CODE:000C CALLED NUMBER INPUT:4C
CALLING NUMBER SOURCE:1C MODULE CODE:042C
CALL RECORD SEQUENCE NUMBER:0000036C MODULE CODE:316C LOCAL INDICATOR:1C
MODULE CODE:311C ORIG CALL TYPE:002C MODULE CODE:032C
OPERATOR IDS:1050915009999C ACC OPERATOR WORK TIME:00040C
MODULE CODE:033C **DOMESTIC/INTL INDICATOR:2C** SIG DIGITS NEXT FIELD:011C
TERM OPEN DIGITS 1:10123444444C TERM OPEN DIGITS 2:FFFFFFFFF
COMPLETION IND:001C RATE IND:7C OSS CALL COMPLETION CONDITIONS:1121710C
ALTERNATE ROUTE NUMBER:FFFF MODULE CODE:310C KEYING ACTIONS:221111111C
MODULE CODE:104C TRUNK FACILITY ID:102950000C MODULE CODE:000C

Enabling International DACC

In ISN07 and above loads, this feature is controlled by a SOC option and a TOPSFTR parameter. The intent is to only turn SOC on once and then use TOPSFTR to activate/deactivate the functionality.

SOC Option

SOC Option	
ENSV0108	DA Intl Call Compltn

ENSV0108 requires ENSV0101, OSB00101, OSDA0101, and OSDA0102.

Table TOPSFTR

FTRNAME	FTRENABL
International_DA_Call_Comp	Y

Table TOPSFTR can be set to Y to activate or N to deactivate.

The SOC option and TOPSFTR parameter can be set regardless of the other; however, a warning message will be generated if the other is not set as needed.

TOPSFTR parameter, `cellular_automatic_da_call_comp`, must also be set to Y to utilize table TDBDAOPT field ADACCSRV.

Defining the International_DACC_Prefix

The international DACC prefix is datafillable in table TOPSPARM. It contains the actual prefix digits (0-999). It can be 1, 2, or 3 digits.

Table TOPSPARM

PARMNAME	PARMVAL
INTERNATIONAL_DACC_PREFIX	00

This example datafill will mark requested numbers arriving with a '00' prefix as international. Thus, a requested number of 123456789 sent from DAS as 00123456789 will be translated as international. The 00 prefix will be removed, the 123 will be checked for a country code and the rest stored as the called number. International translations will be called using the country code and called number; the prefix is not used for translations.

Restricting ADACC Overseas calls

Table TDBDAOPT includes a field, ADACCSRV, which indicates the types of calls that can be completed via ADACC. It includes INTER, INTRATOLL, INTRALCL, ALL, and NONE. A new option, OVERSEAS, is added to the range. Thus, IDACC calls can be eligible for ADACC service if the datafill includes either OVERSEAS or ALL.

Table TDBDAOPT

TDBDAIDX	ADACCSRV	BILLOPT	ADASERV
0	ALL	ALL	N
1	INTRALCL	ALL	N
2	NONE	ALL	N
3	OVERSEAS	ALL	N
4	INTER, INTRATOLL, OVERSEAS	ALL	N

In the example, calls which index tuples 0, 3, or 4 are eligible for IADACC service.

Table TDBDAOPT is indexed by table TOPSDB, which can be indexed by tables DNSCRN, TOPEACAR, and COANISCR.

Note: ADACCSRV is only used for carrier calls. Thus, the call must be either an EA call (north american) or GCA call (international).

Manual DA Call Completion and Operator Functions

IDACC is supported for manual DA call completion at an TOPS operator position or OSSAIN Service Node (SN).

The international requested number can be obtained from either a DAS message or the operator/SN entering the requested number. For all cases, the international requested number must arrive to TOPS with the datafilled international prefix indicator.

Thus, the international prefix indicator must be prepended to the international requesting number in all DAS messages, when the operator enters the requested DN at position, or when the SN sends in a DN request. In all cases, TOPS will scan the requested number for the international prefix.

Note: This means TOPS operators and SN applications will need to be able to recognize an international listing and prepend the prefix for TOPS to treat the number as international. An operator must enter prefix+cc+number when entering an international requested number. SNs must send prefix+cc+number in the called DN update message.

When the international prefix is found, TOPS will treat the requested number as international/overseas and will utilize overseas tables such as OVSBILL instead of DOMBILL.

Note: The DA forward function available at some operator positions currently only supports domestic numbers. Since this function is intended for emergency calls only, there is currently no need to enhance this function to include international numbers. In addition, the DA forward function uses a called number for outpulsing; the IDACC feature is for requested numbers. If a requested number is entered prior to the DA forward function, then the requested number is overwritten.

Interactions

The following note the interactions with the existing DA system.

Local-Toll Activation

Table VROPT has a parameter, DACC_LOCAL_TOLL_ACTIVATION, which is used for activating call completion for local and/or toll calls. Currently, the parameter can be set to NONE, LOCAL, TOLL, ALL. NONE and LOCAL are not affected; however, the TOLL and ALL settings will now included International requested numbers.

Auto-Collect

Auto-collect is for business numbers which allow the subscriber to automatically bill collect. No verification is required for these collect calls. This option can be applied to the requested number in the DAS and sent to TOPS with the requested number. This functionality is currently provided with the following options: none, local, toll, all, and surcharge. All options remain the same except for the toll and all options. International requested numbers are now included in the toll and all auto-collect options.

Billing Restrictions

All existing DA and TA billing restrictions will be maintained with the addition of utilizing table OVSBILL for international requested numbers in comparison to table DOMBILL for domestic calls.

Invalid Country Code

Country codes must be datafilled in table CCTR to be valid. International requested numbers with invalid country codes can still be announced and generate an AMA record but cannot be completed. Calls with invalid country codes are not allowed to utilize ADACC and will be presented to an operator.

Direct and Alternate Routes

ADACC requires a direct route to complete international calls. If a direct route is not available, the call will be presented to an operator to select an alternate route, if available.

Software Requirements or Dependencies

This feature is dependent upon base TOPS and DA functionality being present and activated. It also requires the ADACC functionality.

ENSV0108 is the SOC option for this functionality. It requires ENSV0101, OSB00101, OSDA0101 and OSDA0102.

Limitations and restrictions

- Table TDBDAOPT field ADACCSRV is only for carrier calls.
- DA forward key function supports domestic/local numbers only. It has not been enhanced to support international numbers.
- This feature will remove the international prefix from the requested number so that existing translations can be used. It is not outpulsed nor included in any log or AMA record. The prefix is intended to only mark the call as international for translations and thus is removed for all other purposes. External listing announcements controlled by the DAS vendor may include the prefix in the announcement according to the vendor implementation. Contact DAS vendor for specifics.
- International Requested numbers will be treated as toll (same as Domestic numbers) for activation and auto-collect.
- ADACC requires direct routes to the country. If a direct route is not available, this feature is not supported.
- LNP is not supported in Global loads.

Glossary

Term	Description
IADACC	International Automated Directory Assistance Call Completion
ADACC	Automated Directory Assistance Call Completion

Appendix A for A00002740: International ADACC (IADACC)

Limitations

IADACC is described as the functionality and limitations provided by TOPS when the DAS vendor only supports the EXT ARU Request message for International DA Call Completion (IDACC).

For IADACC, TOPS **can** support the following:

- International Indicator recognition

- International DA AMA record generation
- Call completion to the international number based on TDBDAOPT

TOPS **cannot** support the following with IADACC:

- Manual DA call completion (DACC) - DA call which receives an international listing then the operator switches service to Toll to complete the call. This is not supported.
- Multiple Requests - DA call at position with international listing; GEN AMA for first listing; obtain second listing. This is not supported.
- Verbal quotes - Operator verbally quotes listing to subscriber and releases call. This is not supported.
- Recalls / Reconnects - DA call obtains listing and is released to announcement; call recalls back to position; if a GEN AMA, service switch or position release is performed then the call is not supported. (If a second listing is obtained, without gen ama for first listing, and is then released to announcement, the call can be supported.)
- Transfer with context scenarios are not supported.
- Alternate Routes are not supported since they require manual call completion which is not supported. Automated DA Call Completion (ADACC) requires direct routes.
- IADACC Error handling is limited since manual call completion is not available. Any scenario in which ADACC cannot service the international call is not supported.
- Any scenario utilizing DAS protocol messages - AMA transfer, Service Request, Position Request, and Position Release are not supported.

Product = TOPS

A00002765 -- Station Paid Routing (Succession on DMS)

Functional Description

This feature enhances the Unbundling Translations and Routing functionality by adding the ability to refine the XLAGRP based upon the calling service class and the billing method. With this feature, outgoing translations can now be applied specifically to a coin station-paid call.

The implementation of this feature allows the full range of calling service class and billing methods to be utilized in XLAGRP refinements. New table XLACCLASS allows XLAGRP refinements based on a range including coin, station, hotel, and restricted. New table XLABILL allows XLAGRP

refinements based on a range including paid, collect, third, cards, special calling, special called.

Background

In TOP09, AF7159 introduced the XLAGRP refinement mechanism for unbundling translations and routing. It created tables XLAGRP, XLASPID, XLAODIGS, and TOPSDP to setup the refinement structure including SPID² and originating digits.

Translations Group (XLAGRP) names are datafilled in table XLAGRP, which allows the operating company the ability to datafill various names to represent groupings for translation purposes as needed. These XLAGRP names are then used in the refinement tables to arrive at a final XLAGRP to be used in table TOPSDP (TOPS Dial Plan).

Table TOPSDP centralizes translation and screening attributes. The index into table TOPSDP is chosen in a flexible manner, giving the operating company the ability to fit their individual network needs. Obtaining an XLAGRP and indexing into table TOPSDP is referred to as the **XLAGRP** method of performing translations and screening for TOPS calls.

AF7159 provided an initial XLAGRP to be defined in table TOPSTOPT, which is indexed based on a trunk group. It also provided XLAGRP refinements for SPID and originating digits.

In TOP12, A59006822 enhanced the XLAGRP method with additional definitions for the initial XLAGRP and additional refinements. It allowed the initial XLAGRP to be defined in table TOPEATRK for EA calls and in table OPRINFO for operator calls. It also provided XLAGRP refinements for Carrier Identification Code (CIC) and EA region, which is based on either a LATA or a ZONE as defined by feature 59006827.

This feature supports all existing XLAGRP methods and enhances the refinement characteristics by adding calling service class and billing methods.

New XLAGRP Refinement Order

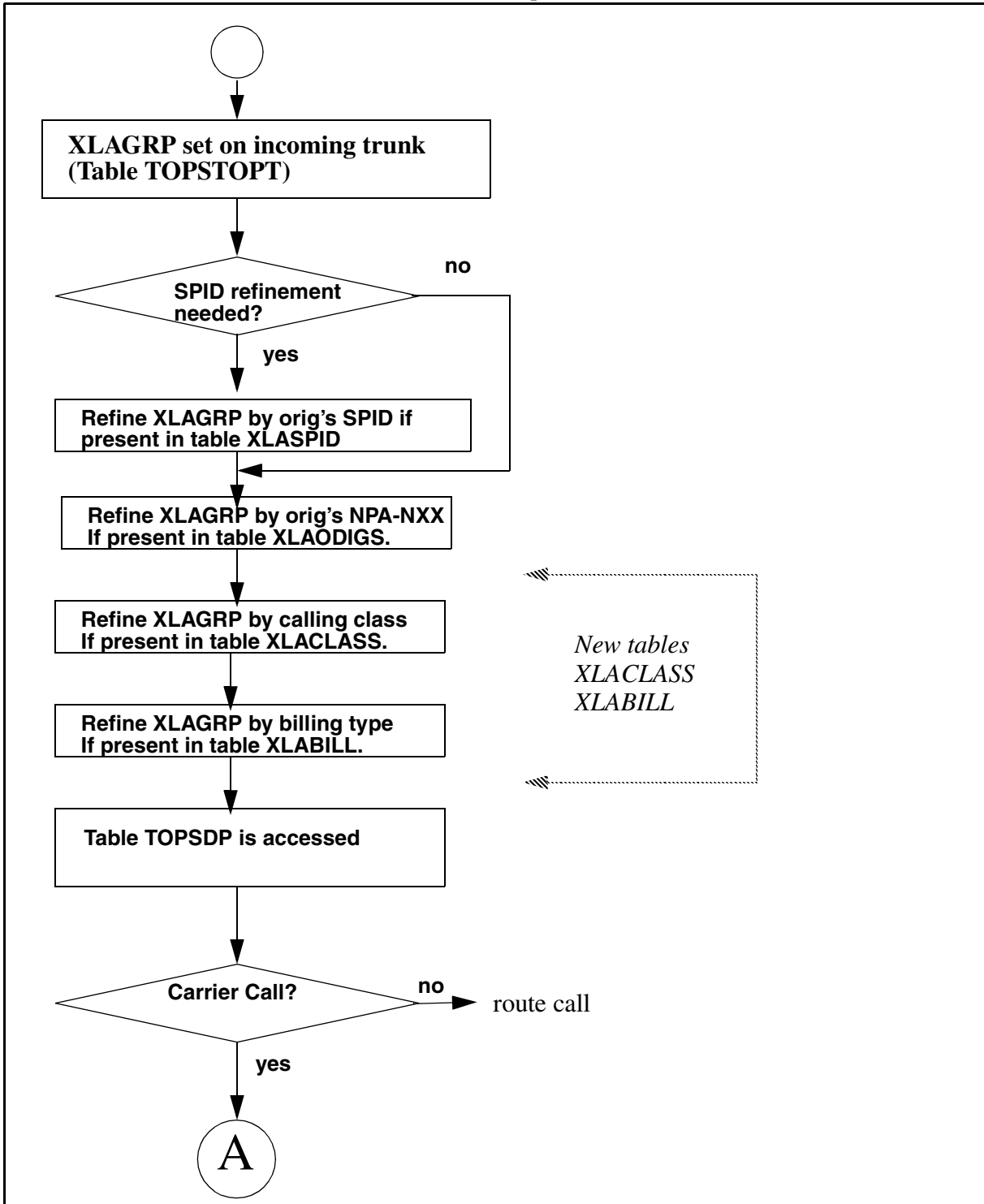
To preserve the existing XLAGRP refinement datafill, the new refinements are added at the end of the existing order list for non-EA calls. Thus XLACCLASS then XLABILL will refine after XLAODIGS. For EA calls, XLACCLASS and XLABILL will refine after XLAODIGS as well. Although this inserts the new refinement tables in the middle of refinement for EA calls, it saves the extra datafill needed in XLACCLASS and XLABILL to accommodate those XLACIC and XLAEAREG XLAGRPs.

2. Service Provider Identification

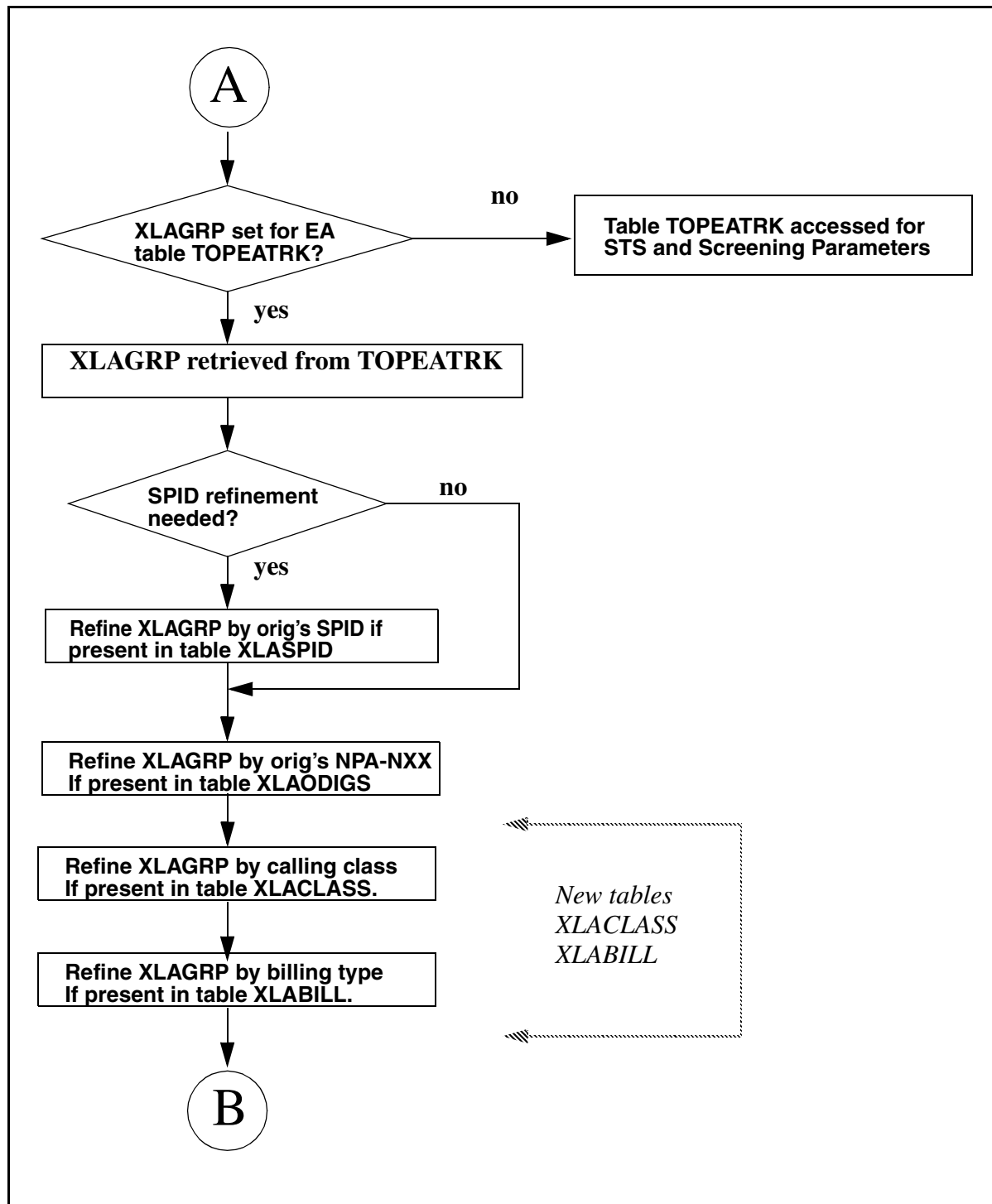
The following diagrams illustrate the existing XLAGRP refinement order with the new tables, XLACCLASS and XLABILL, included.

The figures below outline the refinement order for both EA and NON-EA calls:

XLAGRP Refinement Order NON Equal Access



XLAGRP Refinement Order For Equal Access Calls



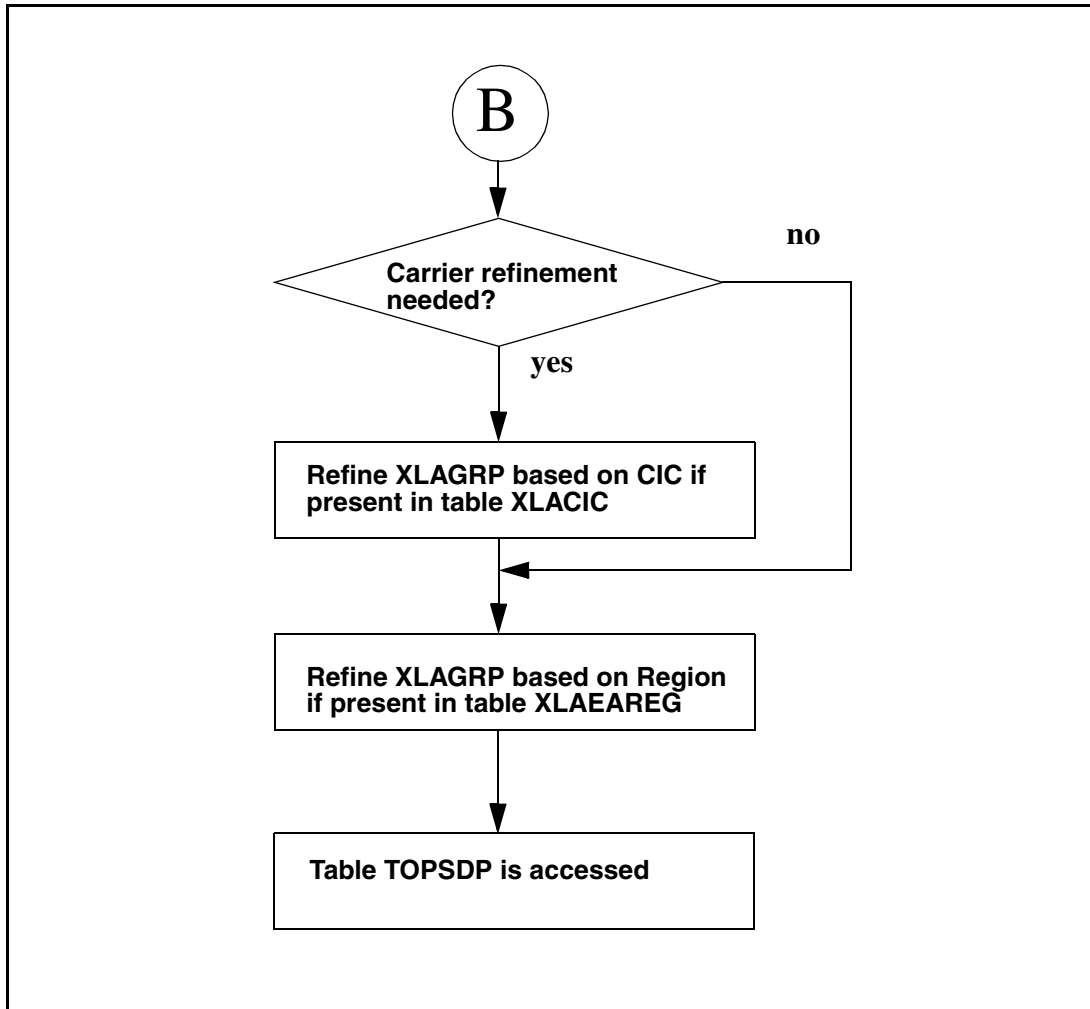
XLAGRP Refinement Order For Equal Access Calls

Table XLACCLASS

Table XLACCLASS allows the XLAGRP to be refined based upon the calling service class. The index of the table is the existing XLAGRP and the calling service class. It then provides a new XLAGRP if a match is found.

Example of Table XLACCLASS

XLAGRP	CLGCLASS	NEWXLAGRP
TRK1	COIN	TRK1COIN
TRK1	STATION	TRK1STA

The XLAGRP names in fields XLAGRP and NEWXLAGRP must first be datafilled in table XLAGRP.

Field CLGCLASS supports a range of {UNKNOWN, STATION, COIN, HOTEL, RESTRICTED}.

Table XLABILL

Table XLABILL allows the XLAGRP to be refined based upon the billing type. The index of the table is the existing XLAGRP and the bill type. It then provides a new XLAGRP if a match is found.

Example of Table XLABILL

XLAGRP	BILLTYPE	NEWXLAGRP
TRK1COIN	PAID	TRK1COINPAID_ROUTE
TRK1COIN	COLLECT	TRK1COIN_NOROUTE

The XLAGRP names in fields XLAGRP and NEWXLAGRP must first be datafilled in table XLAGRP.

Field BILLTYPE supports a range of {UNSPEC, PAID, COLLECT, THIRD, CCARD, SPLCLG, SPLCLD}.

Note: Station paid and person paid are both handled by the PAID criteria. Both are PAID calls but may have a different rate applied. Since this refinement is to capture the billing method not the rate, station and person ratings are treated the same. This applies to all billing types.

Table Flow Example

This example section illustrates the new refinement tables and how they achieve special routing for coin station paid calls. It is simplified by using an incoming trunk group with non-EA calls. A59006822 fully details XLAGRP methods for EA and operator calls. It is further simplified by not having SPID or originating digit refinements. These are fully documented in AF7159.

TOPSTOPT

GRPKEY	ACDDATA	DISPCLG	ADASERV	ADASANS	ANITOCCLI	OLNSQRY	DCIBIDX	LNPCLGAM	XLA SCHEM		SPIDPRC	TRKSPID	
									NEWXLA	XLAGRP		DFTLSPID	SPID
TRK1	QMSCAM	N	NONE	NA	N	NONE	0	N	Y	TRK1	N	N	

XLASPID does not have a match

XLAODIGS does not have a match

XLACCLASS

XLAGRP	CLGCLASS	NEWXLGRP
TRK1	COIN	TRK1COIN
TRK1	STATION	TRK1STA

XLACCLASS

XLAGRP	CLGCLASS	NEWXLGRP
TRK1COIN	PAID	TRK1COINPAID_ROUTE
TRK1COIN	COLLECT	TRK1COIN_NOROUTE

TOPSDP

XLAGRP	STS	OPERPRTN	ORIGSCRN	OPERSCRN	MCCSPRTN	MCCSSCRN	LCANAME
TRK1	619	PRTNM1	SCR1	OPR1	PRTNM1	MCCS1	LCA00001
TRK1COINPAID_ROUTE	619	PRTNM1	SCR1	OPR1	PRTNM1	MCCS1	LCA00001
TRK1COIN_NOROUTE	619	NPRT	NSCR	NSCR	NPRT	NSCR	NLCA
TRK1COIN	619	NPRT	NSCR	NSCR	NPRT	NSCR	NLCA

- STS - This is the service translations scheme which is also the index into code translations (i.e. Table HNPACONT).

- OPERPRTN - This is the operator pretranslator name that is used for performing pretranslations from the operator position. It is used to index into Table STDPRTCT.
- ORIGSCRN - This is the class of service screening name that is used for screening based upon the location of the originator. It is used to index into Table CLSVSCRC.
- OPERSCRN - This is the class of service screening name that is used for screening when an operator or service node is associated with the call. It is also used to index into Table CLSVSCRC.
- MCCSPRTN - This is the pretranslator name that is used for performing pretranslations for the Mechanized Calling Card Service (MCCS) sequence calls. It is used to index into Table STDPRTCT.
- MCCSSCRN - This is the class of service screening name that is used for screening when performing the call screening for Mechanized Calling Card Service (MCCS) sequence calls. It is used to index into Table CLSVSCRC.
- LCANAME - This is the local call area screening name which is used to determine if the call is local. It is used to index into table LCASCRN or LCAINFO.

For non-EA COIN PAID calls arriving on TRK1, the initial XLAGRP is determined from table TOPSTOPT and refinements are performed as follows. The current XLAGRP is noted after the arrow.

1. Table TOPSTOPT provides the initial XLAGRP name

----> TRK1

2. SPID refinements are not needed, no change
3. Originating digits are not found in XLAODIGS, no change
4. Table XLACCLASS finds TRK1 COIN, changes XLAGRP

---> TRK1COIN

5. Table XLABILL finds TRK1COIN PAID, changes XLAGRP

----> TRK1COINPAID_ROUTE

The final XLAGRP for this non-EA COIN PAID call is TRK1COINPAID_ROUTE. This XLAGRP is indexed in table TOPSDP to find the screening and translations indices.

Note: In this example, if the coin call was billed collect then the final XLAGRP would have been TRK1COIN_NOROUTE which can be setup in table TOPSDP to have screening and translations indices which do not route or route to treatment. Also note that the XLAGRP, TRK1COIN, can be added to TOPSDP and be setup for indices which do not route. This ability limits the amount of datafill needed to only allow coin paid calls to complete. Thus, the refinement TRK1COIN COLLECT in XLABILL is not needed nor the TRK1COIN_NOROUTE XLAGRP. These were only included here to illustrate the options.

Activation

When activating feature A00002765 in a site where XLAGRPs are already in use, the following is recommended.

- For a new trunk group to begin using the XLAGRP translations and is not dependent on existing translations, a new XLAGRP name should be assigned to the trunk group and the new XLAGRP used in the refinement tables as needed. This has no interaction with existing translations since existing XLAGRPs will not find matches in the new tables.
- For an existing trunk group with XLAGRP translations (or a new trunk group which will use existing XLAGRP translations), it is recommended to work backwards in the refinement order. By adding the final XLAGRP first, no matches will be found until the first refinement using the existing XLAGRP is datafilled. For example, if TRK1 has XLA1 defined in TOPSTOPT and has existing translations for SPID where (XLA1 SPID XLA1SPID) is datafilled in table XLASPID, then to create a coin station_paid route for these calls, first add new XLAGRPs (XLA1SPIDCOIN and XLA1SPIDCOINPAID) to table XLAGRP then add to table XLABILL (XLA1SPIDCOIN PAID XLA1SPIDCOINPAID) [so far no changes will occur]. Then add to table XLAClass (XLA1SPID COIN XLA1SPIDCOIN) - [once this is added coin station_paid calls will route using XLA1SPIDCOINPAID].

Note: Ensure all XLAGRPs have datafill in table TOPSDP; be sure that XLA1SPIDCOIN can still route correctly. These are the calls which are coin but not paid for that trunk group with that SPID. TOPSDP will need to point to something that goes to treatment (if desired) otherwise they will route to the last route found in standard translations.

Hardware Requirements or Dependencies

NA

Software Requirements or Dependencies

UNBN0101, OSB00101

Limitations and restrictions

- XLAClass is limited to a range containing UNKNOWN, STATION, COIN, HOTEL, RESTRICTED.
- XLABILL is limited to a range including UNSPEC, PAID, COLLECT, THIRD, CCARD, SPLCLG, SPLCLD.
- Station billing and person billing may have different rates but are both treated the same in table XLABILL. For example, station paid and person paid will both refine under the PAID criteria.
- This feature is intended to be used with the dollar pre-pay coin functionality. Limitations for this function include:
 - External rater not support with OSSAIN
 - External rater, Coin signalling, ACTS not supported in Global loads

Interactions

This feature can alter the translations and route selected for calls using the XLAGRP method.

Glossary

Term	Description
XLAGRP	Translations Group

References

REF #	Description of Reference
297-8403-903	TOPS Unbundling User's Guide

Configuration for A00002765

Upgrade Impact

Dump and Restore

Although these new tables are potentially patched to prior loads, there are no changes between the patched tables and the open stream tables. Therefore, the tables will restore intact.

Data schema (DS)

New tables

Table name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
XLACCLASS	New	New
XLABILL	New	New

Table information

The following further describe new tables XLACCLASS and XLABILL.

Name: XLACCLASS

XLAGRP Translation Refinement for Calling Service Class

Functional description

This feature provides the mechanism to refine the XLAGRP based on the calling service class when using the XLAGRP method of translations through new table XLACCLASS.

Usage sequence and implications

Tables must be datafilled in the following sequence:

- XLAGRP
- TOPSDP
- XLACCLASS

Size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
XLACCLASS	0	40950 Maximum tuples is the maximum XLAGRPs (8190) times the class range (5)	Allocated dynamically when new XLAGRP added to table.

Fields

The following table lists fields for XLAClass.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
XLAGRP	New	N/A	N/A	Is the current XLAGRP associated with the call.
CLGCLASS	NEW	N/A	N/A	The Calling Service Class has the following range: {UNKNOWN, STATION, COIN, HOTEL, RESTRICTED}
NEWXLGRP	NEW	N/A	N/A	The new XLAGRP.

Datafill example

The following example shows sample datafill for table XLAClass.

Example of Table XLAClass

XLAGRP	CLGCLASS	NEWXLGRP
TRK1	COIN	TRK1COIN
TRK1	STATION	TRK1STA

Table release history update

Table XLAClass is implemented in TOP20 for SN07 loads.

Supplementary information

This table was patched back to previous loads. When this table ONPs, it will remain intact. No changes are made between the patched table and the table in the open stream.

Translation verification other tools

XLAClass does not use translation verification tools.

Name: XLABILL

XLAGRP Translation Refinement for Billing Types

Functional description

This feature provides the mechanism to refine the XLAGRP based on the billing type when using the XLAGRP method of translations through new table XLABILL.

Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

- XLAGRP
- TOPSDP
- XLABILL

Size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
XLABILL	0	57330 Maximum tuples is the maximum XLAGRPs (8190) times the bill range (7)	Allocated dynamically when new XLAGRP added to table.

Fields

The following table lists fields for XLABILL.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
XLAGRP	New	N/A	N/A	Is the current XLAGRP associated with the call.
BILLTYPE	NEW	N/A	N/A	The Billing Type has the following range: {UNSPEC, PAID, COLLECT, CCARD, THIRD, SPLCLG, SPLCLD}
NEWXLGRP	NEW	N/A	N/A	The new XLAGRP.

Datafill example

The following example shows sample datafill for table XLABILL.

Example of Table XLABILL

XLAGRP	BILLTYPE	NEWXLGRP
TRK1COIN	PAID	TRK1COINPAID_ROUTE
TRK1COIN	THIRD	TRK1COIN_NOROUTE
TRK1COIN	COLLECT	TRK1COIN_NOROUTE

Table release history update

Table XLABILL is implemented in TOP20 for SN07 loads.

Supplementary information

This table was patched back to previous loads. When this table ONPs, it will remain intact. No changes are made between the patched table and the table in the open stream.

Translation verification other tools

XLABILL does not use translation verification tools.

Product = TOPS**A00003687 -- Integration (Succession on DMS)*****Functional Description***

This feature enhances Table TOPSTLDN, introduced in SN06, to make it easier to deploy and maintain TOPS feature A00000816: "TOPS Wireless ADACC with Release." The enhancement is to allow the temporary local directory number (TLDN) to be chosen based on the identity of the originating mobile switching center (MSC). MSC is a generic term for a wireless (cellular) end office.

This feature also allows TOPS to send short text messages to a wireless phone using Short Message Service (SMS). TOPS can send short text messages using either Interim Standard 41 (IS-41) or Global System for Mobile Communications (GSM) specifications. IS-41 and GSM provide different definitions of a Mobile Application Part (MAP) layer which sits on the Transaction Capabilities Application Part (TCAP) layer of Signalling System #7 (SS7).

This feature also adds some preparatory work for supporting ADACC with Release in a GSM environment. This function cannot be used at this time.

Finally, this feature removes operational measurement (OM) group IS41TOPS and replaces it with three new OM groups. The new groups can be used for GSM as well as IS-41 and for SMS as well as wireless ADACC.

Background**TOPS support of wireless intelligent network (WIN) capabilities**

In SN06, TOPS feature A00000816: "TOPS Wireless ADACC with Release" added the capability to release cellular directory assistance (DA) calls back to the originating MSC for call completion. This release is accomplished using IS-41 messages to transmit the requested directory number (DN) from TOPS to the MSC. The MSC then releases the trunk to TOPS and connects forward to the requested DN. Prior to this SN06 feature, such calls were "hairpinned,"

meaning the trunks to and from TOPS stayed in the voice path between the calling and called parties for the duration of the call.

The IS-41 TCAP messages used for the TOPS DA call completion call flow are part of the Wireless Intelligent Network (WIN) modifications to IS-41. These modifications are described in standard IS-771.

A successful IS-41/IS-771 ADACC with Release call flow is depicted in Figure “Successful TOPS IS-41 ADACC with release, introduced in SN06” on page 2280.

TOPS support of short message service (SMS)

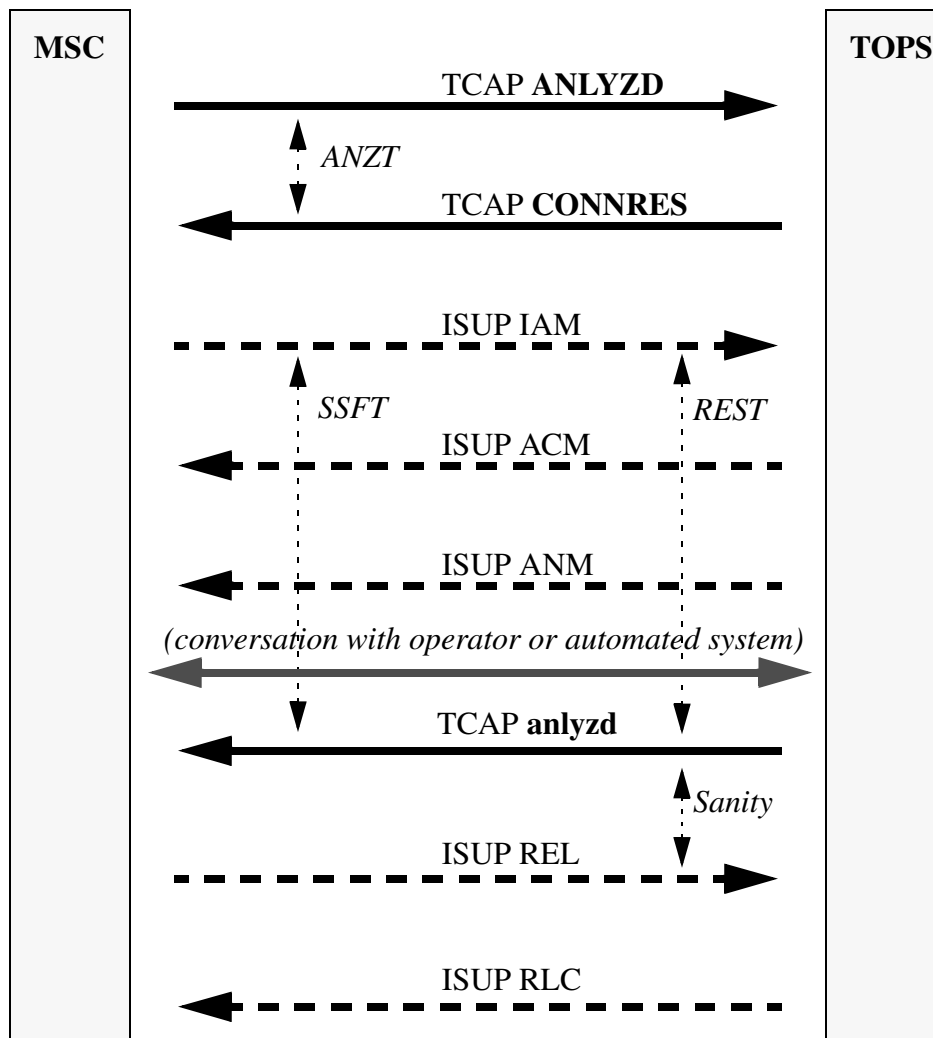
TOPS positions can already send short text messages using an e-mail interface over the Internet. Such an SMS message might contain the address of the requested listing on a DA call. The TOPS switch is not aware of these messages.

TOPS switches have supported SS7 TCAP applications for a long time, and SS7 TCAP is a common way to transport SMS in today's wireless networks. This feature allows TOPS to send SMS using either IS-41 or GSM, which are based on SS7 TCAP. By using TCAP to send TOPS SMS, the customer can avoid IP security and connectivity issues. The customer can also track the performance of TOPS SMS via operational measurements (OMs) and logs.

Specifications

This feature is based on the following IS-41 and GSM specifications:

- ANSI-41D (Wireless Intersystem Operations, formerly IS-41)
- 3GPP TS 29.002 V4.C.0: Mobile Application Part (MAP) specification, phase 4

Successful TOPS IS-41 ADACC with release, introduced in SN06

In the above diagram,

- A horizontal solid arrow and a message type in **bold** represents a TCAP message as defined in the IS-41 WIN specifications.
- A horizontal dashed arrow represents an ISUP message.
- A vertical dashed arrow on the MSC side represents an IS-41-defined timer. A vertical dashed arrow on the TOPS side represents an internal TOPS timer.
- The horizontal double-ended arrow represents two-way speech path between the wireless caller and TOPS.

Feature overview

This feature contains the following components. The work is divided into two areas, with some changes affecting both.

Wireless ADACC with Release

- Modified DMS table TOPSTLDN (TOPS Temporary Local Directory Number) which allows the customer to datafill TLDNs to be used in TOPS IS-41 call flows. Previously, any TLDN could be sent to any wireless end office. This feature allows TLDNs to be chosen on a per MSC basis. This helps the telco when they are activating WIN TOPS call flows in new MSCs (and desire a smaller or different TLDN range) but do not wish to affect existing MSCs.
- New table MSCIDMAP (MSC Identifier Mapping) which provides a mapping from MSC identifiers (MSCIDs) to entries in Table TOPSTLDN. This mapping allows the telephone company to control which TLDNs are sent to which MSCs.
- Addition of a new RLT type, `RLT_GSM`, to Table ISUPTRK. This table already allows datafill of three different RLT types: `RLT_REL`, `RLT_FAR`, and `RLT_IS41`. **Value `RLT_GSM` is for future use and cannot be datafilled at this time.**
- Removal of tuple `NUM_OF_IS41TOPS_EXT_BLKs` in Table OFCENG. This parameter controlled the number of extension blocks allocated for TOPS IS-41 calls. This parameter had to be set manually. It is replaced by to `NUM_OF_WIN_TOPS_EXT_BLKs` in Table OFCAUT. Table OFCAUT automatically allocates extension blocks for IS-41 and GSM calls. Also, the name of the EXT block is changed from `IS41TOPS_EXT_BLK` to `WIN_TOPS_EXT_BLK`. This name shows up when using OMSHOW to view the registers in OM group EXT.
- Addition of tuple `RLT_FOR_GSM` in Table TOPSFTR. This tuple will be used to control GSM ADACC with Release. **Tuple `RLT_FOR_GSM` is for future use and cannot be set to 'Y' at this time.** GSM ADACC with Release is under the control of existing Software Optionality Control (SOC) option OSEA0104, and tuple `RLT_FOR_GSM` acts as an on/off switch once the SOC option is enabled. This SOC option also controls IS-41 ADACC with Release.

Short message service (SMS)

- TOPS support of the following TCAP SMS messages, as described in the specifications listed in section “Specifications” on page 2279. These messages allow TOPS to send short text messages to wireless phone callers and receive acknowledgment from the message center (MC).
 - IS-41 SMSDeliveryPointToPoint INVOKE (from TOPS to MC)

- IS-41 SMSDeliveryPointToPoint RETURN RESULT (from MC to TOPS)
- GSM ForwardShortMessage (from TOPS to MC)
- GSM ForwardShortMessage Ack (from MC to TOPS)
- New field, `WIRELESS`, in Table TOPSTOPT. This field allows the customer to mark a trunk group as connecting to a wireless network. If so, the customer can datafill whether the network uses IS-41 or GSM for TCAP messaging. This field is used when TOPS sends a short message on a non-WIN call. On a WIN call the network type is already known.
- New TOPS parameter in Table TOPSPARM, `SMS_LOG_MC_FAILURE`. This parameter controls whether a TOPS131 log is generated when the message center returns a negative acknowledgment following a TOPS SMS attempt. A negative acknowledgment always pegs OMs in new groups SMSTOPS and TC7WRLSS, but the TOPS131 log can provide additional information.
- New TOPS parameter in Table TOPSPARM, `SMS_TIMEOUT`. This parameter controls the duration of the timer which is set when TOPS sends an SMS. If TOPS does not receive a response from the message center when the timer expires, the message is considered timed out, and resources are freed. See “TOPS short message service (SMS)” on page 2287 for more information.
- A new SS7 global title translation name, `MDNMCGT`. This translation name is used to route IS-41 and GSM short messages to the correct message center (MC).
- New DMS table TOPSMCDB for lab testing of TOPS SMS.
- Two additional DMS SS7 subsystems, `TIS41SIM` and `TGSM SIM`, to be used for TOPS lab testing.

Changes affecting both areas

- Creation of three new operational measurement (OM) groups to record events for IS-41 SMS, GSM SMS, IS-41 WIN, and GSM WIN³. The new groups will record application level events as well as transport level events. The new OM groups are SMSTOPS, WINTOPS, and TC7WRLSS. These three groups replace group IS41TOPS, which is removed.
- Update to TOPS131 log added in SN06. This feature allows the log to be used for GSM as well as IS-41, and for short message service as well as ADACC service.

3. GSM WIN is known as Customised Applications for Mobile network Enhanced Logic (CAMEL). TOPS uses the term Wireless Intelligent Network (WIN) to describe both IS-41 WIN and GSM CAMEL calls flows. These call flows attach a TOPS operator or service node to provide a transient service, and then the MSC releases TOPS and the wireless call proceeds.

- A new DMS Signaling System #7 (SS7) subsystem, GSMTOPS. This subsystem resides on the TOPS node and will initially be used to send and receive GSM SMS messages. The subsystem number is datafilled in Table C7LOCSSN.

This feature does not introduce any TOPS Automatic Message Accounting (AMA) changes.

TLDN selection by mobile switching center identifier (MSCID)

Changes to Table TOPSTLDN

Prior to this feature, Table TOPSTLDN defined one large pool of TLDNs to be used on WIN calls. Several tuples might be present in Table TOPSTLDN, but these tuples were combined together to make a single pool. When an IS-41 AnalyzedInformation (ANLYZD) message arrived from an MSC, TOPS would pick any idle TLDN from the overall pool and send it to the MSC in the ConnectResource (CONNRES) message. These messages are shown in Figure on page 2280.

This strategy works for a few MSCs but is not sufficient when deploying the feature across many MSCs. If hundreds of MSCs from across a region are using TOPS IS-41, they must all share the same TLDN pool. This means that when the customer is initially provisioning their network for TOPS IS-41, they must ensure that every TOPS TLDN is available and usable in every MSC as well as in every intermediate tandem switch on the way to the TOPS switch.

A better approach is to allow differentiation of TLDN chosen based on the identity of the originating MSC. To do this requires a change in Table TOPSTLDN as well a new table, MSCIDMAP, which is described in the next section.

This feature changes Table TOPSTLDN such that each group of TLDNs is identified by a pool ID. A maximum of 2,000 pools can be datafilled, and a maximum of 2,000 TLDNs can be datafilled. The pool ID is used in Table MSCIDMAP. The following figures show the change to Table TOPSTLDN.

Note that each tuple defines a range of TLDNs. In Table , “Table TOPSTLDN in SN06, prior to this feature,” on page 2284, the following ranges of TLDNs are defined:

- 2012201234 to 2012201234: 1 TLDN
- 2013364400 to 2013364899: 500 TLDNs
- 2018591400 to 2018591489: 90 TLDNs

Table TOPSTLDN in SN06, prior to this feature

TABLE: TOPSTLDN	
	KEY

2012201234	2012201234
20133644	20133648
201859140	201859148

This feature identifies each range of TLDNs with a pool ID, and expands the TLDNs to 10 digits for better readability. So the datafill in Figure on page 2284 would appear as follows in SN07. This datafill still represents 591 TLDNs.

Table TOPSTLDN in SN07

TABLE: TOPSTLDN		
POOLID	FROMDIGS	TODIGS

0	2012201234	2012201234
1	2013364400	2013364899
2	2018591400	2018591489

TLDN ranges in Table TOPSTLDN are allowed to overlap. This helps the customer when they are verifying the function on a new MSC while other MSCs are processing live traffic. The following figure shows overlapping TLDN ranges.

Table TOPSTLDN in SN07

TABLE: TOPSTLDN		
POOLID	FROMDIGS	TODIGS

0	2012201200	2012201259
1	2012201250	2012201269
2	2012201200	2012201200

TLDN methodology

The telco's goal should be to have one large TLDN pool, or several smaller TLDN pools, serving all MSCs. This allows the TLDNs to be selected quickly. So the goal should be to minimize the number of tuples in Table MSCIDMAP (see next section).

The main reason for these tables is to assist in deployment of TOPS wireless intelligent network services. Established MSCs might be using hundreds of

TOPS TLDNs, while a new MSC might need TLDNs from the same pool, but only a small subset while the feature is being set up. Once the feature is verified on the new MSC, the MSC's datafill can be changed so it uses the main pool.

The telco providing operator services will reserve the TOPS TLDNs for these call types. Even in a nationwide network it should be possible to find enough TLDNs, since the TLDNs chosen probably begin with the NPA-NXX of the TOPS switch. If the TOPS switch supports several NXXs, this makes finding available DNs easier.

2,000 is the maximum number of TLDNs which can be datafilled on a TOPS switch. Due to the short holding time of under one second, a couple hundred TLDNs should be enough to handle heavy WIN TOPS traffic. If problems begin to occur, TLDNs can remain held for up to 30 seconds before the TLDN selection code re-uses them.

Dump and restore for Table TOPSTLDN

When upgrading from SN06 to a later release, each TOPSTLDN tuple from the SN06 side is restored with sequential pool IDs starting at 0, and each TLDN is expanded to 10 digits. So the Figure on page 2284 and Figure on page 2284 represent a dump and restore from SN06 to a later release.

New table MSCIDMAP

This feature introduces Table MSCIDMAP which allows the selection of TLDNs on a per-MSC basis.

The MSC Identifier (MSCID) is defined in IS-41D, chapter 5, section 6.5.2.82. It consists of a market identifier (16 bits) and a switch number (8 bits). It is a mandatory field in the IS-41 ANLYZD message which initiates a TOPS IS-41 ADACC with Release call.

When TOPS receives an ANLYZD, it selects an idle TLDN from Table TOPSTLDN and sends it back to the MSC in the TCAP CONNRES message. This feature allows TOPS to select a TLDN based on the MSCID in the ANLYZD. This is done using new Table MSCIDMAP. Table MSCIDMAP maps the MSCID from the ANLYZD to a list of TLDN pool IDs from Table TOPSTLDN. TOPS then selects an idle TLDN from one of these pools.

The following figure shows sample datafill in Table MSCIDMAP. Up to 255 TLDN pool IDs can be datafilled against a given MSCID.

Table MSCIDMAP

TABLE: MSCIDMAP					
MSCID		POOLIDS			

12	100	(0)	(1)	(2)	\$
65	2		(0)	(1)	\$
65	3			(0)	\$
66	27			(1)	\$
66	29		(1)	(2)	\$
700	2			(2)	\$

Switch number wildcarding

Because a TOPS switch might be serving hundreds if not thousands of MSCs, Table MSCIDMAP is designed with some wildcarding capabilities. It is not necessary to datafill every switch number within a market ID. If a tuple is datafilled with just the market ID, and no switch number, the tuple will match all MSCIDs with the same market ID.

It is also possible to datafill several market ID and switch number combinations for the same market ID, and then add a market ID wildcard tuple for all other switch numbers using the same market ID.

The following figure shows examples of switch number wildcarding. All MSCIDs beginning with market ID 65 will match the first tuple, except MSCID (65, 3) which matches the second tuple.

Table MSCIDMAP with switch number wildcarding

TABLE: MSCIDMAP					
MSCID		POOLIDS			

65	\$	(0)	(1)	(2)	\$
65	3			(0)	\$
66	27			(1)	\$
66	29	(1)	(2)		\$
67	\$	(0)	(2)		\$

Market ID wildcarding

Tuple { \$, \$ } matches any MSCID not otherwise matched in Table MSCIDMAP. If present, it is the default tuple. If the MSCID in the TCAP ANLYZD message does not match any other tuple in Table MSCID (including any tuples with wildcarded switch numbers), tuple { \$, \$ } is used.

Table MSCIDMAP with default tuple

TABLE: MSCIDMAP						
MSCID		POOLIDS				

\$	\$	(0)	(1)	(2)	\$	
65	3			(0)	\$	
66	\$			(1)	\$	
66	29		(1)	(2)	\$	
67	\$		(0)	(2)	\$	

Failure to match MSCID

If the MSCID for a given call does not match any tuple in Table MSCIDMAP (either explicitly or via wildcarding), a RETURN ERROR is sent to the MSC so the wireless 411 call is disconnected. A TOPS131 log is generated indicating no TLDNs are available.

A failure to match implies that the market ID wildcard tuple is not present, since this tuple matches any MSCID.

Dump and restore

When performing a switch upgrade from an SN06 TOPS switch to a later release, the following steps are performed automatically:

1. Table TOPSTLDN is restored as described in “Changes to Table TOPSTLDN” on page 2283.
2. If TOPSTLDN contains any datafill on the restore side, a {\$, \$} tuple is created in Table MSCIDMAP containing all pools from Table TOPSTLDN.

This will create one large pool serving all MSCs, which is equivalent to the SN06 function of Table TOPSTLDN.

TOPS short message service (SMS)**Message flow**

This feature allows TOPS to send short text messages into the SS7 network. TOPS sends these messages when requested by the operator position or automated service node. The message flow is summarized below. Later subsections show message diagrams, OMs pegged, etc.

- A TOPS call arrives from a wireless (cell) phone. TOPS knows the calling party is using a wireless phone if at least one of the following conditions hold:
 - The call originated with a WIN message transaction (ANLYZD/CONNRES)

- New TOPSTOPT field `WIRELESS` indicates the calling trunk group is from a wireless network (non-WIN)

When presenting the call to the Open Position Protocol (OPP) compliant position or Open Automated Protocol (OAP) compliant service node, TOPS indicates that the calling party is using a wireless phone.

- The operator position sends a short text message and a destination directory number (DN) to TOPS switch using OPP, or the service node sends a short text message and a destination DN using OAP.
- TOPS checks whether the destination DN is the same as the calling number. This feature allows TOPS to send an SMS to the calling party only. TOPS denies the SMS attempt with an appropriate OPP or OAP message if the destination DN is not equal to the calling number.
- TOPS decides whether to send SMS using IS-41 or GSM. This decision is made as follows:
 - If the TOPS call originated using IS-41 WIN, TOPS already knows the originating wireless network type, and TOPS uses IS-41.
 - If the TOPS call did not originate using IS-41 WIN, TOPS looks at the calling trunk group datafill in Table TOPSTOPT. New field `WIRELESS` in Table TOPSTOPT indicates whether the calling trunk is IS-41 or GSM. TOPS chooses to use IS-41 or GSM based on the contents of this field.
 - If the TOPS call did not originate using IS-41 WIN, and calling trunk group is not marked as wireless in Table TOPSTOPT, TOPS sends a failure indication to the operator position or service node using OPP or OAP, respectively. The call is not a wireless phone call, and TOPS did not indicate to the position or service node that the call is from a wireless phone. The position or service node should not request an SMS when the calling phone is not a wireless phone.
- Once TOPS has decided which standard to use, TOPS composes an outgoing TCAP INVOKE containing the short message.
- To route the TCAP INVOKE, TOPS looks in the global title translation tables `C7GTTTYPE` and `C7GTT`. This feature adds a new SS7 translation name, `MDNMCMT`, for routing short messages to the message center (MC). TOPS uses the destination number to index the global title translation tables. This will route the SMS to the calling party's home message center.
- TOPS sends the TCAP INVOKE. If the message is sent successfully, TOPS returns a success indication to the position or service node using OPP or OAP, respectively. If the message is not sent successfully, TOPS indicates the failure to the position or service node.

- TOPS starts an internal timer equal to the new `SMS_TIMEOUT` parameter in Table TOPSPARM. If this timer expires, a log and OM are generated to notify the telephone company.
- When the acknowledgment from the message center arrives, TOPS pegs an OM and/or generates a log based on the response (success or failure). TOPS does not send a notification to the position if the SMS succeeded or failed.

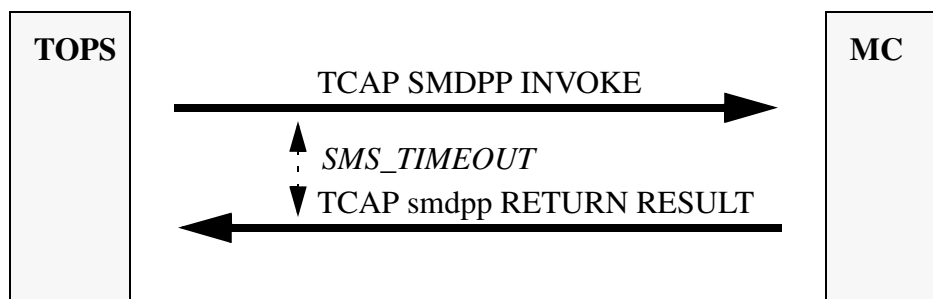
The following sections show diagrams of SMS messaging for IS-41 and GSM.

Successful IS-41 SMS transaction

In this scenario, TOPS sends the SMS to the message center, which responds with a positive acknowledgement. According to IS-41, the absence of a Cause Code parameter indicates success.

TOPS pegs OMs `SMSSENT` and `SMSSUCC` in group `SMSTOPS` (key `IS41`). TOPS also pegs OMs `INVOKES` and `RETRESR` in group `TC7WRLSS` (key `SMS_IS41`).

Successful TOPS IS-41 SMS to message center



Unsuccessful IS-41 SMS transaction

In this scenario, TOPS sends the SMS to the message center, but failures occur in the network, or the message center cannot process the SMS. TOPS receives a negative acknowledgment from an intervening node or from the message center, depending on where the error occurred. The message center's response contains a Cause Code field indicating why the message could not be delivered.

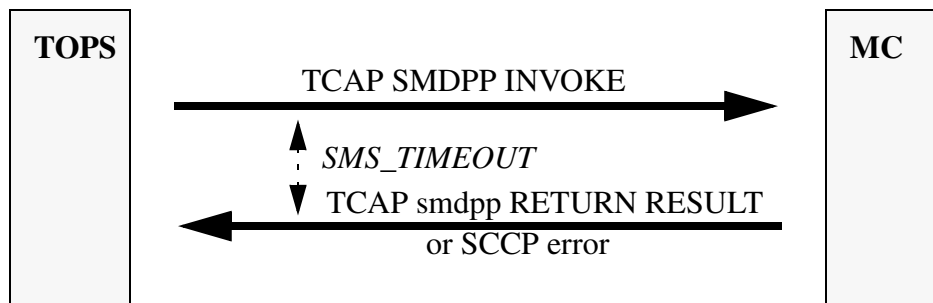
Possible reasons for failure include network problems, terminal (cell phone) problems, radio interface problems, and other miscellaneous problems (e.g. message format).

TOPS pegs OMs `SMSSENT` and `SMSFAIL` in group `SMSTOPS` (key `IS41`). TOPS also pegs one of the failure reason OMs (`SMSNETWK`, `SMSTERM`,

SMSRADIO, and SMSMISC). TOPS also pegs OMs INVOKES and RETRESR in group TC7WRLSS (key SMS_IS41).

TOPS generates a TOPS131 log indicating the reason for failure, as directed by new Table TOPSPARM parameter SMS_LOG_MC_FAILURE.

Unsuccessful TOPS IS-41 SMS to message center (smdpp contains cause code)



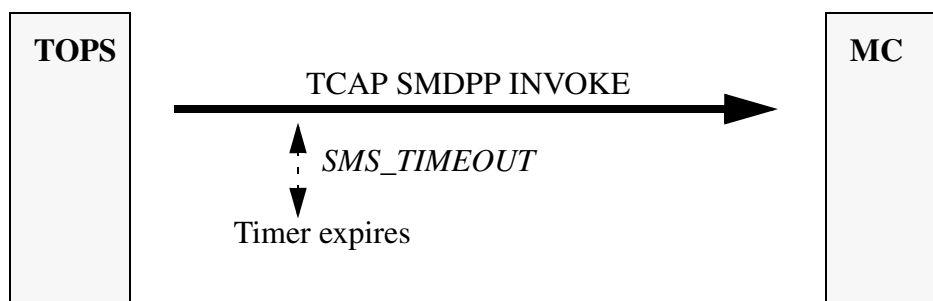
SMS time-out (IS-41)

In this scenario, TOPS sends the SMS to the message center but receives no reply within the time-out period (as defined by parameter SMS_TIMEOUT in Table TOPSPARM).

TOPS pegs OMs SMSENT and SMSTIME in group SMSTOPS (key IS41). TOPS also pegs OM INVOKES in group TC7WRLSS (key SMS_IS41).

TOPS generates a TOP131 indicating an SMS time-out occurred.

SMS time-out (IS-41)

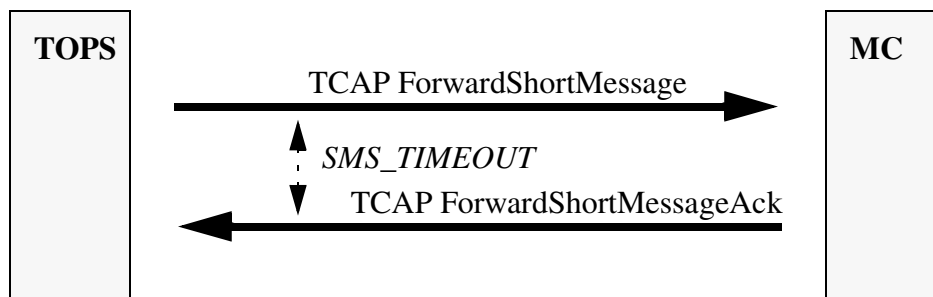


Successful GSM SMS transaction

In this scenario, TOPS sends the SMS to the message center, which responds with a positive acknowledgement.

TOPS pegs OMs SMSSENT and SMSSUCC in group SMSTOPS (key GSM). TOPS also pegs OMs INVOKES and RETRESR in group TC7WRLSS (key SMS_GSM).

Successful TOPS GSM SMS to message center



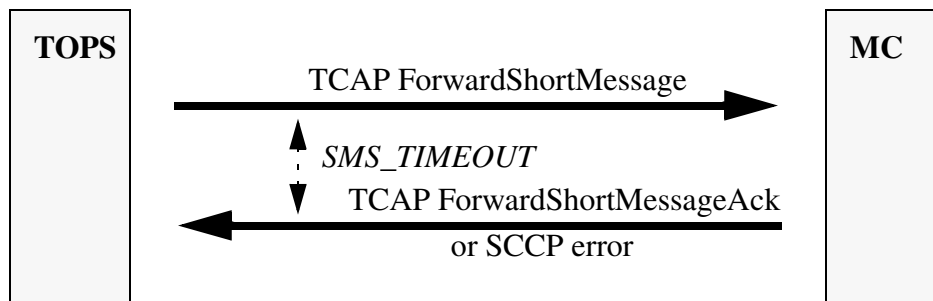
Unsuccessful GSM SMS transaction

In this scenario, TOPS sends the SMS to the message center, but failures occur in the network, or the message center cannot process the SMS. TOPS receives a negative acknowledgment from an intervening node or from the message center, depending on where the error occurred. The message center's response contains the error cause and any diagnostic information.

Possible reasons for failure include network problems, terminal (cell phone) problems, radio interface problems, and other miscellaneous problems (e.g. message format).

TOPS pegs OMs SMSSENT and SMSFAIL in group SMSTOPS (key GSM). TOPS also pegs one of the failure reason OMs (SMSNETWK, SMSTERM, SMSRADIO, and SMSMISC). TOPS also pegs OMs INVOKES and RETRESR in group TC7WRLSS (key SMS_GSM).

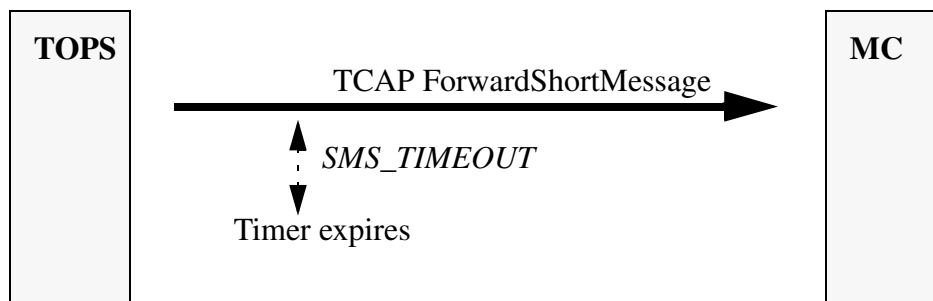
TOPS generates a TOPS131 log indicating the reason for failure, as directed by new Table TOPSPARM parameter SMS_LOG_MC_FAILURE.

Unsuccessful TOPS GSM SMS to message center (ack contains cause code)**SMS time-out (GSM)**

In this scenario, TOPS sends the SMS to the message center but receives no reply within the time-period (as defined by parameter `SMS_TIMEOUT` in Table TOPSPARM).

TOPS pegs OMs SMSSSENT and SMSTIME in group SMSTOPS (key GSM). TOPS also pegs OM INVOKES in group TC7WRLSS (key SMS_GSM).

TOPS generates a TOP131 indicating an SMS time-out occurred.

SMS time-out (GSM)**TOPS SMS engineering considerations**

Short messages sent by TOPS can be up to 200 characters in length. When headers and ancillary fields are added in, the overall message length can reach 250 bytes. Each time a position or automated node sends a SMS which is then forwarded to the SS7 network, the SMS is actually sent twice: once using OPP or OAP over IP from the position or service node to the switch, and once over the SS7 links into the network.

If a switch is supporting 300 active operators handling 20-second directory assistance calls, and an SMS containing the listing is sent on each call, this

represents 54,000 calls per hour at 250 bytes per call. The total is 13.5 megabytes per hour which is equivalent to 3.75 kilobytes per second.

Both the IP links to the positions and service nodes as well as the SS7 links to the network must be able to handle this increased messaging. Call durations, numbers of operators, and SMS-to-call ratio should be taken into account when deploying this feature.

Operator and automated node interaction

Operators and automated service nodes receive an immediate indication that the SMS was successfully sent or could not be sent. They do not receive the later acknowledgment from the message center. The reason is that the SMS might be sent at the end of the call, and TOPS call throughput would be diminished if the operator or automated service node had to wait for the acknowledgment from the message center before leaving the call.

TOPS still tracks the message center results of the SMS (using OM s and logs) but the operator or service node is not aware of the outcome.

Another effect is that the response from the message center might arrive after the AMA record for the call is generated. So this feature does not record in AMA whether the SMS was successfully received by the message center.

IS41TOPS OM group modification

In SN06, the original TOPS IS-41 feature added OM group IS41TOPS. This group recorded application-level and transport-level events for the IS-41 ADACC with release call flow.

This SN07 feature is adding support of GSM and SMS. The number of registers to record application-level and transport-level events for combinations of the two applications (RLT and SMS) and the two protocol standard (IS-41 and GSM) requires more than 32 registers, which is the maximum number of registers in an OM group.

So this feature creates the following three groups. All three groups use a key field with values IS-41 and GSM, so all three groups are used for both wireless network standards.

- **SMSTOPS:** This group records application-level events for the TOPS short message service.
- **WINTOPS:** This group records application-level events for wireless ADACC with release. This group uses WIN in the name since wireless intelligent network capabilities are used to provide ADACC with release for both IS-41 and GSM.

- **TC7WRLSS:** This group records transport-level events such as types of TCAP messages sent and received, SS7 errors, etc. on TOPS wireless calls (SMS and WIN, as well as IS-41 and GSM).

All events formerly pegged in IS41TOPS are now pegged in the new groups. The following table shows the new representations of the IS41TOPS OMs.

IS41TOPS register (SN06)	New group (SN07), key IS41 or WIN_IS41	New register (SN07)
ANINFINV	WINTOPS	WINBEGIN
ANINFIN2	WINTOPS	WINBEG12
CONNRES	WINTOPS	REQCONN
CONNRES2	WINTOPS	REQCONN2
ANINFRR	WINTOPS	CONNECT
ANINFRR2	WINTOPS	CONNECT2
ANINFRD	WINTOPS	DISCONN
ANINFRD2	WINTOPS	DISCONN2
RESTIMR	WINTOPS	RESTIMR
RESTIMR2	WINTOPS	RESTIMR2
TLDNTIME	WINTOPS	TLDNTIME
SANTIMR	WINTOPS	SANTIMR
CFRABAN	WINTOPS	ABANDON
CFRDISC	WINTOPS	ERRDISC
CFRFAIL	WINTOPS	ERRCONN
CFRSSFT	WINTOPS	ERRSSFT
RETERRS	TC7WRLSS	RETERRS
RETERRR	TC7WRLSS	RETERRR
REJECTS	TC7WRLSS	REJECTS
REJECTR	TC7WRLSS	REJECTR
NOTLDNS	WINTOPS	NOTLDNS
NODATA	WINTOPS	NODATA
RXLAFAIL	WINTOPS	RXLAFAIL
MBFULL	TC7WRLSS	MBFULL

IS41TOPS register (SN06)	New group (SN07), key IS41 or WIN_IS41	New register (SN07)
RTFNOXLA	TC7WRLSS	RTFNOXLA
RTFNOXLS	TC7WRLSS	RTFNOXLS
RTFSUBCG	TC7WRLSS	RTFSUBCG
RTFSUBFL	TC7WRLSS	RTFSUBFL
RTFUNEQ	TC7WRLSS	RTFUNEQ
RTFNETFL	TC7WRLSS	RTFNETFL
RTFNETCG	TC7WRLSS	RTFNETCG
RTFMISCE	TC7WRLSS	RTFMISCE

For more information on the groups created by this feature, refer to the Performance chapter of this document.

Customer visible changes

As mentioned in “Feature overview” on page 2281, this feature has several customer-visible changes.

Wireless ADACC with Release

- Table TOPSTLDN (changed) and Table MSCIDMAP (new): Together, these tables map MSC identifiers to TLDN pool(s) used when selecting a TLDN at the beginning of an IS-41 WIN call. See “TLDN selection by mobile switching center identifier (MSCID)” on page 2283, as well as the Configuration chapter of this document.
- Changed tables OFCENG, OFCAUT, and ISUPTRK: The TOPS IS-41 extension block parameter is removed from Table OFCENG and added to Table OFCAUT. In Table ISUPTRK, a value is created for future use. See the Configuration section of this document.
- Table TOPSFTR: This feature adds a new tuple, `RLT_FOR_GSM`, which controls GSM ADACC with Release. GSM ADACC with Release is under the control of existing SOC option OSEA0104.

Short message service (SMS)

- Changed table TOPSTOPT: A new field, `WIRELESS`, is added for defining the wireless network type on a non-WIN wireless call.
- Changed table TOPSPARM: Two new TOPS parameters, `SMS_LOG_MC_FAILURE` and `SMS_TIMEOUT`, are added. See the Configuration chapter of this document.

- SS7 datafill and maintenance: Action is required on the TOPS switch to define and activate the new SS7 subsystem, GSMTOPS, in order to send and receive GSM SMS TCAP messages. Please refer to “Datafill changes for SMS” on page 2301.
- SS7 global title translation name: A new translation name, MDNMC GT, is added to allow TOPS to route IS-41 and GSM short messages to message centers. This translation name is datafilled in existing table C7GTTYPE. Please refer to “Datafill changes for SMS” on page 2301.
- Existing OM groups: This feature creates a new SS7 subsystem, and many existing OM groups have registers which are pegged when this new subsystem is in use. See “Operational measurements (OMs)” on page 2303 for more information.
- Test tool: This feature adds a TOPS SMS test tool consisting of new Table TOPSMCDB and new SS7 subsystems TIS41SIM and TGSMSIM. See “TOPS message center (TOPSMC) test tool” on page 2305 for more information.

Changes affecting both areas

- Changed operational measurement (OM) group IS41TOPS: OM group IS41TOPS is replaced by three new OM groups: SMSTOPS, WINTOPS, and TC7WRLSS. See section, as well as the Performance chapter of this document.
- Changed log TOPS131: This log appears when problems occur during the course of a wireless TOPS RLT call. Additional text reasons are added for SMS failures. See the Fault Management chapter of this document.
- Existing logs: This feature generates existing TCAP logs (such as the TCAP100) when errors occur in TCAP message formats, or unexpected TCAP messages are received. See Nortel Networks Log Report Reference Manual (297-8021-840) for more information about TCAP logs.

Hardware Requirements or Dependencies

Not applicable.

Software Requirements or Dependencies

Not applicable.

Limitations and restrictions

General restrictions

- TOPS Wireless ADACC with Release is supported in North American TOPS offices only.

TOPS Wireless Intelligent Network restrictions

- Only one form of RLT (ISUP, IS-41, or GSM) can be employed a given trunk group. A trunk group cannot support both IS-41 and GSM RLT.
- A maximum of 4,096 market identifiers can be datafilled in Table MSCIDMAP (see “New table MSCIDMAP” on page 2285).
- A maximum of 32,767 MSCIDs can be datafilled in Table MSCIDMAP. An MSCID is a combination of a market ID and a switch number.
- TOPS does not support GSM CAMEL calls at this time. The `RLT_GSM` value in field RLT of Table ISUPTRK is for future use.
- Pool IDs cannot be added to Table TOPSTLDN unless they already exist in Table MSCIDMAP.
- TLDN pools in Table TOPSTLDN cannot be changed or deleted if they are in use in Table MSCIDMAP. This helps prevent the customer from altering a TLDN's internal store while the TLDN is in use.
- It is not possible to add a wildcard market ID and non-wildcard switch number tuple to Table MSCIDMAP.

TOPS SMS restrictions

- The SMS can be sent to the calling party only.
- In North America, the length of the SMS destination number must be 10 digits.
- The position or service node cannot send a second SMS while the first is in progress.
- SMS is supported on IP positions only, due to the maximum length of the SMS (200 bytes). Service nodes already use an IP datapath.
- SMS is not supported in the Time Division Multiplex (TDM) operator centralization (OC) environment⁴, again due to length. If the OC environment uses a TDM data path, the SMS cannot be transmitted from the host switch to the remote switch, so the SMS attempt is denied. To support sending the SMS from the host to the remote, OC-IP must be employed.
- SMS is supported in the Operator Services System Automated Intelligent Network (OSSAIN) centralization environment, known as OSAC. OSAC already uses an IP data path so SMS messages can be transmitted.
- Since TOPS might not have the International Mobile Subscriber Identity (IMSI) or Mobile Identification Number (MIN), there is no provision for routing SMS based on these numbers.

4. TDM OC uses the TOPS Message Switch (TMS) for the OC data path.

- Since TOPS only sends SMS to the calling party, there is no provision for prepending the country code prior to global title translation. The routing is based on the national number only.
- TOPS does not support SMS notification, a supplementary service which informs the message originator that the SMS was delivered to the destination phone. TOPS indicates in outgoing SMS TCAP messages that SMS notification is not required. If TOPS receives an SMS notification message, it is ignored.
- The AMA record does not indicate if the SMS was successfully acknowledged by the message center. For more information, see “Operator and automated node interaction” on page 2293.

Interactions

Interactions with cell phone users

Interactions involving wireless (cell) phone features and IS-41 or GSM processing on the MSC are outside the scope of this feature. This feature is limited to TOPS behavior given the following inputs:

- IS-41 and GSM messaging
- ISUP messaging
- Behavior of operator or automated service node

Interactions with intelligent TOPS peripherals

This feature allows Open Position Protocol (OPP) compliant operator positions to send short messages into the SS7 network via the TOPS switch. This feature also allows Open Automated Protocol (OAP) compliant automated service nodes to send short messages via the TOPS switch. To support these capabilities, OPP and OAP are updated. Please refer to the latest releases of OPP and OAP for information on the transport of SMS from the operator position or service node to the TOPS switch.

Wireless number portability

Wireless number portability allows a wireless customer to keep their dialable Mobile Directory Number (MDN) while moving to another service provider. Their nondialable IS-41 mobile identification number (MIN) or GSM international mobile subscriber identity (IMSI) changes, but their MDN remains the same.

The MDN is sent to TOPS as the calling party number when originating a call from a cell phone which has been ported. When a land line calls a ported cell phone, the original (“donor”) MSC uses WNP capabilities to determine where the call should be routed.

This has the following effects on the call flows and functions of this feature.

Wireless intelligent network

TOPS WIN call setup is based on the initial WIN message and the originating trunk group. Whether the calling party has ported or not, the originating MSC sends an IS-41 ANLYZD or GSM InitialDP to start the call, and TOPS knows which protocol to use when handling the call.

The call arrives on an ISUP trunk group in Table ISUPTRK. IS-41 RLT or GSM RLT is datafilled against the trunk group, so the calling party number is not a consideration.

In a different case, a wireless caller uses TOPS WIN to connect to another wireless phone which has been ported. The TOPS WIN call flow is not changed. TOPS forwards the MDN of the called wireless phone to the MSC using the **analyzed** or Connect message. The MSC must then determine if the MDN has been ported. In other words, the WNP work is done after TOPS leaves the call, and TOPS does not need to indicate if a number is ported.

Short message service

At this time, TOPS can only send an SMS to the calling party. The MDN is sent as the calling party number. So TOPS sends the SMS to the MDN, which routes the SMS to the message center associated with the “donor” switch. The donor switch’s MC then does the work to determine that the MDN has been ported. The donor switch’s MC then forwards the SMS to the proper MC. So again, TOPS is not affected by WNP.

Applicable customer facing sections

Fault Management

Logs	<u> X </u>
Alarms	<u> N/A </u>

Configuration

Data Schema	<u> X </u>
User Interface	<u> N/A </u>
Element Management	<u> N/A </u>
Security	<u> N/A </u>
Service Order	<u> N/A </u>
Office Parameters	<u> X </u>

Accounting (includes AMA billing)	<u> N/A </u>

Performance (includes operational measurements)	<u> X </u>

Glossary

Acronym	Expansion
ACM	ISUP Address Complete message
ADACC	Automated DA Call Completion
AMA	Automatic Message Accounting
ANLYZD	IS-41 AnalyzedInformation message
ANM	ISUP Answer message
CONNRES	IS-41 ConnectResource message
DA	Directory Assistance
GSM	Global system for mobile communications
IAM	ISUP Initial Address message
IMSI	International Mobile Subscriber Identity
IP	Intelligent Peripheral
IP	Internet Protocol
IS-41	Interim Standard 41
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
MC	Message Center
MDN	Mobile Directory Number
MIN	Mobile Identification Number
MSC	Mobile Switching Center
OAP	Open Automated Protocol
OC	Operator Centralization
OPP	Open Position Protocol
OSAC	OSSAIN Centralization
OSSAIN	Operator Services System Advanced Intelligent Network
RLT	Release Link Trunking
RTP	Release To Pivot
SCCP	Signaling Connection Control Part

Acronym	Expansion
SCP	Service Control Point
SMS	Short Message Service
SS7	Signaling System #7
TCAP	Transaction Capabilities Application Part
TDM	Time Division Multiplex
TLDN	Temporary Local Directory Number
TMS	TOPS Message Switch
TOPS	Traffic Operator Position System
WNP	Wireless Number Portability

Datafill changes for SMS

Enabling TOPS SMS requires datafill and other action in the following categories:

- **SS7:** Enable the IS41TOPS and GSMTOPS subsystems.
- **Global title translation:** Update Table C7GTTYPE and C7GTT to route SMS TCAP messages to the proper message centers.
- **Trunk group:** Mark incoming wireless calls as IS-41 or GSM on a trunk group basis in Table TOPSTOPT.

These actions are described in this appendix.

SS7 datafill and maintenance

The following items are required to enable TOPS IS-41 and GSM TCAP messaging.

- **Table C7LOCSSN:** Add tuples for the IS41TOPS and GSMTOPS subsystems. Define two different subsystem numbers which will be used by MSCs to send TCAP messages to TOPS.
- **MAP operation:** From the SCCPLOC level of the MAP (MAPCI;MTC;CCS;CCS7;SCCPLOC), post and return to service the IS41TOPS and GSMTOPS subsystems.
- **Table C7RTESET:** TOPS SMS will not work unless there are CCS7 route set(s) defined to the message centers of calling parties. Depending on the configuration of the SS7 network, it might be possible to reuse the ISUP trunk route sets for TOPS SMS.

Global title translation

This feature adds an SS7 translation name, MDNMC GT, which is used for routing outgoing TOPS SMS messages to the appropriate message center. MDNMC GT is datafilled in Table C7GTTYPE and is already present in Nortel Networks MTX switches.

The following figures show datafill for Table C7GTTYPE and Table C7GTT. This datafill routes all TOPS SMS (whether IS-41 or GSM) messages to a service transfer point (STP) which already has significant SMS translation datafill. This TOPS datafill offloads the SMS global title translation to the customer's existing STP named STPA. The datafill assigns a global title number of 17 which is commonly used for mobile directory number (MDN) to message center (MC) routing.

Table C7GTTYPE

```
TABLE: C7GTTYPE
GTTNAME GTTYPE GTTID
-----
TOPSSMS ANSI7 17 (MDNMC GT) $
```

Table C7GTT

```
TABLE: C7GTT
GTTKEY GTTRSLT
-----
TOPSSMS 0 9 PONLY (TOPSTOSTPA_RS 0) $ GT
```

Trunk group datafill

On a WIN call, the wireless network type is already known, since IS-41 messages were exchanged to begin the call. On a non-WIN wireless call (e.g. 0-, or 411 when WIN is not supported) the call arrives with standard trunk signalling and no indication that the calling party is using a cellular phone.

This feature allows customers to mark trunk groups as carrying wireless (cellular) traffic, and to further indicate whether the wireless network connected by the trunk group is IS-41 or GSM. TOPS uses this datafill when composing a short message. The trunk group datafill determines whether TOPS composes the SMS using IS-41 or GSM.

This requires the customer to segregate incoming trunk groups into IS-41 wireless, GSM wireless, and non-wireless categories. This is necessary since there is no ISUP signal which indicates that the calling party is using a cellular phone. Also, with wireless number portability (WNP), the NPA-NXX of the calling party number can no longer be used to determine the network type based on the originating MSC. A WNP user may have ported their mobile directory number from an IS-41 switch to a GSM switch or vice versa.

The following diagram shows three trunk groups in Table TOPSTOPT. One is from a wireline end office, one is from an IS-41 end office, and one is from a GSM end office.

Table TOPSTOPT

TABLE: TOPSTOPT																	
GRPKEY ORGAREA DISPCLG ADASERV ADASANS ANITOCCLI OLNSQRY DCIBIDX LNPCLGAM																	
XLASCHEM SPIDPRC TRKSPID BILLSCRN ANIFSPL MAXCONNS DISPSPID WIRELESS																	

LANDLINE_EO	N	Y	NONE	NA	Y	N	NONE	0	N	N	N	N	N	N	0	N	N
WIRELESS_IS41	N	Y	NONE	NA	Y	N	NONE	0	N	N	N	N	N	N	0	N	Y IS41
WIRELESS_GSM	N	Y	NONE	NA	Y	N	NONE	0	N	N	N	N	N	N	0	N	Y GSM

Operational measurements (OMs)

This feature creates three new OM groups: SMSTOPS, WINTOPS, and TC7WRLSS. The registers in these groups count specific events occurring during TOPS IS-41 and GSM call processing. Please refer to “IS41TOPS OM group modification” on page 2293 and the Performance chapter of this document for more information on these new OM groups.

The following appendix describes this feature’s effects on existing OM groups.

SS7 operational measurements

Several existing OM groups are defined for pegging events relating to SS7 and TCAP messaging. These groups usually start with “C7” or “TCAP.” More information about these groups can be found in NTP 297-8021-814: “Operational Measurements Reference Manual.”

Two existing TCAP OM groups, TCAPUSAG and TCAPERRS, are useful when tracking this feature, since these OM groups have SS7 subsystem as their key. To track TOPS IS-41 events, use subsystem name IS41TOPS as the key. To track TOPS GSM events, use subsystem name GSMTOPS as the key.

OM group TCAPUSAG contains several registers which are pegged during the course of a wireless TOPS call in addition to the pegs in the new groups introduced by this feature. The following table maps the OM registers in group TCAPUSAG to messages sent and received during a wireless TOPS call.

TCAPUSAG mapping to TOPS IS-41 and GSM ADACC event

Register	Description and applicability to TOPS IS-41 ADACC
TCMSGOUT, TCMSGOU2	Total TCAP messages originating on this node Pegged for all IS-41 and GSM TCAP messages sent by TOPS
TCMSGIN, TCMSGIN2	Total TCAP messages terminating at this node Pegged for all IS-41 and GSM TCAP messages received by TOPS
TCUNIDIR, TCUNIDI2	Total TCAP msgs sent/rcvd w/ package type UNIDIRECTIONAL Not pegged on wireless TOPS calls
TCQWPERM ,TCQWPER2	Total TCAP msgs sent/rcvd w/ package type QUERY W/ PERM Pegged when TOPS receives ANLYZD. Also pegged when TOPS sends an SMS.
TCQNPERM, TCQNPER2	Total TCAP msgs sent/rcvd w/ package type QUERY W/O PERM Not pegged on wireless TOPS calls
TCCWPERM ,TCCWPER2	Total TCAP msgs sent/rcvd w/ package type CONV W/ PERM Pegged when TOPS receives CONNFAILRPT
TCCNPERM, TCCNPER2	Total TCAP msgs sent/rcvd w/ package type CONV W/O PERM Pegged when TOPS sends CONNRES and RESETTIMER
TCRESPNS, TCRESPN2	Total TCAP msgs sent/rcvd w/ package type RESPONSE Pegged when TOPS sends anlyzd. Also pegged when TOPS receives response from message center.
TCINVKL, TCINVKL2	Total components sent/rcvd of type INVOKE LAST Pegged when TOPS received ANLYZD and CONNFAILRPT; also when TOPS sends CONNRES and RESETTIMER; also when TOPS sends an SMS.
TCINVKNL, TCINVKN2	Total components sent/rcvd of type INVOKE NOT LAST Not pegged on wireless TOPS calls
TCRSLTL, TCRSLTL2	Total components sent/rcvd of type RETURN RESULT LAST Pegged when TOPS sends anlyzd
TCRSLTNL, TCRSLTN2	Total components sent/rcvd of type RETURN RESULT NOT LAST Not pegged on wireless TOPS calls
TCRTERR, TCRTERR2	Total components sent/rcvd of type RETURN ERROR Pegged when TOPS sends AnalyzedInformation RETURN ERROR

TCAPUSAG mapping to TOPS IS-41 and GSM ADACC event

Register	Description and applicability to TOPS IS-41 ADACC
TCREJECT, TCREJEC2	Total components sent/rcvd of type REJECT Pegged when TOPS sends AnalyzedInformation REJECT, or receives SMS REJECT
TCABORT, TCABORT2	Total TCAP msgs sent/rcvd w/ package type ABORT Not pegged on wireless TOPS calls

TOPS message center (TOPSMC) test tool

This feature introduces a test tool for verifying TOPS short message service. The test tool consists of two service control point (SCP) processes, one for IS-41 and one for GSM, which simulate message centers (MCs). These SCP processes run on the TOPS switch.

The simulated message centers are reached using the SS7 network. When an operator or automated node creates an SMS, TOPS formats the SMS into a TCAP message. TOPS uses either IS-41 or GSM, depending on the wireless network type of the calling party. TOPS then uses global title translation to send the TCAP message into the SS7 network.

The message arrives at one of the SCP simulators, which uses the destination number to index new Table TOPSMCDB (TOPS Message Center Database) to determine the disposition of the message. Possible results are:

- Successful acknowledgment sent back to TOPS switch
- Negative acknowledgment with cause code sent back to TOPS switch
- TCAP REJECT with reject reason sent back to TOPS switch
- Time-out (no response)

When TOPS receives the response (or the `SMS_TIMEOUT` timer expires), TOPS pegs OMs in new groups SMSTOPS and TC7WRLSS. In failure situations TOPS generates a TCAP log or a TOPS131 log.

Recall that the protocol chosen (IS-41 or GSM) is based on WIN messaging. If the call is not a WIN call, the protocol chosen is based on incoming trunk group datafill in Table TOPSTOPT. If the protocol is IS-41, but the global title translation datafill routes the SMS to the GSM simulator, the GSM simulator will generate a TCAP log and reject the SMS before accessing Table TOPSMCDB. The same is true for sending a GSM SMS to the IS-41 MC simulator.

The components are as follows, and the remainder of this appendix describes them in more detail.

- Table TOPSMCDB: This table allows datafill of destination numbers and SMS dispositions for these numbers.
- SS7: New subsystems TIS41SIM and TGSMSIM
- Global title translation: C7GTTTYPE and C7GTT datafill is required to route SMS messages to the simulators.

Table TOPSMCDB

Table TOPSMCDB allows datafill of up to 64 SMS destination numbers. The disposition of the short message attempt is datafilled against each number. Table TOPSMCDB can serve short messages based on IS-41 and GSM.

The available dispositions are as follows:

- **SUCCESS:** A successful SMS acknowledgment is sent back to TOPS.
- **ERROR:** A negative acknowledgment with a cause code is sent back to TOPS. The cause codes are different for IS-41 and GSM, so datafilling ERROR requires the datafill of an IS-41 cause code and a GSM cause code.
- **REJECT:** Setting a disposition of REJECT causes a TCAP REJECT message to be sent back to TOPS. Since IS-41 and GSM share TCAP REJECT reasons, separate fields are not necessary. The reject reason consists of two fields, a problem type and a problem code.

If an SMS arrives at a simulator and the destination number is not found in Table TOPSMCDB, the SMS is ignored. Eventually the TOPS SMS timer will expire and the SMSTOPS OM TIMEOUT will be pegged. The TOPS SMS timer is set by parameter SMS_TIMEOUT in Table TOPSPARM.

A final TOPSMCDB field, DELAYSEC, indicates how long the simulators should wait before sending the SMS response. This is used to simulate real-world exchanges with message centers. It is datafilled for all dispositions.

Note: The simulator is not multi-threaded. SMS messages arriving during the DELAYSEC delay are not processed until the delay time has expired. If several SMS messages arrive at once, they are processed sequentially. So the response time for the later short messages can easily exceed normal SMS time-out values.

The following figure shows three destination numbers in Table TOPSMCDB.

Table TOPSMCDB

```

TABLE: TOPSMCDB
DESTDIGS RESPAREA DELAYSEC
-----
6199421465 ERROR SMSNOTSUPPORT FACILITYNOTSUPPORT 2
9194321234 REJECT GENPROB BADCOMPSTRUCT 2
9199910000 SUCCESS 2

```

SS7 datafill and maintenance

The following items are required to enable the TOPS IS-41 and GSM message center simulators.

- Table C7LOCSSN: Add tuples for the TIS41SIM and TGSMSIM subsystems.
- MAP operation: From the SCCPLOC level of the MAP (MAPCI;MTC;CCS;CCS7;SCCPLOC), post and return to service the TIS41SIM and TGSMSIM subsystems.
- Table C7RTESET: Datafill of Table C7RTESET is optional, since it is possible to define an internal SS7 link to the simulators, as described in the next section.

It is also possible to set up looparound SS7 links, or to set up a looparound which goes through an STP. When setting up looparound links, datafill in C7RTESET and other SS7 tables (e.g. C7LKSET) is required. Using looparound links, or links to a second test switch where the TOPS MC simulators are running, is a more realistic way to test the SMS function.

Global title translation

The following figure shows datafill which will route all SMS attempts to the TOPS MC IS-41 simulator using internal SS7 links. The tuple in Table C7GTT can be split into several tuples in order to send some SMS attempts to the IS-41 MC simulator while other SMS attempts go to the GSM MC simulator.

Table C7GTTTYPE

```

TABLE: C7GTTTYPE
GTTNAME GTTYPE GTTID
-----
TOPSSMS ANSI7 17 (MDNMCMT) $

```

Table C7GTT

TABLE: C7GTT GTTKEY GTTRSLT ----- TOPSSMS 0 9 SSNONLY TIS41SIM \$

Fault Management for A00003687

Fault management strategy

The TOPS131 log was added in SN06 by feature A00000816: “TOPS Wireless ADACC with Release.” TOPS generates this log in failure situations when interacting with a cell phone caller and a Mobile Switching Center (MSC).

This SN07 feature updates the text title string in the log. The log was formerly titled “TOPS IS-41 Trouble.” To make it more general, it is now titled “TOPS Wireless Trouble.” An additional line of text is added to identify whether the trouble occurred on an IS-41 or GSM call.

This feature also adds some new reasons to the Reason field.

Fault management tools and utilities

LOGUTIL and related log tables (LOGCLASS, LOGDEV) can be used to view and collect logs relating to TOPS wireless applications.

Logs

Explanation

Log Title: TOPS131

Name: TOPS Wireless Trouble (changed from TOPS IS-41 Trouble)

Description: This log is generated in the TOPS switch when problems occur on a wireless ADACC with release call, or when problems occurs when TOPS tries to send a short text message using Short Message Service (SMS).

In the ADACC case, the log indicates TOPS attempted to provide ADACC with Release Link Trunking (RLT) to a wireless customer, but an unexpected problem prevented this.

This log is not generated when the call is disconnected prior to call completion due to normal reasons (e.g. calling party abandons, or operator can't locate DA listing and ends call).

In the SMS case, this log indicates an SMS did not reach the cell phone user. The log text gives an indication of the problem.

Event type: Major. Each log can represent the loss of one call, or that requested information could not be provided. On RLT calls, the wireless customer is disconnected prior to call completion to the requested number.

Format

```
TOPS131 <mmdd hh:mm:ss ssdd> TBL TOPS Wireless Trouble
CKT      <CPID>
MSC route set: <serving MSC route set from Table C7RTESET>
Called digits: <digits>
Reason:      <reason text>
Wireless type: <IS-41 or GSM>
```

Example:

```
TOPS131 OCT01 15:07:54 7100 TBL TOPS Wireless Trouble
MSC route set:      RTP8_STPA_N_RS
Called digits:      201-220-1234 (TLDN)
Reason:             Failure at MSC
Wireless type:      IS-41
```

Example:

```
TOPS131 OCT01 15:07:54 7100 TBL TOPS Wireless Trouble
CKT RTPC RTP8_ISUP 2
MSC route set:      RTP8_STPA_N_RS
Called digits:      619-322-1234 (Destination number)
Reason:             SMS failure: Network problem (2)
Wireless type:      IS-41
```

Field descriptions

This feature does not change TOPS131 fields CKT, MSC route set, or Called digits. This feature adds additional text reasons to the Reason field as indicated in the table in this section. This feature also adds a new field, Wireless type, which indicates whether the log was generated on an IS-41 or GSM call.

The Reason field describes the category of the error. When the log is generated due to a negative acknowledgment from the message center, the exact byte value of the cause code is included in parentheses at the end of the Reason field. The meaning of the byte value can be found in the specifications as follows:

- IS-41-D: Chapter 5, section 6.5.2.125 (SMS Cause Code), table 171
- GSM: 3GPP TS 29.002 V4.12.0 (2003-06), sections 7.6.1 and 12.2.3.

Field descriptions

Field	Value	Description
Reason	SMS failure: Network problem <nn>	The message center encountered a network problem and could not process the TOPS SMS.
Reason	SMS failure: Terminal problem <nn>	The message center could not process the TOPS SMS due to problems with the terminal (cell phone) specified by the destination number.
Reason	SMS failure: Radio interface problem <nn>	The message center could not process the TOPS SMS due to problems with the radio interface to the cell phone.
Reason	SMS failure: Miscellaneous problem <nn>	The message center could not process the TOPS SMS for a reason other than the above three. One example is if the format of the TOPS SMS was not understood by the message center.
Reason	SMS failure: Time-out	A response was not received to the TOPS SMS within the time period defined in Table TOPSPARM parameter SMS_TIMEOUT.
Reason	SMS failure: Global title translation	Tables C7GTTTYPE and C7GTT cannot accommodate the destination number listed in the log.
Reason	No transaction IDs	No transaction ID could be obtained when TOPS attempted to send an INVOKE, whether for IS-41 WIN, GSM CAMEL, or SMS. This means the message could not be sent.
Reason	WIN: Wireless protocol mismatch	The wireless network protocol established by the IS-41 ANLYZD or GSM InitialDP message did not match the trunk group datafill (RLT_IS41 or RLT_GSM) in Table ISUPTRK when the call arrived. The call cannot proceed because the version of IS-41 or GSM RLT is unknown.
Wireless type	IS-41	The log was generated on a TOPS IS-41 call.
Wireless type	GSM	The log was generated on a TOPS GSM call.

Action

The action taken depends on the contents of the reason field as follows.

Reason to action mapping

Reason text	Action
SMS failure: <i>(any SMS failure except GTT)</i>	Examine SS7 and TCAP logs on the TOPS switch and at the message center. Use an operator position to send SMS messages and verify the messages arrive at the message center. Use message center tools to verify SMS can be forwarded to the cell phone. If time-outs are occurring, investigate whether the <code>SMS_TIMEOUT</code> parameter in Table TOPSPARM needs to be increased.
SMS failure: Global title translation	Check datafill in Tables C7GTTYPE and C7GTT for the destination number listed in the log. Look for tuples containing MDNMC GT (mobile directory number to message center global title).
No transaction IDs	Contact Nortel Networks. TOPS automatically allocates transaction IDs when needed.
WIN: Wireless protocol mismatch	Correct the datafill mismatch in Table ISUPTRK. The MSC specified in the log is sending one kind of protocol to TOPS, but is datafilled in Table ISUPTRK as another kind.

Associated Operational Measurements or Performance Measurements**Reason to OM mapping**

TOPS131 reason text	OM
SMS failure: Network problem	Group SMSTOPS, register SMSNETWK
SMS failure: Terminal problem	Group SMSTOPS, register SMSTERM
SMS failure: Radio interface problem	Group SMSTOPS, register SMSRADIO
SMS failure: Miscellaneous problem	Group SMSTOPS, register SMSMISC
SMS failure: Time-out	Group SMSTOPS, register SMSTIME
SMS failure: Global title translation	Group TC7WRLSS, register GTTFAIL
No transaction IDs	Group TC7WRLSS, register NOTRIDS
WIN: Wireless protocol mismatch	None

Additional information

Since short messaging can fail in many expected situations (such as wireless phone powered off, destination number not subscribed to SMS, etc.), the TOPS131 logs can be throttled. A new parameter in Table TOPSPARM, SMS_LOG_MC_FAILURE, determines when TOPS131 logs are generated as a result of SMS failure. TOPS131 to be generated in some SMS failure scenarios but not others. See the Configuration chapter for more information.

Alarms

No new or changed alarms.

Related documentation

Not applicable.

Configuration for A00003687

Hardware and Software Requirements

The Mobile Switching Centers (MSCs) and the TOPS switches must have SS7 connectivity. ISUP voice trunk connectivity is necessary for Wireless ADACC with Release.

The customer's SS7 network must have global title translations set up such that short messages from the TOPS node can route to the correct message centers.

The MSCs must have MSC and network translations set up such that the TOPS TLDN routes the call to the TOPS node for service processing.

Initial Configuration

Not applicable.

Office parameters (OP)

Existing Table OFCENG parameter NUM_OF_IS41TOPS_EXT_BLKs is replaced with new Table OFCAUT parameter NUM_OF_WIN_TOPS_EXT_BLKs. This parameter provisions the WIN TOPS extension block (formerly IS41TOPS_EXT_BLK; now WIN_TOPS_EXT_BLK). The extension block serves both IS-41 and GSM TOPS calls, so it has been renamed to be more general. Since it has been moved to Table OFCAUT, it is now allocated automatically.

New/modified office/subnet parameters

Parm table	Parameter name	NEW/CHANGE D/DELETED/RE LOCATED	Domain (CM or Subnet Management)
OFAUT	NUM_OF_WIN_TOPS_EXT_BLKs	New	CM
OFCENG	NUM_OF_IS41TOPS_EXT_BLKs	Deleted	CM

Parameter information**NUM_OF_WIN_TOPS_EXT_BLKs**

Number of Wireless Intelligent Network TOPS Extension Blocks

Functional description

This parameter controls how many extension blocks are allocated for use by Wireless Intelligent Network (WIN) TOPS calls.

WIN TOPS extension blocks are used for TOPS calls originating from IS-41 wireless networks as well as calls originating from GSM wireless networks. Each extension block stores data about a wireless call while TOPS is waiting for the MSC to outpulse to TOPS on a voice trunk.

Provisioning rules

This parameter is located in Table OFAUT, so additional EXT blocks are allocated automatically when needed.

By default, WIN TOPS extension blocks are allocated in groups of 100 using the capabilities of Table OFAUT.

Range information

Minimum	Maximum	Default
0	32767	0 (no WIN TOPS extension blocks allocated)

Activation

The parameter is allocated automatically. No restarts are necessary.

Dependencies

None.

Consequences

Since the parameter is under the control of Table OFCAUT, it should not be under provisioned. If there are not enough extension blocks, TOPS131 logs will appear, and wireless calls will be routed to treatment in the MSCs.

By default, WIN TOPS extension blocks are allocated in blocks of 100, so the extension blocks should normally be over provisioned, using slightly more memory than is required during peak periods.

Verification

To verify that the WIN TOPS extension blocks are allocated, use the CI command `OMSHOW EXT ACTIVE WIN_TOPS_EXT_BLK`.

Memory requirements

Each WIN TOPS extension block requires 128 words. So the total memory used by the EXT blocks is $(\text{NUM\_OF\_WIN\_TOPS\_EXT\_BLKS} * 128 \text{ words})$.

Parameter release history update

SN06: Parameter `NUM_OF_IS41TOPS_EXT_BLKs` created.

SN07: Parameter `NUM_OF_IS41TOPS_EXT_BLKs` removed and parameter `NUM_OF_WIN_TOPS_EXT_BLKs` added to accommodate IS-41 and GSM.

Upgrade Impact**Dump and Restore**

Not applicable. `NUM_OF_WIN_TOPS_EXT_BLKs` starts with a default value of 0 and is increased automatically as needed.

Element Management Upgrade

Not applicable.

Data schema (DS)**New/modified tables**

Table name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
ISUPTRK	Changed	Unchanged
MSCIDMAP	New	New
TOPSFTR	Changed	Unchanged
TOPSMCDB	New	New

Table name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
TOPSPARM	Changed	Unchanged
TOPSTLDN	Changed	Unchanged
TOPSTOPT	Changed	Unchanged

Table information

Name: ISUPTRK

ISUP Trunk

Functional description

Table ISUPTRK is a TOPS table which associates TOPS options and features with ISUP trunk groups. TOPS ISUP calls use standard ISUP trunk group datafill in Table TRKGRP, and Table ISUPTRK was created to allow datafill of TOPS options and features without affecting standard ISUP trunk group datafill.

Usage sequence and implications (CM Only)

A trunk group must be datafilled in Table TRKGRP and Table TRKSGRP before it can be datafilled in Table ISUPTRK. This sequence is unchanged.

Size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ISUPTRK	Unchanged	Unchanged	Unchanged

Fields

The following table lists changed fields for Table ISUPTRK.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RLT	Changed	Unchanged	NONE, RLT_REL, RLT_FAR, RLT_IS41, RLT_GSM	Release link trunking: Value RLT_GSM is added by this feature. When the user selects RLT_GSM, they are presented with the existing subfields added in SN06 for value RLT_IS41: RLT_VERSION, RESETTIMER, and TIMERVAL Note that RLT_GSM cannot be datafilled at this time. RLT_GSM is for future use.

Datafill example

The following example shows sample datafill for Table ISUPTRK. The RLT type is set to GSM, the RLT version is set to 1, and the reset timer is enabled and set to 20 seconds.

RLT_GSM is for future use and cannot be datafilled at this time.

TABLE: ISUPTRK							
GRPKEY		CONNTYPE		LCANAME		BILLCD CALLSRC	
ANI2CLI		RLT	SNTPDRST	DNLKUP	DISPLAY	ININTWRK	BRANDCHC

MSC_DACC1		CELL_MOBILE		IEC	NLCA	TOPSBC	0 ORIG
Y	RLT_GSM	1	Y	20	N	N	0
				N	N	NONE	N

Table release history update

SN06: Value RLT_IS41 plus subfields RLT_VERSION, RESETTIMER, and TIMERVAL added to RLT field to accommodate WIN TOPS calls using IS-41.

SN07: Value RLT_GSM added to RLT field to accommodate WIN TOPS calls using GSM. The same subfields are used.

Supplementary information

No dump and restore necessary, since value RLT_GSM did not exist in SN06.

Translation verification other tools

Not applicable.

Table information

Name: MSCIDMAP

Mobile Switching Center Identifier Mapping

Functional description

This table maps Mobile Switching Center Identifiers (MSCIDs) to TLDN pool identifiers from Table TOPSTLDN. This allows the customer to control TLDN allocation on a per-MSC basis.

An MSCID consists of a Market ID (16 bit value) and a Switch ID (8 bit value). Less than 1,000 market IDs are in use today in the United States, so the datafill of Table MSCIDMAP is held to a maximum of 4,096 different market IDs to limit data store usage.

The switch ID can be any number from 0 to 255. The total number of tuples which can be datafilled is 32,767 (the DMS maximum for any table).

Wildcarding can be used to limit datafill in this table. The market ID and switch ID can be wildcarded as follows:

Market ID	Switch number	Meaning
\$	\$	Match all MSCIDs not otherwise found in table. This combination, when datafilled, serves as the default.
<0 to 65535>	\$	Match exact market ID and any switch number, providing exact MSCID and exact switch number is not datafilled.
<0 to 65535>	<0 to 255>	Match exact market ID and switch number
\$	<0 to 255>	Not allowed. A wildcard market ID cannot be datafilled with a specific switch number.

Usage sequence and implications (CM Only)

Table TOPSTLDN must be datafilled before Table MSCIDMAP.

Size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MSCIDMAP	0	32767	128 words per tuple.

Fields

The following table lists fields for Table MSCIDMAP.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
MARKETID	New	None	{0 to 65535}, or '\$'	Market Identifier (vector). First part of two-part key MSCID.
SWITCHID	New	None	{0 to 255}, or '\$'	Switch Identifier (vector). Second part of two-part key MSCID.
POOLLIST	New	None	Vector of up to 255 TLDN pool identifiers from Table TOPSTLDN	Temporary local directory number pool list. Pointer to TLDN pool IDs in Table TOPSTLDN.

Datafill example

The following example shows sample datafill for Table MSCIDMAP.

TABLE: MSCIDMAP						
MSCID		POOLIDS				

\$	\$	(0)	(1)	(2)	(3)	\$
64	\$			(0)	(2)	\$
64	5			(0)	(1)	\$
312	444		(0)	(1)	(2)	\$
312	445		(0)	(1)	(2)	\$

Table release history update

Created in SN07

Supplementary information

During dump and restore from SN06 to a later load, Table TOPSTLDN is checked. If it has any entries, they are restored using sequential pool IDs beginning with pool ID 0. Then a single tuple with the key {\$, \$} is added to Table MSCIDMAP. This is a wildcard tuple which matches all MSCIDs and which contains all pool IDs from restored Table TOPSTLDN.

Translation verification other tools

Not applicable.

Table information

Name: TOPSFTR

TOPS Feature

Functional description

Table TOPSFTR is a TOPS table which allows optional TOPS functions to be activated and deactivated easily. Once the SOC option has been turned on for a TOPS feature, the customer can use Table TOPSFTR to turn the function on and off.

This feature adds tuple `RLT_FOR_GSM`, which controls GSM ADACC with Release. **This tuple is for future use and cannot be set to 'Y' at this time.**

Usage sequence and implications (CM Only)

Tuple `RLT_FOR_GSM` must be set to Y in order for TOPS to process wireless calls using GSM CAMEL.

Size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TOPSFTR	Unchanged	Increased by 1	Unchanged

Fields

The following table lists fields for Table TOPSFTR.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
FTRNAME	Changed	None	RLT_FOR_GSM	Feature name: This tuple is for future use. It will allow the customer to enable GSM TOPS ADACC with release. In order to activate the feature, the SOC option OSEA0104 must be on, and this tuple must be set to Y.
FTRENABL	Unchanged	None	Y/N	Feature enable: Activates or deactivates an optional TOPS feature. The tuple's default value is N.

Datafill example

The following example shows sample datafill for Table TOPSFTR. The TOPS WIN and TOPS SMS features have been activated.

```
TABLE: TOPSFTR
      FTRNAME FTRENABL
-----
      RLT_FOR_GSM      Y
```

Table release history update

Table initially added in TOPS15.

Supplementary information

None.

Translation verification other tools

Not applicable.

Table information**Name: TOPSMCDB**

TOPS Message Center Database

Functional description

This table provides datafill for a TOPS SMS SS7-based message center simulator. An operator position or automated node can send SMS messages using either IS-41 TCAP or GSM TCAP. When the simulator receives the SMS, it looks up the data stored against the SMS destination number to determine the disposition of the SMS. The simulator can successfully acknowledge the SMS, send back a failure message, or ignore the SMS so the TOPS SMS time-out code executes.

Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order.

Size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TOPSMCDB	0	64	2 words per tuple

Fields

The following table lists fields for TOPSMCDB.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DESTDIGS	New	None	1-18 digits	Digilator field containing the destination number
RESULT	New	See below	SUCCESS, REJECT, or ERROR	Tells disposition of SMS to this destination number
PROBTYPE	New	Subfield of RESPAREA when RESULT set to REJECT	GENPROB, TRANSPROB, ERRPROB, RESPPROB, INVPROB	Defines problem type.
PROBCODE	New	Subfield of RESPAREA when RESULT set to REJECT	tbd: Numerous codes, depending on contents of PROBTYPE, will copy them in here later	Defines problem code. The choices for problem code vary based on the problem type.
IS41CODE	NEW	Subfield of RESPAREA when RESULT set to ERROR	tbd: Numerous cause codes defined in IS-41, will copy them in here later	Contains cause code to send for IS-41 message center negative acknowledgment. Several dozen cause codes are defined in IS-41.
GSMCODE	New	Subfield of RESPAREA when RESULT set to ERROR	tbd: Numerous cause codes defined in GSM, will copy them in here later	Contains cause code to send for GSM message center negative acknowledgment. Several dozen cause codes are defined in GSM.
DELAYSEC	New	None	0 to 255	Delay in seconds before sending response. Helps simulate real-world response time.

Datafill example

The following example shows sample datafill for Table TOPSMCDB.

```
TABLE: TOPSMCDB
DESTDIGS RESPAREA DELAYSEC
-----
6199421465 ERROR SMSNOTSUPPORT FACILITYNOTSUPPORT 2
9194321234 REJECT GENPROB BADCOMPSTRUCT 2
9199910000 SUCCESS 2
```

Table release history update

Created in SN07

Supplementary information

None.

Translation verification other tools

Not applicable.

Table information**Name: TOPSPARM**

TOPS Parameter

Functional description

Table TOPSPARM is a TOPS-specific version of the office parameter tables. This feature adds two new parameters, SMS_MC_LOG_FAILURE and SMS_TIMEOUT.

SMS MC LOG FAILURE

The telco can use the first parameter, SMS_LOG_MC_FAILURE, to limit the number of TOPS131 logs generated in SMS failure situations. There are many normal situations in which the message center (MC) will return an error code. These might include wireless phone powered off, or destination number not subscribed to SMS. The telco might not wish to have TOPS131 logs generated for these situations. Note that OMs in group SMSTOPS are pegged for these situations.

SMS_LOG_MC_FAILURE is a set field consisting of the following values. These values are related to the cause code returned by the MC when an SMS fails. This parameter only controls the TOPS131 log upon receipt of a negative acknowledgment from the MC. The TOPS131 is always generated as a result of global title translation failure, SS7 routing failure, or SMS time-out.

- NONE: Do not generate the TOPS131 for any of the following reasons.
- NETWK: Generate the TOPS131 when a negative acknowledgment is received from the MC with the Cause Code set to a network problem value.

- **TERM:** Generate the TOPS131 when a negative acknowledgment is received from the MC with the Cause Code set to a terminal problem value.
- **RADIO:** Generate the TOPS131 when a negative acknowledgment is received from the MC with the Cause Code set to a radio interface problem value.
- **MISC:** Generate the TOPS131 when a negative acknowledgment is received from the MC with the Cause Code set to a general problem value.
- **ALL:** Generate the TOPS131 for all of the above reasons.

SMS_LOG_MC_FAILURE can be set to NONE, ALL, or any combination of NETWK, TERM, RADIO, and MISC.

The default value of SMS_LOG_MC_FAILURE is ALL.

SMS TIMEOUT

The second parameter, SMS_TIMEOUT, controls how long TOPS waits before marking an SMS attempt as timed out. The time-out period is datafilled in seconds. The default value of SMS_TIMEOUT is 30 seconds, since operators and automated nodes do not wait while the SMS attempt is in progress, and the SMS acknowledgment can be received after the call is ended.

The time-out value is required since the position or service node cannot send a second SMS while the first SMS transaction is in progress. Also, the time-out ensures DMS resources are cleaned up if the SMS is lost in the network.

Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order.

Size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TOPSPARM	Increased by 2	Increased by 2	Unchanged

Fields

The following table lists fields for Table TOPSPARM.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
PARMNAME	Changed	None	SMS_LOG_MC_FAILURE is added to the range of TOPS parameters.	This parameter controls when the TOPS131 log is generated in certain SMS failure situations.
PARMVAL	Unchanged	None	Set of {NONE, NETWK, TERM, RADIO, MISC, ALL}	This parameter can be set to NONE, ALL, or any combination of the four remaining values. Its default value is ALL, meaning generated the TOPS131 in all failure situations.
PARMNAME	Changed	None	SMS_TIMEOUT is added to the range of TOPS parameters.	This parameter controls the amount of time in seconds before TOPS marks an SMS attempt as timed out.
PARMVAL	Unchanged	None	0 to 255	Parameter SMS_TIMEOUT can be set to values 0 to 255. Its default value is 30.

Datafill example

The following example shows sample datafill for Table TOPSPARM.

```
TABLE: TOPSPARM
PARMNAME PARMVAL
```

```
-----
SMS_LOG_MC_FAILURE    ALL $
SMS_TIMEOUT           30
```

Table release history update

Table initially added in BCS31.

Supplementary information

When performing a dump and restore from an SN06 load to an SN07 or later load, SMS_LOG_MC_FAILURE will be restored with a value of ALL, and SMS_TIMEOUT will be restored with a value of 30.

Translation verification other tools

Not applicable.

Table information**Name: TOPSTLDN**

TOPS Temporary Local Directory Numbers

Functional description

Table TOPSTLDN provides all TLDNs which can be used by TOPS when providing a Wireless Intelligent Network (WIN) service such as ADACC with release. When a cell phone caller initiates a wireless directory assistance (DA) call and TOPS receives an IS-41 AnalyzedInformation or a GSM InitialDP, TOPS selects an idle TLDN from Table TOPSTLDN and sends it back to the originating mobile switching center (MSC).

Tuples in Table TOPSTLDN define pools of TLDNs from a low TLDN to a high TLDN. Each pool has a numerical index, the pool ID. A new table, MSCIDMAP, maps MSC identifiers (MSCIDs) to one or more pool IDs. When an MSC sends an AnalyzedInformation or InitialDP, the MSCID in the message is used to index Table MSCIDMAP to determine a pool ID. Then an idle TLDN is selected from the pool in Table TOPSTLDN and sent back to the MSC.

A maximum of 2,000 TOPS TLDNs can be defined. The holding time of a TOPS TLDN is very short (around one second), so this number of TLDNs should be able to accommodate heavy TOPS WIN traffic.

Usage sequence and implications (CM Only)

Table TOPSTLDN must be datafilled before Table MSCIDMAP.

Size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TOPSTLDN	0	2000	Memory for all 2000 tuples (10 words each) is allocated when the first tuple is added. Memory is deallocated when the last tuple is deleted.

Fields

The following table lists fields for Table TOPSTLDN.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
POOLID	New	None	0-1999	Pool Identifier: an integer field identifying the pool of TLDNs.
FROMDIGS	Changed	None	10 digits	From Digits: the start of the TLDN range for this tuple.
TODIGS	Changed	None	10 digits	To Digits: the end of the TLDN digit range for this tuple.

Datafill example

The following example shows sample datafill for Table TOPSTLDN.

```
TABLE: TOPSTLDN
POOLID   FROMDIGS   TODIGS
-----
0        2012201234  2012201234
1        2013364400  2013364899
2        2018591400  2018591489
```

Table release history update

SN06: Added by Feature A00000816

SN07: Modified to use a pool ID as the key field.

Supplementary information

During dump and restore from SN06 to a later release, if Table TOPSTLDN contains datafill on the SN06 side, it is restored into Table TOPSTLDN on the restore side with sequential pool IDs beginning with 0.

See the Functional Description chapter for illustrations of Table TOPSTLDN before and after a dump and restore.

Translation verification other tools

Not applicable.

Table information

Name: TOPSTOPT

TOPS Trunk Options

Functional description

This table contains various options datafilled against trunk groups used by TOPS.

Usage sequence and implications (CM Only)

There is no requirement to datafill tables in a specific order.

Size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
TOPSTOPT	Unchanged	Unchanged	Negligible (additional 4 bits per tuple)

Fields

The following table lists fields for Table TOPSTOPT.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
WIRELESS	New	None	Y/N If Y, then a further refinement, NETTYPE, appears.	Wireless: Indicates if the trunk group carries wireless (cellular) traffic. This field controls whether TOPS can use wireless functions on a non-WIN (non-CAMEL) call. If the field is set to Y, all traffic is assumed to be from a wireless phone.
NETTYPE	New	None	IS41 or GSM	Network type: Indicates if the wireless network type connected by the trunk group is IS-41 or GSM.

Datafill example

The following example shows sample datafill for Table TOPSTOPT.

TABLE: TOPSTOPT

GRPKEY ORGAREA DISPCLG ADASERV ADASANS ANITOCCLI OLNSQRY DCIBIDX LNPCLGAM
XLASCHEM SPIDPRC TRKSPID BILLSCRN ANIFSPL MAXCONNS DISPSPID WIRELESS

TEAOSSIC N Y NONE NA Y N NONE 0 N N N N N N 0 N N
TOSSIC N Y NONE NA Y N NONE 0 N N N N N N 0 N Y IS41
TBELLBIC N Y NONE NA N NONE 0 N N N N N N 0 N Y GSM

Table release history update

SN07 - Added field WIRELESS.

Supplementary information

The default value of WIRELESS on a dump and restore is N. Currently this field is only used when sending a TOPS SMS on a non-WIN (non-CAMEL) call. On an IS-41 WIN or GSM CAMEL call, the originating wireless network type is already known through signaling.

Translation verification other tools

Not applicable.

Service Orders (SO)

Not applicable.

Software optionality control (SOC)

No new SOC's are added by this feature. Regarding the two main components of this feature:

- GSM ADACC with Release is under the control of an existing SOC (OSEA0104, which also controls IS-41 ADACC with Release).
- TOPS SMS is not under the control of SOC.

Element Management

Not applicable.

Command interface changes

Not applicable.

Security

Not applicable.

Configuration Walkthrough

Tables C7GTTTYPE and C7GTT must be datafilled before TOPS can send short messages into the SS7 network. These must use a global title translation number for MDN to Message Center (MDNMCGT) routing such that when the

TOPS-sent SMS arrives at the STPs, it is routed to the calling party's message center.

Since SMS has been supported over SS7 for some time, much of the necessary SMS global title translation datafill is probably already present. TOPS might require large amounts of MDNMCGT datafill, but a more likely scenario is that large blocks of MDNMCGT global title translations can be off-loaded to existing STPs using a small number of MDNMCGT tuples in the TOPS switch.

Performance for A00003687

Performance management strategy

This feature is an extension of SN06 feature A000000816: "Wireless ADACC with Release." This feature provides additional functions involving TCAP messaging between mobile switching centers (MSCs), message centers (MCs), and TOPS. The main tools used to monitor the performance of these features are operational measurements (OMs).

OM group IS41TOPS was created by feature A000000816 in SN06. With the functional additions of this SN07 feature, OM group IS41TOPS is no longer sufficient. This feature creates three new OM groups (SMSTOPS, WINTOPS, and TC7WRLSS) and removes group IS41TOPS.

Events which previously pegged registers in group IS41TOPS will now peg registers in OM groups WINTOPS and TC7WRLSS. For more information including a complete mapping of old to new registers, see the Functional Description chapter of this document.

Performance management tools and utilities

The new OM group is accessed using the OMSHOW command from the Maintenance and Administrative Position (MAP).

Operational Measurements (OMs)

This feature creates the following OM groups:

- SMSTOPS
- WINTOPS
- TC7WRLSS

This feature removes the following OM group:

- IS41TOPS

All events formerly pegged in group IS41TOPS are now pegged in groups WINTOPS and TC7WRLSS.

OM group SMSTOPS

Register	Meaning
SMSSSENT, SMSSSENT2	SMS sent
SMSSUCC, SMSSUCC2	SMS success
SMSFAIL, SMSFAIL2	SMS failure
SMSTIME, SMSTIME2	SMS time-out
SMSNETWK	SMS failure due to network problems
SMSTERM	SMS failure due to terminal (cell phone) problems
SMSRADIO	SMS failure due to radio interface problems
SMSMISC	Miscellaneous SMS failure

OM group WINTOPS

Register	Meaning
WINBEGIN, WINBEGIN2	IS-41 AnalyzedInformation or GSM InitialDP received
REQCONN, REQCONN2	IS-41 ConnectResource or GSM EstablishTemporaryConnection sent
DISCONN, DISCONN2	IS-41 AnalyzedInformation with action code of "disconnect call" or GSM DisconnectTemporaryConnection sent. This event is not part of the normal IS-41 call flow, but it is part of the normal GSM call flow. If this is pegged for IS-41, it means ADACC with release was not provided.
CONNECT, CONNECT2	IS-41 AnalyzedInformation or GSM Connect sent
WINEND, WINEND2	GSM Application End received; no equivalent IS-41 message
ERRCONN	MSC could not connect to TOPS using TLDN
ERRDISC	TOPS disconnected unexpectedly while providing operator assistance. IS-41 only; when this occurs in a GSM call, WINEND is pegged but not DISCONN or CONNECT.
ERRSSFT	MSC's service switching function timer expired. Should not happen if TOPS Reset Timer is datafilled properly in Table ISUPTRK.
ABANDON	Wireless caller disconnected prior to receiving ADACC with release.
RESTIMR, RESTIMR2	ResetTimer sent (IS-41 and GSM)

OM group WINTOPS

Register	Meaning
NOTLDNS	No TLDNs available in Table TOPSTLDN
NODATA	TOPS could not find EXT block associated with incoming TLDN call from MSC
RXLAFAIL	TOPS call could not obtain original called digits and defaulted to 411
SANTIMR	MSC did not release trunk to TOPS, or MSC did not send Application End
TLDNTIME	A TLDN was allocated for an MSC call which never arrived. The TLDN is allocated to a new call.

OM group TC7WRLSS

Register	Meaning
INVOKES, INVOKES2	TCAP INVOKE sent
INVOKER, INVOKER2	TCAP INVOKE receives
RETRESS, RETRESS2	TCAP RETURN RESULT sent
RETRESR, RETRESR2	TCAP RETURN RESULT received
RETERRS	TCAP RETURN ERROR sent
RETERRR	TCAP RETURN ERROR received
REJECTS	TCAP REJECT sent
REJECTR	TCAP REJECT received
ABORTS	TCAP ABORT sent
ABORTR	TCAP ABORT received
NOTRIDS	No transaction identifiers
MBFULL	Incoming message from MSC ignored due to heavy traffic
RTFNOXLA	SCCP routing failure: No translation of such nature
RTFNOXLS	SCCP routing failure: No translation for this specific address
RTFSUBCG	SCCP routing failure: Subsystem congestion
RTFSUBFL	SCCP routing failure: Subsystem failure
RTFUNEQ	SCCP routing failure: Unequipped user

OM group TC7WRLSS

Register	Meaning
RTFNETFL	SCCP routing failure: Network failure
RTFNETCG	SCCP routing failure: Network congestion
RTFMISCE	SCCP routing failure: Failure other than the above seven
GTTFAIL	Global Title Translation failure

OM format

These OMs apply to events occurring on the TOPS switch during the course of a wireless (cellular) phone originated call to TOPS. In large TOPS offices, many such calls can occur during the reporting period, so several of the OMs introduced by this feature include extension registers. The extension registers are noted in the OM register text.

OM Group SMSTOPS**OM description**

SMSTOPS

Short Message Service - TOPS

Release history update

Created in SN07

Registers

OM group registers display on the MAP terminal as follows:

OM Group Display

SMSENT	SMSENT2	SMSSUCC	SMSSUCC2
SMSFAIL	SMSFAIL2	SMSTIME	SMSTIME2
SMSNETWK	SMSTERM	SMRADIO	SMSMISC

Group structure

OM group SMSTOPS provides one tuple for each wireless network type.

Key field: IS41 and GSM. There are two tuples in OM group SMSTOPS: one for IS-41 SMS and one for GSM SMS.

Info field: None

Associated OM groups

Registers in groups SMSTOPS and TC7WRLSS are pegged when TOPS sends an SMS and receives an acknowledgment.

Associated functional groups

None

Associated functionality codes

None

OM group registers logic flow chart

Register SMSSENT is pegged when TOPS sends a short message into the SS7 network.

Register SMSSUCC is pegged when TOPS receives a positive acknowledgment from the message center.

Register SMSFAIL is pegged when TOPS receives a negative acknowledgment from the message center.

Register SMSTIME is pegged when TOPS receives no acknowledgment from the message center within a customer-defined time period.

Patterns

- Every SMS attempt will peg SMSSENT plus one of the other registers. If an acknowledgment arrives after the time period has expired, the success or failure OM is pegged in addition to the time-out OM.
- The value of register SMSSENT should be close to the value of register SMSSUCC, with any slight inequality due to reporting period boundaries. If the value of SMSSUCC is significantly less than the value of SMSSENT, SMS failures are occurring either at TOPS, within the SS7 network, or at the message center.

Register SMSFAIL**Register description**

Short Message Service Failure

SMSFAIL is a peg register. It is incremented whenever TOPS receives a negative acknowledgment from the message center following an SMS attempt.

Register release history update

Created in SN07

Associated registers

Extension register SMSFAIL2

Associated logs

TOPS131 or TCAP100, depending on type of failure

Register SMSMISC**Register description**

Short Message Service Miscellaneous failure

SMSMISC is a peg register. It is incremented whenever TOPS receives a negative acknowledgment from the message center saying the message could not be delivered due to a miscellaneous failure (not network, terminal, or radio interface).

Register release history update

Created in SN07

Associated registers

None

Associated logs

TOPS131

Register SMSNETWK**Register description**

Short Message Service Network failure

SMSNETWK is a peg register. It is incremented whenever TOPS a negative acknowledgment from the message center saying the message could not be delivered due to a network failure.

Register release history update

Created in SN07

Associated registers

None

Associated logs

TOPS131

Register SMSRADIO**Register description**

Short Message Service Radio interface failure

SMSRADIO is a peg register. It is incremented whenever TOPS receives a negative acknowledgment from the message center saying the message could not be delivered due to a radio interface failure.

Register release history update

Created in SN07

Associated registers

None

Associated logs

TOPS131

Register SMSSENT**Register description**

Short Message Service Sent

SMSSENT is a peg register. It is incremented whenever TOPS sends an SMS to a message center.

Register release history update

Created in SN07

Associated registers

Extension register SMSSENT2

Associated logs

None

Register SMSSUCC**Register description**

Short Message Service Success

SMSSUCC is a peg register. It is incremented whenever TOPS receives a successful acknowledgment from a message center following an SMS attempt.

Register release history update

Created in SN07

Associated registers

Extension register SMSSUCC2

Associated logs

None

Register SMSTERM

Register description

Short Message Service Terminal failure

SMSTERM is a peg register. It is incremented whenever TOPS receives a negative acknowledgment from the message center saying the message could not be delivered due a terminal (cell phone) failure.

Register release history update

Created in SN07

Associated registers

None

Associated logs

TOPS131

Register SMSTIME

Register description

Short Message Service Time-out

SMSTIME is a peg register. It is incremented whenever TOPS receives no acknowledgment from a message center following an SMS attempt in the allotted time-out period. The time-out period is datafilled in Table TOPSPARM (parameter SMS_TIMEOUT).

Register release history update

Created in SN07

Associated registers

Extension register SMSTIME2

Associated logs

TOPS131

OM Group WINTOPS

OM description

WINTOPS

Wireless Intelligent Network - TOPS

Release history update

Created in SN07

Registers

OM group registers display on the MAP terminal as follows:

OM Group Display

WINBEGIN	WINBEG12	REQCONN	REQCONN2
DISCONN	DISCONN2	CONNECT	CONNECT2
WINEND	WINEND2	RESTIMR	RESTIMR2
ABANDON	ERRCONN	ERRDISC	ERRSSFT
NOTLDNS	NODATA	RXLAFAIL	SANTIMR
TLDNTIME			

Group structure

OM group WINTOPS provides one tuple for each wireless network type.

Key field: IS41 and GSM. There are two tuples in OM group WINTOPS: one for IS-41 WIN and one for GSM CAMEL (Customized Applications for Mobile network Enhanced Logic).

Info field: None

Associated OM groups

Registers in groups WINTOPS and TC7WRLSS are pegged when TOPS provides a Wireless Intelligent Network service such as wireless ADACC with release.

Associated functional groups

None

Associated functionality codes

Functionality codes associated with OM group

Functionality	Code
TOPS Wireless RLT	00034426

OM group registers logic flow chart

For a description of when these OMs are pegged, refer to the IS-41 call flow figure at the beginning of the Functional Description chapter.

Patterns

- Every WIN call flow, whether successful or not, will peg WINBEGIN.
- A successful WIN call flow (IS-41 or GSM) pegs registers WINBEGIN, REQCONN, and CONNECT.

- A successful GSM CAMEL call flow also pegs registers DISCONN and WINEND.
- Registers ABANDON and RESTIMR are pegged under normal circumstances and do not indicate problems.
- Register DISCONN on an IS-41 WIN call does not necessarily indicate a problem. In IS-41, it is always pegged in conjunction with another register. The other register indicates if a problem has occurred.
- Problems are indicated by the following registers: ERRCONN, ERDISC, ERRSFT, NOTLDNS, NODATA, RXLAFAIL, SANTIMR, and TLDNTIME.

Register ABANDON

Register description

Abandon

ABANDON is a peg register. It is incremented on a WIN call when the calling party disconnects before receiving ADACC with release.

This is a common occurrence. The wireless caller can hang up while in queue for operator, or hang up because the operator couldn't find the listing, or hang up without accepting call completion. In all of these cases, ABANDON is pegged.

Register release history update

Created in SN07

Associated registers

None

Associated logs

None

Register CONNECT

Register description

Connect

CONNECT is a peg register. It is incremented when TOPS directs the MSC to connect to the requested number. In IS-41, this is when TOPS sends the AnalyzedInformation RETURN RESULT. In GSM, this is when TOPS sends the Connect.

Register release history update

Created in SN07

Associated registers

Extension register CONNECT2

Associated logs

None

Register DISCONN**Register description**

Disconnect

DISCONN is a peg register. It is incremented when TOPS directs the MSC release the trunk to TOPS. In IS-41, this is when TOPS sends the AnalyzedInformation RETURN RESULT with an Action Code of “disconnect call.”. In GSM, this is when TOPS sends the DisconnectTemporaryConnection.

This register is not normally pegged on an IS-41 call. When it is, it indicates the caller did not receive ADACC with release.

This register is pegged on all successful GSM wireless ADACC with release calls.

Register release history update

Created in SN07

Associated registers

Extension register DISCONN2

Associated logs

None

Register ERRCONN**Register description**

Error Connect

ERRCONN is a peg register. It is incremented on a WIN call when the MSC cannot connect to TOPS using the TLDN provided by TOPS. This might be due to translation or circuit failures at the MSC or in the network.

Register release history update

Created in SN07

Associated registers

None

Associated logs

TOPS131

Register ERRDISC**Register description**

Error Disconnect

ERRDISC is a peg register. It is incremented on a WIN call when TOPS unexpectedly releases its trunk to the MSC. This register is only pegged on an IS-41 call. On a GSM call, registers WINBEGIN, REQCONN, and WINEND are pegged, but not DISCONN and CONNECT.

Register release history update

Created in SN07

Associated registers

None

Associated logs

TOPS131

Register ERRSSFT**Register description**

Error Service Switching Function Timer

ERRSSFT is a peg register. It is incremented on a WIN call when the MSC's SSFT timer expires. This timer ensures TOPS does not take too long to process the WIN call. TOPS can reset this timer using the ResetTimer message. This message is controlled by datafill in Table ISUPTRK.

Register release history update

Created in SN07

Associated registers

None

Associated logs

TOPS131

Register NODATA**Register description**

No TCAP data

This is a peg register which is incremented whenever TOPS cannot locate a call's IS-41 or GSM TCAP data in the temporary table. See the error scenarios in the Functional Description chapter of this document for more information.

Register release history update

Created in SN07.

Associated registers

Register RXLAFAIL is always pegged when register NODATA is pegged, since the original called number cannot be determined, and a default of 411 must be used.

Associated logs

TOPS131

Register NOTLDNS**Register description**

No temporary local directory numbers

This is a peg register which is incremented whenever TOPS cannot obtain an idle temporary local directory number (TLDN) from Table TOPSTLDN. See the error scenarios in the Functional Description chapter of this document for more information.

Register release history update

Created in SN07.

Associated registers

None.

Associated logs

TOPS131

Register REQCONN**Register description**

Request Connection

This is a peg register which is incremented whenever TOPS sends an IS-41 ConnectResource or GSM EstablishTemporaryConnecction to the MSC.

Register release history update

Created in SN07.

Associated registers

Extension register REQCONN2

Associated logs

None.

Register RESTIMR**Register description**

ResetTimer

This is a peg register which is incremented whenever TOPS sends an IS-41 or GSM ResetTimer to the MSC.

Register release history update

Created in SN07.

Associated registers

Extension register RESTIMR2

Associated logs

None.

Register RXLAFAIL**Register description**

Retranslation Failure

This is a peg register which is incremented when a TOPS IS-41 or GSM call arrives, but TOPS cannot find the original called number and must use a default of 411. This register can be pegged in conjunction with NODATA, if the reason the original called number cannot be found is that there is no extension block.

Register release history update

Created in SN07.

Associated registers

None.

Associated logs

A TOPS131 is generated if the reason for using the default 411 is that the TCAP data was not found.

Register SANTIMR**Register description**

TOPS sanity timer expiration

This is a peg register which is incremented whenever the TOPS IS-41 or GSM call end sanity timer expires. TOPS starts this timer after sending the IS-41 AnalyzedInformation RETURN RESULT or GSM Connect to the MSC. If the MSC does not release the trunk and end the TOPS call before the timer expires, TOPS ends its call and frees resources.

Register release history update

Created in SN07.

Associated registers

None.

Associated logs

TOPS131

Register TLDNTIME**Register description**

TLDN time-out

This is a peg register which is incremented whenever the TOPS IS-41 or GSM SCP process finds a TLDN which has been allocated for more than 30 seconds. The TLDN is idled, then selected for use by the next TOPS IS-41 or GSM call. This allows the TLDN list to be cleaned up if some MSC calls end before routing to TOPS.

Register release history update

Created in SN07.

Associated registers

None.

Associated logs

None.

Register WINBEGIN**Register description**

Wireless Intelligent Network Begin

This is a peg register which is incremented whenever TOPS receives an IS-41 AnalyzedInformation or a GSM InitialDP from an MSC. This signifies the beginning of the WIN TOPS call.

Register release history update

Created in SN07.

Associated registers

Extension register WINBEGI2

Associated logs

None.

Register WINEND**Register description**

Wireless Intelligent Network End

This is a peg register which is incremented whenever TOPS receives a GSM Application End from the MSC. This signifies the end of a successful WIN TOPS call.

This message is not used in the IS-41 call flow, so this OM is not pegged for IS-41 TOPS calls.

Register DARLT in group TOPSISUP can also be used to count instances of successful ADACC with RLT.

Register release history update

Created in SN07.

Associated registers

Extension register WINEND

Associated logs

None

OM group TC7WRLSS**OM description**

TC7WRLSS

TOPS - Common Channel Signalling System #7 - Wireless

Release history update

Created in SN07

Registers

OM group registers display on the MAP terminal as follows:

OM Group Display

INVOKES	INVOKES2	INVOKER	INVOKER2
RETRESS	RETRESS2	RETRESR	RETRESR2
RETERRS	RETERRR	REJECTS	REJECTR
ABORTS	ABORTR	NOTRIDS	MBFULL
RTFNOXLA	RTFNOXLS	RTFSUBCG	RTFSUBFL
RTFUNEQ	RTFNETFL	RTFNETCG	RTFMISCE
GTTFAIL			

Group structure

OM group TC7WRLSS provides one tuple for each combination of wireless network type and TOPS wireless application.

Key field: There are four tuples as follows:

- SMS_IS41
- SMS_GSM
- WIN_IS41
- WIN_GSM

Info field: None

Associated OM groups

Registers in groups SMSTOPS and WINTOPS are also pegged during wireless TOPS calls.

Associated functional groups

None

Associated functionality codes**Functionality codes associated with OM group**

Functionality	Code
TOPS Wireless RLT	00034426

OM group registers logic flow chart**SMS TOPS calls**

Register INVOKES is pegged when TOPS sends a short message into the SS7 network.

Register RETRESR is pegged when TOPS receives a positive or negative acknowledgment from the message center (MC). Group SMSTOPS has registers indicating SMS failure has occurred.

The remainder of the registers are pegged in failure scenarios. If registers GTTFAIL or NOTRIDS are being pegged, this means SMS messages are not being sent due to failure at TOPS. If registers beginning with “RTF” (route failure) are being pegged, failures are occurring in the SS7 network before the SMS arrives at the MC.

WIN TOPS calls

A successful WIN TOPS call should peg only registers INVOKES, INVOKER, and RETRESS.

The remainder of the registers are pegged in failure scenarios. If registers GTTFAIL or NOTRIDS are being pegged, this means WIN TOPS messages are not being sent due to failures at TOPS. If registers beginning with “RTF” (route failure) are being pegged, failures are occurring in the SS7 network before the TOPS message arrives at the MSC.

Register ABORTR**Register description**

Abort Received

ABORTR is a peg register. It is incremented whenever TOPS receives a TCAP ABORT.

Register release history update

Created in SN07

Associated registers

None

Associated logs

TCAP100

Register ABORTS**Register description**

Abort Sent

ABORTS is a peg register. It is incremented whenever TOPS sends a TCAP ABORT.

Register release history update

Created in SN07

Associated registers

None

Associated logs

TCAP100

Register GTTFAIL**Register description**

Global Title Translation Failure

GTTFAIL is a peg register. It is incremented whenever TOPS cannot look up GTT information for a destination number. The GTT information is datafilled in Tables C7GTTTYPE and C7GTT. When TOPS cannot obtain this information, it cannot send the SMS into the network. The operator or automated node receives a failure indication.

A TOPS131 log is generated containing the destination number which caused the failure. Table C7GTT must be updated to include the destination number.

Register release history update

Created in SN07

Associated registers

None

Associated logs

TOPS131

Register INVOKER**Register description**

INVOKE Received

INVOKER is a peg register. It is incremented whenever TOPS receives a TCAP INVOKE.

Register release history update

Created in SN07

Associated registers

Extension register INVOKER2

Associated logs

None

Register INVOKES**Register description**

INVOKE Sent

INVOKES is a peg register. It is incremented whenever TOPS sends a TCAP INVOKE.

Register release history update

Created in SN07

Associated registers

Extension register INVOKES2

Associated logs

None

Register MBFULL**Register description**

Mailbox full

This is a peg register which is incremented whenever a TOPS IS-41 or GSM TCAP message arrives at the TOPS SCP interrupt handler but cannot be sent to the TOPS SCP process due to heavy switch load. This means TOPS is receiving more IS-41 or GSM traffic than it can handle.

On wireless DA calls, the incoming message is ignored, which will result in calls going to treatment in the MSC. It is not anticipated that TOPS IS-41 or GSM messaging will ever be high enough to peg this register. If this register is pegged, contact Nortel Networks to increase the number of internal mailboxes available to the TOPS IS-41 SCP application.

Register release history update

Created in SN07.

Associated registers

None.

Associated logs

None. Generating a log under these circumstances would further degrade switch performance.

Register NOTRIDS**Register description**

No transaction identifiers

NOTRIDS is a peg register. It is incremented whenever TOPS attempts to send an IS-41 or GSM TCAP message but cannot because no transaction identifiers (TRIDs) are available. Each TCAP operation requires a TRID to process the response.

TRIDs are allocated automatically by the DMS, so if this register is pegged, contact Nortel Networks.

Register release history update

Created in SN07

Associated registers

None

Associated logs

TOPS131

Register REJECTR**Register description**

REJECT received

REJECTR is a peg register. It is incremented whenever TOPS receives a TCAP REJECT from the MSC or MC. This indicates a problem with the TCAP message sent by TOPS, so Nortel Networks should be contacted.

Register release history update

Created in SN07

Associated registers

None

Associated logs

TCAP100

Register REJECTS**Register description**

REJECT sent

REJECTS is a peg register. It is incremented whenever TOPS sends a TCAP REJECT to the MSC. This indicates a problem with the TCAP message sent by the MSC, so the MSC's vendor should be contacted.

Register release history update

Created in SN07

Associated registers

None

Associated logs

TCAP100

Register RETERRR**Register description**

RETURN ERROR received

RETERRR is a peg register. It is incremented whenever TOPS receives a TCAP RETURN ERROR from the MSC. This might indicate a problem on the MSC or TOPS switches, so logs at both switches should be investigated.

Register release history update

Created in SN07

Associated registers

None

Associated logs

TCAP100

Register RETERRS**Register description**

RETURN ERROR sent

RETERRS is a peg register. It is incremented whenever TOPS sends a TCAP RETURN ERROR to the MSC. This might indicate a problem on the MSC or TOPS switches, so logs at both switches should be investigated.

Register release history update

Created in SN07

Associated registers

None

Associated logs

TCAP100

Register RETRESR**Register description**

RETURN RESULT received

RETRESR is a peg register. It is incremented whenever TOPS receives a TCAP RETURN RESULT from the MC.

Register release history update

Created in SN07

Associated registers

Extension register RETRESR2

Associated logs

None

Register RETRESS**Register description**

RETURN RESULT sent

RETRESS is a peg register. It is incremented whenever TOPS sends a TCAP RETURN RESULT to the MSC.

Register release history update

Created in SN07

Associated registers

Extension register RETRESS2

Associated logs

None

Register RTFMISCE**Register description**

SCCP routing failure: Miscellaneous failure

This is a peg register which is incremented when the TOPS IS-41 SCP process receives a UDTs message containing a diagnostic other than the next seven.

Register release history update

Created in TOPS19 (SN06).

Associated registers

None.

Associated logs

A TCAP101 log is generated containing the incoming UDTs message.

Register RTFNETCG**Register description**

SCCP routing failure: Network congestion

This is a peg register which is incremented when the TOPS IS-41 or GSM SCP process receives a UDTs message containing a diagnostic indicating “network congestion”.

Register release history update

Created in SN07.

Associated registers

None.

Associated logs

A TCAP101 log is generated containing the incoming UDTs message.

Register RTFNETFL**Register description**

SCCP routing failure: Network failure

This is a peg register which is incremented when the TOPS IS-41 or GSM SCP process receives a UDTs message containing a diagnostic indicating “network failure”.

Register release history update

Created in SN07.

Associated registers

None.

Associated logs

A TCAP101 log is generated containing the incoming UDTs message.

Register RTFNOXLA**Register description**

SCCP routing failure: No translation of such nature

This is a peg register which is incremented when the TOPS IS-41 or GSM SCP process receives a UDTs message containing a diagnostic indicating “no translation of such nature”.

Register release history update

Created in SN07.

Associated registers

None.

Associated logs

A TCAP101 log is generated containing the incoming UDTs message.

Register RTFNOXLS**Register description**

SCCP routing failure: No translation for this specific address

This is a peg register which is incremented when the TOPS IS-41 or GSM SCP process receives a UDTs message containing a diagnostic indicating “no translation for this specific address”.

Register release history update

Created in SN07.

Associated registers

None.

Associated logs

A TCAP101 log is generated containing the incoming UDTs message.

Register RTFSUBCG**Register description**

SCCP routing failure: Subsystem congestion

This is a peg register which is incremented when the TOPS IS-41 or GSM SCP process receives a UDTs message containing a diagnostic indicating “ subsystem congestion”.

Register release history update

Created in SN07.

Associated registers

None.

Associated logs

A TCAP101 log is generated containing the incoming UDTs message.

Register RTFSUBFL**Register description**

SCCP routing failure: Subsystem failure

This is a peg register which is incremented when the TOPS IS-41 or GSM SCP process receives a UDTs message containing a diagnostic indicating “ subsystem failure”.

Register release history update

Created in SN07.

Associated registers

None.

Associated logs

A TCAP101 log is generated containing the incoming UDTs message.

Register RTFUNEQ**Register description**

SCCP routing failure: Unequipped user

This is a peg register which is incremented when the TOPS IS-41 or GSM SCP process receives a UDTs message containing a diagnostic indicating “unequipped user”.

Register release history update

Created in SN07.

Associated registers

None.

Associated logs

A TCAP101 log is generated containing the incoming UDTs message.

Product = TOPS**A00003704 -- OSSAIN Enhancements for SN07 (Succession on DMS)*****Functional Description***

The feature enhances the OSSAIN product with the following:

- Short Messaging Service
- Wireless Directory Assistance Call Completion Release Link Trunking
- Alternate Hosting for Passive Operators
- Alter Speech Path for no ANI Calls
- Passive Operator Message Capacity Enhancement
- DA SN Request for DAS Only Service

- Alter Speech Path during Passiver Function Provider Connections
- OSAC Session Pool State Inform Message Usage
- Authorization Codes
- AMA Service ID Usage
- Resource Increases
- OSSAIN Open Automated Protocol (OAP) Version 9.0 and SOC

Short Messaging Service (SMS) is fully designed under feature A00003687; however this feature provides the needed OSSAIN changes to support SMS for SNs. This includes informing the SN of a wireless caller, and processing an SMS message received from the SN.

Wireless Directory Assistance Call Completion Release Link Trunking (RLT) is designed under feature A00000816 and A00003687; however, this feature will add the wireless RLT functionality for OSSAIN SN calls.

Alternate Hosting for Passive Operators is supported by this feature. It allows an alternate host to be selected for passive operator requests which cannot be serviced by the primary host.

Alter Speech Path for no-ANI Calls is supported by this feature. Incoming IT trunks which do not forward ANI but use DA SN functionality require the ability to split/join the calling party as needed.

Passive Operator Message Capacity Enhancement reduces the amount of OPP messaging sent to position when a SN releases itself from the call.

DA SN Request for DAS-only service allows a SN to request DAS services without attaching an operator.

Alter Speech Path during Passive Function Provider Connections allows a SN to forward an optional datablock to the switch to indicate the switch should alter the speech path when connecting a passive operator.

OSAC Session Pool State Inform Message Usage allows the SN to be informed of OSN state changes for SN originated session pools. It disables the message from being used for other origination types such as subscriber originated.

Authorization Codes allow a SN to send an authorization code to TOPS to be included in AMA for calling cards, commercial credit cards, and authcodes.

AMA Service ID ensures the service id sent from the SN will be used in AMA records instead of one defined in datafill in either table AMASRVID or TQMSSERV.

Resource Increases ensures OAP can support increases to the number of operators, positions, services, and call queues. This feature also allows OAP to send a 10 digit Account Code.

OAP Protocol Version 9.0 adds support for the above new functions. With the addition of version 9.0, the number of back releases will be increased to also support version 5.0. Version 9.0 is included in SOC option, OSAN0102; however, it has a new TOPSFTR entry, OSSAIN_RELEASE_20, to activate the functionality.

Short Messaging Service (SMS)

SMS functionality, as provided by feature A00003687, can be used to send text messages to a wireless caller. It allows an operator or a SN to forward SMS text messages to TOPS; TOPS will forward the message on to a Message Center (MC); and the MC forwards it to the subscriber. In order for a SN to send a SMS message to TOPS, OAP enhancements are needed and provided by this feature.

To send SMS messages, a SN will need to know if the caller is wireless. TOPS will use phone class type of 'mobile' for all wireless callers supported.

Thus, for wireless (mobile) calls, a SN can utilize a new OAP operation to send SMS message to the caller. The new operation, **SMS Request Operation**, includes one new datablock. The new datablock, **SMS Datablock**, contains the following fields:

- existing field, **Directory Number Digit Count**, to record number of digits in the destination number
- existing field, **Directory Number**, to record the destination number
- new field, **SMS Text Block Length**, to indicate length of text message
- new field, **SMS Text Block**, to include the text message up to 200 bytes

The switch will respond with either one of the following responses:

- **SMS Success Response**
- **SMS Error Response**

The responses indicate the switch has processed the message and attempted to forward it to the Message Center. Any responses from the Message Center are not forwarded to the SN.

New OM registers are added to existing OM group, OAPCP10, to record the usage of this new operation and it's responses.

Note: OAP will not restrict the allowed character set for SMS messages.

Wireless Directory Assistance Call Completion (DACC) RLT

Features A00000816 and A00003687 provide wireless services which include DACC and RLT for the TOPS environment. This feature supports RLT for wireless DACC calls in the OSSAIN environment

Alternate Hosting for Passive Operators

Alternate hosting, as provided by feature NC0152, is supported in OSSAIN for passive operators with this feature's release. If a passive operator is requested from a host which either is not available or the call deflects/overflows, then table OCHOSTQ is consulted to determine if an alternate host is datafilled.

If an alternate host is defined in table OCHOSTQ for the passive operator's call queue, then it will be used based on the options datafilled. The options include datalink failure, deflection, and queue overflow. If one of these options occurs and is datafilled, then the call will route to the alternate host datafilled. Only one alternate host can be datafilled for all options per call queue.

Thus, if a passive operator request was received by TOPS and the call was sent to a host which deflected the call (for example), then TOPS would check table OCHOSTQ, per the call queue, and determine if an alternate host is available for deflect purposes. If found, TOPS would request an operator from the alternate host giving the passive operator request a second chance.

OSSAIN supports both standalone and OC environments for alternate hosting as defined by existing table OCHOSTQ and OCPARMS parameter, SWITCH_NAME.

Alter Speech Path for no ANI calls

A SN is able to alter the speech path for a calling party with no directory number. This is necessary for IT trunks which do not send ANI but do use Service Nodes for DA Automation.

Passive Operator Message Capacity Enhancement

This feature enhances the AN1926: OSSAIN Simultaneous Interactions design by reducing the number of OPP messages sent to position when the SN releases itself. The original design sent all call details when the position was connected and again when the SN was released. The new design will only send call details when the SN is released if it is necessary due to a change.

DA SN Route to DAS-only Service

A DA SN may need to route a call to the DAS environment without attaching an operator. It may do this to utilize DAS automated functions such as announcements and call completion.

This feature changes the TOPSAUTO option of table OAFUNDEF to include a DAS option. Since the DAS option will require a CT4Q and refinement

option similar to TOPSOPER, the TOPSAUTO option is now broken into refinement areas for each automated system.

When the DAS automated function is used, the call will be routed to the DAS without an operator being attached. If ADASPLUS is available for the call, the DAS Call Begin message will contain the ADASPLUS eligible indicator.

Table OAFUNDEF

FUNCID	FUNCNAME	FUNCAREA
1	DAS_NO_OPER	TOPSAUTO DAS DAS_ONLY N
2	DAS_OPER	TOPSOPER DAS_OPER N
3	AABS	TOPSAUTO AABS AABS_CT4Q
4	DA_SN	SN DASERV N N N N Y CQ17 N

```

TYPE IS FUNCTYPE_VAR_AREA      MULTIPLE WITH
FUNCTYPE                       {SN, TOPSOPER, TOPSAUTO} REFINEMENTS:
{SN}                           MULTIPLE WITH
    ... unchanged

{TOPSAUTO}                     MULTIPLE WITH
    AUTOSYS_AREA               MULTIPLE WITH
        AUTOSYS                {AABS, MCCS, ACTS, BRANDING, DAS} REFINEMENTS:
        {AABS}                 MULTIPLE WITH
            OPRONFL             TQMS_SR_CALL_TYPE_FOR_QUEUEING
        {MCCS}                 MULTIPLE WITH
            OPRONFL             TQMS_SR_CALL_TYPE_FOR_QUEUEING
        {ACTS}                 MULTIPLE WITH
            OPRONFL             TQMS_SR_CALL_TYPE_FOR_QUEUEING
        {BRANDING}             MULTIPLE WITH
            OPRONFL             TQMS_SR_CALL_TYPE_FOR_QUEUEING
        {DAS}                  MULTIPLE WITH
            DASCT4Q             TQMS_SR_CALL_TYPE_FOR_QUEUEING
            QMS_AREA            MULTIPLE WITH
                QREFINMT        {N, Y} REFINEMENTS:
                {Y}             MULTIPLE WITH
                CQORDER         {PREOPR, POSTAUTO, RECALL, ASST}
                {N}             QMS_REFINE_N_REFINEMENT

{TOPSOPER}                     MULTIPLE WITH
    ... unchanged

```

Alter Speech Path during Passive Function Provider Connections

Since OSSAIN functionality gives as much control as possible to the Service Node (SN), there are times when a SN sends in a request message that can be processed a tad too late.

For example, for DA SN, a passive operator request can result in the caller being placed into queue for a brief period of time. When an operator becomes available, he/she is connected to the call and the SN is notified. The SN may respond by sending speech path change requests to alter the speech path for the calling party so they do not hear the call arrival tones and the operator does not hear the music on hold announcement.

Since there is a small amount of processing time, current functionality does allow the subscriber to hear call arrival tones and the operator to hear part of the music on hold announcement (all varying based upon processing time).

Following is a possible DAA passive operator call scenario and OAP messaging:

1. Subscriber dials a DA call. TOPS connects a service node voice link to the call and routes the call to a DAA node.
2. TOPS sends the Session Begin message to the DAA node.
3. The DAA node (active node) collects the city and listing information from the subscriber.
4. DAA node sends TOPS a Passive Function Provider Request.
5. TOPS responds by sending a Call Queue Information DB indicating the call has been queued.
6. At this point the DAA node begins playing an announcement to the subscriber indicating their queued condition.
7. Once a position becomes available, TOPS informs the DAA node by sending a Passive Operator Being Connected Message.
8. Shortly after the above message, TOPS sends the Passive Operator Connected Message.
9. The DAA node sends TOPS a Speech Path Request message instructing TOPS to make the subscriber voice path 0-way.

Here is the problem. Before TOPS can execute the Node's instruction the call arrival tones have already been played. Note the operator may also hear part of the music on hold announcement.

10. The DAA node plays the city and listing information to the operator.

OAP 9.0 will allow the Speech Path DB as an optional datablock to the Passive Function Provide Request operation. The speech path status field is increased to support a new range which will indicate to alter the speech path when the operator is connected.

OSAC Session Pool State Inform Message Usage

For Operator Services Nodes (OSN) in an OSAC remote, this feature restricts the usage of the Session Pool State Inform message to SN originated session pools only. Thus, when a session pool, datafilled as SN origtype in table OASESNPL of the OSAC remote, changes state (busy or return to service), the SN will be informed so it does not attempt to originate a session to the remote.

When other session pool originators (subscriber, OSACORIG, OSACTERM) change state in the remote, the SN does not need to be notified. This feature removes the attempt to notify the SN of state changes for these other session pools.

Authorization Codes

There are a few scenarios in which a SN may need to send TOPS an authorization code to be placed into the AMA record. This feature enhances OAP to provide such a means.

OAP version 9.0 will support a new datablock and fields to provide authorization codes from the SN to TOPS.

To support both alphanumeric and numeric codes, the new OAP field allows up to 20 ASCII characters. The SN will need to ensure any BCD formatted authcode is converted prior to populating OAP. TOPS will read the field as ASCII and convert to other formats as needed.

The SN will also need to populate OAP with the type of authorization code being sent. Currently included in existing AMA records, and available in OAP, are the following:

- Calling cards - Module Code 611 with generic context id 80002 supports up to 15 digits to record authorization code received from the bank.
- Commercial Credit cards - Module Code 611 with generic context id 80002 supports up to 15 digits⁵ to record the authorization code received from the bank.
- Authcode - Module Code 102 supports 14 digits to record the authorization code entered by the subscriber and validated by the bank.

Note: This feature enhances OAP to allow a SN to send authorization codes up to 20 bytes; however, it does not enhance AMA records. Thus, the above restrictions apply unless expansions are supported through another feature.

5. Some clearing houses use an alphanumeric authorization code; however, TOPS currently only supports a 15 digit code in AMA for all card calls. Thus, if the bank sends an alphanumeric code, TOPS will convert the string to a digits format for the existing AMA record. It will not accept characters outside of the DIGIT range (0-F). A new AMA field is needed for this purpose. The service provider is encouraged to seek other feature work which supports a new AMA field for this purpose.

AMA Service ID Usage

TOPS currently allows a user-defined service id to be placed into AMA. TOPS can obtain the service id from datafill or from an OAP message. This feature ensures a service id sent from a SN via OAP is used regardless of datafill defined in tables AMASRVID or TQMSSERV.

Resource Increases

This feature ensures OAP can support resource increases for the following:

- Operator IDs up to 65,535
- Position IDs up to 9999
- Call Queue IDs up to 8190
- Account Codes up to 10 digits for user-entered group billing

Note: Although this feature ensures OAP can send and receive these higher ranges, it does alter TOPS base nor AMA functionality. To utilize these new ranges, ensure TOPS base and AMA modifications have been completed.

OAP Protocol Version 9.0

OAP protocol version 9.0 includes all new OAP information provided by this feature and discussed in this document. The enhancements include:

New / changed Fields

- New field, SMS Text Block
- New field, SMS Text Block Length
- Existing field, Speech Path Status is expanded to include options to indicate to alter speech path when the operator is connected
- New field, Authorization Number Type (Format)
- New field, Authorization Code Length
- New field, Authorization Code

New / Changed Datablocks

- New datablock, SMS DB
- New datablock, Authorization Number DB

New / Changed Operations

- New operation, SMS Request
- New operation, SMS Success Response
- New operation, SMS Error Response

- Existing operation, Passive Function Provide Request has a new optional datablock, Speech Path DB.
- Existing operation, Class Charge Request, has a new optional datablock, Authorization Code DB.

Note: OAP 5.0 will be supported along with OAP 9.0. This feature changes support for 3 versions back to 4 versions back.

Please reference *OSSAIN OAP Specification Document - NIS Q235-1 (version 2.0)* for details of the changes.

SOC and Table TOPSFTR

OAP 9.0 and functionality described in this document are controlled by existing SOC option OSAN0102; however, table TOPSFTR is changed to include a new entry for OSSAIN_RELEASE_20. TOPSFTR can be used to turn this feature's functionality on/off as needed.

Hardware Requirements or Dependencies

None

Software Requirements or Dependencies

- OSSAIN Enhancements, SOC option OSAN0102
- OSSAIN base functionality, SOC option OSAN0101
- TOPS base functionality, SOC option OSB00101

Limitations and restrictions

- SNs using SMS will affect the EIU provisioning.
- Although this feature ensures OAP can handle resource increases as noted, it does not modify TOPS base nor AMA functionality necessary to utilize the new ranges.
- New TOPSAUTO function, DAS can be used for transferring; however, like all TOPSAUTO functions, it is not available for triggering/recalls nor passive operator requests.

Interactions

The new DAS function in table OAFUNDEF does not interact with existing ADAS+ functionality. ADAS+ can be setup for the DAS function, but is not required to obtain DAS-only service.

Glossary

Term	Description
ANI	Automated Number Identifier
CT4Q	Call Type For Queuing
DAA	Directory Assistance Automation
DACC	Directory Assistance Call Completion
DB	DataBlock
EIU	Ethernet Interface Unit
OAP	OSSAIN Open Automated Protocol
OSAC	OSSAIN Centralization
OSN	OSAC Service Node
OSSAIN	Operator Services Systems Advanced Intelligent Network
RLT	Release Link Trunking
SMS	Short Messaging Service
SN	Service Node

Product = TOPS

A00005160--OSSAIN XA-Core Data Messaging Capacity Enhancements (Succession on DMS)

Functional Description

This activity makes it possible for OSSAIN data messaging to use XA-Core Ethernet interfaces such as the HIOP and the new HCMIC card. Prior to this activity, all OSSAIN messaging used the EIU (Ethernet Interface Unit). The EIU has insufficient capacity to support some service providers' requirements for OSSAIN.

This section includes background material on both OSSAIN and XA-Core Ethernet interfaces.

OSSAIN background

The OSSAIN product uses a messaging protocol between TOPS (Traffic Office Position System) switches and external service nodes (SNs), allowing the SNs to provide services for and control switch functionality associated with directory and operator services calls. In an OSAC (OSSAIN centralization) configuration, one or more centralized SNs provide services for multiple TOPS switches. These TOPS switches are referred to as OSAC hosts and OSAC remotes, and they exchange messages with each other as well as with SNs. All of this messaging uses the UDP protocol at the transport level.

Until recently, OSSAIN was used mainly for toll and assistance (TA) calls. Now service providers are beginning to use OSSAIN for directory assistance automation (DAA) as well. Since most TOPS switches handle many more DA than TA calls, and since DAA calls may use OSSAIN for both front end and back end automation, service providers are requiring more OSSAIN messaging capacity than EIUs can provide. Throughput of an EIU is between roughly 10 and 40 KBytes/second in each direction, depending on how heavily the LPP or FLIS is used for other applications besides OSSAIN. And because of the way EIU selection is done, adding more EIUs for OSSAIN may not increase the messaging capacity. For more information about EIU capacity, refer to *OSSAIN User's Guide* (297-8403-901) and *Ethernet Interface Unit User Guide* (297-8991-910).

XA-Core Ethernet interface background

In the XA-Core architecture, I/O processor cards in the core can be used to provide Ethernet LAN connectivity. These cards communicate directly with the PEs (processing elements) using a shared memory system. The first-generation card was the IOP, a host card that accommodates specialized packets for different interfaces. An IOP with Ethernet packet(s) is called an EIOP. The second-generation card is the HIOP. HIOP cards do not host packets. Three versions of HIOP have been developed—one with only an Ethernet interface, and two with both Ethernet and AMDI (for ATM). Next-generation HCMIC cards with CMIC, RTIF, and Ethernet interfaces are under test at the time of this writing.

XA-Core Ethernet interface cards are datafilled in switch table CMIPADDR. The datafill includes two active host CM IP addresses, which the switch dynamically associates with physical links. As long as at least two links are in-service, the two IP addresses are always associated with different links. If a link fails while another is in-service, the IP address that was associated with the failed link is automatically reassigned to a different one. Unsolicited ARP (Address Resolution Protocol) replies are used to inform the network of the association between IP addresses and physical interfaces.

XA-Core I/O cards are maintained from the switch at MAP level MAPCI;MTC;XAC;IO. Their functional components, including Ethernet

ports and links, are maintained at level MAPCI;MTC;XAC;ETHR. *Port* refers to a hardware interface on the card, and *link* represents the transmission medium connecting the XA-Core to other nodes. For more information, refer to documentation for the following features:

A59019176	XA-Core ethernet packetlet - OA&M
A59029980	HIOP Maintenance Software
A00002012	XA-Core CMIC/RTIF HIOP Maintenance Software

New functionality

This feature adds new fields to switch table OANODINV, the inventory table for OSSAIN SNs and OSAC nodes, to allow the service provider to specify the data path to be used for messaging with each node. Thus it is possible for a TOPS switch to use EIU for messaging with some OSSAIN nodes and XA-Core Ethernet interface cards for messaging with others. This enables a gradual transition, on a node-by-node basis, to using XA-Core Ethernet interface cards.

Which data path the switch uses is transparent to the far-end node, except that the far-end node must be configured to use a different IP address for the switch depending on which data path the switch uses when messaging with that node.

For the EIU data path, far-end nodes are configured to send messages to the IP address in the CMIPADDR tuple of table IPNETWRK. This is existing functionality, and is unchanged.

For the XA-Core Ethernet interface data path, each far-end node is configured to send messages to one of the two active CM host IP addresses datafilled in table CMIPADDR. That address is also datafilled against the node in table OANODINV, and is used as the source IP address when the switch sends messages to the node.

Under normal conditions of no failure, traffic should be balanced over the physical links. This is accomplished by configuring half of the far-end nodes to use one of the active CM host IP addresses, and the other half to use the other active CM host IP address.

TOPS does not restrict which XA-Core Ethernet interface cards can be used. However, some of the earlier XA-Core I/O cards have been or will soon be manufacture discontinued, and the product platform on which TOPS runs may have restrictions on which cards are supported. Contact your Nortel Networks representative for more information.

This activity also adds a new OM group, TDGTHRU (TOPS Datagram Throughput), which counts the number of UDP messages sent and received in

each of several “buckets” or message size ranges. The OM group has tuples for several TOPS applications, and it has separate tuples for OSSAIN using EIU and OSSAIN using XA-Core Ethernet interface. The pegs are meant to help in studies of messaging bandwidth utilization of TOPS applications.

Capacity engineering considerations

Paper studies suggest that if the LPP or FLIS that houses the EIU is used primarily for OSSAIN messaging, an OSAC remote can process roughly 100,000 DA busy hour calls/hour, with DA front and back end automation using Nortel Networks service nodes, before it approaches EIU messaging capacity limits. If the LPP or FLIS is also used heavily for ISUP signaling or other applications, the OSSAIN traffic limit may be closer to 25,000 calls/hour. Capacity decreases if the SNs send a significant number of SMS (Short Message Service) requests to the switch. Other features may also decrease capacity.

Similar studies suggest that a pure OSAC host can process roughly a million busy hour OAP sessions for its remotes if the EIU in the host is used primarily for OSSAIN traffic. Using Nortel Networks service nodes, separate OAP sessions are used for DA front end and back end automation, so this translates to 500,000 DA calls/hour. If the LPP or FLIS housing the EIU in the OSAC host is also used heavily for ISUP signaling or other applications, the OSAC host’s limit is closer to 125,000 DA calls/hour from its OSAC remotes. The host’s capacity decreases if it is also processing standalone OSSAIN calls.

Note: Messaging patterns may be different if service nodes from other vendors are used. Nortel Networks does not have message flows for calls that are serviced by other vendors’ SNs, and does not do capacity engineering for these SNs.

Ethernet throughput capacity of XA-Core interface cards depends on factors such as the extent to which other interfaces on the card are used and the sizes of the individual messages. Committed throughput numbers for NTLX04CA (HIOP) and NTLX17AA (HCMIC) were not available at the time of this writing, but both cards will have Ethernet throughput capacity much higher than the EIU, even if other interfaces on the card are used.

It is anticipated that in offices that are not using XA-Core interfaces for Succession packet call signaling, a pair of NTLX04CA or NTLX17AA cards (for redundancy) can easily accommodate both CBM (Core and Billing Manager, the next-generation Supernode Data Manager replacement) and all existing DA traffic, using OSSAIN for both front and back end automation, with no capacity concerns.

In TOPS CS2000 switches in which OSSAIN messaging is sharing the available Ethernet interface bandwidth with high-runner Succession call signaling, the CS2000 capacity for handling non-TOPS calls is decreased. At

the time of this writing, Succession CS2000 capacity numbers published by Nortel Networks were based on office models that did not include OSSAIN. Contact your Nortel Networks representative for the status of capacity engineering work for CS2000 switches that use Ethernet interface cards for both OSSAIN and Succession packet call signaling.

Hardware Requirements or Dependencies

This functionality is available only on XA-Core equipped with Ethernet interface cards such as HIOP (NTLX04CA) or HCMIC (NTLX17AA).

Software Requirements or Dependencies

This functionality is first available in the SN07 and ISN07 core software loads.

Limitations and restrictions

From an end user's perspective, this activity introduces no limitations or restrictions that were not present in OSSAIN using EIU.

From a service provider's perspective, the following limitations and restrictions apply:

- Use of XA-Core Ethernet interface cards is supported only for OSSAIN applications that use the UDP protocol. It is not supported for OSSAIN QMS MIS, which uses TCP.
- Unlike EIUs, XA-Core Ethernet interface cards do not provide screening capabilities. (EIUs can be configured to protect the core by screening out incoming messages from unwanted IP addresses, including addresses that do not match datafilled nodes and addresses of nodes that are off-line or have been declared babblers.)

Since call processing can be adversely affected if the core is flooded with unwanted messages, it is especially important that the network be properly configured with firewalls and router filters when XA-Core Ethernet interfaces are used.

- In TOPS CS2000 switches in which OSSAIN is sharing the Ethernet interface cards with high-runner Succession calls, OSSAIN decreases the capacity of the CS2000 for non-TOPS calls. CS2000 capacity numbers published by Nortel Networks engineering groups do not apply in this case, unless the office model has specifically included OSSAIN calls.
- The XA-Core does not provide a way to reserve portions of its total Ethernet interface bandwidth for specific applications. All applications compete for the same bandwidth.
- This limitation applies when (a) an OSAC remote switch is being changed to use XA-Core Ethernet interface to communicate with a centralized SN, and (b) either the OSAC host is below SN07/ISN07, the centralized SN is at an OAP release below 9, or both. In this situation, if the service node is

incorrectly configured (in the service node) to use the wrong IP address for the OSAC remote, the mismatch is not detected when the links to the centralized SN are returned to service in the OSAC remote. The OSAC remote will present calls to the centralized SN. The incorrectly configured SN will probably not attempt to send the switch any messages regarding these calls. Depending on datafill for OSSAIN time-outs and on how quickly callers abandon these calls, there may be no logs in the OSAC remote indicating any problem. However, the incorrectly configured SN should be raising alarms using its own event reporting system if this happens.

This is not a new problem with XA-Core Ethernet interface; however, the configuration mismatch may be more likely to be introduced with this feature, since the service provider now has to be aware of more than one IP address for any particular switch.

The OSAC and OAP protocols are enhanced in SN07 and OAP Release 9 to eliminate this limitation. If the SN is at OAP 9 or higher, and both the OSAC remote and host are at SN07 or higher, then the OSAC remote cannot RTS its links to the centralized SN if the SN has incorrect datafill for the OSAC remote's IP address.

Interactions

Existing OSSAIN services are not affected by the choice of which data path the switch uses for Ethernet connectivity.

Applicable customer facing sections

An X indicates that the corresponding DDOC section is applicable. N/A indicates it is not.

Fault Management

Logs	N/A
Alarms	N/A

Configuration

Data Schema	X
User Interface	X
Element Management	N/A
Security	X
Service Order	N/A
Office Parameters	N/A
Configuration Walkthrough	X

Accounting (includes AMA billing)	N/A

Performance (includes operational measurements)	X

Realtime	X
Engineering Information	X

Glossary

This activity does not introduce new or non-standard terms. For convenience, this section expands standard acronyms used in this FN.

Term	Description
AMDI	ATM Multi-mode Data Interface
ARP	Address Resolution Protocol
ATM	Asynchronous Time Multiplexing
CBM	Core and Billing Manager
CM	Computing Module
CMIC	Computing Module Interface Card
CS2000	Communication Server 2000
DA	Directory Assistance
DAA	Directory Assistance Automation
EIOP	Ethernet Input Output Processor
EIU	Ethernet Interface Unit
FLIS	Fiber Link Interface Shelf
HCMIC	High Performance Computing Module Interface Card
HIOP	High Speed Input Output Processor
IOP	Input Output Processor
IP	Internet Protocol
ISUP	Integrated Services Digital Network
LAN	Local Area Network
LPP	Link Peripheral Processor
MAP	Maintenance and Administration Position
OAP	Open Automated Protocol
OSAC	OSSAIN Centralization
OSSAIN	Operator Services System Advanced Intelligent Network
QMS MIS	Queue Management System Management Information System

Term	Description
RTIF	Reset (or Remote) Terminal Interface
SMS	Short Message Service
SN	Service Node
TA	Toll and Assistance
TCP	Transmission Control Protocol
TOPS	Traffic Office Position System
UDP	User Datagram Protocol
XA-Core	Extended Architecture Core

Fault Management for A00005160

Fault management strategy

This feature does not change the fault management strategy for XA-Core Ethernet interface cards or for the OSSAIN product. It does modify the reason texts that can appear in two OSSAIN log reports.

Fault management tools and utilities

Unchanged.

Logs

This activity modifies the values that can appear in the existing OAIN606 and OAIN607 logs. It does not add any new logs or change the format of any existing logs.

Explanation

Log Title: OAIN606

Name: UNDELIVERABLE MESSAGE

Description: This log is generated when OSSAIN data communication software cannot route an incoming message to the appropriate software to process it. The reason text in the log indicates why the message could not be routed.

Event type: INFO

Format

The format is unchanged. Following is an example.

```

RTPC07BZ  OAIN606 MAR12 13:56:45 8500 INFO UNDELIVERABLE MESSAGE
MESSAGE PROTOCOL RELEASE: 5
MESSAGE PROTOCOL INCREMENT: 0
SENDERS PROTOCOL RELEASE: 5
SENDERS PROTOCOL INCREMENT: 0
NODE NAME: TO_RTPV                      NODE ID: 70
SESSION POOL NAME:                      SESSION POOL ID: 0
SESSION ID: 0
MESSAGE CLASS: OSAC NODE CLASS          MESSAGE CLASS ID: 22
NETWORK ADDRESS : 47 245 9 1 : 5290
REASON: MSG RECEIVED AT UNEXPECTED DESTINATION ADDRESS
MESSAGE:
16000000360012000005000546006400FF0082A1
26000202640102020B0282041A0005E016002000
000300FFF52F0109FFFFFFFFFFFFFFFFFFFFFFFF
00FF00FF00FF00FF00FF00FF00FF00FF00FF00FF
00FF00FF00FF00FF00FF00FF00FF00FF00FF00FF

```

Field descriptions

The overall field descriptions are unchanged. The values that can appear in the REASON field are changed as follows:

- **INVALID NETWORK ADDRESS**

This value, which could appear in earlier releases, no longer appears as of SN07/ISN07. It is replaced by MSG RECEIVED WITH UNEXPECTED SOURCE ADDRESS

- **MSG RECEIVED WITH UNEXPECTED SOURCE ADDRESS**

This new reason indicates that the source IP address, port, or both in the incoming message do not match switch datafill for the node whose node name and ID are shown in the log. The NETWORK ADDRESS field shows the actual source address. The most likely explanation is incorrect datafill for the node's IP address at the switch at which the log is generated. Another possibility is that the security of the service provider's network may have been compromised, and a rogue node may be sending OAP messages to the switch.

- **MSG RECEIVED AT UNEXPECTED DESTINATION ADDRESS**

This new reason indicates that a message incoming from the node whose name and ID are shown in the log was delivered to a core IP address other than the one datafilled in the switch for the far-end node. The NETWORK ADDRESS in the log is the actual destination address at which the message was received.

The most likely explanation is that the node that sent the message is configured to have the wrong one of the core's IP addresses. If the switch where the log was generated is datafilled to use an EIU for messaging with the far-end node, the IP address in table IPNETWRK at the switch should be configured in the far-end node as the switch address. If the switch is datafilled to use XA-Core Ethernet interface for messaging with the node,

the CM IP address datafilled against the node in table OANODINV in the switch should be configured in the node as the switch IP address.

Another possibility is that the security of the service provider's network may have been compromised in a way that causes messages to be misrouted.

Note the REASON field can also have other values, which are unchanged by this feature.

Action

Check parallel datafill between the node that sent the message and the switch at which the log was generated. Check for logs or alarms at the node that sent the message. If the problem is not resolved, contact the next level of support.

Associated Operational Measurements or Performance Measurements

Unchanged.

Explanation

Log Title: OAIN607

Name: TRANSPORT INTERFACE ERROR

Description: This log indicates that OSSAIN software encountered an error when interfacing with lower-layer transport software in the switch.

Event type: INFO

Format

The format is unchanged. Following is an example.

```

RTPC07BZ  OAIN607 FEB29 13:03:30 7499 INFO TRANSPORT INTERFACE ERROR
NODE NAME: TEST_NODE1                      NODE ID: 185
SESSION POOL NAME:                          SESSION POOL ID: 0
MESSAGE CLASS:                              MESSAGE CLASS ID: 256
NETWORK ADDRESS : 47 142 224 185 : 7000
REASON: XAETHR TRANSMIT FAILURE
MESSAGE:
00010000002600120800090000200000008300FF
00FF00FF00FF00FF00FF00FF00FF00FF00FF00FF
00FF00FF00FF00FF00FF00FF00FF00FF00FF00FF
00FF00FF00FF00FF00FF00FF00FF00FF00FF00FF
00FF00FF00FF00FF00FF00FF00FF00FF00FF00FF

```

Field descriptions

The overall field descriptions are unchanged. This activity adds one new value that can appear in the REASON field:

- XAETHR TRANSMIT FAILURE

This value indicates that the OSSAIN attempted to send a message using the XA-Core Ethernet interface, but the lower-layer transport software reported back to OSSAIN that the message could not be sent. The cause of the problem is more likely to be in lower-layer software or hardware than in OSSAIN code.

Action

Investigate the underlying transport facilities. Check logs for any that might suggest the root cause of the transport failure. Investigate at MAP levels MAPCI;MTC;XAC;IO and MAPCI;MTC;XAC;ETHR. The peg counts in CI XAIPTOOL may be useful.

Associated Operational Measurements or Performance Measurements

Unchanged.

Additional information

OSSAIN does not generate an OAIN607 log if the reason for failure to send an OAP message via XA-Core Ethernet interface is that no route exists for the source IP address. In this case, the problem is definitely with the underlying transport, and OAIN logs would only clutter up the reporting and possibly make it more difficult to troubleshoot the underlying problem. The underlying transport always raises an XAC alarm when there is no route for messages from a CM host IP address.

Related documentation

Refer to 297-8403-901, OSSAIN User's Guide, for information about OSSAIN fault management.

Configuration for A00005160**Hardware and Software Requirements**

A data network must be engineered and commissioned to enable UDP and ICMP echo messaging between OSSAIN/OSAC switches and OSSAIN service nodes. Refer to "Security" on page 2395 for information relevant to configuring the data network. Refer to the FN section of this DDOC for more information about capacity engineering.

XA-Core Ethernet interface cards should be commissioned on the switch before attempting to convert OSSAIN nodes to use them.

OSSAIN service nodes, provided either by Nortel Networks or by a third party vendor, must be in place.

Initial Configuration

For overall information about configuring OSSAIN, refer to the *OSSAIN User's Guide* (297-8403-901) and to SN-specific documentation.

If this feature is being commissioned on a switch that does not already have XA-Core Ethernet interfaces, it is important to develop an overall IP address plan that will last when the switch begins to use Succession functionality. Refer to Nortel Networks system engineering documentation for more information.

Also refer to engineering documentation for specific information about commissioning XA-Core Ethernet interface cards. Existing CI XAIPTOOL may be useful in working with XA-Core Ethernet interfaces.

Note this feature does not restrict whether the CM IP address used for XA-Core Ethernet interfaces is in the same or a different subnet than the CM IP address used with EIUs.

Migration from EIU to XA-Core Ethernet interface at a switch can be done gradually, on a per far-end node basis. OSAC hosts and remotes do not have to be converted at the same time. For example, an OSAC remote can send messages via its EIU to the host's XA-Core Ethernet interface IP address, and the host responds using its XA-Core Ethernet interface to the IP address that the remote uses with its EIU. Also, an OSAC host or remote can use XA-Core Ethernet interface for messaging with some service nodes, and EIU for messaging with others. A service node can communicate with some switches that use XA-Core Ethernet interface and with others that use EIU.

See "Configuration Walkthrough" on page 2396 for the steps in converting a switch to use XA-Core Ethernet interface rather than EIU for messaging with a specific far-end node (SN or OSAC switch).

Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable.

Upgrade Impact

Dump and Restore

No customer action is required. On an ONP from pre-SN07 to SN07 or later, OSSAIN nodes are automatically datafilled in table OANODINV to use the EIU data path.

Element Management Upgrade

Not applicable.

Data schema (DS)

New/modified tables

Table name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
Table OANODINV	changed	unchanged
Table CMIPADDR	changed	unchanged
Table QMSMIS	changed	unchanged

Table information

Name: Table OANODINV

Operator Services System Advanced Intelligent Network Node Inventory

Functional description

This table maps an OSSAIN node identifier to a unique node name. It defines the transport layer protocol used for messaging to the given node and specifies protocol related network address information. This table also allows datafilling OSSAIN node specific information.

Usage sequence and implications (CM Only)

The following tables must be datafilled before OANODINV:

- ENSITES
- ENTYPES
- OANODNAM
- CMIPADDR, for OANODINV tuples with field DATAPATH = XAETHR

Current datafill sequence is unchanged for tables that are datafilled after table OANODINV.

Size

This activity increases the store for each OANODINV tuple by 4 bytes.

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
OANODINV	0	768 (unchanged)	Approximately 1038 bytes per tuple. Refer to the Engineering (EI) section of this DDOC for more information.

Note: The amount of store used by table OANODINV depends on the NODEID values that are datafilled in table OANODNAM. To avoid wasting store, avoid datafilling higher NODEID values than needed.

Fields

The following table shows the top-level fields for table OANODINV.

Table OANODINV field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NODENAME	unchanged			
NODEAREA	refinements changed	This field consists of subfield ONPMTYPE and refinements		
ONPMTYPE	unchanged	This is a selector field.	OSN, OSNM, or OSAC (unchanged)	unchanged
AUDTRIES	unchanged			
AUDRTIMR	unchanged			
AUDFREQ	unchanged			

ONPMTYPE = OSN

If the entry in subfield ONPMTYPE is OSN, datafill refinements as shown in the following table.

OSN refinement field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
ENNODENO	unchanged			
PROTOCOL_AREA	unchanged			
ADDRESS_AREA	unchanged			
DATAPATH_AREA	New	This field consists of subfield DATAPATH and refinements		

OSN refinement field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DATAPATH	New	This is a selector field.	EIU or XAETHR	Data path. Enter EIU if the data path for this OSN is to use Ethernet Interface Unit. Enter XAETHR if the data path for this OSN is to use XA-Core Ethernet interface cards, and also datafill refinement field CMIPADDR.
CMIPADDR	New	This is a refinement field, present only if selector DATAPATH = XAETHR	four numbers, each 0 to 255	Computing Module Internet Protocol Address. Enter an IP address from the ACTIVEIP field of a CMHOST tuple in table CMIPADDR. To distribute messaging over the physical links, datafill one ACTIVEIP address for half of the nodes and the other ACTIVEIP address for the other half.
HOSTNAME	unchanged			
FAIL_DET	unchanged			
ONODTYPE	unchanged			
ONODLOC	unchanged			
ONODSITE	unchanged			
ONODINFO	unchanged			

ONPMTYPE = OSNM

If the entry in subfield ONPMTYPE is OSNM, datafill refinements as shown in the following table.

OSNM refinement field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
ENNODENO	unchanged			
PROTOCOL_AREA	unchanged			

OSNM refinement field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
ADDRESS_ AREA	unchanged			
NMTCPORT	unchanged			
DATAPATH_ AREA	New	This field consists of subfield DATAPATH and refinements		
DATAPATH	New	This is a selector field.	EIU or XAETHR	Data path. Enter EIU if the data path for this OSNM is to use Ethernet Interface Unit. Enter XAETHR if the data path for this OSNM is to use XA-Core Ethernet interface cards, and also datafill refinement field CMIPADDR.
CMIPADDR	New	This is a refinement field, present only if selector DATAPATH = XAETHR	four numbers, each 0 to 255	Computing Module Internet Protocol Address. Enter an IP address from the ACTIVEIP field of a CMHOST tuple in table CMIPADDR. To distribute messaging over the physical links, datafill one ACTIVEIP address for half of the nodes and the other ACTIVEIP address for the other half.
FAIL_DET	unchanged			
TSTTIME	unchanged			
RTSTIME	unchanged			
ONODTYPE	unchanged			
ONODLOC	unchanged			
ONODSITE	unchanged			
ONODINFO	unchanged			

ONPMTYPE = OSAC

If the entry in subfield ONPMTYPE is OSAC, datafill refinements as shown in the following table.

OSAC refinement field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
RELATION_ AREA	A refinement of this field is changed	This field consists of subfield RELATION and refinements		
RELATION	unchanged	This is a selector field. If SELF is entered, there are no refinements. If OTHER is entered, datafill the refinement fields shown below.	SELF or OTHER	unchanged
ENNODENO	unchanged			
PROTOCOL_ AREA	unchanged			
ADDRESS_ AREA	unchanged			
DATAPATH_ AREA	New	This field consists of subfield DATAPATH and refinements. This field is present only if selector RELATION = OTHER.		
DATAPATH	New	This is a selector field.	EIU or XAETHR	Data path. Enter EIU if the data path for this OSAC node is to use Ethernet Interface Unit. Enter XAETHR if the data path for this OSAC node is to use XA-Core Ethernet interface cards, and also datafill refinement field CMIPADDR.

OSAC refinement field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CMIPADDR	New	This is a refinement field, present only if DATAPATH = XAETHR	four numbers, each 0 to 255	Computing Module Internet Protocol Address. Enter an IP address from the ACTIVEIP field of a CMHOST tuple in table CMIPADDR. To distribute messaging over the physical links, datafill one ACTIVEIP address for half of the nodes and the other ACTIVEIP address for the other half.
ONODTYPE	unchanged			
ONODLOC	unchanged			
ONODSITE	unchanged			
ONODINFO	unchanged			

Datafill example

The following example shows sample datafill for table OANODINV. A bold font is used to highlight the new fields introduced by this activity.

NODENAME	NODEAREA	AUDTRIES AUDRTIMR AUDFREQ			
SWITCH_A	OSAC SELF		4	5	30
SWITCH_B	OSAC OTHER	0 UDP IPV4 172 16 10 2	XAETHR 172 16 1 108		
		SWITCH 3 B 11 CITYB REMOTEOSAC	4	5	30
SWITCH_C	OSAC OTHER	1 UDP IPV4 172 16 20 5	EIU		
		SWITCH 1 A 12 CITYC HOSTOSAC	4	5	30
BRAND_01	OSNM 0	UDP IPV4 172 16 1 200 7000	EIU		
		Y 2 240 60 SN 2 BB 3 CITYA BRANDING1	4	5	60
DEBIT_01	OSNM 1	UDP IPV4 172 16 1 210 7001	XAETHR 172 16 1 109		
		Y 2 240 30 SN 2 BB 8 CITYA DEBIT1	4	5	60
DAA_01	OSN 1	UDP IPV4 172 16 20 205	XAETHR 172 16 1 108		
		SWITCH_C Y 2 SN 1 DD 33 CITYC DAA1	4	5	60
DAA_02	OSN 0	UDP IPV4 172 16 20 206	EIU		
		SWITCH_C Y 2 SN 1 DD 34 CITYC DAA2	4	5	60

Table release history update

The DATAPATH_AREA field, with selector subfield DATAPATH and refinement CMIPADDR, is added for OSN, OSNM, and OSAC OTHER tuples. The CMIPADDR refinement field is present only if DATAPATH = XAETHR.

Supplementary information

When XAETHR is entered as the data path, the IP address in the OANODINV CMIPADDR refinement field must be used by the far-end node as the destination address for OSSAIN messages. This same IP address will be the source IP address for OSSAIN messages sent to the far-end node.

The XAETHR data path cannot be datafilled in table OANODINV unless the IP address in refinement field CMIPADDR has been previously added to table CMIPADDR, as the ACTIVEIP entry in a CMHOST tuple. If an attempt is made to violate this restriction, the following error message is displayed:

```
The CMIPADDR entry in OANODINV must match an ACTIVEIP
entry in a CMHOST tuple in table CMIPADDR.
```

The XAETHR data path cannot be datafilled in table OANODINV if the node is identified in table QSMIS as a server for OSSAIN QMS MIS. If an attempt is made to change the OSSAIN QMS MIS server's data path to XAETHR, the following error message is displayed:

```
This node is datafilled in table QSMIS. DATAPATH XAETHR
is not supported for an OSSAIN QMS MIS server.
```

Translation verification tools

Table OANODINV does not use translation verification tools.

Name: Table CMIPADDR

Computing Module Internet Protocol Addresses

Note: The only changes are a new cross-check with table OANODINV and a new error message. However, because earlier releases of Nortel Networks documentation may have missed some of the details about this table, this feature goes into some detail in documenting the fields.

Functional description

Table CMIPADDR contains the IP addresses and subnet masks associated with the XA-Core, as well as the gateway router IP address and the edge device IP addresses and subnet masks.

Usage sequence and implications (CM Only)

Table CMIPADDR is datafilled during commissioning of the Ethernet interfaces in an XA-Core switch. Changing the gateway or host address information after that may cause data mismatches between various nodes in the IP network.

This activity (A00005160, OSSAIN XA-Core Data Messaging Capacity Enhancements) adds the following dependency: Table CMIPADDR must be

datafilled before a tuple with DATAPATH = XAETHR can be added to table OANODINV.

Size

Current size unchanged.

Fields

The following table lists the top-level fields for table CMIPADDR.

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
KEY	unchanged	This field consists of subfields KEYCLASS and ENTRYNO.		
KEYCLASS	unchanged		GATEWAY, CMHOST, AMDIHOST, ETHRLNK	Key class. Indicates the class of tuple being datafilled. Enter GATEWAY to datafill the IP address of a gateway router. There can be only one GATEWAY tuple. Enter CMHOST to datafill an active IP address for the XA-Core. There can be two CMHOST tuples (total two active host IP addresses). Enter ETHRLNK to datafill a physical Ethernet link. There can be up to 8 ETHRLNK tuples, with each tuple corresponding to a physical link. AMDIHOST was added to allow datafill of an IP address to be used with an AMDI link for CLIP (Classical IP) over ATM. This value cannot be datafilled in SN07 or ISN07.
ENTRYNO	unchanged		0 to 7	Entry number. This is used to create a unique key. The KEYCLASS limits the ENTRYNO values that can be datafilled: GATEWAY: 0 to 0 CMHOST: 0 to 1 AMDIHOST: N/A ETHRLNK: 0 to 7

Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DATA	unchanged	This field consists of selector field SELCLASS and refinements.		
SELCLASS	unchanged	This is a selector field	GW, HOST, AMDI, ETHR	Selector class. The KEYCLASS in the key must match the SELCLASS entry as follows: GATEWAY: GW CMHOST: HOST AMDIHOST: AMDI ETHRLNK: ETHR

SELCLASS = GW

If the entry in subfield SELCLASS is GW, datafill refinements as shown in the following table.

GW refinement field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GTWYIP	unchanged		four numbers, each 0 to 255	Gateway IP address. Enter an address for a gateway router. This address is downloaded to the Ethernet interface card or packet. Note 1: VRRP and similar redundancy schemes allow a pair of routers to use a single IP address. Note 2: The GTWYIP entry may be the same as an address entered for an edge device in an ETHRLINK tuple, in case there is an Ethernet LAN but no WAN. It may not be the same as any other IP address in table CMIPADDR.
NETID	unchanged		0 to 1	Network (i.e., subnet) identifier. Enter 0. In SN07 there can be only one Ethernet-based subnet for the core.

SELCLASS = HOST

If the entry in subfield SELCLASS is HOST, datafill refinements as shown in the following table.

HOST refinement field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
ACTIVEIP	unchanged		four numbers, each 0 to 255	Active IP address for the XA-Core. This will be one of the IP addresses used by applications and advertised outside of the core. The active IP addresses are dynamically associated with physical interfaces. If an active IP address is bound to a physical interface that suffers a failure, it will be automatically rebound to a different interface in the same subnet.
NETMASK	unchanged		1 to 30	Subnet mask. Enter the number of leading '1's in the mask.
NETID	unchanged		0 to 1	Network (i.e., subnet) identifier. Enter 0. In SN07 there can be only one Ethernet-based subnet for the core.

SELCLASS = AMDI

This value cannot be datafilled in SN07/ISN07.

SELCLASS = ETHR

If the entry in subfield SELCLASS is ETHR, datafill refinements as shown in the following table.

ETHR refinement field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SLOTID	unchanged	This field consists of subfields SLOT and SIDE		
SLOT	unchanged		0 to 18	Slot. The physical slot number on the XA-Core shelf where the Ethernet interface card resides. (For EIOP, this is where the IOP resides.) Note: Refer to XA-Core engineering documentation for packfill restrictions.

ETHR refinement field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SIDE	unchanged		UNKNOWN, FRONT, REAR	Side. The location on the XA-Core shelf where the Ethernet interface card resides. Enter FRONT or REAR. Note: Refer to XA-Core engineering documentation for packfill restrictions.
PACKLET	unchanged		NONE, LOWER, UPPER	Packlet. For EIOP, enter the location of the Ethernet packlet on the IOP card. For other Ethernet interfaces such as HIOP and HCMIC, enter NONE.
CARDIP	unchanged		four numbers, each 0 to 255	Card IP address. This address is used only within the interface card or packlet, and is not advertised.
CARDNETM	unchanged		1 to 30	Card subnet mask. Enter the number of leading '1's in the mask.
MTCIP	unchanged		four numbers, each 0 to 255	Maintenance IP address. This is used by the core for maintenance of the interface card or packlet from the core. This address is not advertised.
MTCNETM	unchanged		1 to 30	Maintenance subnet mask. Enter the number of leading '1's in the mask.
EDGEIP	unchanged		four numbers, each 0 to 255	Edge device IP address. This is the address of the device to which the Ethernet interface is directly attached. This address is used by the core in performing integrity checks, using ICMP echo requests, on the point-to-point link between the Ethernet interface card or packlet and the edge device to which it is attached. Assuming the edge device is a Passport 8600, datafill the physical IP address of the CallP VLAN/subnet on the Passport 8600 that the HIOP or HCMIC subtends.
NETID	unchanged		0 to 1	Network (i.e., subnet) identifier. Enter 0. In SN07 there can be only one Ethernet-based subnet for the core.

Datafill example

The following example shows sample datafill for table CMIPADDR.

KEY	DATA
GATEWAY 0	GW (172 16 0 1) 0
CMHOST 0	HOST (172 16 14 108) 20 0
CMHOST 1	HOST (172 16 14 109) 20 0
ETHRLNK 1	ETHR 12 REAR NONE (172 16 14 104) 20 (172 16 14 110) 20 (172 16 0 2) 0
ETHRLNK 2	ETHR 6 REAR NONE (172 16 14 106) 20 (172 16 14 112) 20 (172 16 0 3) 0

Table release history update

Table CMIPADDR was introduced and modified in CSP16 by the following features:

- A59025829, IRM Plan B
- A59029386, CLIP on the XA-Core
- A59029980, Succession HIOP Maintenance Software

In CSP20 (SN07), new cross-checks and error messages are added by the following features:

- A00002510, LANCOMM IP over IRM - adds cross-checks with table IPNETWRK.
- A00005160, OSSAIN XA-Core Data Messaging Capacity Enhancements (this feature) - adds cross-checks with table OANODINV.

Supplementary information

In SN07/ISN07, only one subnet is supported for the core Ethernet interfaces. All active IP, maintenance IP, and card IP addresses must be unique, and they must all have the same netmask and the same subnet.

A GATEWAY or CMHOST tuple can be changed or deleted only if all links associated with the subnet are off-line. An ETHRLNK tuple can be changed or deleted only if the link is off-line.

Warning: Changes to the GATEWAY or CMHOST IP addresses or subnet information in this table after the initial commissioning may cause data mismatches between various nodes in the IP network.

This activity (A00005160, *OSSAIN XA-Core Data Messaging Capacity Enhancements*) adds the following error message. This message is printed if an attempt is made to delete or change a CMHOST tuple whose active IP address is datafilled in table OANODINV.

ERROR: The active IP address in this tuple is referenced by table OANODINV. The tuple cannot be changed or deleted as long as table OANODINV references it.

Translation verification and other tools

Table CMIPADDR does not use translation verification tools.

Name: Table QMSMIS

QMS MIS Link Definition Table

Note: The only changes are a new cross-check and a new error message.

Functional description

Table QMSMIS defines the links used by a Queue Management System Management Information System (QMS MIS) application and also defines the audit frequency for the links.

Usage sequence and implications (CM Only)

Current datafill order unchanged.

Size

Current size unchanged.

Fields/OIDs

The following table lists the top-level fields for table QMSMIS.

QMSMIS field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
INDEX	unchanged			
DATALINK	unchanged			

Datafill example

The following example shows sample datafill for table QMSMIS.

```

INDEX                                     DATALINK
-----
OSSAIN                                ETHERNET MIS_OSSAIN 24 7001
TOPS                                MPC (3 3 1) (4 4 2) $

```

Table release history update

Cross-checks are added to enforce that an OSSAIN QMS MIS server cannot be datafilled in table OANODINV with data path XAETHR.

Supplementary information

If an attempt is made to datafill an OSSAIN tuple whose node has data path XAETHR in table OANODINV, the following error message is displayed:

This node has DATAPATH XAETHR in table OANODINV. OSSAIN QMS MIS servers must use the EIU. XA-Core Ethernet data path is not supported for OSSAIN QMS MIS.

Translation verification and other tools

Tools unchanged.

Service Orders (SO) (CM & SESM)

Not applicable.

Software optionality control (SOC)

SOC option name:	OSSAIN Base
SOC option title:	OSSAIN Base
SOC option control type:	state
New SOC option?	No
SOC option order code	OSAN0101
Option defined in DRU:	TOPS
Affected products:	SN0x, ISN0x

Element Management

Not applicable.

Command interface changes

Command: QUERYPM (in OAINPMDIR directory)

Command type: Listed MENU

Command target: All

Command availability: RES

Command description

The QUERYPM command is available in a number of different MAP levels. In general, it is used to display information about the posted peripheral module (PM).

This feature changes the output that is displayed when the QUERYPM command is issued with no arguments in the OAINPMDIR directory. The OAINPMDIR directory is entered from the MAPCI;MTC;PM level by posting an OSN, OSNM, or OSAC node. These node types are used for the TOPS OSSAIN application.

Command syntax

The command syntax is unchanged. In the OAINPMDIR directory, the QUERYPM command may be entered with no parameters or with the constant FLT parameter. This feature only changes the output when QUERYPM is entered with no parameters.

Qualifications and warnings

None.

Responses

This feature changes only the success response. It does not change the error responses.

The success response displays information about the posted node, from table OANODINV. None of the information that was displayed prior to this feature is changed in format or meaning. This feature adds a new line to the success response, corresponding to new information in table OANODINV.

The new line displays the data path used for the posted node. The data path can be EIU or XAETHR. EIU refers to the Ethernet Interface Unit. XAETHR refers to XA-Core Ethernet interface cards such as HIOP and HCMIC. If the node uses an XAETHR data path, the display also shows the active CM host IP address that the switch uses in messaging with the node.

The success response does not require any user action. It is visible on both XA-Core and BRISC. On BRISC the data path will always be EIU. On XA-Core, it can be either EIU or XAETHR.

Example

The following figure shows an example success response for a posted node with connectivity through XA-Core Ethernet cards using active host IP address 172.16.1.109. The figure uses a bold font to highlight the new line that has been added to the display.

```
NODENAME: DAA_01
NODEID: 1
PROTOCOL: UDP
IPADDR: 172.16.20.205
DATAPATH: XAETHR (172.16.1.109)
ONODTYPE: SN
ONODLOC: 1 DD 33
ONODSITE: CITYC
HOSTNAME: SWITCH_C
```

Actual data values depend on datafill in table OANODINV.

Command: BUFSTATS (in OSSAINCI directory)

Command type: NON-MENU

Command target: All

Command availability: RES

Command description

OSSAINCI is an existing directory that provides non-menu commands that are used primarily by Nortel Networks customer support personnel. The OSSAINCI directory is accessed by entering the directory name. Most of the commands are related to tracing of OSSAIN messages. The new BUFSTATS command is not related to tracing; it is related to buffer resources.

The BUFSTATS command allows the user to view information about the queues and buffer pools that are used for processing messages incoming to OSSAIN via an XA-Core Ethernet interface. It also allows the user to reset the low water marks associated with the free queues.

Command syntax

BUFSTATS command parameters and variables

Command	Parameters and variables
BUFSTATS	DISPLAY, RESET
Parameters and variables	Description
DISPLAY	Displays information about buffer resources
RESET	Resets low water marks associated with free queues used by the application.

Qualifications and warnings

Low water marks are inaccurate unless they fall below a threshold set by BMS.
In-queue counts are approximate.

Displaying buffer stats frequently during peak traffic hours can cause blocking.

Responses

MAP outputs with associated meanings and actions

Response to command BUFSTATS with no parameters, or with DISPLAY parameter

The system displays information about the queues. Following is an example. The numbers will vary.

```
XAETHR Free Qs/Pools
=====
Bytes/buff  Alloc  Count  LWM
-----
    64      500   470    12
   128      400   381    70
   320      200   198   103
```

```
XAETHR Inuse Qs
=====
Use      Count
-----
CallP    45
Mtce      3
```

Meaning:

Bytes/buff	number of message body bytes in buffers
Alloc	number of buffers allocated
Count	approximate number of buffers currently in queue
LWM	low water mark
Use	kind of messages the queue/pool is used for

User actions:

No user action is required.

MAP outputs with associated meanings and actions

Success response to command BUFSTATS with RESET parameter

LWMs have been reset for all FreeQs

Meaning:

The System has reset the low water marks of the free queues.

User actions:

No user action is required.

Example

Usage example for OSSAINCI BUFSTATS command

Description of task:	Study free queue low water marks during a defined study period.
At the beginning of the study period:	
Command: MAP response:	>OSSAINCI OSSAIN:
Command: MAP response:	>BUFSTATS RESET LWMs have been reset for all FreeQs
Command: MAP response:	>LEAVE CI:
At the end of the study period:	
Command: MAP response:	>OSSAINCI OSSAIN:
Command: MAP response:	>BUFSTATS DISPLAY <display similar to that in Table on page 2392>
Command: MAP response	>LEAVE CI:

Command: SCREENTAB (in OSSAINCI directory)

Command type: NON-MENU

Command target: All

Command availability: RES

Command description

OSSAINCI is an existing directory that provides non-menu commands that are used primarily by Nortel Networks customer support personnel. The OSSAINCI directory is accessed by entering the directory name. Most of the commands are related to tracing of OSSAIN messages. The new SCREENTAB command is not related to tracing; it is related to an internal table that the switch maintains.

The SCREENTAB command allows Nortel Networks support personnel to view the contents of the internal table. The internal table does not affect any functionality in the SN07/ISN07 releases. It is for possible future use.

Command syntax

SCREENTAB command parameters and variables

Command	Parameters and variables
SCREENTAB	none

Qualifications and warnings

None.

Responses

MAP outputs with associated meanings and actions

Response to command SCREENTAB		
The system displays information about the internal table. Following is an example. The numbers will vary.		
idx (hex)	entry	collisions
-----	-----	-----
00B9	2F8EE0B9 (47.142.224.185)	0
0201	2FF50E01 (47.245.14.1)	0
Meaning:		
	idx	index into internal hash table
	entry	data in internal hash table
	collisions	number of hash collisions to access entry
User actions:		
No user action is required.		

Example

Usage example for OSSAINCI SCREENTAB command

Description of task:	View contents of internal hash table.

Usage example for OSSAINCI SCREENTAB command

Command:	>OSSAINCI
MAP response:	OSSAIN:
Command:	>SCREENTAB
MAP response:	<display similar to that in Table on page 2394>
Command:	>LEAVE
MAP response:	CI:

Security

A secure network is assumed. The risk in using OSSAIN in an insecure network is greater with XA-Core Ethernet interface cards than with the EIU. This is because the EIU can offer some protection to the core by screening out messages from unwanted IP addresses. With XA-Core Ethernet interface cards, anyone with access to the central office LAN has direct access to the core.

Network configuration

Firewalls and routers must allow UDP datagrams to and from the IP addresses and ports used for OSSAIN.

- IP addresses
 - In the core, OSSAIN may use the active CMHOST IP addresses datafilled in table CMIPADDR, the IP address in the CMIPADDR tuple of table IPNETWRK, or both. Which core IP addresses OSSAIN uses is based on datafill in table OANODINV.
 - IP addresses of OSSAIN and OSAC nodes are datafilled in the IPV4ADDR field of table OANODINV.
 - If OSSAIN is configured to use EIUs, it uses them as routers.
- Ports
 - OSSAIN uses UDP ports 5289 through 5293 in the core, regardless of whether it is configured to use EIUs or XA-Core Ethernet interfaces.
 - UDP ports used in service nodes for OSSAIN messaging are datafillable in the following tables and fields:
 - table OANODINV, field NMTCPORT in OSNM refinement
 - table OASESNPL, fields CPPORT and MTCPORT in various refinements

Note: Although an OSAC remote switch does not have datafill for a centralized service node's maintenance port, it does send messages to and receive messages from this port. The centralized

service node is datafilled in the OSAC remote as an OSN node, and in the OSAC host as an OSNM node. The OSAC remote sends datagrams to and receives datagrams from the centralized service node at the NMTCPORT datafilled in the OSAC host, as well as at the session pool ports datafilled in both switches.

OSSAIN also requires that the data network support ICMP echo requests and replies to and from the IP addresses used for OSSAIN nodes (both OSAC switches and service nodes).

This activity does not restrict whether the active host IP addresses in table CMIPADDR are in the same or a different subnet than the CM IP address used by the EIU.

Key management

N/A.

Protocol

N/A.

Authentication

N/A.

Configuration Walkthrough

This section outlines steps for converting OSSAIN to use XA-Core Ethernet interface, rather than EIU, for messaging with a single far-end node (SN or OSAC switch). This procedure has the following prerequisites:

- The secure, engineered data network must be up and configured.
- The XA-Core Ethernet interfaces must be commissioned.
- If an SN is involved (it will be unless it's an OSAC link being changed), the method for changing the switch IP address on the SN must be understood. This method is different for different service nodes.

Once the prerequisites are satisfied, there are several ways the change could be made. The sequence shown here is straightforward and will not cause sessions in progress to fail; however, it may cause SysB alarms in switches in the OSAC network. These alarms will clear automatically once the conversion is successfully completed. If avoiding such alarms is a priority, more steps may be needed. For example, if an OSAC host is being converted to use XA-Core Ethernet interface for messaging with a particular SN, it will need to briefly off-line the SN, and this will raise alarms in the OSAC remotes unless the SN's session pools and the SN itself have first been busied in the remotes.

1. At the switch that is to start using XA-Core Ethernet interface cards:

- a. Drain all session pools datafilled against the far-end node. This is done at the SesnPool level (SESNPOOLDIR) of the DMS MAP. Wait for the session pools to transition to ManB.
 - b. Off-line all session pools datafilled against the far-end node.
 - c. At the OAINPMDIR directory, busy and off-line the far-end node.
 - d. In table OANODINV, modify the tuple for the far-end node to use XAETHR data path, and datafill the CMIPADDR field.
2. At the far-end node, change its configuration to use the new IP address for the switch.
 - If the far-end node is an SN, follow SN-specific procedures for this step.
 - If the far-end node is an OSAC switch, follow the steps given here at that switch. These steps assume that switch A is the one being changed to use XA-Core Ethernet interfaces, and switch B is the one where the following steps are performed.
 - a. Busy and off-line all session pools associated with switch A; then busy and off-line switch A at the OAINPMDIR directory.
 - b. Modify the tuple for switch A in table OANODINV, changing the IPV4ADDR field to the IP address that was datafilled in switch A against switch B in the CMIPADDR field of table OANODINV.
 - c. At the OAINPMDIR MAP directory, Busy and RTS switch A.
3. At the switch that is to start using XA-Core Ethernet interface cards:
 - a. Busy and RTS the far-end node.
4. Check logs at both ends, and if desired, make test calls.
5. Configure firewalls and routers in the data network to disallow messaging between the CM IP address datafilled in table IPNETWRK and the far-end node, if desired.

Note: Refer to the FN section of this DDOC (A00005160, *OSSAIN XA-Core Data Messaging Capacity Enhancements*) for a limitation regarding inconsistent IP address datafill detection. This limitation exists only in OSAC remote switches, and only if the OSAC host switch is below SN07/ISN07, the service node is below OAP release 9, or both.

Performance Management for A00005160

Performance management strategy

Performance management for the OSSAIN product is described in 297-8403-901, *Operator Services System Advanced Intelligent Network (OSSAIN) User's Guide*.

This feature (A00005160, *OSSAIN XA-Core Data Messaging Capacity Enhancements*) adds one new OM group in the DMS Core. The new OM group can be used in analyzing messaging throughput of TOPS applications that send and receive UDP datagrams.

Performance management tools and utilities

Standard DMS tools for managing OMs.

Operational Measurements (OM)

OM Group template

OM description

OM group TDGTHRU

TOPS Datagram Throughput

Release history update

The OM group is being created in TOPS20/SN07/ISN07.

Registers

OM group registers display on the MAP terminal as follows:

OM Group TDGTHRU Display

SND48	SND48X	SND96	SND96X
SND160	SND160X	SND224	SND224X
SND296	SND296X	SND368	SND368X
SND512	SND512X	SNDLG	SNDLGX
RCV48	RCV48X	RCV96	RCV96X
RCV160	RCV160X	RCV224	RCV224X
RCV296	RCV296X	RCV368	RCV368X
RCVLG	RCVLGX		

Each register counts the number of messages in a particular size range that a TOPS application sent or received during the reporting period. The numbers in the register names indicate the size ranges or “buckets,” as explained in Table , “TOPUDPTH Registers,” on page 2408.

Group structure

OM group TDGTHRU provides 1 tuple for each of the four fixed key values as shown here.

Key field: TOPS_DGRAM_IDX specifies the TOPS application and data path to which the peg counts in the tuple apply. The fixed key values are listed here along with their meanings:

Key values for OM group TDGTHRU

Key Value	Meaning
OA_EIU	OSSAIN application using Ethernet Interface Unit
OA_XAETHR	OSSAIN application using XA-Core Ethernet interface
POS_IPXPM	TOPS position application using IP-XPM
OC_IPXPM	Operator Centralization application using IP-XPM

Info field: None

Associated OM groups

None.

Associated functional groups

None.

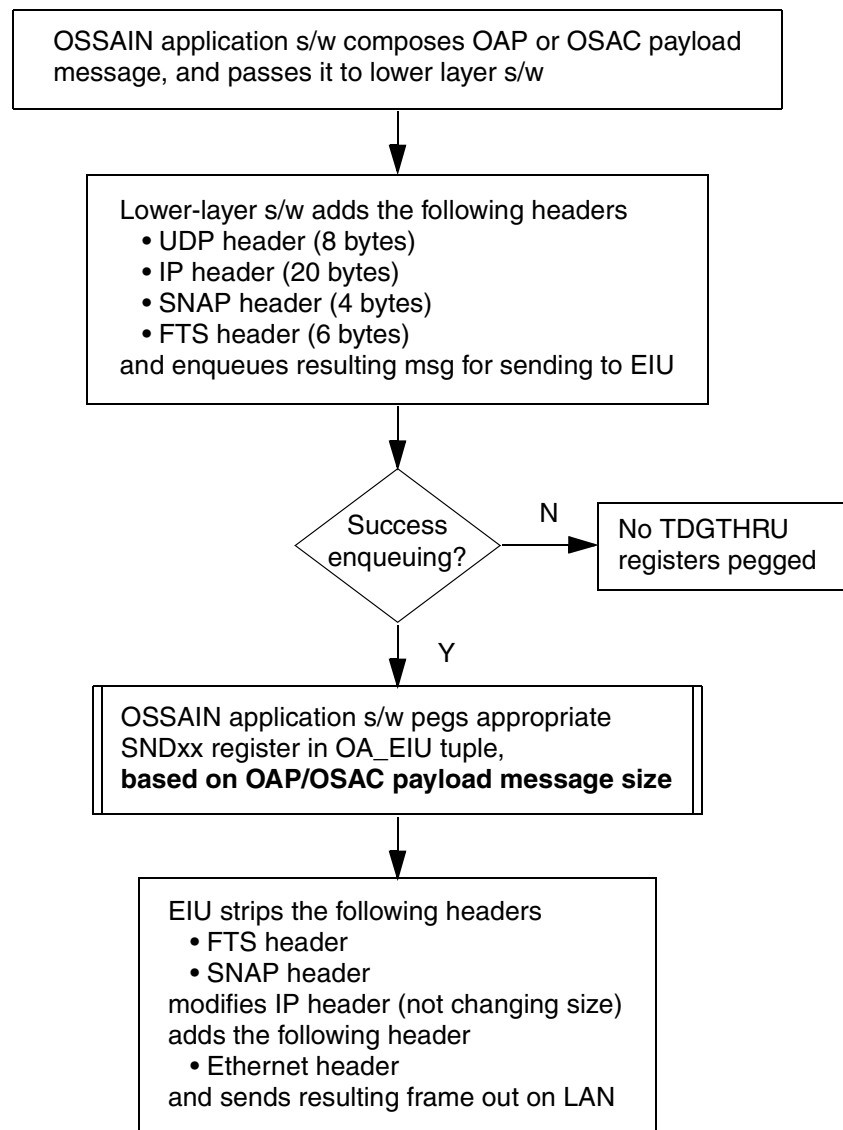
Associated functionality codes**Functionality codes associated with OM group**

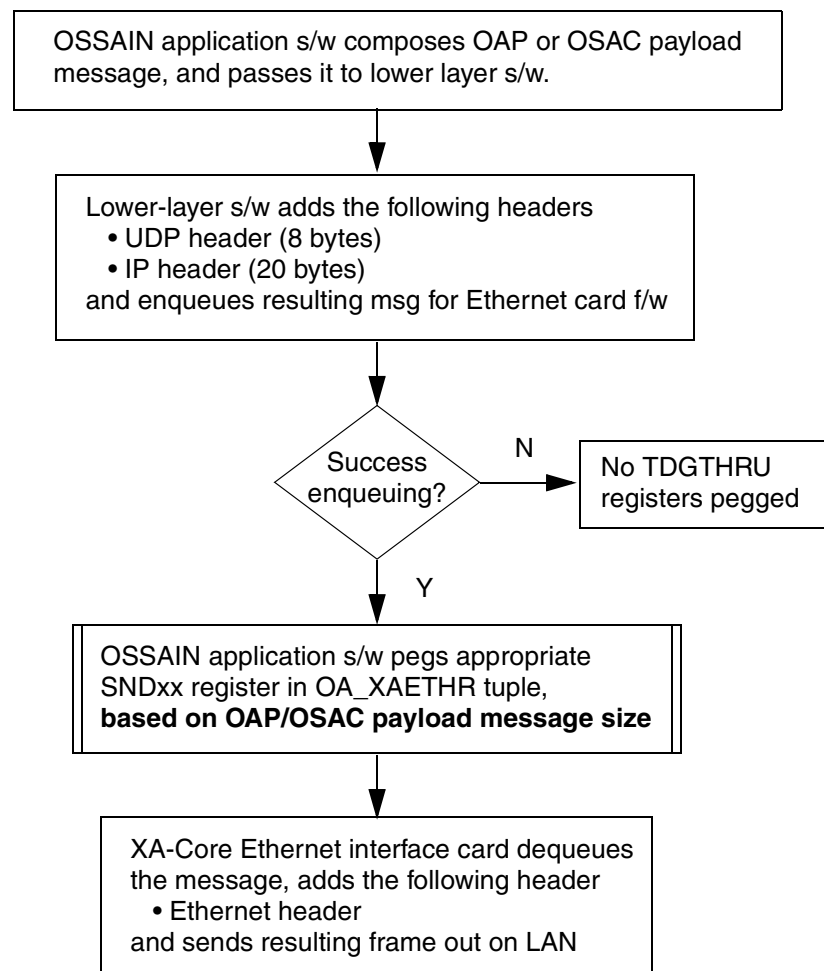
Functionality	Code
Base TOPS	OSB0101

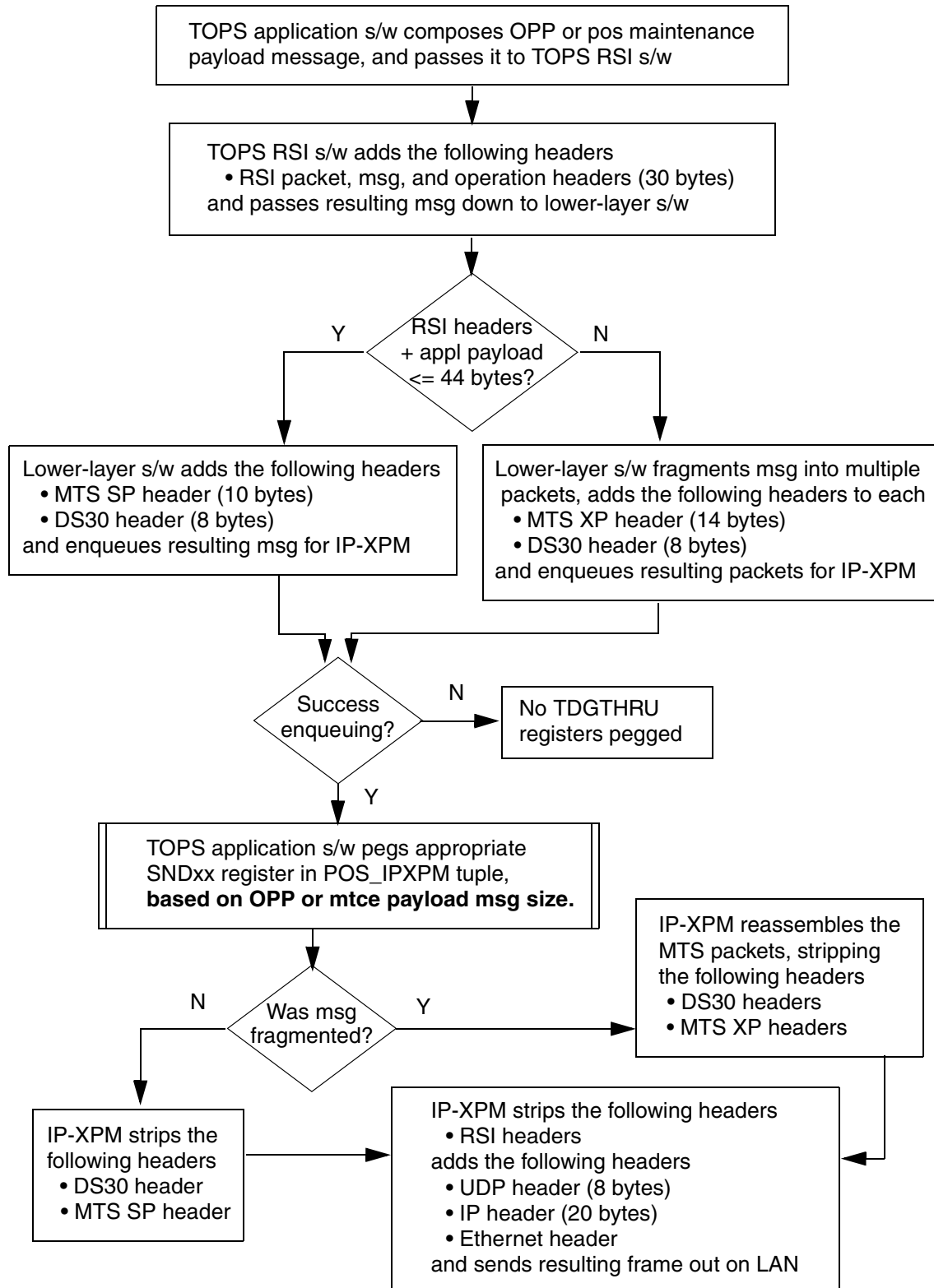
OM group registers logic flow charts

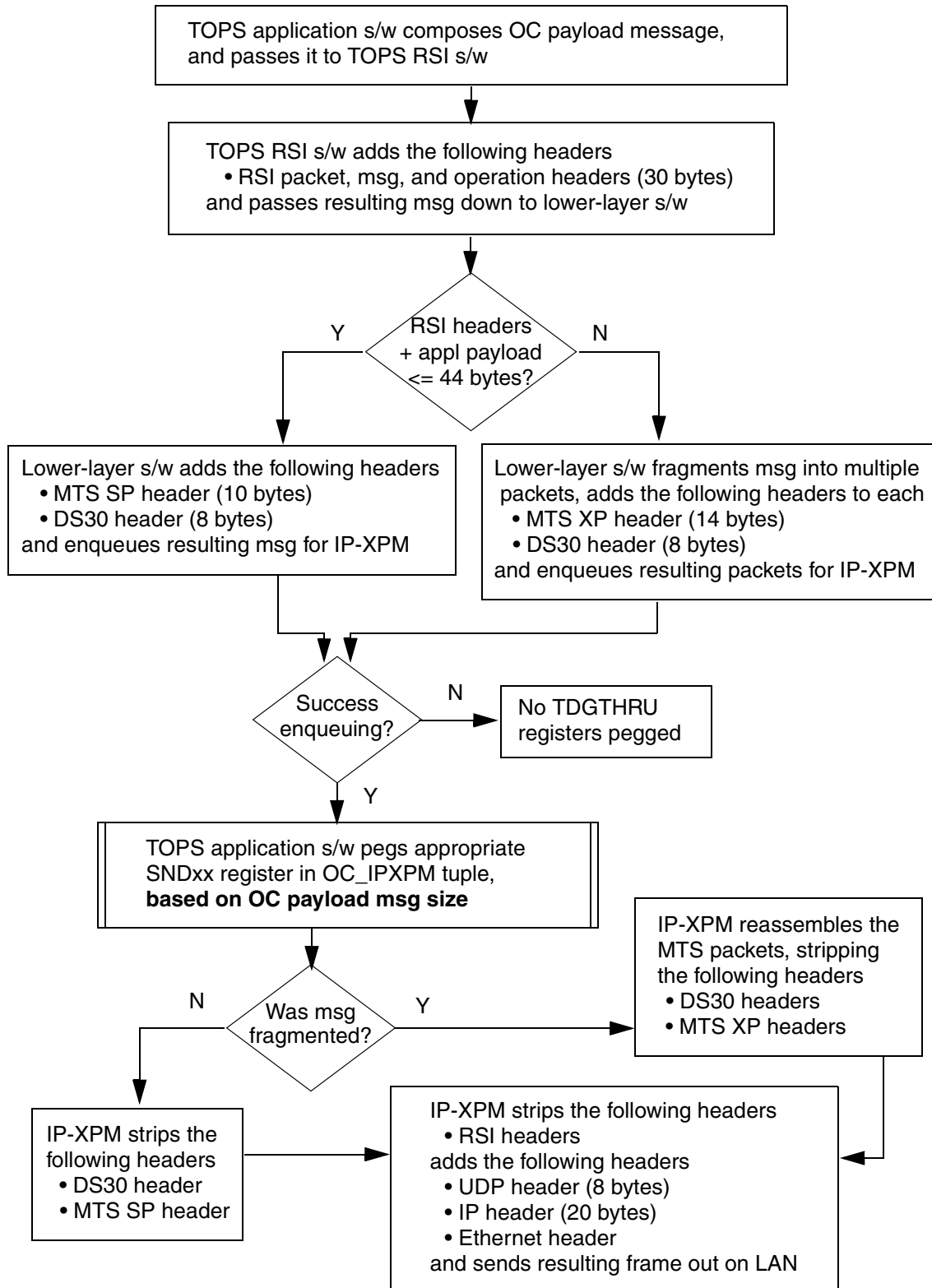
This section includes 8 flow charts: one for pegging SNDxxx registers and one for pegging RCVxxx registers, for each of the four tuples.

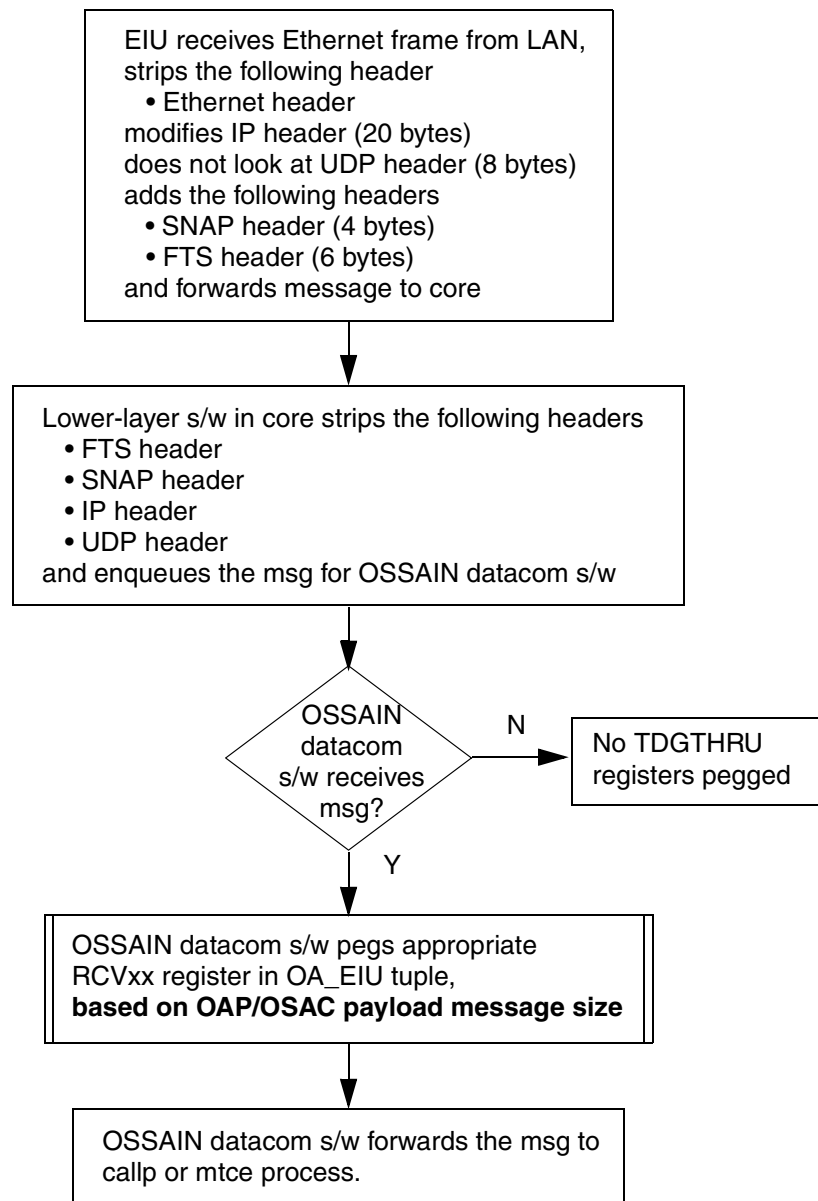
For more information about the specific registers, please refer to Table , “TOPUDPTH Registers,” on page 2408.

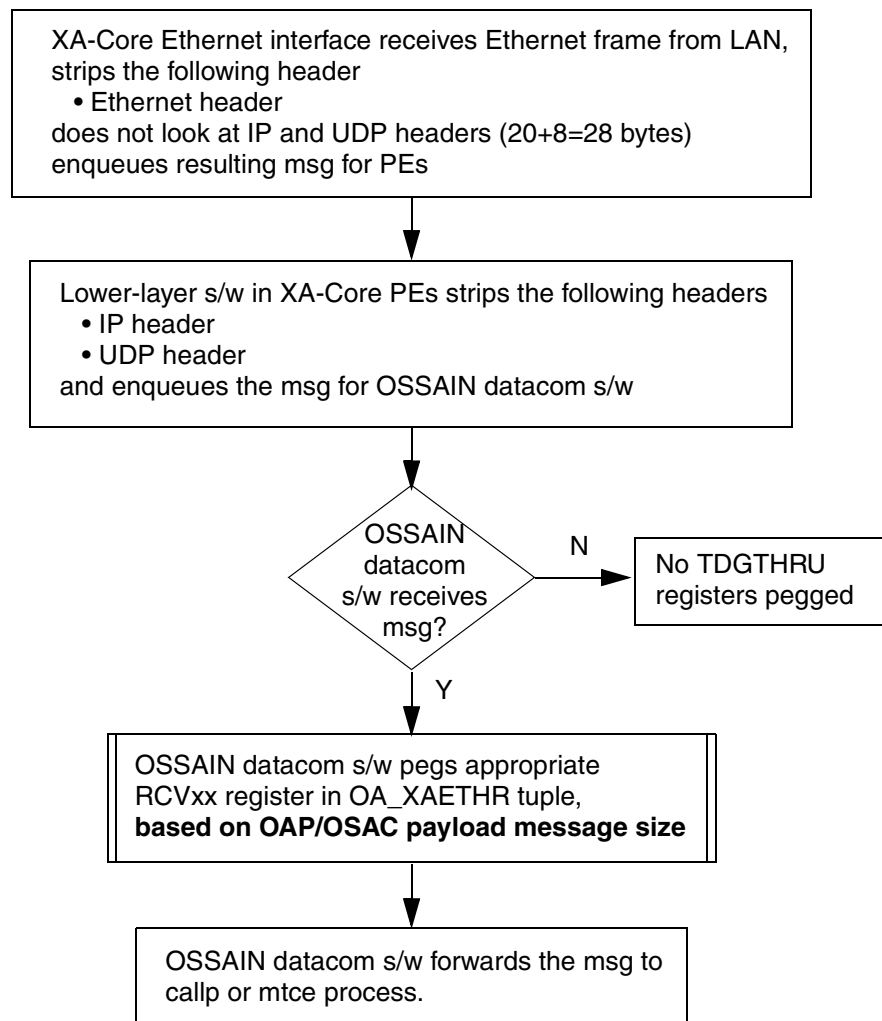
Flow chart for pegging send (SND) registers in OA_EIU tuple

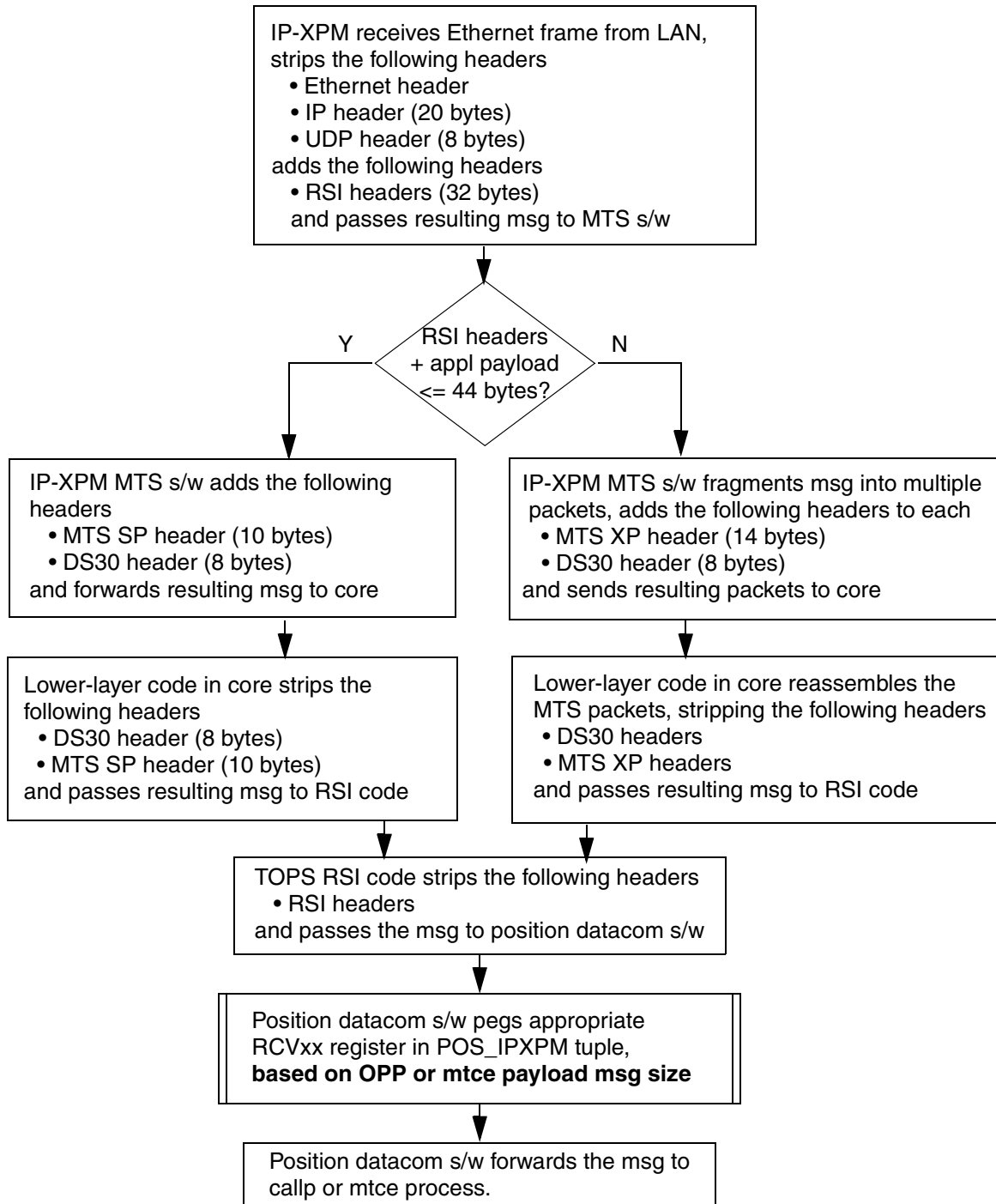
Flow chart for pegging send (SND) registers in OA_XAETHR tuple

Flow chart for pegging send (SND) registers in POS_IPXPM tuple

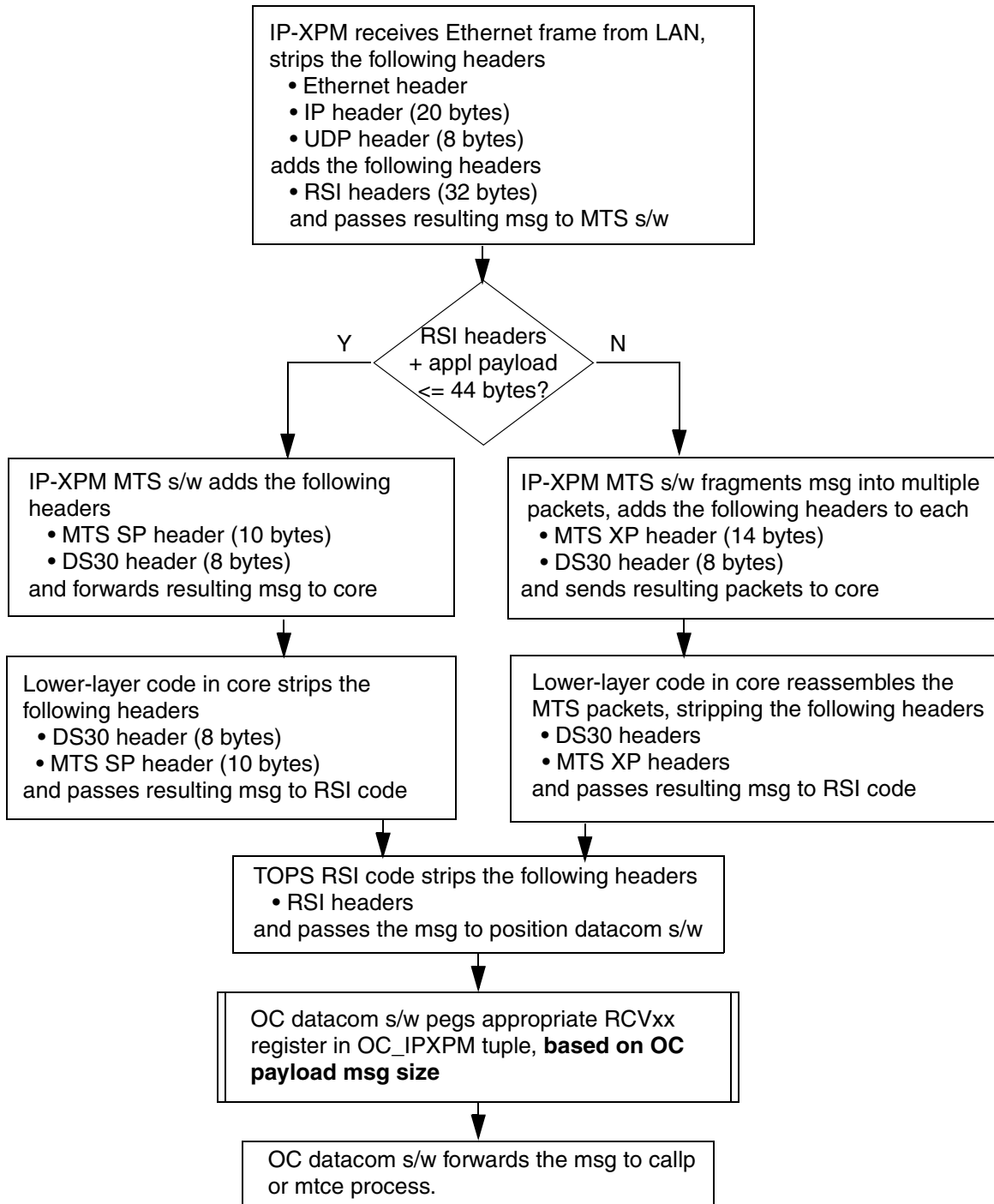
Flow chart for pegging send (SND) registers in OC_IPXPM tuple

Flow chart for pegging receive (RCV) registers in OA_EIU tuple

Flow chart for pegging receive (RCV) registers in OA_XAETHR tuple

Flow chart for pegging receive (RCV) registers in POS_IPXPM tuple

Note: Failure at any point before the message gets to position datacom s/w results in no registers being pegged in group TDGTHRU.

Flow chart for pegging receive (RCV) registers in OC_IPXPM tuple

Note: Failure at any point before the message gets to OC datacom s/w results in no registers being pegged in group TDGTHRU.

Registers

Register description

Each register in this group counts the number of messages in a specific size range that were sent by or received by a particular TOPS application, using a particular Ethernet interface.

These registers may be useful for estimating the resources that TOPS applications need for their UDP messaging. Depending on what resources are being studied, it may or may not be necessary to take into account various headers that are added and stripped at various points in the message processing. Message sizes used in pegging registers in this group include only the TOPS application payload part of the message. Refer to the flow charts in [“OM group registers logic flow charts”](#) beginning on page 2399 for details.

The following table explains each register.

TOPUDPTH Registers

Short Register Name	Long Name	Explanation
SND48 and SND48X	Send 48 Bytes	Peg register. Counts the number of messages sent from the core, of size <= 48 bytes. SND48X is an extension register.
SND96 and SND96X	Send 96 Bytes	Peg register. Counts the number of messages sent from the core, of size > 48 bytes and <= 96 bytes. SND96X is an extension register.
SND160 and SND160X	Send 160 Bytes	Peg register. Counts the number of messages sent from the core, of size > 96 bytes and <= 160 bytes. SND160X is an extension register.
SND224 and SND224X	Send 224 Bytes	Peg register. Counts the number of messages sent from the core, of size > 160 bytes and <= 224 bytes. SND224X is an extension register.
SND296 and SND296X	Send 296 Bytes	Peg register. Counts the number of messages sent from the core, of size > 224 bytes and <= 296 bytes. SND296X is an extension register.

TOPUDPTH Registers

Short Register Name	Long Name	Explanation
SND368 and SND368X	Send 368 Bytes	Peg register. Counts the number of messages sent from the core, of size > 296 bytes and <= 368 bytes. SND368X is an extension register.
SNDLG and SNDLGX	Send Large	Peg register. Counts the number of messages sent from the core, of size > 368 bytes. SNDLGX is an extension register.
RCV48 and RCV48X	Receive 48 Bytes	Peg register. Counts the number of messages received by the core, of size <= 48 bytes. RCV48X is an extension register.
RCV96 and RCV96X	Receive 96 Bytes	Peg register. Counts the number of messages received by the core, of size > 48 bytes and <= 96 bytes. RCV96X is an extension register.
RCV160 and RCV160X	Receive 160 Bytes	Peg register. Counts the number of messages received by the core, of size > 96 bytes and <= 160 bytes. RCV160X is an extension register.
RCV224 and RCV224X	Receive 224 Bytes	Peg register. Counts the number of messages received by the core, of size > 160 bytes and <= 224 bytes. RCV224X is an extension register.
RCV296 and RCV296X	Receive 296 Bytes	Peg register. Counts the number of messages received by the core, of size > 224 bytes and <= 296 bytes. RCV296X is an extension register.
RCV368 and RCV368X	Receive 368 Bytes	Peg register. Counts the number of messages received by the core, of size > 296 bytes and <= 368 bytes. RCV368X is an extension register.

TOPUDPTH Registers

Short Register Name	Long Name	Explanation
RCVLG and RCVLGX	Receive Large	Peg register. Counts the number of messages received by the core, of size > 368 bytes. RCVLGX is an extension register.

Register release history update

All registers in this group were created in TOPS20/SN07/ISN07.

Associated registers

None.

Associated logs

None



Succession baseline information

This chapter provides information on all Succession Logs/faults, and on all Succession operational measurements (OMs). Future releases will add other OAM&P categories (data schema, office parameters, software optionality control, and others).

Logs/Faults information

A log report is a record of a message that your system generates whenever a significant event has occurred in the switch or one of its peripherals. Log reports include status and activity reports, as well as reports on hardware or software faults, test results, changes in state, and other events or conditions likely to affect the performance of the switch. Either a system action or a manual action can generate a log report.

Note: Some of the element managers use a graphical user interface (GUI), so they display faults on the workstation monitor screen rather than generating log reports.

Alarms are generated by the system when problems or conditions are detected that can change the performance or working state of a network or network element. Daily operation of the network requires monitoring for alarms and checking that functions continue without interruption. Alarms provide notification that a system hardware or software-related event has occurred.

Using Syslog in Succession

In SN06 an alternative is introduced to log/fault delivery from each separate element management system. Syslog can be used to aggregate some of the individual fault/log streams into the SCC2/NT STD stream on the CS 2000 Core Manager/SDM.

Succession will be using syslog in several ways:

- Alarms/Faults - custlog stream - Many element managers and network elements, including SDM Platform, CS 2000 SAM21 Manager, STORM, CS 2000 GWC Manager, UAS Manager, MDM (for PVG), and some CS 2000 Management Tools applications, use syslog as one mechanism for notify other systems of fault events. One consumer of those fault events is the SCC2/NT STD log converter provided on the CS2000 Core

Manager/SDM. The SCC2/NT STD log converter will collect events from those sources via the custlog format and merge those events into the SCC2/NT STD stream with the CS2000 Core fault events.

- Audit trail - Succession is also using syslog to capture the user audit trail our network elements and element managers. The audit trail contains a history of significant user and OSS activity. Syslog is the only protocol which will contain the audit trail.
- Security log - Succession is also using syslog to capture the security logs from our network elements and element managers. The security log contains both success and failure history of authentication and authorization activities. This stream will also contain security related events from IPSec/KCE and other key negotiation systems. Syslog is the only protocol which will contain the security log stream.
- Debug log - some components use syslog for diagnostic and debug information used by the Nortel support personnel. This stream is not exported beyond the EMSs and is not configured or documented for end user or customer access.

Alarm reporting for DMS and SPM-based equipment

The alarm reporting system integrates event detection and alarm notification functions. An alarm becomes active when reduced service, reliability, or a test condition occurs in the network or network element. The alarm remains active until a system event or activity performed by operating company personnel clears the alarm condition. The alarm system includes audible notification and visual display through warning lights and the MAP terminal. Many alarms generate automatic logs reports when raised or cleared.

For DMS and SPM-based equipment, the MAP terminal displays alarm codes in the banner and the subsystem status summary field (SSSF). The alarm banner displays alarm codes that indicate the effect of the alarm event on the network or network element. The SSSF displays alarm codes that indicate equipment faults of system states.

Log Delivery Service application

The Log Delivery Service application collects logs generated by the Communications Server 2000 (CS2000) and from the CS2000 Core Manager log stream, formats these logs, and can deliver them as a single stream to the downstream Operational Support Systems (OSS).

The CS2000 log feed includes logs for itself and all peripherals managed by it, such as: MG 4000, IW-SPM, DPT-SPM and SPM. Logs are generated locally on the CS2000 Core Manager for its own faults and status changes and are merged with the CS2000 feed. The Log Delivery Service application provides log reports in ASCII text format at a single interface for inbound or outbound TCP/IP connections.

Log formats

The Log Delivery service provides reports in either Switching Control Center 2 (SCC2) or Standard (STD) format. Some of the high-level differences between SCC2 format logs and STD format logs are as follows:

- SCC2 has no CS2000 identifier as found in the top left hand corner of the STD log. This field is datafilled on the CS2000 in table OFCVAR, tuple LOG_OFFICE_ID.
- SCC2 logs do not contain the date in the header on which the log was generated.
- SCC2 logs only give the minutes past the hour in which the log was generated, while the STD log gives the hour, minutes, and seconds.
- A critical severity log is represented by *C in SCC2 format, and by *** in STD format.
- If applicable, the SCC2 log will have the name of the component and/or peripheral generating the log in the log header.
- When ECORE_FORMAT (table OFCVAR on the CS2K) is enabled, SCC2 formatted logs display the optional parameter NodeName on a new line immediately following the header. This new line is not indented and has the following format: Log from node <NodeName>.
- SCC2 headers (having less information) are less likely to have the Equipment Identifier field found in some logs wrapped to the next line. (See NT STD format definition section below).

See the following example to see the difference in the formats, using a CARR811 log.

Standard format:

```
ASN06SWITCH * CARR811 FEB24 00:45:05 3320 TBL CARRIER SPM 39
  CKT: 63 CarrName: SPM39_STS1P_1_VT15P_1_DS1P_28
  Carrier: STS1P 1 VT15P 28 DS1P 1
  UAS-N Threshold Crossing Alert: 10
  Accumulation Interval: 0:00:10 Period: 15 minutes
  Location: SPM 39 Type: SMG4 Fabric: ATM
```

SCC2 format:

```
ASN06SWITCH * CARR811 FEB24 00:45:05 3320 TBL CARRIER SPM 39
  CKT: 63 CarrName: SPM39_STS1P_1_VT15P_1_DS1P_28
  Carrier: STS1P 1 VT15P 28 DS1P 1
  UAS-N Threshold Crossing Alert: 10
  Accumulation Interval: 0:00:10 Period: 15 minutes
  Location: SPM 39 Type: SMG4 Fabric: ATM
```

NT Standard log format and definitions

NT Standard log format:

```
<LogOfficeId>_<NodeName>_<POA><Threshold><LogName><ReportNumber>_<DateIndicator>_<TimeIndicator>_<SequenceNumber>_<EventType>_<EventLabel>_<EquipmentIdentifier>CR
<LOG BODY>CR
```

where:

- The < and > denote the beginning and end of a field.
- **Bold** text denotes optional fields that may or may not be there.
- CR = carriage return.
- <LOG BODY> = 0 to n lines of text - usually each line begins following an indentation of 8 spaces.
- _ denotes a space delimiter between fields.

Office Identifier <LogOfficeId>:

Field Length/Format: variable length (1 to 12 characters)

Field Value(s): typically an 11-character Office CLI name

Comment: This field's value corresponds to what is datafilled in your switch's table OFCVAR, tuple LOG_OFFICE_ID. A maximum of 12 characters can be datafilled into the LOG_OFFICE_ID tuple. Normally though, the value of this tuple in customer sites matches that of the Office CLI name. The Office CLI name has a standard length of 11 characters. In the switch it is datafilled in table OFCENG, tuple OFFICE_CLI_NAME. (So OFFICE_CLI_NAME and LOG_OFFICE_ID would be datafilled the same). In a log sent downstream to an OSS, the Office Identifier field will be seen by the OSS as 1 word with no spaces. No padding of spaces will occur with this field to make it 12 characters. i.e. If the log_office_id value is 6 characters in length, the space following the field will be the delimiter to the next field.

Node Name:

Field Length/Format: fixed length (8 characters)

Field Value(s): Node name that is left justified within the 8 character field. Padding of spaces will occur to ensure 8 character length.

Comment: This optional field is generally not recommended for implementation. The value of the field is often "CM" which has low value and the extra 9 characters (8 + space) increases the length of the header. A longer header may result in line wrapping of the Equipment Identifier field which is present in

some logs. A wrapped header is difficult for OSSs to accommodate.

Alarm Level Indicator / Priority of Action (POA) / Severity:

Field Length/Format: fixed length (3 characters)

Field Values: '***' or '**' or '*' or ' ' (Note the right justification of the *s).

Threshold:

Field Length/Format: 1 character field (Note: there are no space delimiters before/after)

Field Value(s): A + sign if the log is thresholded. A space if the log is not thresholded.

Log Name/Report Name/Log Prefix:

Field Length/Format: fixed length (4 characters)

Field Value(s): The log name is right justified within the 4 character field.

Padding of spaces will occur at the beginning for names less than 4 characters.

E.g. 'CARR' or ' SPM'. Note that the Log Name and the Report Number are considered a single entity. i.e. The SPM300 log.

Report Number:

Field Length/Format: fixed length (3 characters)

Field Value(s): The number will always be 3 digits. i.e. 100 to 999.

Date Indicator:

Field Length/Format: fixed length (5 characters); MMMDD where MMM is JAN through to DEC and DD is 01 through to 31

Field Value(s): E.g. DEC04

Time Indicator:

Field Length/Format: fixed length (8 characters); HH:MM:SS where HH is 00 through 23, MM is 00 through 59, and SS is 00 through 59

Field Value(s): E.g.: 20:39:13 or 00:00:00 or 23:59:59

Sequence Number:

Field Length/Format: fixed length (4 characters); NNNN where the range is 0000 through 9999

Field Value(s): E.g. 0000 or 2358 or 9999. Once 9999 is reached, the number will go back to 0000. In SDM, STD_OLD and SCC2_OLD formats should increment the sequence number by 1 and SCC2/STD formats increment the

sequence number in the same fashion as the CS2K does. In IEMS, SCC2/STD formats increment the sequence number by 1.

Event Type:

Field Length/Format: fixed length (4 characters);

Field Value(s): Left justified text with spaces at the end to pad to 4 character length. Examples: 'INFO', 'TBL ', 'FLT ', 'OFFL', 'SYSB', ' ', and so on.

Event Label:

Field Length/Format: variable length of characters; can contain more than 1 word separated by spaces

Field Value(s): E.g.: “SDM BASE MAINTENANCE”, or “CARRIER”.

Equipment Identifier: (last field to be considered part of the header)

Field Length/Format: fixed length (4 characters) node type, followed by a space, followed by a numeric node number

Field Value(s): Node type portion is left justified and padded with spaces at the right if less than 4 characters. The node number portion is left justified. E.g. 'SPM 0', 'LIU7 43', 'SPM 71'.

Comment: This field is not found in all logs and should be considered rare. Known log types where this field is present are CARR and in some PM logs.

Log Body: (Not part of header. It follows the header).

Field Length/Format: Text in the log body usually follows an indentation of 8 spaces. Each line of text is variable in length.

Field Value(s): Can be anything but each unique log should typically always get sent out the door in the same format.

Notes

- Not all logs have an Equipment Identifier at the end of the header. There is no list of logs that have an Equipment Identifier and it would be an exhaustive task to determine all of which they are. Known log types that make use of the Equipment Identifier are CARR and PM. Since the Event Label can be any number of words separated by spaces, there is no obvious delimiter between the Event Label and the Equipment Identifier beyond the space that will be present. There are a couple things OSSs can do with this: take the Event Label and Equipment Identifier as just 1 string of characters OR try to extract the Equipment Identifier out of the header independently of the Event Label. Note that the latter may not always be necessary because the body of the log may mention the Node as well. The

presence of the Equipment Identifier in logs appears to be very rare and appears to be an old legacy thing that was done but isn't common practice anymore.

- For logs originating from the CS2000/XA-Core/DMS, Event Types and Event Labels for specific logs can be determined on the switch using the 'logutil' tool. In logutil, the 'listreps' and 'listroute' commands can be used to view that information. Note that the presence of a log in the tool's output list of logs does not mean that the log is actually active code where an OSS will see it downstream. Some are benign logs or development not yet completed that are sometimes listed there.

Example

```
LOGUTIL:
>listreps spm
Log Rep.      Event                               Suppressed/
Name No. Class Type  Event Label Thresholded Syslog
-----
SPM  650      0    PASS
SPM  651      0    FAIL
SPM  300      0    TBL   Device Fault Report
SPM  331      0    TBL   Failed Device Pro...
....
SPM  709      0    INFO  SPM ISDNPROT DDM ...
SPM  710      0    INFO  SPM ISDNPROT DDM ...
XX report(s) printed
>listroute report spm 710
REPORT  SPM 710 (SPM ISDNPROT DDM Audit) IS CLASS 0
ADDED:
DELETED:
```

- An actual SDM log sample file or feed should be analyzed for determination of a log's character by character format information. For determining things such as how many carriage returns there are between logs, or where spaces are, this is crucial. Note that a log header for a specific log very rarely changes in going from one software release to the next. The only fields that could change is the Severity, Event Type, Event Label and presence of an Equipment Identifier. Changes would be as a result of a feature change or resolve an issue with those fields' values.

Audio Codes Media Server (AMS)--available logs/faults for Succession

The following table lists the AMS logs available in Succession. The MS2010 server is for IP networks and uses the AudioCode TP-1610 card. For detailed

information on logs, refer to NN10275-909, *Succession Fault Management Log Reference*.

AMS Logs/Faults available in Succession

Log/Fault	Description
AMS300	ac Board Resetting Cleared only by a acBoardEvBoardStarted trap; or ac Board Fatal Error
AMS301	ac Board Configuration Error
AMS302	ac Board Temperature Alarm
AMS303	ac Feature Key Error
AMS304	ac Board Call Resources Alarm
AMS305	ac Board Controller Failure Alarm
AMS306	ac Board Ethernet Link Alarm
AMS307	ac Board Overload Alarm
AMS308	ac Active Alarm Table Overflow
AMS500	ac Board Event Board Started. This trap is a signal to clear the active alarm table.
AMS501	cgw Administrative State Change

Audio Provisioning Server (APS)--available logs/faults for Succession

The following table lists the APS logs available in Succession. For detailed information on logs, refer to NN10275-909, *Succession Fault Management Log Reference*.

APS Logs/Faults available in Succession

Log/Fault	Description
APS398	Indicates a raised alarm in the APS device.
APS399	Indicates an alarm clear in the APS device.

Compact Call Agent (CCA) --available logs/faults for Succession

The following table lists the Compact Call Agent (formerly Call Agent (CA)) Logs/Faults available in Succession. These logs were also previously referred to as 3PC. For detailed information on logs, refer to NN10275-909, *Succession Fault Management Log Reference*.

Compact Call Agent supports SCC2 or NT STD formatted logs through SDM functionality, or it can be supported through IEMS. For details on the IEMS interface, refer to the section in this document titled "SN07 IEMS

Functionality.” For details on the SDM protocol/format, refer to FCAPS documentation NN10023-111.

CCA Logs/Faults available in Succession

Log/Fault	Description
Network Element: Call Agent For details on these Logs/Faults, refer to the Fault section of documentation related to Compact CS2K, NN10023-911.	
CCA300	Response to a minor, major, or critical alarm; indicates that free space in RAM is low. Severity is determined by the amount of free space remaining.
CCA301	Response to a minor, major, or critical alarm; indicates one or more time segments has exceeded the threshold. Severity is determined by the number of time segments affected.
CCA302	Response to a minor, major, or critical alarm; indicates that free space on the root file system is low. Severity is determined by the amount of free space remaining.
CCA303	Response to minor, major, or critical alarm; indicates that one or more software processes have terminated abnormally. Severity is determined by the number of process affected.
CCA304	Response to a minor, major, or critical alarm; indicates that one or more Network File Systems is inaccessible. Severity is determined by the number of systems affected.
CCA305	Response to a minor, major, or critical alarm; indicates that time synch is lost to one or more NTP servers. Severity is determined by the number of servers affected.
CCA309	Response to a major or critical alarm; may be a PCI bus fault, an ECC memory fault, or a parity error. A critical alarm requires card replacement.
CCA315	SOS application simplex
CCA316	SOS application is out-of-service
CCA322	Image test failed
CCA331	Unable to communicate to mate via ethernet/fiber
CCA335	Ethernet interface down
CCA336	Unable to communicate to the network
CCA351	Response to major CON and APL alarms because the mate Call Agent unit is unavailable.
CCA355	Response to a minor alarm; indicates the inactive unit is jammed to prevent a SWACT.
CCA362	Response to a minor alarm; indicates at what point one or more REx tests has failed.
CCA365	System REx has not started for over 7 days
CCA375	One unit has a different CPU type than the other
CCA380	One unit has a different committed patch file version than the other
CCA600	Indicates the alarm referenced in log CCA300 has been cleared.
CCA601	Indicates the alarm referenced in log CCA301 has been cleared.
CCA602	Indicates the alarm referenced in log CCA302 has been cleared.
CCA603	Indicates the alarm referenced in log CCA303 has been cleared.

CCA Logs/Faults available in Succession

Log/Fault	Description
CCA604	Indicates the alarm referenced in log CCA304 has been cleared.
CCA605	Indicates the alarm referenced in log CCA305 has been cleared.
CCA609	Indicates the alarm referenced in log CCA309 has been cleared.
CCA615	Alarm referenced in CCA315 has been cleared
CCA616	Alarm referenced in CCA316 has been cleared
CCA620	Image test started
CCA621	Image test finished
CCA631	Able to communicate via ethernet/fiber
CCA635	Ethernet interface ok
CCA636	Able to communicate to the network
CCA651	Indicates the alarm referenced in log CCA351 is cleared and duplex operation is restored.
CCA655	Indicates the alarm referenced in log CCA355 is cleared.
CCA660	Response to a minor alarm; indicates that a REx test has started.
CCA661	REx test finished
CCA663	REx test rejected
CCA665	Alarm referenced in CCA365 has been cleared
CCA670	Swact failover started
CCA671	Swact failover finished
CCA675	Alarm referenced in CCA375 has been cleared
CCA680	Alarm referenced in CCA380 has been cleared

CS2K Management Tools (CMT)--available logs/faults for Succession

The following table lists the CS2000 Management Tools logs available in Succession. CS2K supports SCC2 or NT STD formatted logs through SDM functionality, or it can be supported through IEMS. For details on the IEMS interface, refer to the section in this document titled “SN07 IEMS Functionality.” For details on these logs, refer to the Fault Management

section of CS2K Management Tools, NN10325-900 and to NN10275-909, *Succession Fault Management Log Reference*.

CS2K Management Tools Logs/Faults available in Succession

Log/Fault	Description
CMT300	Critical. Data is mismatched between the SESM server and the Core. The SESM audit, CS2K Data Integrity Audit, has 10 unresolved problems. To view and correct the problems, open the audit problem report from the Audit System found under the SESM Maintenance menu item.
CMT301	Critical. The GWC element manager cannot download data to GWC on recovery so the process has terminated early, and the GWC remains out of service. To clear, determine and remedy the cause of the data download failure.
CMT302	SNMP Timeout. Critical. SNMP poller cannot communicate to the network device due to an SNMP timeout.
CMT399	Indicates a cleared alarm in the CMT device
CMT500	Generated by the SESM alarm system to indicate the system is initializing.
CMT501	Generated by the SESM alarm system upon shutdown.
CMT502	Generated by the SESM alarm system to inform northbound alarm clients that alarm notifications cannot be generated. This log will be sent via the SSPFS syslog feed to the customer log.

SAM21--available logs/faults for Succession

The following table lists the SAM21 Logs/Faults available in Succession. The Shelf Controller Unit (SCU) raises alarms on behalf of itself or on behalf of the cards in the I/O slots, power sleds, fan sleds and power supply. Therefore, the alarm IDs for some of the alarms will have the same label, but the slot location that is included in the body of the alarm will indicate the actual card that is having problem. Alarms with the label IPOA are the alarms raised by the SCU with the PMC ATM card.

SAM21 supports SCC2 or NT STD formatted logs through SDM functionality, or it can be supported through IEMS. For details on the IEMS interface, refer to the section in this document titled “SN07 IEMS Functionality.” For details on the logs/faults themselves, refer to the Fault

Management section of SAM21 FCAPS documentation NN10089-911 and NN10275-909, *Succession Fault Management Log Reference*.

SAM21 Logs/Faults available in Succession

Log/Fault	Description
Network Element: SAM21 Platform	
SCU310	Shelf controller unit. CPU load is high Major. The One minute load average is greater than 20. Critical. The five minute load average is above 15, or the fifteen minute load average is above 7.
SCU332	Shelf controller unit. Memory usage is high Major. Total free memory has fallen below 15%. Critical. Total free memory has fallen below 10%.
SCU349	Shelf controller unit Disk usage is high. Major. Total free space on the root file system has fallen below 10%. Critical. Total free space on the root file system has fallen below 5%.
SCU346	Shelf controller unit. Large number of processes abnormally terminated Major. More than 4 zombie processes in system. Critical. More than 15 zombie processes in system.
SCU329	Shelf controller unit. Loss of communications either to its mate or to the SDM. Minor. The upper or lower serial cable connection is down. Major. This shelf controller cannot ping its mate through the ethernet interface Major. This shelf controller cannot ping the SDM, but can ping its mate Major. Both the lower (upper) serial cable and the mate's Ethernet are not connected. Major. This shelf controller cannot ping the SDM, but can ping its mate. The upper (lower) serial cable connection is down. Major. Both serial cable connections are down. Critical. Shelf cannot ping its mate or the SDM through the Ethernet interface. Critical. Shelf cannot ping its mate or the SDM through the Ethernet interface. The upper (lower) serial cable connection is down. Critical. This shelf controller cannot ping its mate through the Ethernet interface. Both serial cable connections are down. No synching of state changes are occurring. Critical. The shelf cannot see out at all.
SCU335	Major: Power Supply in Sled 1/2/3 has been removed. Most likely the whole sled has been removed. Critical. Power Supply in Sled 1/2/3 is down. The power supply in that sled has failed.
SCU315	Major. Fan in Sled 1/2/3 has been removed. Fan has been removed from the sled, or the entire sled has been removed.

SAM21 Logs/Faults available in Succession

Log/Fault	Description
	Critical. Fan in Sled 1/2/3 is down Fan has failed.
SCU335	Critical. Power feed 1/2 is down. Either the feed has failed, or the cable has been removed.
SCU356	Critical. Mate Shelf Controller Down. Operating in Simplex Mode. The inactive SC has been detached, or Mama on the active SC has not received a ping from the inactive SC in 20 seconds.
SCU315	Major. Temperature in Sled 1/2/3 is High. Temperature in the sled has reached about 40 degrees. Critical. Temperature in Sled 1/2/3 is High. Temperature in sled has reached about 50 degrees.
SCU301	Critical. Extension Bridge in Slot 15/16 is Down/Up. Depending on the actual text, one or both of the Extension Bridges has been detached and/or removed.
SCU315	Major. Diagnostic Failed during testing in a non-system card at the specified I/O Slot A diagnostic test was run, and the board failed at least one of the tests. Major. Diagnostic Failed due to SWACT in a non-system card at the specified I/O Slot. A diagnostic test was interrupted by a SWACT. Major. Diagnostic Failed n a non-system card at the specified I/O Slot for a specified reason. The diagnostic failed due to the reason stated. (There are 11 possible statements.)
SCU346	Critical. Firmware Flashing could not connect to the non-system card at the specified I/O Slot. Either there is another process currently attached to the board, or the bus is too busy to allow the request. Auto Flash is now turned off on the SC for this slot. Critical. Firmware Flashing failed at downloading firmware to the non-system card at the specified I/O Slot. The firmware file does not exist on the SDM or has incorrect parameters. Critical. Firmware Flashing failed at validating firmware to the non-system card at the specified I/O Slot. The firmware file is corrupt on the SDM, or there was an error in the transfer. Critical. Firmware Flashing failed at backing up the firmware to the non-system card at the specified I/O Slot. The copy operation from one bank to the other failed. Possible bad memory. Critical. Firmware Flashing failed flash to the non-system card at the specified I/O Slot. Could not connect to the board after the flash. Critical. Provision of a non-system card at the specified I/O Slot. Provisioning of the board failed due to some system problem. System may have been abnormally busy.
SCU500	Reports a change in state of a card. The new state can be Unlocked, Enabled, or None.

SAM21 Logs/Faults available in Succession

Log/Fault	Description
SCU501	Reports an equipment insertion, specifying the shelf, card, and slot.
SCU502	Reports an equipment removal, specifying the shelf, card, and slot.
IPOA301	A system log in response to a loss of cell delineation (LCD) alarm from SC-IPoA card.
IPOA302	A system log in response to a SONET carrier fault of type AIS from the SC-IPoA card
IPOA303	A system log in response to an ATM connection fault from the SC-IPoA card
IPOA304	A system log in response to an ATM connection set fault detected by the SAM21 Element Manager.
IPOA801	A system log in response to an ATM CRC32 threshold fault.
SM21300	A system log in response to an alarm that there has been a loss of communication, and the remote network is down.
LOS/LOF	These section, line and path faults indicate that SONET connectivity between the SC and the far end node is unavailable on one fiber.
AIS-L/RDI-L	
AIS-P/RDI-P	
LOP	
ATM Overrun Count	Indicates the number of times cells were dropped due to a shortage of buffer space.
ATM Overrun Date	Indicates the date of the last overrun.
CPU load high	Major. The One minute load average is greater than 20. Critical. The five minute load average is above 15, or the fifteen minute load average is above 7.
Memory usage high	Major. Total free memory has fallen below 15%. Critical. Total free memory has fallen below 10%.
Disk usage high	Major. Total free space on the root file system has fallen below 10%. Critical. Total free space on the root file system has fallen below 5%.
Large number of processes abnormally terminated	Major. More than 4 zombie processes in system. Critical. More than 15 zombie processes in system.
Loss of Communications: Serial Connection 1 (2) is down	Minor. The upper (lower) serial cable connection is down.
Loss of Communications: Mate Ethernet is down	Major. This shelf controller cannot ping its mate through the ethernet interface.

SAM21 Logs/Faults available in Succession

Log/Fault	Description
Loss of Communications: Remote network is down.	Major. This shelf controller cannot ping the SDM, but can ping its mate.
Loss of Communications: Mate Ethernet, Serial Connection 1 (2) is down.	Major. Both the lower (upper) serial cable and the mate's Ethernet are not connected.
Loss of Communications: Remote network, Serial connection 1 (2) is down.	Major. This shelf controller cannot ping the SDM, but can ping its mate. The upper (lower) serial cable connection is down.
Loss of Communications: Serial Connection 1, Serial Connection 2 is down.	Major. Both serial cable connections are down.
Loss of Communications: Local Ethernet interface is down.	Critical. Shelf cannot ping its mate or the SDM through the Ethernet interface.
Loss of Communications: Local Ethernet interface, Serial Connection 1 (2) is down	Critical. Shelf cannot ping its mate or the SDM through the Ethernet interface. The upper (lower) serial cable connection is down.
Loss of Communications: Mate Ethernet, Serial Connection 1, Serial Connection 2 is down	Critical. This shelf controller cannot ping its mate through the Ethernet interface. Both serial cable connections are down. No synching of state changes are occurring.
Loss of Communications: All Communications Paths Down	Critical. The shelf cannot see out at all.
Power supply in Sled 1/2/3 has been removed.	Major. Most likely the whole sled has been removed.

SAM21 Logs/Faults available in Succession

Log/Fault	Description
Power supply in Sled 1/2/3 is down.	Critical. The power supply in that sled has failed.
Fan in Sled 1/2/3 has been removed	Major. Fan has been removed from the sled, or the entire sled has been removed.
Fan in Sled 1/2/3 is down	Critical. Fan has failed.
Power Feed 1/2 is down.	Critical. Either the feed has failed, or the cable has been removed.
Mate Shelf Controller Down. Operating in Simplex Mode.	The inactive SC has been delatched, or Mama on the active SC has not received a ping from the inactive SC in 20 seconds.
Temperature in Sled 1/2/3 is High	Major. Temperature in the sled has reached about 40 degrees.
Temperature in Sled 1/2/3 is High.	Critical. Temperature in sled has reached about 50 degrees.
Extension Bridge in Slot 15/16 is Down/Up.	Critical. Depending on the actual text, one or both of the Extension Bridges has been detached and/or removed.
Diagnostic Failed at test case.	Major. A diagnostic test was run, and the board failed at least one of the tests.
Diagnostic Failed due to SWACT	Major. A diagnostic test was interrupted by a SWACT.
Diagnostic Failed, xxxxxx	Major. The diagnostic failed due to the reason stated. (There are 11 possible statements.)
Firmware Flashing could not connect to the board.	Critical. Either there is another process currently attached to the board, or the bus is too busy to allow the request. Auto Flash is now turned off on the SC for this slot.
Firmware Flashing failed at downloading firmware	Critical. The firmware file does not exist on the SDM or has incorrect parameters.
Firmware Flashing failed at validating firmware	Critical. The firmware file is corrupt on the SDM, or there was an error in the transfer.
Firmware Flashing failed at backing up the firmware.	Critical. The copy operation from one bank to the other failed. Possible bad memory.

SAM21 Logs/Faults available in Succession

Log/Fault	Description
Firmware Flashing failed flash	Critical. Could not connect to the board after the flash.
Provision failed: process ended abnormally.	Critical. Provisioning of the board failed due to some system problem. System may have been abnormally busy.
Provision failed, could not connect to board.	
Provision failed to set application type.	

CS2000 XA-Core--available logs/faults for Succession

The following table lists the CS 2000 XA-Core Logs/Faults available in Succession.

CS 2000 supports SCC2 or NT STD formatted logs through SDM functionality, or it can be supported through IEMS. The SDM would remain the CS2000 Core Manager but can forward the CS2000 logs to IEMS instead of directly to the OSS. For details on the IEMS interface, refer to the section in this document titled "SN07 IEMS Functionality." For details on the logs/faults themselves, refer to the Fault Management section of CS 2000 FCAPS documentation, NN10083-911. For information on XA-Core logs and faults, refer to NTP 297-8991-810, *XA-Core Reference Manual* and NN10275-909, *Succession Fault Management Log Reference*.

CS2000 XA-Core Logs/Faults available in Succession

Log/Fault	Description
Network Element: CS2000 XA-Core	
ABI messaging alarms	Links down ABI external messaging alarm Links Down - Alarm Set (or Alarm cleared).
	Severely Degraded ABI external messaging alarm Severely Degraded - Alarm Set (or Alarm cleared).
	Degraded ABI external messaging alarm Degraded - Alarm Set (or Alarm cleared).
Alarm Database logs	Report Alarm Log Sent when requested by the entity that is reporting an alarm.
	Clear Alarm Log Generated when a client clears an existing alarm in the alarms database managed by Alarmd.
	Alarm Summary Log Sent periodically by Alarmd to summarize the Alarms in the database managed by Alarmd.

CS2000 XA-Core Logs/Faults available in Succession

Log/Fault	Description
ATM log	ATM606 Generated when the Succession Network receives a UNI Release Complete message informing the craftsperson of an unsuccessful attempt to set up ATM bearer path (SVC) through the ATM network.
AUDT logs	AUDT105 Trunk state incorrect.
	AUDT106 Call is forced down due to the release of a trunk.
	AUDT109 Trouble conditions detected.
	AUDT110 Terminal trunk state is invalid.
	AUDT116 Terminal state indicator (TSI) of an idle trunk is invalid.
	AUDT117 TSI (terminal state indicator) of a given call state and the CCB (call condense block) TSI do not match.
	AUDT209 Generated whenever the audit process finds a problem with a multi CPTLB.
Baseln alarm	“Baseln” alarm is raised whenever any XA-Core Field Replaceable Unit (FRU) installed in the shelf is not at Hardware (HW) or Firmware (FW) baseline. Only the Major level is used.
C7UP logs	C7UP100 No acknowledgment received from far-end office after circuit reset, group circuit reset, blocking or unblocking, group blocking or unblocking, or release messages. For field descriptions and actions, see Logs Reference Manual (Volume 1), 297-2621-840.
	C7UP101 Unreasonable message received on trunk.
	C7UP102 CCS7 connection is released due to abnormal condition.
	C7UP103 Blocked or unblocked circuit conditions.
	C7UP104 Group blocking or unblocking conditions.
	C7UP105 Unsuccessful ISDN call attempt.
	C7UP106 Shortage of resources.
	C7UP107 Request for continuity check test by an IAM (Initial Address Message), a continuity check request (CCR) message, or a demand continuity test (DCT) from the MAP.
	C7UP109 ISUP trunk state change to match far-end office trunk state.
	C7UP110 Serious communication problem with far-end office.
	C7UP111 Outgoing call attempt failure.
	C7UP112 Call in progress has received an unreasonable message in the current call state.
	C7UP113 ISUP trunk maintenance problem.
	C7UP114 Response from far-end office not received from a REL (circuit release) or RSC (reset circuit) message.

CS2000 XA-Core Logs/Faults available in Succession

Log/Fault	Description
C7UP119	ISUP has not received, from the far-end office, second GRS (circuit group reset), CGB (circuit group blocking), or CGU (circuit group unblocking) message.
C7UP120	ISUP invalid number in circuit-group message RANGE field (0 or a number greater than 23).
C7UP130	System has detected that the hop counter (HC) limit has been exceeded. For details, see Logs Reference Manual (Volume 2), 297-2621-840 and the CS2000 fault information.
C7UP300	ISUP trunk time-out waiting for acknowledgement from first RLC (remote line controller).
C7UP301	System has received a release message with the value "Exchange Routing Error."
CARR logs	CARR300 Carrier failure event occurred. Also applies to STS-1 carrier. For more info, see general SPM fault information.
	CARR310 Carrier failure events are cleared. Also applies to an STS-1 carrier. For more info, see general SPM fault information.
	CARR330 A protection switch has occurred. A previously inactive carrier in the protection group takes over as the active carrier.
	CARR331 A protection switch was attempted but failed.
	CARR340 The inactive carriers in a protection group have changed state in such a way that they cannot carry traffic. The protection group is now running in simplex mode.
	CARR341 Both carriers have become available and normal protection switching can occur.
	CARR500 Carrier state change to InSv from ManB or SysB. For more info, see general SPM fault information.
	CARR501 Carrier state change to CBsy from ManB or SysB. For more info, see general SPM fault information.
	CARR510 Carrier state change to SysB from InSv or CBsy. For more info, see general SPM fault information.
	CARR511 Carrier state change to SysB from InSv or CBsy. For more info, see general SPM fault information.
	CARR512 OC3 carrier state change to CBsy from InSv, ManB, or SysB. For more info, see IW-SPMgeneral SPM fault information.
	CARR600 Value of an instance of apsChanSwitchover increments.
	CARR800 Threshold crossing alert (TCA) for a metered performance parameter has been cleared. For more info, see general SPM fault information.

CS2000 XA-Core Logs/Faults available in Succession

Log/Fault	Description
	CARR810 TCA event for metered performance parameter has occurred. For more info, see general SPM fault information.
	CARR811 TCA event for non-metered performance parameter has occurred. Also applies to STS-1 carrier on MG4000. For more info, see general SPM fault information.
DQoS alarm	This raises a DQoS link alarm when link failure occurs.
Authoriza- tion logs	SESM MI2 applications have user authorization by group. Authorization failures generate logs through the SSPFS log reporting service.
Database logs	DB600 Generated when an attempt to allocate a database connection encounters an I/O error. These errors can occur when the database has been stopped momentarily for administrative purposes.
	DB601 Generated when an attempt to allocate a database connection encounters detects that the connection is already closed. These errors can occur when the database has been stopped momentarily and then again started.
	DB602 Generated when an attempt to allocate a database connection encounters an invalid password error. These errors can occur when the database log in password for a database user is changed.
	DB603 Generated when an attempt to allocate a database connection encounters maximum database sessions exceeded error. These errors can occur when an unusual event has occurred that caused sustained high levels of system activity.
	DB604 Generated when an attempt to allocate a database connection encounters maximum database processes exceeded error. These errors can occur when an unusual event has occurred that caused sustained high levels of system activity.
DBSE log	DBSE300 A Session Server Provisioning Trouble (TBL) log which is generated any time a change in database connectivity is detected. It reports 'No Solid DB Connection' when database connectivity is lost. It reports 'Solid DB Connection Restored' when database connectivity is reestablished. Correlates to the critical alarm "No Database Connection" raised when a loss of connectivity to the database is detected.
EXT log	EXT108 Generated upon raising and clearing of EXT alarm HIGH_MEM_BLOCKING.
EXT alarm	HIGH_MEM_BLOCKING Appears at the MAPCI EXT alarm banner when there is a high memory blocking level detected in the system. Correlates to XACP300 log when raised, and to XACP500 log when cleared.
FPS log	FPS100 Generated when the FPS counter of a subscriber is loaded.
SFPS log	SFPS100 Generated when a craft person enters an invalid LFPS password three times.

CS2000 XA-Core Logs/Faults available in Succession

Log/Fault	Description
GAME logs	GAME101 Created if the RSPTMOUT OM count is greater than zero. The log is created during the RSPTMOUT OM transfer period and records the RSPTMOUT OM count value. GAME102 Created if RSPTMOUT OM count becomes equal to the office parm T1_TIMER _EXPIRY_MSG_SUPPRESS threshold value.
ITN logs	ITN307 An INFO log to indicate that IP transmit failed.
RMGC log	When a major RMGC alarm is raised or cleared, an SNMP trap is sent from the GWC to the GWC EM.
RSIP status log	The RMGC application produces a syslog performance report once an hour which is sent to the Solaris syslog daemon. It contains the counts of the total number of RSIPs processed successfully and the number failed.
LOST logs	LOST101 Generated when an outgoing message fails to find an open path to the destination or an incoming message fails checks done by the receiving application. LOST102 Generated when an incoming message cannot be forwarded to Call Processing because software resources (buffers) have been exhausted or the limit for outstanding messages has been exceeded and no additional messages can be enqueued. LOST103 Generated when a message that originated from the CM is rebounded back to the CM for additional processing because a node intermediate along the path was unable to deliver the message to the final destination. The failure code instructs the CM to attempt to re-route the message over an alternate path but the original message contains the re-route inhibit flag LOST104 Generated when an outgoing message fails a VID-to-TID translation or an incoming message fails sanity checks on the terminal identifier (TID). LOST105 Generated when an outgoing message fails to find an open CM-MS link. Also generated when a message that originated from the CM is rebounded back to the CM for additional processing because a node intermediate along the path was unable to deliver the message to the final destination. The failure code instructs the CM to attempt to re-route the message over an alternate path but sanity checks fail on the original route. LOST106 Generated when a message fails application sanity checks. Also generated when a message that originated from the CM is rebounded back to the CM for additional processing because a node intermediate along the path was unable to deliver the message to the final destination. The failure code indicates "unspecified reason." LOST107 Generated when an incoming message specifies an unassigned terminal identifier (TID). LOST108 Generated when the buffer (containing an outgoing message) is reclaimed by a system audit. The message is deemed to be stale as the buffer has not been accessed for a long period of time.

CS2000 XA-Core Logs/Faults available in Succession

Log/Fault	Description
LOST109	Generated when a message that originated from the CM is rebounded back to the CM for additional processing because a node intermediate along the path was unable to deliver the message to the final destination. The failure code instructs the CM to attempt to re-route the message over an alternate path but all alternatives have been previously tried without success.
LOST110	Generated when Call Processing gets a failure indication on attempting to output a message).
LOST111	Generated when an incoming message cannot be delivered. The specific failure reason is displayed in the log.
LOST112	Generated when an outgoing message fails sanity checks on length or an incoming message fails sanity checks on length.
LOST113	Generated when the needed software resources are again available. The log displays the number of discarded events during the period of exhausted resources
LOST114	Generated when an incoming (BFP) message cannot be forwarded to Call Processing due to message buffer exhaustion. This is similar to the more generic LOST102 log
LOST115	Generated when the (BFP) buffer (containing an incoming message) is reclaimed by a system audit. The message is deemed to be stale as the buffer has not been accessed for a long period of time. This is similar to the more generic LOST108 log.
LOST116	Generated when an outgoing message encounters a failure. The specific failure reason is displayed in the log
LOST117	Generated when an outgoing message encounters a failure. The specific failure reason is displayed in the log.
NGSS logs	NGSS700 Indicates when a SIPT CS2CS call is rejected because it would exceed the LIMIT setting of the CS2B0008 SOC.
	NGSS701 Generated when a CS2AS call is rejected because it would exceed the LIMIT setting of the CS2B0009 SOC. The SIPT call is not allowed to complete through the NGSS. The CS2ASOV register in OM group NGSSOM is pegged.
NWM logs	NWM102 Cancel To (CANT) control is applied to or removed from a specific trunk group. For details, see CS2000 configuration information and Solution-level configuration information.
	NWM103 Cancel From (CANF) control is applied to or removed from a specific trunk group. For details, see CS2000 configuration information and Solution-level configuration information.
	NWM104 SKIP control is applied to or removed from a specific trunk group. For details, see CS2000 configuration information and Solution-level configuration information.

CS2000 XA-Core Logs/Faults available in Succession

Log/Fault	Description
	NWM107 Flexible ReRoute (FRR) control is applied to or removed from a specific trunk group. For details, see CS2000 configuration information and Solution-level configuration information.
	NWM202 HTR code has been added to or deleted from EADAS or MAP terminal. For details, see CS2000 configuration information and Solution-level configuration information.
SIP Gate- way Applica- tion CallP Alarms	Database Access Alarm (Critical) occurs when the CallP application tries to access the database and it fails due to a loss of connectivity between the database and the CallP application. Correlates with the 310 log.
	ACL Trouble Alarm Raised when incoming SIP messages are dropped due to Access Control List enforcements. The severity of the alarm is based on the number of packets dropped in last 15-minute time interval. Correlates with the SIPC750 log.
SIPC logs	SIPC301 A critical log that is generated when the SIP Gateway Call Processing Application will not receive any incoming SIP messages due to Access Control List being enabled and no valid entries in the Remote SIP server or ACL list.
	SIPC310 "SIP CallP No Database Connection" is associated with the generation of the Critical alarm due to a loss of connectivity between the database and the CallP application. The same log number is used for "SIP CallP Database Connection Established" when the connection that caused the first SIPC 310 log is re-established and the alarm is cleared.
	SIPC650 An informational log that is generated when the CallP application goes to get data from the database for a particular table and no data is found.
	SIPC750 Generated when the SIP Gateway Call Processing Application drops incoming SIP messages due to Access Control List restrictions. A Minor, Major, or Critical log is generated based on the number of SIP messages dropped in the last 15 minutes.
SIPGW log	SIPGW700 An INFO log that contains one of 34 possible log messages related to SIP call processing.
SIPM logs	SIPM300 A Trouble log which is generated any time the SIP Gateway Application Maintenance software encounters an unexpected condition.
	SIPM301 A Trouble log which is generated any time the SIP Gateway Maintenance Trouble Alarm is raised or lowered.
	SIPM302 A Trouble log which is generated any time the SIP Gateway Maintenance Sync Trouble Alarm is raised or lowered. This occurs when the SIP Gateway application state gets out of sync, or gets back in sync in a duplex Session Server configuration.
	SIPM500 An INFO log which is generated any time the SIP Gateway Application maintenance state changes.

CS2000 XA-Core Logs/Faults available in Succession

Log/Fault	Description
SPFS logs	SPFS310 SPFS 310 is generated for the following reasons:
	- when the CPU load Average threshold is exceeded, or when the related Major or Minor alarm is cleared. - when the Swap Space usage threshold is exceeded, or when the related Critical or Major alarm is cleared. - when the Memory usage threshold is exceeded, or when the related Major or Minor alarm is cleared.
	SPFS 350 is generated when the File System is not mounted, the File System usage threshold is exceeded, a File System read/write failed, or when the related Critical, Major or Minor alarm is cleared.
	SPFS350 A Trouble log which is generated any time the SIP Gateway Maintenance Trouble Alarm is raised or lowered.
STOR logs	STOR605 (Critical) Output when the Store Audit has detected a corruption in the Bstree structures containing the information about the data address space STOR is responsible for.
	STOR606 Indicates that the Store Audit has found a corruption in the allocation information for data store which is dumped (such as DSPROT) and it is very likely that a attempt to perform a dump while in this state would fail.
	STOR607 Generated when the Store Audit detects a mismatch between the Store Allocator's internal setting of an address' blocking attribute and the actual setting of the attribute in memory hardware.
TOPS logs	TOPS131 Generated when problems occur in the call flow for the activity TOPS Wireless Automated Directory Assistance Call (ADACC) with Release.
	AUD690 Generated when a TOPS calls ends unexpectedly with an IS41TOPS extension block attached.
TRK logs	TRK101 Percentage of busy trunks in a trunk group exceeded the threshold value for a minor alarm.
	TRK102 Major alarm threshold reached or exceeded.
	TRK103 Number of trunks in a trunk group exceeded threshold value for a critical alarm.
	TRK104 Percentage of busy trunks dropped below a threshold value.
	TRK110 Trunk state change to SysB (system busy) LO (Lockout) from CPB (call processing busy).
	TRK112 Request to take trunk off the lockout (LO) list and RTS (return to service) initiated by a manual request from the LTP MAP display level or by a system request.
	TRK122 Both planes of the trunk equipment have lost accuracy detected by central control (CC).

CS2000 XA-Core Logs/Faults available in Succession

Log/Fault	Description
TRK123	Peripheral processor (PP) has sent a wrong message to central control.
TRK138	Call routed for treatment after system was call processing busy (CPB).
TRK151	Blue Box Fraud (BBF) detection activated.
TRK152	Blue Box Fraud (BBF) detection deactivated.
TRK153	Blue Box Fraud (BBF) call detected.
TRK154	Blue Box Fraud (BBF) call disconnected to identify calling and called parties.
TRK155	Emergency Service Bureau (ESB) originating the call is off-hook longer than the time designated in customer table TRKGRP.
TRK164	External call routed through local office to a distant office that has requested calling line identification (CLI).
TRK251	UCS: trouble with an invalid authcode.
TRK255	UCS: trouble with database.
TRK257	UCS: trouble translating a partition number to STS due to an invalid partition.
TRK258	UCS: trouble translating STS to partition number, due to an invalid STS.
TRK355	Trunk idle queue sanity trouble or rebuild.
TRK420	UCS: invalid authcode.
TRK424	First call processing threshold error; failed diagnostic test; and call processing error threshold appears again within 15 minutes of the diagnostic test.
TRKT logs	These logs are only generated if OFCVAR office parameter GENERATE_TRKT_LOGS is activated. Otherwise, TRK138 logs are generated with an appropriate treatment reason.
TRKT200	ANI Database Failure.
TRKT201	ANI Account Status Not Allowed.
TRKT202	ANI Acct Recently Disallowed.
TRKT203	Calling Card Invalid
TRKT204	Calling Card Time-out
TRKT205	General No Circuit
TRKT206	Reorder
TRKT207	Restricted Date Time
TRKT208	Storage Overflow Reorder
TRKT209	Start Signal Time-out
TRKT210	Start Signal Time-out

CS2000 XA-Core Logs/Faults available in Succession

Log/Fault	Description
	TRKT211 Vacant Code
	TRKT212 Vacant Country Code
	TRKT213 Trigger Block
XAC logs	XAC300 Low Shared Memory (SM) condition. Accompanied by LowSM alarm.
	XAC302 Low Processor Element (PE) condition. Accompanied by LowPE alarm.
	XAC303 MScomm (Message Switch Communication) problem. Accompanied by MScomm alarm.
	XAC304 TOD (Time of Day clock) problem. Accompanied by TOD alarm.
	XAC305 RTIF (Reset Terminal Interface) problem. Accompanied by RTIF alarm.
	XAC306 Disk problem. Accompanied by DISK alarm.
	XAC307 Tape problem. Accompanied by TAPE alarm.
	XAC308 Image Test failure. Accompanied by Image alarm.
	XAC309 Loss of communication between the AMDI packet and any MG4000.
	XAC310 Card manual busy.
	XAC312 IOP fault. Accompanied by IOPflt alarm. Modified in SN07 to display the new CMIC and RTIF port device and CMIC and RTIF packets and links.
	XAC312 IOP fault. Accompanied by IOPflt alarm.
	XAC320 Cardlist Report.
	XAC321 WgSlot (Shelf Audit Failure - Card Configuration). Accompanied by WgSlot alarm.
	XAC322 PETrbl. Accompanied by PETrbl alarm.
	XAC323 SMTrbl. Accompanied by SMTrbl alarm.
	XAC324 IOTrbl. Accompanied by IOTrbl alarm.
	XAC325 RIBKEY detected. Accompanied by RIBKey alarm.
	XAC326 MS Link configuration mismatch.
	XAC327 WgSlot (Card inserted into wrong slot). Accompanied by WgSlot alarm.
	XAC329 Loss of communication with XA-Core or loss of Ethernet link redundancy. Associated with the following OM groups: XETHRMJU, XETHRCRU, XETHR, XETHRPRT, and XETHRLNK.
	XAC330 FW version mismatch. Accompanied by FWvers alarm.
	XAC333 FW loading failure.
	XAC335 Unknown CO-3 packet fault. Accompanied by AMDI alarm.
	XAC337 Raised when the Baseln alarm is first raised, or the Baseln alarm is still raised and the non-baseline component list changes.

CS2000 XA-Core Logs/Faults available in Succession

Log/Fault	Description
XAC400	XA-Core summary report.
XAC413	REx schedule failure. Accompanied by RExSch alarm.
XAC415	Routine exercise report. SN07 adds “not at baseline” as a reason for not running the SREx test.
XAC600	LowSM condition cleared.
XAC601	MemLim condition cleared.
XAC602	LowPE condition cleared.
XAC603	MScomm alarm cleared.
XAC604	TOD alarm cleared.
XAC605	RTIF alarm cleared.
XAC606	DISK alarm cleared.
XAC607	Tape alarm cleared.
XAC608	Image alarm cleared.
XAC609	AMD link condition cleared.
XAC610	Card returned to service. Modified in SN07 to display the new CMIC and RTIF port device and CMIC and RTIF packets and links.
XAC612	IOP alarm cleared.
XAC613	REx schedule report.
XAC614	XATrap alarm cleared.
XAC615	REx started.
XAC618	Split (Split mode entered).
XAC619	Split mode exited.
XAC622	PETrbl alarm cleared.
XAC623	SMTTrbl alarm cleared.
XAC624	IOTrbl alarm cleared.
XAC625	RIBKEY removed.
XAC626	MS Link configuration restored.
XAC627	WgSlot cleared (card removed).
XAC628	Output when provisioning or deprovisioning.
XAC629	Loss of communication restored.
XAC630	FWvers cleared.
XAC631	FW soaking started. Accompanied by FWsoak alarm.

CS2000 XA-Core Logs/Faults available in Succession

Log/Fault	Description
	XAC632 FW soaking completed.
	XAC633 FW loading started.
	XAC634 FW loading completed.
	XAC635 FW soaking in progress.
	XAC637 Raised when the Baseln alarm is cleared, due to an empty list of non-baseline components.
	XAC640 Manual Test Report.
	XAC641 Alarm enable/disable notification.
	XAC801 MemLim (Memory Limit). Accompanied by MemLim alarm.
	XAC814 XATrap. Accompanied by XATrap alarm.
XACP logs	XACP300 Generated every minute that the EXT alarm HIGH_MEM_BLOCKING is active.
	XACP500 Generated once when the memory blocking level has returned to normal.
	XACP600 Summarizes the minute-by-minute memory blocking level; generated once every 15 minutes. If all 15 minutes had normal blocking levels, the log has only one line of output stating that all 15 minutes had normal blocking levels. If at least one minute out of 15 reported high blocking levels, the log output reports each minute separately.
XAUD logs	XAUD395, 397, 400, 401, 430, 432, 432, 434, 500, 501, 708, 709, 714, 715, 723, 724, 725, 979, 980, 981, 982, 977, 978 These call processing resource dump logs are generated whenever a call processing resource is recovered by the audit process running on the XA-Core. The only difference in the logs is the amount of data dumped. In SN07, the location and number of bits used to represent the extension block's format code in the header (within the hex dump of the log) has changed for all extension block logs. The only noticeable difference to the customer will be the number following the XAUD string in the log title.
XNET logs	XNET600 Connection between nodes has been replaced.
	XNET601 New connection between nodes failed.
	XNET602 Connection between nodes does not exist, and attempts to connect them failed.
	XNET605 The bearer networks of the two parties in a connection attempt are not permitted to inter-connect, based on datafill in table NET2NET.

CS2000 XA-Core Logs/Faults available in Succession

Log/Fault	Description
XNET606	Indicates a software or provisioning problem in the switch, in that an appropriate bearer network could not be determined through provisioned data for a particular party in a connection attempt.
XNET607	Indicates that an IW SPM interworking bridge was not available for the connection request, either because of a bridge exhaust condition, or a bridge is not available.

GWC--available logs/faults for Succession

The following table lists the GWC Logs/Faults available through Succession. GWC supports SCC2 or NT STD formatted logs through SDM functionality, or it can be supported through IEMS. For details on the IEMS interface, refer to the section in this document titled "SN07 IEMS Functionality." For details on the logs/faults themselves, refer to the Fault Management section of GWC FCAPS documentation, NN10090-911 and NN10275-909, *Succession Fault Management Log Reference*.

GWC Logs/Faults available in Succession

Log/Fault	Description
Network Element: GWC (PGC load)	
The PM180, 181, 185, and 177 faults are first sent to the core and are then sent northbound from the CS2000 Core Manager in SCC2 format. The remaining faults are sent from the GWC to the GWC EM and are then sent northbound via CORBA.	
PM180	Indicates a software error (SWERR) has occurred.
PM181	Generates for a variety of GWC-to-core-related communications issues. Modified in SN07 to indicate that the ABI of an ABI-hosted XPM is attempting to or successfully exit(s) ESA.
PM185	Indicates that the GWC has trapped.
PM777	Indicates a hardware fault. Reason text identifies the suspected hardware.
M3UAxxx	Indicates an M3UA signaling link from the GWC to the ISP has become unavailable.
The remaining faults are sent from the GWC to the GWC EM and are then sent northbound via CORBA. The following alarms are generated by the GWC, except for the first one generated by the alarm browser.	
SNMP Timeout	Critical; indicates a communications subsystem failure.
Test	Minor; a test alarm generated from the pmdebug interface.
Active unit disabled	Critical; indicates a unit is out of service and not available.
Standby unit disabled	Critical; indicates a unit is out of service and not available.

GWC Logs/Faults available in Succession

Log/Fault	Description
Core commu- nication lost	Major if active unit; Minor if inactive unit. No response received to Core heartbeat.
Mate unit com- munication lost	Minor; no response received to mate heartbeat.
Gateway com- munication lost	A gateway has stopped responding to heartbeat.
EM communi- cation lost	Major. No response received for Persistent Data Verification SNMP Trap; EM not responding. Problem may be "EM not present, provisioned data loaded from local flash," OR "EM audit indicates provisioned inservice data is old, need manual intervention to recover." Cleared with a busy RTS.
FLASH error	Minor. Error in writing Flash; erase of Flash sector failed. Cleared with hardware replacement.
FLASH life span exceeded	Minor. The number of writes to FLASH has exceeded the recommended/intended limit.
Security_SA_ capacity	Minor or Major. Security Association alarms are nearing capacity. Cleared by the security alarms application which monitors the resource level and cleared the alarm when the alarm condition as been cleared on the GWC. Currently alarms are only managed on the active GWC unit (i.e., data is not mirrored to the inactive unit), and for this reason during a SWACT alarms are automatically cleared on the unit dropping activity.
Security_SA_ fail	Major. The number of Security Association alarms has exceeded the threshold. Cleared by the security alarms application which monitors the resource level and cleared the alarm when the alarm condition as been cleared on the GWC. Currently alarms are only managed on the active GWC unit (i.e., data is not mirrored to the inactive unit), and for this reason during a SWACT alarms are automatically cleared on the unit dropping activity.
Recovery alarm	A GWC recovery process has terminated early, and the GWC remains out of service.
DQOSMTC_ DQoSLinkLoss	A DQoS/COPS connection failure has occurred. Cleared by DCCNXMGR (via DCALARM) when the connection is reestablished or the connection is deleted via provisioning.
Datasync alarm	The GWC does not contain the latest provisioned data. This alarm may be raised by the GWC EM noting the problem and sending a message to the GWC to raise the alarm.
Unit Out of Service	Critical if active unit; minor if inactive unit. The GWC Profile failed to validate, probably because no profile is available to activate. Cleared with a GWC reload.
QOS error log	If the QCA detects an event or an error, a syslog message is generated and a non-QoS record is written to the output stream (file).
QOS connection alarm	An alarm is generated whenever a message cannot be sent to the server. The alarm is cleared as soon as the QoS report application is able to send QoS reports to the server.
GWC Alarm Logs	
GWC300	Active unit disabled. Critical; indicates a unit is out of service and not available.

GWC Logs/Faults available in Succession

Log/Fault	Description
GWC301	Standby unit disabled. Indicates a unit is out of service and not available. Minor if the unit is ManB, but Major if the unit is SysB.
GWC302	Core communication lost. Major if active unit; Minor if inactive unit. No response received to Core heartbeat.
GWC303	Mate unit communication lost. Minor; no response received to mate heartbeat.
GWC304	Gateway communication lost. A gateway has stopped responding to heartbeat. This log is triggered only for gateways that have 64 or more endpoints.
GWC305	This is a test alarm generated from pmdebug interface. Severity level changed in SN06; can have a severity level of critical, major, minor or warning.
GWC306	DQOSMTC_DQoSLinkLoss. A DQoS/COPS connection failure has occurred. Cleared by DCCNXMGR (via DCALARM) when the connection is reestablished or the connection is deleted via provisioning
GWC307	EM communication lost. Major. No response received for Persistent Data Verification SNMP Trap; EM not responding. Problem may be "EM not present, provisioned data loaded from local flash," OR "EM audit indicates provisioned inservice data is old, need manual intervention to recover." Cleared with a busy RTS. Datasync alarm The GWC does not contain the latest provisioned data. This alarm may be raised by the GWC EM noting the problem and sending a message to the GWC to raise the alarm.
GWC308	FLASH error Minor. Error in writing Flash; erase of Flash sector failed. Cleared with hardware replacement.
GWC309	Security_SA_capacity. Minor or Major. Security.Association alarms are nearing capacity. Cleared by the security alarms application which monitors the resource level and clears the alarm when the alarm condition has been cleared on the GWC. Currently alarms are only managed on the active GWC unit (i.e., data is not mirrored to the inactive unit), and for this reason during a SWACT alarms are automatically cleared on the unit dropping activity.
GWC310	Security_SA_fail. Major. The number of Security Association alarms has exceeded the threshold. Cleared by the security alarms application which monitors the resource level and cleared the alarm when the alarm condition as been cleared on the GWC. Currently alarms are only managed on the active GWC unit (i.e., data is not mirrored to the inactive unit), and for this reason during a SWACT alarms are automatically cleared on the unit dropping activity.
GWC311	Provisioned GWC Profile not yet activated.
GWC312	QoS connection alarm. An alarm is generated whenever a message cannot be sent to the server. The alarm is cleared as soon as the QoS report application is able to send QoS reports to the server.
GWC313	Major. RMGC can't process all coming requests. RMGC can't process all coming requests. It is in the processing error category. The probable cause is the resource at or nearing capacity.

GWC Logs/Faults available in Succession

Log/Fault	Description
GWC314	Raised in connection with a Location Id Reporting connection failure alarm.
GWC398	SNMP Timeout Critical; indicates a communications subsystem failure.
GWC399	Is the clear log for all GWC alarms and for CMT alarms. This log is triggered only for gateways that have 64 or more endpoints.
GWC501	Unable to maintain connection to remote gateway
GWC502	Connection to remote gateway restored.
GWC503	Connection drop initiated by remote gateway.
GWC506	Generated for any of 3 events: Time to Live Expired, Gateway Unregistration by CS2K Successful, or Gateway Initiated Unregistration Successful.
GWC507	Generated to indicate Gateway Registration Successful.

SPM--available logs/faults for Succession

The following table lists the SPM family Logs/Faults available through Succession.

The SPM family supports SCC2 or NT STD formatted logs through SDM functionality, or it can be supported through IEMS. For details on the IEMS interface, refer to the section in this document titled “SN07 IEMS Functionality.” For details on the logs/faults themselves, refer to the Fault Management section of the appropriate SPM FCAPS documentation and NN10275-909, *Succession Fault Management Log Reference*.

- SPM: NN10075-911
- DPT-SPM: NN10079-911 (IP)
- IW-SPM: NN10077-911 (IP)

General SPM Logs/Faults available in Succession

Log/Fault	Description
Network Element: SPM (all variants)	
ATM300	Generated when a Loss of Cell Delineation (LCD) alarm condition is raised on an SPM with ATM RMs.
ATM500	The system's ATM ILMI status has changed.
ATM501	The system's ATM signaling status has changed.
ATM600	The ATM framework has gained a registered ATM address.
ATM601	The ATM framework has been de-registered by the ATM network.
ATM604	System software cannot recover the ATM Framework (ATM RM will be busied and RTS'ed)
ATM605	ATM overload event.

General SPM Logs/Faults available in Succession

Log/Fault	Description
ATM606	ATM service failure.
ATM800	A trouble log that indicates possible degradation of service related to ATM Performance Monitoring thresholds.
ATMBCN	This alarm is raised when the ATM framework cannot support bearer connections. The alarm causes the SPM to show at the PM portion of the alarm banner as "SPM *C*." This alarm complements the ATMFWD alarm currently displayed beneath the APPL banner.
BITS300	A clock sync critical alarm has been raised for one of these: MTIE Performance, Alarm Indication Signal, Loss of Signal, or Out of Frame. Correlates with BITS600.
BITS301	A clock sync non-critical alarm has been raised for one of these: Timing Link Degradation, Bipolar Violation, or Cyclic Redundancy Check. Correlates with BITS601.
BITS500	BITS link state change capturing old/new states and reason for change (including degradation of carrier (LOS, LOF)).
BITS600	BITS Fault Report Cleared; critical alarm from BITS300 is cleared.
BITS601	BITS Fault Report cleared; non-critical alarm from BITS301 is cleared.
BITS610	Reference Quality Change to a new SSM state.
BITS612	BITS Reference Switch; indicates the reason for the reference switch.
C7UP109	A CQ state change has occurred.
C7UP113	Indicates ISUP maintenance trouble.
C7UP114	Generated for an ISUP alert.
C7UP120	An invalid range field exists.
C7UP130	The HOP counter has expired.
C7UP301	The HC value is not sufficient.
CARR300	A carrier failure event cleared. Correlates to alarms AIS, APSAM, APSCHMM, APSIC, APSMM, BERSD, BERSF, LOF, LOP, LOS, PLM, RAI, RFI, SIMPLEX, TIM. Correlates with CARR310.
CARR310	A carrier failure event has occurred. Correlates to alarms AIS, APSFC, APSFEPLF, APSLCK, APSMAN, BERSD, BERSF, LOF, LOP, LOS, PLM, RAI, RFI, SIMPLEX, TIM.
CARR315	A trouble log that includes the actual fault description text sent by the MG9K.
CARR330	A protection switch has occurred. A previously inactive carrier in the protection group takes over as the active carrier.
CARR331	A protection switch was attempted but failed.
CARR340	The inactive carriers in a protection group have changed state in such a way that they cannot carry traffic. The protection group is now running in simplex mode.
CARR341	Both carriers have become available and normal protection switching can occur.
CARR500	A carrier changes to an in service (InSv) state from manual busy (ManB) or system busy (SysB). Correlates to a MANB and SYSB alarm. Correlates with CARR511.

General SPM Logs/Faults available in Succession

Log/Fault	Description
CARR501	A carrier changes to central-side busy (CBsy) from ManB or SysB. Correlates to a MANB and SYSB alarm.
CARR510	A carrier changes to ManB from InSv, SysB, or CBsy. Correlates to a MANB and SYSB alarm.
CARR511	Carrier state change to SysB from InSv or CBsy. Correlates to a SYSB alarm.
CARR512	OC3 carrier state change to CBsy from InSv, ManB, or SysB. Correlates to a MANB and SYSB alarm.
CARR800	Threshold crossing alert (TCA) for a metered performance parameter has been cleared.
CARR801	Indicates that maintenance limits have been re-set.
CARR810	TCA event for metered performance parameter has occurred. Correlates with CARR800.
CARR811	TCA event for non-metered performance parameter has occurred. Also applies to STS-1 carrier on MG4000.
DPTM500	The state of DPT Terminals changed to IDL state from any other state.
DPTM501	The state of DPT Terminals changed to SYSB state from any other state.
DPTM502	The state of DPT Terminals changed to MANB state from any other state.
DPTM503	The state of DPT Terminals changed to PMB state from any other state.
DPTM504	The state of DPT Terminals changed to INB state from any other state.
DPTM700	Bulk downloading or dynamic update of DPT data failed, so there is a data mismatch in the CM and node. Correlates with DPTM701.
DPTM701	The DDM audit process cleared a DPT data mismatch between the core and the node.
DPTM702	Indicates a call is rejected because the DPT SOC limit is reached.
DPTM800	Office-wide DPT terminal usage exceeds the level 1 threshold of 70%. Logs DPT800-803 are associated with OM group DPTOFC, registers DPUSAG and DPUSAG2; and OM group DPTNODE, registers DPTUSAG and DPTUSAG2.
DPTM801	Office-wide DPT terminal usage drops below the level 1 threshold of 70%.
DPTM802	Office-wide DPT terminal usage exceeds the level 2 threshold of 90%.
DPTM803	Office-wide DPT terminal usage drops below the level 2 threshold of 85%.
EAD115	Problems with performance data collection associated with an OSS.
EAD116	Problems with the collection of MG 4000 performance data.
ENET308	ISTb state occurs or is cleared on a PSLINK. Correlates to an ISTB alarm. Associated with OM group ENLKERR.
ENET311	The SPM ATM node is SYSB, and a network error has caused it to be isolated from the ENET links or the MS ports. Correlates to a SYSBNA alarm.
IOAU112	Information log related to changes in System REX controller operation or schedule.

General SPM Logs/Faults available in Succession

Log/Fault	Description
IWBM500	One of the following is out of service: C-side link, STS3cP carrier, ATM network state, or the ATM address state for the IW bridge software.
IWBM501	The out-of-service item in IWBM500 has returned to service.
IWBM600	The IW bridge receives an invalid terminal ID during an attempt to free a bridge causing a connectivity mismatch. An INFO log.
IWBM601	Automatic system audit finds a problem and performs a corresponding action. An INFO log.
IWBM602	No IDL bridges are available. An INFO log.
IWBM603	An IWBM audit is being performed. An INFO log.
IWBM700	A maintenance action is being performed. An INFO log.
IWBM800	Number of available IW bridges exceeds the first threshold (70%) when attempting to retrieve an IW-bridge ID from the IW bridge manager.
IWBM801	Number of available IW bridges falls to less than 65% of bridges in the pool in use. This log always occurs after IWBM 800.
IWBM802	Number of available IW bridges exceeds the second threshold (90%) when attempting to retrieve an IW-bridge ID from the IW bridge manager.
IWBM803	Number of available IW bridges falls to less than 85% of bridges in the pool in use. This log always occurs after IWBM 802.
Link300	A transport resource fault indicating a mis-connected DS512 link.
NODE300	The integrated node maintenance (INM) generates this log when a trouble condition is present with the node. The log indicates INM recovery actions when the node state is system busy.
NODE302	Reports a software alarm.
NODE303	Generated to report the Wrong Application Data on the SPM.
NODE326	Generated to report a hardware fault on the SPM.
NODE500	System node state change. Correlates to a SYSB alarm.
NODE600	An INFO log to notify of a system recovery action.
NODE601	An INFO log that provides system status notification.
NODE602	Indicates the reason for CEM state transition, generated only when the CEM state transitions from Insv to Istb or Insv to Sysb.
PM231	Indicates that a PM failed to acknowledge an audit request to add or delete a channel connection.
PM232	Indicates that a PM operation from an audit request to add or delete a channel connection has succeeded.

General SPM Logs/Faults available in Succession

Log/Fault	Description
PM233	Indicates that a PM operation from an audit request to add or delete a channel connection has failed. The request is from Special Connection Table Control Facility (SPECCONN) to add or delete a channel connection. The subsystem generates the modified log when the operation to update to the correct status fails for two consecutive audit cycles.
PM234	Indicates that a PM failed to acknowledge an audit request to add or delete a channel connection.
PM236	Generated when the system finds integrity, does not find integrity, or loses integrity. Displayed when one of the following scenarios occurs: the system makes a special connection; integrity was lost or not found; or the SPECCONN audit acted on a special connection that has the status of NO_IINTEG.
PRSM400	A DPT SPM ATM loadfile containing DPT SPM ATM PRSU fixes has been datafilled in table PMLOADS.
SOC802	A warning log that the current configuration of the number of DPT ports is not authorized by Nortel, due to a conflict between the SOC limit and the setting of office parameter DPT_MAX_PORTS.
SPM300	A device fault has occurred. Correlates to a MANB, PROTFAIL, SYSB, and NOSPARE alarm.
SPM300	A device fault has occurred. Correlates to a MANB, PROTFAIL, SYSB, and NOSPARE alarm. SN07 adds a new text reason showing that it is generated when a STS3L carrier experiences an RFI alarm. SN07 adds the aestivate/status of the unit/device. SN07 adds next text "Device Fault Report" due to being triggered via resource exhaustion/overload conditions on the ATMRM.
SPM301	SPARTS patching log. An SPM patch is missing after an RTS occurred. Correlates to the PATCHFAIL, VCXO70, and VCXO90 alarms.
SPM310	The CM has received performance data from the DPT SPM ATM as a result of the DPT SPM ATM-based automatic monitoring process.
SPM311	A software exception report (SWER) has occurred, OR one of the BITS links is out-of-service. Correlates to an LOR alarm.
SPM312	A TBL trap has occurred on the CEM.
SPM313	A fault has been recorded in the Module Information Memory (MIM) of the SPM.
SPM314	A generic IMC fault report to indicate a change in IMC status.
SPM330	The two CEMs have either come into datasync or have gone out of datasync. Correlates to an ISTB alarm.
SPM331	A device had a protection switch failure. Modified to place IP RM in the circuit pack field. Correlates to a MANB, PROTFAIL, SYSB, ISTB, and NOSPARE alarm.
SPM332	The synchronization reference source was switched by manual action, switched by system action, or lost the last synchronization reference in the OC-3 protection group.
SPM333	Indicates an SPM Rex test failure.
SPM334	An alternate synchronization source is not available and the timing configuration no longer conforms to SONET specifications. Correlates to a CLKOOS alarm.

General SPM Logs/Faults available in Succession

Log/Fault	Description
SPM335	A device had a protection switch failure.
SPM336	The clock oscillator tuning range has reached 90% of the maximum range. Correlates to a VCXO90 alarm.
SPM337	SPM has entered Holdover. Correlates with SPM637.
SPM338	SPM has been in Holdover over 24Hours. Correlates with SPM638.
SPM339	The clock oscillator tuning range has reached 70% of the maximum range. Correlates to a VCXO70 alarm.
SPM340	A CM warm switch of activity (SWACT) failed.
SPM341	A SyncRM has entered into 3E Holdover state due to a clock mode change. Correlates with SPM641.
SPM342	A SyncRM has entered into 3E Holdover 24 State. Correlates with SPM642.
SPM344	The SyncRM Loss of BITS Redundancy (LOR) alarm has been set. Correlates with SPM644.
SPM350	There is the potential for resource exhaustion of a particular resource type. Correlates to the COTLOW, DTMFLOW, MFLOW, TONESLOW, and ECANLOW alarms. The log also generates when the alarm is cleared.
SPM352	Both of the Sync RMs are in holdover, so the SPM has entered Stratum 3E Holdover. Alarm ST3EHLDOVR is raised. Correlates with SPM652.
SPM353	Both of the Sync RMs are in holdover for 24 hours, so the SPM has entered Stratum 3E Holdover24. Alarm ST3EHLDOVR24 is raised. Correlates with SPM653.
SPM354	Both of the Sync RMs are out-of-service, so the SPM has entered SMC holdover. Alarm SMCHLDOVR is raised. Correlates with SPM654.
SPM355	Both of the Sync RMs are out-of-service for 24 hours, so the SPM has entered SMC holdover24. Alarm SMCHLDOVR24 is raised. Correlates with SPM655.
SPM356	One of the Sync RMs is out-of-service, so the SPM has lost clock unit redundancy. Alarm SPMLOCR is raised. Correlates with SPM656.
SPM358	A tuple change from EXTERNAL to LINE, or from LINE to EXTERNAL, is performed, and the SPM clock reference change failed. Correlates with SPM658.
SPM370	A log report of an SPM health monitor event. Connection errors have been corrected by the DLC Audit. Correlates with SPM670, the clearing log.
SPM399	Generated whenever an SPM enters or leaves an overload condition. SN07 adds next text "SPM Overload Report" due to being triggered via resource exhaustion/overload conditions on the ATMRM.
SPM500	A SyncRM device state change has occurred with new state and reason for change (e.g. SYSB, MANB). Modified to place IP RM in the circuit pack field. Correlates to a MANB, PROTFAIL, SYSB, and ISTB alarm.
SPM605	Indicate that a particular resource RM protection group is excluded by the SPMRESALIGN tool, without align RMID-PWID values.

General SPM Logs/Faults available in Succession

Log/Fault	Description
SPM610	Generated whenever an SPM node SSM value changes.
SPM611	A reference node switch has occurred.
SPM630	A device protection switch (i.e. clock unit switch) has occurred. Modified to place IP RM in the circuit pack field. Correlates to a MANB, SYSB, and ISTB alarm.
SPM632	Generated when the REX test on the SPM is successful.
SPM633	Generated when the REX test has started on an SPM node.
SPM637	The clock mode has changed from Holdover to Sync. Correlates with the HLDOVR alarm.
SPM638	The SPM recovers from the 24-hour Holdover state; the clock mode changes from Holdover to Sync. Correlates to the HLDOVR24 alarm.
SPM641	A SyncRM has exited 3E Holdover state.
SPM642	A SyncRM has exited 3E Holdover 24 state.
SPM644	The SyncRM Loss of BITS Redundancy (LOR) alarm has been cleared.
SPM645	Link Protocol & Messaging Interface Controller (LPMIC) Event Report. This log is generated on every CEM and transported to the core. The log is generated periodically and whenever the number of events crosses a threshold value.
SPM650	A successful in-service loading procedure has occurred. Modified to place IP RM in the circuit pack field.
SPM651	An in-service loading procedure has failed. Modified to place IP RM in the circuit pack field.
SPM652	SPM has exited Stratum 3E Holdover. Alarm ST3EHLDOVR is cleared.
SPM653	SPM has exited Stratum 3E Holdover24. Alarm ST3EHLDOVR24 is cleared.
SPM654	SPM has exited SMC Holdover. Alarm SMCHLDOVR is cleared.
SPM655	SPM has exited SMC Holdover24. Alarm SMCHLDOVR24 is cleared.
SPM656	SPM loss of clock unit redundancy cleared. Alarm SPMLOCR is cleared.
SPM657	Input timing signals degradation cleared. Alarm SPMTLD is cleared.
SPM658	A PM timing mode change has occurred with explicit reason (e.g. line to external due to manual request).
SPM660	A continuous performance-monitored trunk member was involved in an answered echo canceller call. This log reports the performance data.
SPM661	A continuous monitoring ON/OFF command or an SPMECMON AUTO command has successfully completed.
SPM670	An INFO log to report that the health monitor "CallCount PTS no setup fault" has been cleared. Correlates with SPM370, the raise log.
SPM680	Indicates low MBM Application Buffers.
SPM682	Indicates CEM manual reset.

General SPM Logs/Faults available in Succession

Log/Fault	Description
SPM683	Indicates the reason for CEM swact.
SPM684	Indicates that the erase flash command has initiated, is completed, has failed, or has been rejected. SN07 adds the activity/status of the unit/device.
SPM701	A DDM audit has successfully updated an SPM subgroup.
SPM702	A DDM dynamic update has failed for an SPM subgroup.
SPM703	A DDM audit has updated an SPM trunk member in a with a data entry for a trunk that failed to be added during a dynamic update.
SPM704	A DDM dynamic update has failed for an SPM trunk member.
SPM705	A trunk has been set to a lockout (LO) or SysB state. Correlates to SPM706.
SPM706	A trunk has returned to service from a LO state.
SPM707	A dynamic update has failed for the ISDNPARM table.
SPM708	The DDM audit has updated the ISDNPARM table.
SPM709	A dynamic update has failed for the ISDNPROT table.
SPM710	The DDM audit has updated the ISDNPROT table.
SPRF670	Generated every 15 minutes by the SPMACT tool. The logs are a compilation of the tool's results. Each line of the log corresponds to a performance measurement taken every minute by the tool.
SPRF671	Generated every 15 minutes by the SPUSAGE tool to summarize samples taken every minute of the call-processing events that occur in the SPM.
VOIP800 Log	This log is generated for any of the following reasons: - Cyclical Redundancy Check Error- Broadcast Packets - Undersize Packets- Jitter - Oversize Packets- Latency - Fragments- Lost Packets - Jabber- Decoder Under run - Drop Events
XAC329	Enhanced to provide more detailed reason text description for a number of failure scenarios in IRM, including a link state change. A customized text string is added for each IRM error code to help determine the causes resulting from link failure events.
Sync RM alarms	
LOS	Sync RM cannot detect a signal from the BITS timing link. Cleared when a signal is detected.
OOF	Sync RM cannot detect a DS1 frame for a given BITS timing link. Cleared when a DS1 frame is detected.
AIS	Sync RM detects an AIS on an incoming BITS timing reference signal from BITS, or crossover from alternate SPM reference node. Cleared when incoming BITS timing reference signal does not have an alarm.

General SPM Logs/Faults available in Succession

Log/Fault	Description
MTIE2	MTIE performance for input signal exceeds the GR-253 requirement mask threshold, indicating an unusable signal. Cleared when MTIE is below GR-253 requirement mask threshold.
TLD	MTIE performance for input signal exceeds the GR-253 requirement mask threshold, indicating a degraded signal. Cleared when the MTIE Level 1 degradation disappears from timing reference.
BPV	Incoming signal has BPV alarm, indicating a degraded signal. Cleared when BPV disappears from timing reference.
CRC	SyncRM detects a CRC from incoming signal, indicating a degraded signal. Cleared when the CRC disappears from the timing reference.
LOR	SyncRM cannot detect the DS1 frame from BITS timing links or signal from Mate SyncRM, indicating that redundancy is lost. Cleared when a DS1 frame is detected.
HLDOVR	SyncRM has gone into the holdover mode because both BITS timing links were lost. Cleared when SyncRM exits holdover mode.
Bearer connections alarm	An alarm for bearer connections is added to the list of alarms in table MNNODE.

Stormia (STM)-available logs/faults for Succession

The following table lists the STM logs available through Succession. STM logs will only be present in the HLR market. For detailed information on logs, refer to NN10275-909, *Succession Fault Management Log Reference*.

STM logs available in Succession

STM398	Indicates a raised alarm in an STM device.
STM399	Indicates a cleared alarm in an STM device.

MG4000-available logs/faults for Succession

The following table lists the MG4000 logs available through Succession. MG 4000 supports SCC2 or NT STD formatted logs through SDM functionality, or it can be supported through IEMS. For details on the IEMS interface, refer to the section in this document titled “SN07 IEMS Functionality.” For detailed information on logs, refer to NN10275-909, *Succession Fault Management Log Reference*.

MG4000 logs available in Succession

MG4I 300	Media Integrity Failure
MG4I 301	GigE Audit Failure
MG4I 320	Counter overflow in the Operational Measurement pegs

MG4000 logs available in Succession

MG4I 501	SCTP Core Connection State Change
MG4I 502	SCTP Peer Connection State Change

MG9000--available logs/faults for Succession

The following table lists the MG 9000 Faults available through Succession. MG 9000 supports SCC2 or NT STD formatted logs through SDM functionality, or it can be supported through IEMS. For details on the IEMS interface, refer to the section in this document titled “SN07 IEMS Functionality.” For details on the logs/faults themselves, refer to the Fault Management section of MG 9000 FCAPS documentation, NN10074-911 and NN10275-909, *Succession Fault Management Log Reference*.

MG 9000 Faults available in Succession

Network Element: MG 9000	
Fault	Description
MGAUxxx	Generated when audit task starts.
MGAUxxx	Generated when audit task is paused.
MGAUxxx	Generated when audit task is resumed.
MGAUxxx	Generated when audit task is completed with a summary of corrections.
MGAUxxx	Generated when audit schedule is deleted.
MGAUxxx	Generated when audit could not correct a mismatch.
BW300	Reserved bandwidth used on the indicated shelf has exceeded the Bandwidth Congestion Threshold. Correlates with Warning alarm bwResBandwShelfFault.
BW301	Reserved bandwidth use on the network interface has exceeded the Bandwidth Congestion Threshold. The alarm is cleared when reserved bandwidth on the network interface is 10% less than the threshold. Correlates with Warning alarm bwResBandwTotalFault.
BW302	Reserved bandwidth dedicated to switched lines connections on the network interface has exceeded the Bandwidth Congestion Threshold with respect to the amount of bandwidth configured the network interface for switched lines. Correlates with Warning alarm bwResBandwSloaFault.
BW304	An overall cell queue congestion alarm has occurred when overall atm cell queue is at least 90% full, or the alarm has been cleared. Correlates with Warning alarm bwSwitchFabricTotalFault.
BW305	A CBR cell queue congestion alarm has occurred or been cleared. To occur, atm cell queue for this service type is at least 90% full. Correlates with Warning alarm bwSwitchFabricCbrFault.
BW306	An RT-VBR cell queue congestion alarm has occurred or been cleared. To occur, atm cell queue for this service type is at least 90% full. Correlates with Warning alarm bwSwitchFabricRtVbrFault.

MG 9000 Faults available in Succession

BW307	An NRT-VBR cell queue congestion alarm has occurred or been cleared. To occur, atm cell queue for this service type is at least 90% full. Correlates with Warning alarm bwSwitchFabricNrtVbrFault.
BW308	A UBR cell queue congestion alarm has occurred or been cleared. To occur, atm cell queue for this service type is at least 90% full. Correlates with Warning alarm bwSwitchFabricUbrFault.
BW309	A UBR-plus cell queue congestion alarm has occurred or been cleared. To occur, atm cell queue for this service type is at least 90% full. Correlates with Warning alarm bwSwitchFabricUbrPlusFault.
BW310	A control channel cell queue congestion alarm has occurred or been cleared. To occur, atm cell queue for this service type is at least 90% full. Correlates with Warning alarm bwSwitchFabricControlFault.
BW311	Reserved bandwidth dedicated to ABI lines connections on the network interface has exceeded the Bandwidth Congestion Threshold with respect to the amount of bandwidth configured the network interface for switched lines. Correlates with Warning alarm bwResBandwAbiFault.
CES305	No cells are being received from the ATM network. Correlates with Major alarm cesLossOfCell.
ESA300	Communication between GWC and GW is lost. Entered ESA mode. Correlates with Critical alarm Entered ESA.
ESA302	This log corresponds to the nnESADownloadFault.
ESA601	ESA601 is generated from alarm nnESAFault. This alarm was added in Gateway to notify the data inconsistency when MG 9000 finds internal ESA data mapping inconsistency after the ESA data downloading is completed.
ESA602	ESA602 is generated from alarm nnESARetrieveFault, an alarm generated by the EM for ESA Data Retrieval failure.
ESA fault nnESADownl oadFault	Indicates a failure to download ESA data to a given VMG. This alarm will only be generated for autonomous download attempts. This was indicated by a log in releases previous to SN07.
HWMismatch alarm	The Hardware Mismatch alarm indicates an incorrect replacement card has been installed.
QoS alarms	New QoS alarms are generated when any of four configured threshold parameters are exceeded. The alarm browser (at the VMG level) is extended to view these alarms.
Provisioning failure logs	If an operation fails when provisioning Tone, Class, or Physical Ringing data, a customer log is generated.
"Authorization Failed" Security Log	Generated when a user attempts to perform an unauthorized action.
MG9K Server Log	A warning log generated when the MG9K server is either starting up or shutting down.

MG 9000 Faults available in Succession

MGCA301	Loss of signal fault has occurred or been cleared. Correlates with Critical alarm LOS (on OC3) or Minor alarm los (on DS1).
MGCA302	Alarm indication signal fault has occurred or been cleared. Correlates with Critical alarm AIS (on OC3) or Minor alarm ais (on DS1).
MGCA303	Loss of frame fault has occurred or been cleared. Correlates with Critical alarm LOF (on OC3) or Minor alarm lof (on DS1).
MGCA304	Remote alarm indication. Correlates with Minor alarm RAI (on DS1).
MGCA305	Bit error rate signal fault has occurred or been cleared. Correlates with Critical alarm bit error ratio signal default (BERSF) (on OC3).
MGCA306	Bit error rate signal degraded fault has occurred or been cleared. Correlates with Major alarm bit error ratio signal default (BERSD) (on OC3).
MGCA307	Remote defect indication fault has occurred or been cleared. Correlates with Minor alarm remote defect indication (RDI) (on OC3).
MGCA308	Path label mismatch fault has occurred or been cleared. Correlates with Minor alarm alarm path label mismatch (PLM) (on OC3).
MGCA309	Loss of pointer fault has occurred or been cleared. Correlates with Minor alarm loss of pointer (LOP) (on OC3).
MGCA310	An unequipped fault has occurred or been cleared. Correlates with Minor alarm UNEQ (on OC3).
MGCA311	Loss of cell delineation fault has occurred or been cleared (supported in EM only). Correlates with alarm LOD.
MGCA312	IMA link- Loss of IMA Frame. Correlates with Minor alarm imaLinkLif.
MGCA313	IMA link- Loss of delayed synchronization. Correlates with Minor alarm imaLinkLods.
MGCA314	IMA link- Remote failure indication. Correlates with Minor alarm imaLinkRfi.
MGCA315	IMA link- Transmit misconnect. Correlates with Minor alarm imaLinkTxMisConnect.
MGCA316	IMA link- receive misconnect. Correlates with Minor alarm imaLinkRxMisConnect.
MGCA317	IMA link- transmit fault. Correlates with Minor alarm imaLinkTxFault.
MGCA318	IMA link- receive fault. Correlates with Minor alarm imaLinkRxFault.
MGCA319	IMA link- transmit unusable far end. Correlates with Minor alarm imaLinkTxUnusableFe.
MGCA320	IMA link- receive unusable far end. Correlates with Minor alarm imaLinkRxUnusableFe.
MGCA321	IMA group startup far end. Correlates with Major alarm imaGroupStartupFe.
MGCA322	IMA group configuration abort. Correlates with Critical alarm imaGroupCfgAbort.
MGCA323	IMA group configuration abort far end. Correlates with Major alarm imaGroupCfgAbortFe.
MGCA324	IMA group insufficient links. Correlates with Critical alarm imaGroupInsuffLinks.
MGCA325	IMA group insufficient links far end. Correlates with Major alarm imaGroupInsuffLinksFe.
MGCA326	IMA group blocked far end. Correlates with Minor alarm imaGroupBlockedFe.

MG 9000 Faults available in Succession

MGCA327	IMA group timing synchronization. Correlates with Major alarm imaGroupTimingSynch.
MGCA328	ABI Loss of Clock on DS512 optical link. Correlates with Critical alarm abiLossOfClock.
MGCA329	ABI Loss of Frame on DS512 optical link. Correlates with Critical alarm abiLossOfFrame.
MGCA330	ABI Loss of Signal (low light level) on DS512 optical link. Correlates with Critical alarm abiLowLightLevel.
MGCA331	ABI Channel parity error on DS512 optical link. Correlates with Minor alarm abiChannelParityError.
MGCA332	SDH Path Trace Identifier Mismatch Alarm (only applies to SDH and not SONET). The Path Trace Identifier being seen by the OC3 card at the carrier Path level does not match what has been provisioned for that carrier. Correlates with Minor alarm tim.
MGCA333	AlarmIndicationSignal (ds3ais) generates log MGCA333 when an AlarmIndicationSignal fault is received from the Gateway.
MGCA334	LossofFrame (ds3lof) generates log MGCA334 when a LossOfFrame fault is received from the Gateway.
MGCA335	RemoteAlarmIndication (ds3rai) generates log MGCA335 when a RemoteAlarmIndication fault is received from the Gateway.
MGEM300	Generated when MG9000 EM is not able to make connection to the Element Manager Database. Correlates with Major alarm EmDbUnavailable.
MGEM301	In SN06, the NE301 log name changed to MGEM301. Generated when the Succession MG 9000 Manager loses SNMP communication with the MG 9000. Correlates with Critical alarm CommsLostToNE.
MGEM302	In SN06, NE302 log name changed to MGEM302. The MG9000 Manager has added an ne MG9000 and tries to discover the NE. It will check the MG9000 EM IP address provisioned at the MG9000 and if it is incorrect will raise this alarm. Correlates with Major alarm invalidEMIPAddress.
MGEM303	In SN06, the NE303 log name changed to MGEM303. The description of this log is restored faults: "Faults seen while active." Diagnostics will not clear restored faults. The card with the restored faults may not be in the same state it was in before the restart that caused the faults to be restored. The MG9000 sends too many alarms within a 5 second window. When this happens the MG9000 Manager will request this particular MG9000 stop sending Alarms and display this particular alarm. This condition will clear when the number of alarm within 5 sec falls below a set number. Correlates with Critical alarm AlarmsBeingThrottled.
MGEM704	Indicates that an attempt to correct the database has failed
MGEM705	Indicates that the Database is unavailable and correction failed.
MGEM714	An audit log generated whenever a user attempts to image an MG9K device.
NE300	In SN06, the NE300 log (corresponding to all NorNode Faults) split into several logs (grouped according to the clearing procedures). Log NE300 should only be generated if the GW is running on pre-SN06 loads and the MGEM is running on SN06+ loads. It is purely for backward compatibility.

MG 9000 Faults available in Succession

NE301	The NE301 log (Critical) is generated when an incorrect replacement card has been installed.
NE302	The NE302 log indicates software faults of any severity.
NE303	The NE303 log indicates restored faults: "Faults seen while active." Diagnostics will not clear restored faults. The card with the restored faults may not be in the same state it was in before the restart that caused the faults to be restored.
NE304	The NE304 log indicates faults that are ambiguous with regard to the card that is causing the fault. Usually, the alarm on card A indicates that there is a problem on card A, card B, or the link in between card A and B.
NE305	The NE305 log indicates serial device faults of any severity.
NE306	The NE306 log indicates GLAN-related faults of any severity. The GLAN hub is located on the active ITP in the shelf where the fault appears.
NE307	The NE307 log indicates ABI faults of any severity.
NE308	The NE308 log indicates inband messaging faults of any severity.
NE309	The NE309 log indicates clock sync faults of any severity.
NE310	The NE310 log indicates unused hardware faults of any severity.
NE311	The NE311 log indicates time of day faults of any severity - attempts to access the provisioned time server have failed.
NE312	The NE312 log indicates cable faults of any severity -- one of the cables to the ITPs has been connected in an unsupported way.
NE313	The NE313 log indicates an activity cable fault of any severity; the activity control cable is a small cable on the front of the ABI cards that is used for activity determination.
NE314	The NE314 log indicates backplane faults of any severity; the carriers between the two DCC cards cannot communicate.
NE315	The NE315 log indicates bandwidth fault of any severity; some of the carriers are not providing bandwidth.
NE316	The NE316 log indicates line alarms of any severity.
NE317	The NE317 log indicates shelf faults of any severity.
NE318	The NE318 log indicates proxy alarms of any severity; the card referred to in the alarm text (description) is not communicating.
NE319	The NE319 log indicates MTA alarms of any severity.
NE320	The NE320 log indicates data audit faults of any severity; data audit required.
NE609	A software image log generated whenever a user executes an image request.
OVLD808	(Critical) Indicates that an external messaging link has closed and cannot send/receive message.
OVLD809	(Major) Indicates that the message loss is high enough such that the message link is in a degraded service state.

MG 9000 Faults available in Succession

OVLD810	(Minor) Indicates message retransmissions are high enough that system is starting to see performance degradation.
SHLF301	SIC talk battery A alarm occurs. Correlates with Critical alarm shelfTalkBatteryA.
SHLF302	SIC talk battery B alarm occurs. Correlates with Critical alarm shelfTalkBatteryB.
SHLF303	SIC signal battery A alarm occurs. Correlates with Major alarm shelfSignalBatteryA.
SHLF304	SIC signal battery B alarm occurs. Correlates with Major alarm shelfSignalBatteryB.
SHLF305	SIC signal battery A fuse alarm occurs. Correlates with Major alarm shelfSignalBatteryAfuse.
SHLF306	SIC signal battery B fuse alarm occurs. Correlates with Major alarm shelfSignalBatteryBfuse.
SHLF307	SIC shelf fail LED alarm occurs. Correlates with alarm shelfFailLED.
SHLF308	BIP signal battery A1 alarm occurs. Correlates with Major alarm bipSignalBatteryA1.
SHLF309	BIP signal battery A2alarm occurs. Correlates with Major alarm bipSignalBatteryA2.
SHLF310	SIC talk battery B1 alarm occurs. Correlates with Major alarm bipSignalBatteryB1.
SHLF311	BIP signal battery B2 alarm occurs. Correlates with Major alarm bipSignalBatteryB2.
SHLF312	BIP talk battery A alarm occurs. Correlates with Minor alarm bipTalkBatteryA.
SHLF313	BIP talk battery B alarm occurs. Correlates with Minor alarm bipTalkBatteryB.
SHLF314	BIP filter A fail alarm occurs. Correlates with Minor alarm bipFilterA.
SHLF315	BIP filter B fail alarm occurs. Correlates with Minor alarm bipFilterB.
SHLF316	BIP scan point 1 is activated. Correlates with alarm bipScanPoint1.
SHLF317	BIP scan point 2 is activated. Correlates with alarm bipScanPoint2.
SHLF318	BIP scan point 3 is activated. Correlates with alarm bipScanPoint3.
SHLF319	BIP scan point 4 is activated. Correlates with alarm bipScanPoint4.
SHLF320	BIP scan point 5 is activated. Correlates with alarm bipScanPoint5.
SHLF321	BIP scan point 6is activated. Correlates with alarm bipScanPoint6.
SHLF322	BIP scan point 7is activated. Correlates with alarm bipScanPoint7.
SHLF323	BIP scan point 8is activated. Correlates with alarm bipScanPoint8.
SHLF324	BIP scan point 9is activated. Correlates with alarm bipScanPoint9.
SHLF325	BIP scan point 10is activated. Correlates with alarm bipScanPoint10.
SHLF326	BIP scan point 11 is activated. Correlates with alarm bipScanPoint11.
SHLF327	Talk Battery A1 Power Feed. Correlates with Major alarm bipTalkBatteryA1.
SHLF328	Talk Battery A Power Feed. Correlates with Major alarm bipTalkBatteryA2.
SHLF329	Talk Battery B1 Power Feed. Correlates with Major alarm bipTalkBatteryB1.
SHLF330	Talk Battery B2 Power Feed. Correlates with Major alarm bipTalkBatteryB2.

MG 9000 Faults available in Succession

SHLF331	BIP circuit breaker fan alarm occurs (EM only). Correlates with Minor alarm bipFanBreaker.
SHLF332	BIP environmental control unit 0 temperature alarm occurs. Correlates with Minor alarm bipEcuTemp0.
SHLF333	BIP environmental control unit 1 temperature alarm occurs. Correlates with Minor alarm bipEcuTemp1.
SHLF334	BIP environmental control unit 0 fan alarm occurs. Correlates with Minor alarm bipEcuFan0.
SHLF335	BIP environmental control unit 1 fan alarm occurs. Correlates with Minor alarm bipEcuFan1.
SHLF336	BIP remote alarm cut off alarm occurs. Correlates with alarm bipRemoteAlarmcutoff.
SHLF337	BIP local alarm cut off alarm occurs. Correlates with alarm bipLocalAlarmcutoff.
SHLF338	BIP ABS fuse fail alarm occurs. Correlates with Major alarm bipAbsFusefail.
SHLF339	BIP ABS battery power supply alarm occurs. Correlates with Critical alarm bipAbsPowerSupply.
SHLF340	BIP shelf circuit breaker trip alarm occurs. Correlates with Major alarm bipShfBreakerTrip.
SHLF341	Presence of BIP's Current-Sense Card A. Correlates with Major alarm bipCsApresence.
SHLF342	Presence of BIP's Current-Sense Card B. Correlates with Major alarm bipCsBpresence.
SHLF343	Presence of BIP's Alarm Relay Card. Correlates with Major alarm bipAlmRelayPresence.
SHLF344	Current-Sense Card A Shelf 0 High Threshold exceeded. Correlates with Minor bipCSAshf0HighThres alarm.
SHLF345	Current-Sense Card A Shelf 1 High Threshold exceeded. Correlates with Minor bipCSAshf1HighThres alarm.
SHLF346	Current-Sense Card A Shelf 2 High Threshold exceeded. Correlates with Minor bipCSAshf2HighThres alarm.
SHLF347	Current-Sense Card A Shelf 3 High Threshold exceeded. Correlates with Minor bipCSAshf3HighThres alarm.
SHLF348	Current-Sense Card B Shelf 0 High Threshold exceeded Correlates with Minor bipCSBshf0HighThres alarm.
SHLF349	Current-Sense Card B Shelf 1 High Threshold exceeded. Correlates with Minor bipCSBshf1HighThres alarm.
SHLF350	Current-Sense Card B Shelf 2 High Threshold exceeded. Correlates with Minor bipCSBshf2HighThres alarm.
SHLF351	Current-Sense Card B Shelf 3 High Threshold exceeded. Correlates with Minor bipCSBshf3HighThres alarm.
SHLF352	Current High Temperature Threshold exceeded. Correlates with Minor bipTempHighThres alarm.

MG 9000 Faults available in Succession

SHLF353	Current-Sense Card A Shelf 0 Low Threshold exceeded. Correlates with Minor bipCSAshf0LowThres alarm.
SHLF354	Current-Sense Card A Shelf 1 Low Threshold exceeded. Correlates with Minor bipCSAshf1LowThres alarm.
SHLF355	Current-Sense Card A Shelf 2 Low Threshold exceeded. Correlates with Minor bipCSAshf2LowThres alarm.
SHLF356	Current-Sense Card A Shelf 3 Low Threshold exceeded. Correlates with Minor bipCSAshf3LowThres alarm.
SHLF357	Current-Sense Card B Shelf 0 Low Threshold exceeded. Correlates with Minor bipCSBshf0LowThres alarm. Correlates with Minor bipCSBshf1LowThres alarm.
SHLF358	Current-Sense Card B Shelf 1 Low Threshold exceeded. Correlates with Minor bipCSBshf1LowThres alarm.
SHLF359	Current-Sense Card B Shelf 2 Low Threshold exceeded. Correlates with Minor bipCSBshf2LowThres alarm.
SHLF360	Current-Sense Card B Shelf 3 Low Threshold exceeded. Correlates with Minor bipCSBshf3LowThres alarm.
SHLF361	Current Low Temperature Threshold exceeded. Correlates with Minor bipTempLowThres alarm.
SHLF362	Status of the Signal Battery Fuse. Correlates with Major bipSignalBatteryFuse alarm.
SHLF363	Status of Talk Battery A Fuse. Correlates with Major bipTalkBatteryAFuse alarm.
SHLF364	Status of Talk Battery B Fuse. Correlates with Major bipTalkBatteryBFuse alarm.
SHLF365	Status of Cooling Unit 0 Fuse. Correlates with Minor bipEcuFuse0 alarm.
SHLF366	Status of Cooling Unit 1 Fuse. Correlates with Minor bipEcuFuse1 alarm.
SHLF367	Status of the End-Aisle Fuse. Correlates with Minor bipEndAisleFuse alarm.
SHLF368	BIP Signal Distribution Point 1. Correlates with bipSignalDistribution1 alarm.
SHLF369	BIP Signal Distribution Point 2. Correlates with bipSignalDistribution2 alarm.
SHLF370	BIP Signal Distribution Point 3. Correlates with bipSignalDistribution3 alarm.
SHLF371	BIP Signal Distribution Point 4. Correlates with bipSignalDistribution4 alarm.
SHLF372	BIP Visual Critical. Correlates with bipVisualCritical alarm.
SHLF373	BIP Visual Major. Correlates with bipVisual Major alarm.
SHLF374	BIP Visual Minor. Correlates with bipVisualMinor alarm.
SHLF375	BIP Audible Critical. Correlates with bipAudibleCritical alarm.
SHLF376	BIP Audible Major. Correlates with bipAudibleMajor alarm.
SHLF377	BIP Audible Minor. Correlates with bipAudibleMinor alarm.
SHLF378	BIP Alarm CutOff LED. Correlates with bipAlarmCutOffLED alarm.
SHLF379	BIP Talk Battery A Fail LED. Correlates with bipTalkBatteryFailALEd alarm.

MG 9000 Faults available in Succession

SHLF380	BIP Talk Battery B Fail LED. Correlates with bipTalkBatteryFailBLED alarm.
SHLF381	BIP Critical LED Bank. Correlates with bipCriticalLEDbank alarm.
SHLF382	BIP Major LED Bank. Correlates with bipMajorLEDbank alarm.
SHLF383	BIP Minor LED Bank. Correlates with bipMinorLEDbank alarm.
SHLF384	BIP Environmental Control Unit 0 LED. Correlates with bipEcu1LED alarm.
SHLF385	BIP Environmental Control Unit 1 LED. Correlates with bipEcu2LED alarm.
SHLF386	BIP Alarm Processor Card Fail LED. Correlates with bipAlarmFailLED alarm.
SHLF387	BIP Aisle Alarm. Correlates with bipAisleAlarm alarm.
SHLF388	BIP Frame Alarm. Correlates with bipFrameFail alarm.
SHLF389	Presence of BIP's Alarm Relay Card LED. Correlates with bipAlmRelayLed alarm.
SHLF390	Status of Current-Sense Card A LED. Correlates with bipCsAled alarm.
SHLF391	Status of Current-Sense Card B LED. Correlates with bipCsBled alarm.
SHLF392	Generated when a shelfCompatibility fault is received from the MG9kEM server.
SHLF393	Generated when a cardDiscovery fault is received from the MG9kEM server.
SHLF501	A catch-all INFO log for all shelf events. Changed in SN06 to show a Severity of Indeterminate, which means no priority has been assigned to the related BIP event. If a severity had been datafilled, then SHLF383 would generate instead of SHLF 501.
SWLN301	Line in Fault occurred or is cleared. Correlates with Minor lineFault alarm.
SWLN302	Hazardous Voltage line fault occurred or is cleared. Correlates with Minor alarm lineProtectionFault.
SWLN303	Line in Babbling state line fault occurred or is cleared. Correlates with Minor alarm lineBabbleState.
VC301	Minor: atmVcl Alarm indication signal. Correlates with Minor alarm vclTpAis.
VC302	Minor: atmVcl Remote Detection Indicator. Correlates with Minor alarm vclTpRdi.
VC303	Minor: loss of continuity, vcl. Correlates with Minor alarm vclLoc.
VC304	Minor: atmVcc Alarm indication signal. Correlates with Minor alarm vccTpAis.
VC305	Minor: atmVcc Remote Detection Indicator. Correlates with Minor alarm mvccTpRdi.
VC306	Minor: loss of continuity, vcc. Correlates with Minor alarm vccLoc.
VC307	Minor: loss of cell delineation on If (only on the EM). Correlates with alarm atmLcd.
VMG300	Generated when Root Termination goes out of service (Communication between Gateway and GWC is lost and ESA is not enabled). Correlates with Critical alarm VMG OOS.
VMG301	QoS Alarm that is generated when the number of bad call reaches a certain threshold.
VMG302	QoS Alarm that is generated when the number of Packet Loss reaches a certain threshold.

MG 9000 Faults available in Succession

VMG303	QoS Alarm that is generated when IP message Jitter reaches a certain threshold.
VMG304	QoS Alarm that is generated when IP message Latency reaches a certain threshold.
VMG322	Generated when a vMGAdminStatusOutOfService fault is received from the MG9kEM server (Warning).
VMG323	Generated when a cardLocked fault is received from the MG9kEM server (Warning).
VMG324	Generated when a cardDisabled fault is received from the MG9kEM server (Warning).
VMG325	Generated when a cardInitializing fault is received from the MG9kEM server (Warning).
VMG328	Generated when a lineMtceNotReady fault is received from the MG9kEM server (Critical).
VMG329	Generated when a MegacoMtceNotReady fault is received from the MG9kEM server (Critical).
VMG373	Generated when a GWCUnreachable fault is received from the MG9kEM server (Critical).
VMG374	Generated when a noReplyFromGWC fault is received from the MG9kEM server.
VMG376	Generated when an aal1BearerSubsystem OnPairNotReady fault is received from the MG9kEM server.
VMG377	Generated when an ipBearerSubsystem OnPairNotReady fault is received from the MG9kEM server.
VMG600	Indicates that termination data was successfully provisioned in all appropriate areas except for the database.
VMG601	Indicates that an attempt to correct termination data in the database has passed.
VMG Admin State is OOS	Generated when a vMGAdminStatusOutOfService fault is received from the MG9kEM server (Warning). Relates to log VMG322.
VMG Initializing	Generated when a cardInitializing fault is received from the MG9kEM server (Warning). Relates to log VMG325.
VMG OOS-card locked	Generated when a cardLocked fault is received from the MG9kEM server (Warning). Relates to log VMG323.
VMG OOS-card disabled	Generated when a cardDisabled fault is received from the MG9kEM server (Warning). Relates to log VMG324.
VMG OOS- Line Maintenance is not Ready	Generated when a lineMtceNotReady fault is received from the MG9kEM server (Critical). Relates to log VMG328.
VMG OOS- Megaco Maintenance is not Ready	Generated when a MegacoMtceNotReady fault is received from the MG9kEM server (Critical). Relates to log VMG329.
VMG OOS- GWC is not reachable	Generated when a GWCUnreachable fault is received from the MG9kEM server (Critical). Relates to log VMG373.
VMG OOS- no reply from GWC	Generated when a noReplyFromGWC fault is received from the MG9kEM server. Relates to log VMG374.
VMG OOS- AAL1 bearer subsystem not ready	Generated when an aal1BearerSubsystem OnPairNotReady fault is received from the MG9kEM server. Relates to log VMG376.

MG 9000 Faults available in Succession

VMG OOS- IP bearer subsystem not ready	Generated when an ipBearerSubsystem OnPairNotReady fault is received from the MG9kEM server. Relates to log VMG377.
XDSL301	Generated when a loss of signal - local modem fault occurs. Correlates with Minor alarm losATUC.
XDSL302	Generated when a loss of frame - local modem fault occurs. Correlates with Minor alarm lofATUC.
XDSL303	Generated when a loss of power - local modem fault occurs. Correlates with Critical alarm lprATUC.
XDSL304	Generated when a loss of link - local modem fault occurs. Correlates with Minor alarm loiATUC.
XDSL305	Generated when a loss of signal - remote modem fault occurs. Correlates with Minor alarm losATUR.
XDSL306	Generated when a loss of frame - remote modem fault occurs. Correlates with Minor alarm lofATUR.
XDSL307	Generated when a loss of power - remote modem fault occurs. Correlates with Minor alarm lprATUR.
XDSL308	Generated when a loss of link - remote modem fault occurs. Correlates with Minor alarm loiATUR.
XDSL309	Generated when a no modem present fault occurs. Correlates with Minor alarm aturNotPresent.
XDSL310	Generated when a local modem clock failure occurs. Correlates with Critical alarm noClock.
XDSL311	Generated when a protocol error occurs. Correlates with Critical alarm handshakeFail.
XDSL312	Generated when a configuration error occurs. Correlates with Critical alarm linkMismatch.
XDSL313	Generated when an ATM traffic dropped at WAC upstream fault occurs. Correlates with Critical alarm vpiNonzero.
XDSL314	Generated when a loss of sync of ATM cells - upstream fault occurs. Correlates with Critical alarm lcdIATUC.
XDSL315	Generated when a loss of sync of ATM cells - downstream fault occurs. Correlates with Critical alarm lcdIATUR.
XDSL316	Generated when a local modem Critical failure - not responding, in Kernel mode, download failure, or message corrupted fault occurs. Correlates with Critical alarm failATUC.
XDSL317	Generated when a general hardware fault indication - circuit fault occurs. Correlates with Critical alarm circuitHardwareFault.
xDSL600	ATUCs transmit rate has changed (RADSL mode only).
xDSL601	ATUC initialization failed.
xDSL602	ATURs transmit rate has changed (RADSL mode only).

MG 9000 Faults available in Succession

xDSL800	Loss of Framing 15-minute interval threshold reached.
xDSL801	Loss of Signal 15-minute interval threshold reached.
xDSL802	Loss of Power 15-minute interval threshold reached.
xDSL803	Errored Second 15-minute interval threshold reached.
xDSL805	Loss of Framing 15-minute interval threshold reached.
xDSL806	Loss of Signal 15-minute interval threshold reached.
xDSL807	Loss of Power 15-minute interval threshold reached.
xDSL808	Errored Second 15-minute interval threshold reached.
xDSL809	A DSL Interface exceeds the specified threshold on a given performance measurement.
The following items describe the MG9K Clock Sync alarms.	
Loss of Phase Lock	Minor: Phase PLD [altera 7064b] detected a minimum phase difference greater than eight nano seconds.
Loss of Frame Pulse Lock	Minor: Frame pulse alignment did not get established with the active card -- it should occur in the inactive card only
Loss of My Clock	Minor: The high and low levels of the SYNC PLL clock are not toggling.
Loss of Mate Clock	Minor: The high and Low levels of the mate clock are not toggling.
Loss of Clock Output	Major: Phase PLD reference clock oscillator not toggling.
Single Reference Failure	Minor: Single monitored reference source has been lost.
All Reference Failure	Major: Absolute and Delta reference source signals have been lost.
Single Sync Unit Failure	Major: Stratum 3 unit on ITP failed.
Clock Stability	Clock mode can be Acquiring, Acquired, Hold Over, or Free Run.
Signal LOS	Minor: Single/All source reference occurred due to loss of signal.
Signal LOF	Minor: Single/All source(s) reference occurred due to out of frame.
No Signal	Minor: Sync source reference selected does not provide a signal.

NPM--available logs/faults for Succession

The following table lists the Network Patch Manager (NPM) Logs/Faults available through Succession.

NPM supports SCC2 or NT STD formatted logs through SDM functionality,

or it can be supported through IEMS. For details on the IEMS interface, refer to the section in this document titled “SN07 IEMS Functionality.” For details on the logs, refer to the Fault section of the FCAPS documentation on CS 2000 Management Tools, NN10325-900 and NN10275-909, *Succession Fault Management Log Reference*.

NPM Logs/Faults available in Succession

Log/Fault	Description
Network Element: Network Patch Manager	
NPM360	Reports that an alarm has been raised.
NPM370	Reports when an alarm has been cleared.
NPM400	Reports the results of attempted apply, remove, and audit commands.
NPM600	Reports when the NPM server has been started, either by reboot or manually.
NPM601	File failure; reports general problems that could be service affecting. The log contains lines of trouble information text.
NPM603	There are problems between the database and the device during a device audit.
NPM605	General trouble log; reports general problems that could be service affecting. The log contains lines of trouble information text.
NPM610	Provides information related to the execution of a task.
NPM660	Reports problems when a plan fails to execute.
NPM680	Reports problems when a plan is automatically executed.
NPM System Alarms	
Alarm name	Description
ACT_NOT_APP	Activated patch not applied to all applicable devices.
ACT_NOT_ACT	Active patch applied to all applicable devices but not activated in all devices.
DEBUG_APP	Debug patches applied. Minor.
DISABLED_APPLIED	Applied patches that can be enabled, but are disabled. Major.
DNR_NOT_APP	Do Not Remove (DNR) patches not applied. Critical.
EMG_NOT_APP	Emergency patches not applied. Critical.
ENABLED_REMOVED	Patches which can be enabled but are not enabled. Major.
GEN_NOT_APP	General patches not applied. (No severity)
LTD_NOT_APP	Limited patches not applied. (No severity)
OBS_NOT_REMOVED	Obsolete patches not removed. Major.
OBE_NOT_REMOVED	Obsolete emergency patches not removed. Critical.
REMOVED_PATCHES	Removed patches when are not category OBS, OBE, or DBG. (No severity)

NPM Logs/Faults available in Succession

Log/Fault	Description
PATCH_ONHOLD	Patches on hold. Minor.
DEVICE_ONHOLD	Devices on hold. Minor.

CS2000 Core Manager--available logs/faults for Succession

The following table lists the CS2000 Core Manager Logs/Faults available in Succession.

The CS 2000 Core Manager supports SCC2 or NT STD formatted logs through SDM functionality, or it can be supported through IEMS. For details on the IEMS interface, refer to the section in this document titled “SN07 IEMS Functionality.” For details on the faults themselves, refer to the Fault Management section of CS 2000 FCAPS documentation, NN10082-911 and NN10275-909, *Succession Fault Management Log Reference*.

CS2000 Core Manager Logs/Faults available in Succession

Log/Fault	Description
Network Element: CS2000 Core Manager	
	For details on previously existing Logs/Faults, refer to the SDM15 release of NTP 297-5051-840.
SDM267	Indicates a change in the condition of a CBM link
SDM300	The connection from the Preside CS200 Core Manager to the CM or operating company LAN server(s) is down.
SDM301	The maintenance system detects the logical volume mirroring status.
SDM302	Use of a system resource exceeds the threshold. Associated with log SDM602.
SDM303	A process has failed more than 3 times in a day, or some other application fault has occurred. Reports an application alarm condition where action is required. Associated with log SDM603 which indicates a clearing of the alarm. CR Q00537118 and CR Q00600912 also impact this log for consistent formatting changes.
SDM304	Log Delivery application has failed to reconnect to a device.
SDM305	A problem exists with DTH commissioning. The log indicates which device and suggests a recommended action. Associated with a Minor alarm.
SDM306	Table access software versions on the CM side and the SDM side are not compatible. Associated with a Minor alarm.
SDM307	Indicates trouble with the SDMCI. The connection to the CM was lost more than 3 times. Check the telnet port.
SDM308	An I-tape or S-tape backup has failed.
SDM309	Fault detected on HW device or user took HW device OOS.

CS2000 Core Manager Logs/Faults available in Succession

Log/Fault	Description
SDM310	System found a pending transaction at startup time. Check the audit log to find out which command was involved. Rollback of the transaction was successful. Use the SDMdbAdmin tool to sync CM and SDM again. Associated with a Minor alarm.
SDM311	System found a pending transaction at startup time. Check the audit log to find out which command was involved. Rollback of the transaction was NOT successful. Use the SDMdbAdmin tool to sync CM and SDM again. Associated with a Major alarm.
SDM312	Postprocessing of a command failed. The transaction was rolled back. Use the SDMdbAdmin tool to sync CM and SDM again. Associated with a Minor alarm.
SDM313	Postprocessing of a command failed. The transaction was rolled back. Use the SDMdbAdmin tool to sync CM and SDM again. Associated with a Major alarm.
SDM314	Indicates two SDM link connections are physically crossed. Associated with Major alarm "Crossed Link."
SDM315	Corruption of file detected during data dictionary download.
SDM317	DCE subsystem has detected a problem.
SDM318	OM report failed to complete within one report interval. Associated with a Major alarm.
SDM321	Reports that a split-system upgrade is in progress. Associated with a Minor alarm.
SDM325	The connection to a network management component in a given domain has been lost. Log reports may be lost as a result.
SDM328	Indicates that the signal on receive/ transmit fibre to OC3 card is faulty or not present. Associated with Major alarm OC3 Card Fault.
SDM329	Indicates a probable link equipment malfunction. Associated with Minor alarm Minor Link Fault.
SDM332	Indicates the status of an unsuccessful SDM system audit. An INFO log.
SDM336	Indicates that a response to CBM 800 heartbeat is not received from the core. Associated with major alarm Core Heartbeat
SDM500	The SDM node control process has restarted.
SDM501	The node control process updated SDM run state to INSV.
SDM502	The node control process updated SDM run state to MANB. Logs SDM502-505 are included in the CS2000 Core Manager Log Delivery stream, but do not appear on the RMI.
SDM503	The node control process updated SDM run state to SYSB.
SDM504	The node control process updated SDM run state to ISTB.
SDM505	The node control process updated SDM run state to OFFL from MANB.
SDM550	An SDM Node Status Change has occurred. Modified in SN06 so that the log occurs in only one type of format and it no longer reports application state change events of OffL, ManB, and process starts.
SDM600	An SDM maintenance connection has been re-established.

CS2000 Core Manager Logs/Faults available in Succession

Log/Fault	Description
SDM601	Logical volume mirroring is re-established.
SDM602	A system resource is below the threshold.
SDM603	The SDM303 alarm has been cleared. Or a state change has occurred that does not require manual intervention to clear. With SN06, this log now reports application state change events of OffL, ManB, and process starts. CR Q00600912 also impacts this log for consistent formatting changes.
SDM604	CM had too little time to format log(s) and log(s) is/are lost.
SDM607	Internal CS 2000 Core Manager log; indicates when a process controller starts or restarts a process. The system does not send SDM607 to the OSS. You can see the SDM607 report from the remote maintenance interface (RMI), when logged onto the CS 2000 Core Manager.
SDM608	I-tape or S-tape process has completed.
SDM609	A hardware device has returned to the INSV state.
SDM614	Reports that the crossed link alarm associated with SDM314 is cleared.
SDM615	Log Thresholding is in effect for logs managed by exception application. Exception reports may be inaccurate
SDM616	An unauthorized connection attempt is detected by the Log Delivery application. The connection is refused.
SDM617	A DCE problem has been cleared.
SDM618	Logical volume /var is 98 percent full. Log files in /var/adm have been deleted.
SDM619	OM Access Service detected a corrupt OM group during an OM schema download.
SDM620	Reports current system performance data at set times.
SDM621	The split-system upgrade is finished.
SDM622	Max file size reached for a file device handled by GDD.
SDM625	The connection to a Network Management component in a given domain has been re-established.
SDM626	An info log generated whenever the OMDD application starts and it detects that the tuple number option has been changed since the last time the application was launched. The log is used to inform the OSS of the state change, which inherently signifies a change in the OMDD CSV files. The log will indicate the new (current) state as being either ACTIVATED or DISABLED.
SDM630	Indicates the SDM REX Test start and complete time. An INFO log.
SDM632	Indicates the status of a successful SDM system audit. An INFO log.
SDM633	A CBM info log that indicates a change in the condition of a CBM link.
SDM634	Indicates that the OC3 Card Fault alarm raised with SDM328 has been cleared.
SDM635	Indicates that the Minor Link Fault alarm raised with SDM329 has been cleared.
SDM636	Indicates that the heartbeat alarm raised with SDM336 has been cleared.

CS2000 Core Manager Logs/Faults available in Succession

Log/Fault	Description
SDM650	Link maintenance requests a report on a failed link maintenance action.
SDM700	Reports a Warm, Cold, or Reload restart or a norestartswact on the core.
SDM739	Indicates file transfers between the FTP Client and the CORE and to show user log-ons to the CORE.
SDMB logs (SDM billing)	
SDMB300	Memory allocation failed for SDM billing system.
SDMB310	Indicates a communication problem with the SDM Billing System.
SDMB315	A software-related problem has occurred.
SDMB316	A billing-related process has been manually killed.
SDMB320	A billing-backup problem affecting more than one file.
SDMB321	A billing-backup problem affecting one file.
SDMB350	The billing application has reached a death threshold (a process has died > 3 times < 1 minute apart) and there is a request to restart.
SDMB355	A disk-related problem has occurred, such as problems writing to disk (related to alarm DSKWR) or with disk utilization (related to alarm LODSK).
SDMB365	A new version of the billing application does not support a stream format on an active stream present in previous load.
SDMB367	Value has been set on a trappable MIB object.
SDMB370	CDR-to-BAF conversion encountered a problem that prevented it from converting CDR to BAF; BAF record lost.
SDMB375	Generated when a problem occurs during the transfer of a file to the data processing management system (DPMS). It may be problems and alarms related to FTP, RTB (real-time billing), AFT (automatic file transfer), or Secure File Transfer Protocol.
SDMB380	The file transfer mode for the stream indicated has an invalid value.
SDMB390	A schedule-related problem has occurred.
SDMB400	Generated every hour for every active stream to list all current active alarms.
SDMB530	The configuration or status of a stream has changed.
SDMB531	Configuration for backup volumes was changed correctly.
SDMB550	The billing application has shut down.
SDMB600	Generic information for the overall SDM Billing System.
SDMB610	A communications-related problem has been resolved.
SDMB620	A backup-related problem has been resolved.
SDMB621	A new backup file is being started.
SDMB625	Recovery has started on a backup file.

CS2000 Core Manager Logs/Faults available in Succession

Log/Fault	Description
SDMB650	The billing application is restarting one or more processes.
SDMB655	Indicates file state changes and disk utilization, OR disk utilization has dropped below a threshold, OR the billing application cannot move a file to the closeSentProcessed directory.
SDMB665	A software problem on the CM prevents the downloading (synch) of FLEXCDR data at the SDM.
SDMB675	An information log that identifies a event related to the transfer of billing files. An event may be a normal operation, a problem, or the resolution of a problem related to SDMB375.
SDMB680	Information not related to the file system or creating links needs to be communicated to the customer.
SDMB690	Indicates that an SBAIF alarm and the fault that caused it have cleared.
SDMB691	Generates when a problem occurs with the scheduled transfer of billing files and when that fault clears. It also generates when a file transfer schedule is manually deactivated or deleted.
SDMB820	A backup has hit a threshold.

Passport 8600--available traps/faults for Succession

Passport 8600 supports SCC2 format through SDM functionality and the IEMS interface. For details on the IEMS interface, refer to the section in this document titled "SN07 IEMS Functionality." The following table lists the Passport 8600 traps available in Succession.

Passport 8600 Traps available in Succession

Trap Name	Description
Network Element: Passport 8600	
Faults from the Passport 8600 are provided via an SNMP Northbound interface that is provided on the Passport 8600 itself.	
rcCardDown	The SNMPv2 entity, acting in an agent role, has detected that the rcCardOperStatus object for one of its cards is about to transition into the down state.
rcCardUp	The SNMPv2 entity, acting in an agent role, has detected that the rcCardOperStatus object for one of its cards is about to transition into the up state.
rcErrorNotification	The SNMPv2 entity, acting in an agent role, has detected that an error condition has occurred.
rcStpNewRoot	The SNMPv2 entity, acting in an agent role, has detected the Spanning Tree Protocol has declared the device to be the new root of the spanning tree.

Passport 8600 Traps available in Succession

Trap Name	Description
rcStpTopologyChange	The SNMPv2 entity, acting in an agent role, has detected the Spanning Tree Protocol has gone due to a topology change event.
rcChasPowerSupplyDown	The SNMPv2 entity, acting in an agent role, has detected that the rcChasPowerSupplyOperStatus object for one of its power supply units is about to transition into the down state.
rcChasFanDown	The SNMPv2 entity, acting in an agent role, has detected that the rcChasFanOperStatus object for one of its power supply units is about to transition into the down state.
rcLinkOscillation	The SNMPv2 entity, acting in an agent role, has detected an excessive number of link state transitions on the specified port.
rcMacViolation	The SNMPv2 entity, acting in an agent role, has received a PDU with an invalid source MAC address.
rcSonetTrap	The SNMPv2 entity, acting in an agent role, has detected a change of status on a Sonet port.
rc2kCardDown	The SNMPv2 entity, acting in an agent role, has detected that the rcCardOperStatus object for one of its cards is about to transition into the down state.
rc2kCardUp	The SNMPv2 entity, acting in an agent role, has detected that the rcCardOperStatus object for one of its cards is about to transition into the up state.
rc2kTemperature	The SNMPv2 entity, acting in an agent role, has detected the chassis is over-heating.
rcChasPowerSupplyUp	The SNMPv2 entity, acting in an agent role, has detected that the rcChasPowerSupplyOperStatus object for one of its power supply units is about to transition into the up state.
rc2kTemperature	The SNMPv2 entity, acting in an agent role, has detected the chassis is over-heating.
rcChasPowerSupplyUp	The SNMPv2 entity, acting in an agent role, has detected that the rcChasPowerSupplyOperStatus object for one of its power supply unit is about to transition into the up state.
rc2kAtmPvcLinkStateChange	The SNMPv2 entity, acting in an agent role, has detected that the rc2kAtmPvcOamVcStatus object for one of the PVCs is about to transition into different state, either from up to down or from down to up.
rcStpTCN	The SNMPv2 entity, acting in an agent role, has detected the Spanning Tree Protocol has gone due a topology change event.
rcSmlt1stLinkUp (see note)	The split MLT link has gone from down to up.
rcSmlt1stLinkDown (see note)	The split MLT link has gone from up to down.
rcSmltLinkUp (see note)	The split SMLT link is up.
rcSmltLinkDown (see note)	The split SMLT link is down.

Passport 8600 Traps available in Succession

Trap Name	Description
rcChasFanUp	The SNMPv2 entity, acting in an agent role, has detected that the rcChasFanOperStatus object for one of its power supply unit is about to transition into the up state.
rcPasswordChange	The SNMPv2 entity, acting in an agent role, has detected that the one of the cli password is changed.
rcEmError	The SNMPv2 entity, acting in an agent role, represents an Em-mode error caused by misconfiguration.
rcStpTCN	The SNMPv2 entity, acting in an agent role, has detected a Spanning Tree topology change notification.
rcPCMCIACardRemoved	The SNMPv2 entity, acting in an agent role, has detected that the PCMCIA card has been removed.
rcSmartCpldTimerFired	The SNMPv2 entity, acting in an agent role, has detected that the CPU is busy; so the chassis task was not run. Card is taken offline due to smart-cpld timer.
rcCardCpldNotUpDate	The SNMPv2 entity, acting in an agent role, has detected that the revision number of an I/O card needs updating. SMLT for single CP feature is not enabled the slot.
rcIgapLogFileFull	The SNMPv2 entity, acting in an agent role, has detected that the log file for IGAP Radius time logs has exceeded the maximum limit.
rcCpLimitShutDown	The SNMPv2 entity, acting in an agent role, has detected that the link down has occurred due to excessive control frames.
rcSshServerEnabled	The SNMPv2 entity, acting in an agent role, has detected that the SSH server is enabled.
rcSshServerDisabled	The SNMPv2 entity, acting in an agent role, has detected that the SSH server is disabled.
rcSshSessionLogin	The SNMPv2 entity, acting in an agent role, has detected that there is a new SSH session login.
rcSshSessionLogout	The SNMPv2 entity, acting in an agent role, has detected that the SSH session logout has occurred.
rcSshUnauthorizedAccess	The SNMPv2 entity, acting in an agent role, has detected an unauthorized attempt to login from host has occurred.
rcHaCpuState	The SNMPv2 entity, acting in an agent role, indicates the state of HA-CPU.
rcInsufficientMemory	The SNMPv2 entity, acting in agent role, has detected that the recommended memory for CPU blade is 256MB. It is available through the Nortel Networks upgrade kit.
rcSaveConfigAction	This SNMPv2 entity, acting in an agent role, has detected that the switch is in the process of saving the runtime or boot configuration
rcLoopDetectOnPort	This SNMPv2 entity, acting in an agent role, has detected that a loop has been detected on a port. The vlan on that port will be disabled.
vrrpTrapStateTransition	This SNMPv2 entity, acting in an agent role, has detected that a state transition has occurred on VRRP interface.

Passport 8600 Traps available in Succession

Trap Name	Description
ospfVirtIfStateChange	This SNMPv2 entity, acting in an agent role, indicates a change in the state of an OSPF virtual interface.
ospfNbrStateChange	This SNMPv2 entity, acting in an agent role, indicates change in the state of a non-virtual OSPF neighbor.
ospfVirtNbrStateChange	This SNMPv2 entity, acting in an agent role, indicates change in the state of an OSPF virtual neighbor.
ospfIfConfigError	This SNMPv2 entity, acting in an agent role, indicates that configuration parameters conflict with a router's configuration.
ospfVirtIfConfigError (see note)	This SNMPv2 entity, acting in an agent role, indicates that configuration parameters conflict with a router's configuration.
ospfIfAuthFailure	This SNMP v2 entity, acting in an agent role, indicates that an authentication key or authentication type conflicts with a router's authentication key or authentication type.
ospfVirtIfAuthFailure	This SNMPv2 entity, acting in an agent role, indicates that an authentication key or authentication type conflicts with a router's authentication key or authentication type.
ospfIfStateChange	This SNMPv2 entity, acting in an agent role, indicates a change in the state of an interface.
risingAlarm	This SNMPv2 entity, acting in an agent role, indicates that the value of a variable has risen above the threshold.
fallingAlarm	This SNMPv2 entity, acting in an agent role, indicates that the value of a variable has fallen under the threshold.
Cold Start Trap	This SNMPv2 entity is generated by poll after a cold start.
Warm Start Trap	This SNMPv2 entity is generated by poll after a warm start.
Accumulated Authentication Failure Trap	This SNMPv2 entity, acting in an agent role, indicates repeated authentication failure traps.
Trap raised by idi_PP8600.pol to indicate Device-Rediscovery	This trap indicates that a device re-discovery has been initiated.
OSPF v2 trap	This trap indicates a variable ospfAddressLessIf (var(2)) takes the value 0 on interfaces with IP addresses and the corresponding value of ifIndex for interfaces having no IP address.
See note: This trap is only available on Passport 8600 devices that are running release 3.2 software and up	

See the design description of feature A00002920, which supports and generates Passport 8600 logs that are received by the PLS application. The design description of this feature is in the Feature Deltas section of the SN06.2 OSS Guide.

PVG Logs/Faults in Succession

For Logs/Faults available in Succession for PVG, refer to NTP 241-5701-500, *Passport 6400, 7400, 15000, 20000 Alarms Guide*.

Preside Multiservice Data Manager logs/faults

For logs and faults information for the Preside Multiservice Data Manager (MDM), refer to the following documents: 241-6001-501, *Preside MDM Proxy Alarms Reference Guide*, and 241-6001-011, *Preside MDM Advisor User Guide*.

QCA Logs/Faults in Succession

The following table lists the QCA Faults/Alarms available through Succession. QCA supports SCC2 or NT STD formatted logs through SDM functionality, or it can be supported through IEMS. For details on the IEMS interface, refer to the section in this document titled “SN07 IEMS Functionality.” For details on the logs, refer to the Fault section of the FCAPS documentation on CS 2000, NN10083-911 and NN10275-909, *Succession Fault Management Log Reference*.

QCA Logs/Faults in Succession

Log/Fault	Description
QCA400	Warning log. Properties file (properties/qca.properties) not available. QCA is starting with default settings.
QCA401	Warning log. portNumber property not in properties/qca.properties. QCA is starting with default port number of 20000.
QCA402	Warning log. portNumber property in properties/qca.properties not in range. QCA is starting with default port number of 20000.
QCA403	Warning log. PortNumber property in properties/qca.properties could not be used. QCA is starting with default port number of 20000.
QCA404	Warning log. MaxFileSize property not in properties/qca.properties. QCA is starting with default maximum file size of 1 MByte
QCA405	Warning log. MaxFileSize property in properties/qca.properties not in range. QCA is starting with default maximum file size of 1 MByte
QCA406	Warning log. MaxFileSize property in properties/qca.properties could not be used. QCA is starting with default maximum file size of 1 MByte.
QCA407	Warning log. MaxFileTime property not in properties/qca.properties. QCA is starting with default maximum file time of 15 minutes
QCA408	Warning log. MaxFileTime property in properties/qca.properties not in range. QCA is starting with default maximum file time of 15 minutes.

QCA Logs/Faults in Succession

Log/Fault	Description
QCA409	Warning log. MaxFileTime property in properties/qca.properties could not be used. QCA is starting with default maximum file time of 15 minutes.
QCA410	Warning log. RetainFileTime property not in properties/qca.properties. QCA is starting with default retain file time of 5 days.
QCA411	Warning log. RetainFileTime property in properties/qca.properties not in range. QCA is starting with default retain file time of 5 day.
QCA412	Warning log. RetainFileTime property in properties/qca.properties could not be used. QCA is starting with default retain file time of 5 days
QCA413	Warning log. recycleToD property not in properties/qca.properties. QCA is starting with default recycle hour of day of 0.
QCA414	Warning log. recycleToD property in properties/qca.properties not in range. QCA is starting with default recycle hour of day of 0.
QCA415	Warning log. recycleToD property in properties/qca.properties could not be used. QCA is starting with default recycle hour of day of 0.
QCA416	Warning log. fileExt property not in properties/qca.properties. QCA is starting with default file extension of xml.
QCA417	Warning log. oldFileCompression property not in properties/qca.properties. QCA is starting with default value of true.
QCA418	Warning log. oldFileCompression property in properties/qca.properties could not be used. QCA is starting with default value of true.
QCA419	Warning log. closedFileCompression property not in properties/qca.properties. QCA is starting with default value of true.
QCA420	Warning log. closedFileCompression property in properties/qca.properties could not be used. QCA is starting with default value of true.
QCA421	Warning log. nodeName property not in properties/qca.properties. QCA is starting with default value of QCA.
QCA422	Warning log. File Recovery: removing closed file retention directory: <i>directory</i> as it is older than x days.
QCA423	Warning log. File Recovery: file <i>file name</i> found in active directory. This could indicate that the QCA failed. Please check debug logs.
QCA300	Critical. File handler or server socket could not be started.
QCA301	No priority. Out of sequence QoS record received.
QCA302	No priority. Problem processing binary QoS record.
QCA303	Minor. QoS Record received with Unsupported Length.
QCA304	Major. 10 sequential QoS Records received with Unsupported Length.
QCA305	Minor. QoS Record received with Unsupported Version.
QCA306	Major. 10 sequential QoS Records received with Unsupported Version.

QCA Logs/Faults in Succession

Log/Fault	Description
QCA307	Major. The binary QoS Record header could not be processed.
QCA308	Major. QoS Record received with Unrecognized Message type.
QCA309	Critical. Disk space shortage, local disk requires more free space. Disk Space is below 100Mb.
QCA310	Major. Disk Space is starting to run seriously low. This means that the available space is below 500Mb.
QCA311	Minor. Disk space is below the minimum threshold. Initially set at 1Gb.
QCA312	Warning. A request to get a new file name has failed, there are either 10000 files with the same name or the new file can not be created.
QCA313	Warning. The QCA has failed to write the footer information to the active file whilst attempting to close, the file could have now been compressed.
QCA314	Major. The active file did not exist when trying to write to it. Attempt to get new file then failed. Further failures will result in the QCA being shutdown.
QCA315	Critical. Attempting to write data to file, the active file does not exist. Try to get new file. This has failed. Sleep The thread and try and get new file again.This also failed. No file to write to, QCA will shutdown.
QCA316	Critical. The XML writer and the file all seem well, unfortunately the file cannot be accessed at in either the first or second attempt, serious problem with file IO. QCA will shutdown.
QCA317	Critical. The QCA has encountered inconsistent errors when building the directory structure for old files, old files may have been deleted and directory locked. The error should never appear, as it is the last resort.
QCA318	Major. Attempt to rename the active file from the active directory to the today directory has failed. Serious error, but no loss of data immediately. Files can be moved by hand if required.
QCA319	Critical. Could not create new active file. Data is being lost.QCA must shut down.
QCA320	Major. Attempt to compress an old active file has failed.
QCA321	Major. Failed to rename directories on the Recycle_day proc. This is where all files are moved along a level and the last gets deleted.
QCA600	Info log. Connection closed.
QCA601	Info log. Client has stopped sending records with unsupported length (clear for QCA 303).
QCA602	Info log. Client has stopped sending records with unsupported version (clear for QCA 305).
QCA603	Info log. Critical disk space issue cleared (clear for QCA 309).
QCA604	Info log. Major disk space issue cleared (clear for QCA 310).
QCA605	Info log. Minor disk space issue cleared (clear for QCA 311).

UAS--available logs/faults for Succession

UAS faults are sent from the UAS to the UAS EM and are then sent northbound via CORBA. UAS alarm information can also be viewed from the

alarm browser that resides with the CS2000 Management Tools. For details on the CORBA protocol/format and the logs, refer to the Fault Management section of UAS FCAPS documentation, NN10073-911 and NN10275-909, *Succession Fault Management Log Reference*.

Refer to the New and Changed section of this document to see if there are SN07 changes in UAS logs and faults.

UAS Logs/Faults available in Succession

Network Element: UAS

UAS faults are sent from the UAS to the UAS EM and are then sent northbound via CORBA. UAS alarm information can also be viewed from the alarm browser that resides with the CS2000 Management Tools.

Fault	Description	For details on these Logs/Faults, refer to the Fault section of documentation for UAS, NN10073-911.
ATM Alarms	AS001 An ATM interface card is missing from the slot.	
	AS002 There is a different ATM card module inserted in the chassis slot.	
	AS003 The ATM card has detected an H.110 bus failure.	
	AP001 The ATM interface port has had a loss of connectivity.	

Ethernet Interface Alarms

	EI_LINK_DOWN; Critical. "Callp was unable to initialize interface to hardware. Check configuration." Clear with a reboot.
88065 (366)	EI_LINK_DOWN; Critical. "Link on host network interface is down."

Call Agent Connection Alarms

8193 (301)	THREAD_DEATH_ALARM; Critical. Either the "incoming" or "outgoing" messaging thread is unable to restart because of some undetermined problem. Clears at the next startup of call processing application.

UAS Logs/Faults available in Succession

- 8194 (302) UDP_INIT_FAIL_ALARM; Critical. This alarm can be raised for various reasons during initialization. The audio server is unable to communicate with the call server. The condition clears at the next startup of the call processing application. Possible reasons and corrective actions follow:
- MGC IP address is not datafilled because the uas.conf file either does not exist, is unreadable, or is missing an entry for "CallAgentIPAddress." Fix the configuration file.
- MGC IP address is not valid because the call agent IP address obtained from the config file is not valid. Fix the IP address in the config file.
- Bad return code from WSASStartup because an attempt was made to initialize the Windows socket library, but failed due to a version mismatch. Report the full text of the alarm to the support group.
- WinSock version is not 1.1 as expected because an attempt was made to initialize the Windows socket library, but failed due to a version mismatch. Report the full text of the alarm to the support group.
- Unable to create socket; an attempt was made to create a UDP communications socket, but failed. Report the full text of the alarm to the support group.
- Unable to bind client name to socket; an attempt was made to bind the communications socket to the port specified in the uas.conf configuration file. Another callp program may already be running. Make sure that another callp program is not running.
- Unable to connect to call agent socket; an attempt was made to associate the communications socket with the address of the call agent, but failed. Report the full text of the alarm to the support group.
- 8195 (800) SOCKET_ERROR_ALARM; Warning. UDP Socket errors are being detected.
- 8196 (801) RETRANS_ALARM Warning, Retransmissions are being detected.
- 8197 (802) EXCEED_MAX_RETRANS_ALARM; Warning, Call_Agent_Connection, The number of retransmissions has now exceeded the maximum number of retransmissions.

System Alarms

- 6154 (379) NODE_NO_CARDS_INSTALLED; Critical. "There are no NMS cards installed."

Call Engine Alarms -- associated with call processing or maintenance state machines.

- 12290 (303) CALLP_THREAD_NOT_RESTARTED; Major. The call processing software thread associated with <endpointId> died due to an unhandled software error, and was not restarted because it died too quickly after the previous start. Escalate this issue to Nortel support, providing any other logs that might have occurred. Clears at the next startup of the call processing application.
- 12291 (304) CALLP_CFG_INVALID; Critical. The resource configuration for endpointId in C:\uas\etc\rm.resources is not valid. Correct the configuration for endpointId in the rm.resources file, and restart the call processing application. Clears at the next startup of the call processing application.
- 12295 (305) AUDIO_VFSDIR_NOT_SET; Critical. The environment variable VFSDIR is not set to the home directory of the VFS hierarchy. Verify that the VFS software is correctly installed. Clears at the next startup of the call processing application.

UAS Logs/Faults available in Succession

12296 (306) CALLP_CONFIG_PROB; Critical. A serious configuration problem has been detected. The Audio Server is unable to initialize. A configuration file is probably in error. Look for an error log to determine the exact cause of the problem. Clears at the next startup of the call processing application.

12297 (307) CALLP_NO_CARDS_AVAILABLE Call_Engine There are no NMS cards available for use.

12298 (308) CALLP_AUDIO_RESYNC_FAILURE Call_Engine Failed to communicate with aliasServer. Check audio installation and aliasServer.

AG4000 Service-level Alarms -- conditions that affect the service-level functionality of the AG4000 card in an ATM system.

14337 (315) AG_GENERIC_ALARM; Major. An attempt was made to load software onto the card and to start the card but failed. Stop the applications, reseal the card and then restart the applications. If the problem persists, contact the Nortel support group. Clears when the applications are restarted and the operation succeeds.

14338 (315) AG_SURPRISE_EXTRACTION Improper extraction of AG4000 card in slot <x> of the SAM 16 chassis.

14339 (316) AG_CARD_DISABLED AG4000 card in slot <x> disabled until next application restart of the UAS.

NodeMtc Alarms -- generated by the callp application if the NMS CT daemon and NMS Clock Fallback Manager services fail to stop or start successfully.

20481 (322) CTDAEMON_SERVICE_FAILURE; Critical. Either the NMS CT daemon service is not installed as a service, or it is in a service state where it cannot accept start and stop service requests. Make sure that the NMS CT daemon service is installed. Stop, uninstall and re-install the service if need be. Clears once the NMS CT daemon service has been successfully started or stopped.

20482 (323) CFBM_SERVICE_FAILURE; Critical. When the NMS CT daemon service is started, it should automatically start the NMS Clock Fallback Manager service (The NMS Clock Fallback Manager service is not automatically stopping the NMS CT daemon service.). If the NMS Clock Fallback Manager service is not automatically started for some reason, either the NMS Clock Fallback Manager service is not installed as a service for it to be started or stopped, or it is in a service state where it cannot accept start and stop service requests. Make sure that the NMS Clock Fallback Manager service is installed. Stop, uninstall and re-install the service if need be. Clears once the NMS Clock Fallback Manager service has been successfully started or stopped.

20483 (324) SERVICE_FAILURE NodeMtc The <x> service could not be _____.

ConfigMgr Alarms

UAS Logs/Faults available in Succession

26625 CM_CONFIG_ERROR; Critical. This alarm can be raised for various reasons during initialization. A serious configuration problem has been detected. The Audio Server is unable to initialize. A configuration file is probably in error. Look for an error log to determine the exact cause of the problem. The condition clears after the configuration problem is fixed. Possible reasons and corrective actions follow:

The specified configuration template files are missing from c:\uas\cfg\templates. Restore the missing files.

The specified configuration file is missing. Restore the missing file.

ConfigMgr was unable to update the uas_pending.conf file. The file may have had incorrect permissions, or the disk is full. Check file permissions. Check to see if the disk is full.

ConfigMgr attempted to create a kernel object but encountered an error. Contact the support group.

ConfigMgr was unable to copy a file. The file may have had incorrect permissions, or the disk is full. Look at logs to determine which file caused the problem. Check file permissions. Check to see if the disk is full.

ConfigMgr could not automatically determine how many AG cards there are in the system. The number of AG cards could not be determined. Ensure that the NMS locate utility is present and is working properly.

ConfigMgr could not update the uas.conf file with the number of AG cards. Check file permissions. Check to see if the disk is full.

A configuration parameter is missing or has an invalid value. Look at logs to determine which configuration parameters are missing.

ConfigMgr attempted to operate on a kernel object but encountered an error. Contact the support group.

CG6000 Service-level Alarms

30721 CG_GENERIC_ALARM; Major. An attempt was made to load software onto the card and to start the card. The attempt failed. Stop the applications, reseal the card and then restart the applications. If the problem persists, contact the Nortel support group. Clears when the applications are restarted and the operation succeeds.

30722 CG_ETHERNET_CONN_ALARM Critical, CG6000 %d failed ethernet connection(s) on (318) CG6000 card in slot %d.

30723 CG_SURPRISE_EXTRACTION Major, CG6000 Improper extraction of CG6000 card in (319) slot %d.

30724 CG_CARD_DISABLED Major, CG6000 card in slot %d disabled until next application (320) restart.

30725 CG_CLOCKING_ALARM Major, CG6000 primary clock source is %s and secondary clock (321) source is %s in slot %d.

UAS Logs/Faults available in Succession

ATM Service Alarms--The ATM_MISSING_CARD alarm and ATM_MISMATCH_CARD alarm are raised in situations where provisioned VCs exist for a given ATM Card in a given slot, and that card has either been removed, is inoperable, or has been replaced with another ATM card.

34817 ATM_MISSING_CARD; Critical. Either the ATM card has been pulled or it has experienced a catastrophic failure and is unable to register with the cPCI chassis. A working ATM card must be inserted into the slot. Alternatively, all the VCs may be deleted which are associated with the missing card. Clears at the next start of the call processing application.

34818 ATM_MISMATCH_CARD; Critical. The ATM card has been replaced with a different model ATM card. Place the correct ATM card back in the slot which originally contained the S007 card. Alternatively, all the VCs may be deleted which are associated with the mismatched card. Clears at the next start of the call processing application.

ATM Port Alarms

34913 ATM_PORT_LOC; Critical. The fiber connecting the ATM port to the network has either been unplugged or damaged. Plug the fiber back in, or replace it if it was damaged. Clears when the signal on the fiber is back to normal.

34819 ATM_H110_FAILURE Critical ATM_Service The ATM card detected an H.110 bus failure.
(328) This alarm may be caused by a bad AG driving the H.110 bus clock or more than one card is trying to drive the clock on the bus. Clears at the next start of the call processing application.

34820 ATM_OUTDATED_FIRMWARE Major ATM_Service The ATM card in slot%d has
(329) outdated firmware ver.:%s recommended version:%s. Please run the ATMFirmware command to upgrade the firmware. This alarm is seen if the ATM card has outdated firmware. Clears at the next start of the call processing application, after the firmware has been upgraded.

34821 ATM_FIRMWARE_NON_UPGRADABLE Major ATM_Service The ATM card in slot %d
(330) has outdated firmware ver.:%s. This firmware needs to be manually updated. Please load the card with a firmware version which is 2.1.0 or later. This alarm is seen when the firmware on the ATM card is outdated and can not be automatically upgraded. A newer firmware load needs to be transfer to the card manually. Clears at the next start of the call processing application.

34822 ATM_HW_API_TOO_MANY_FAILURES Critical ATM_Service The number of
(331) consecutive API calls failures to the ATM card in slot %d, has exceeded the threshold of %d. The card is being taken out of service. Clears at the next start of the call processing application.

Carrier Alarms

40961 CARRIER_CLR_ALARM. Indicates that a carrier alarm cleared.

40962 CARRIER_RAISE_ALARM; Critical. One of these carrier alarms is raised: RAI, AIS, LOF, LOS, E1 LOMFS, or E1 16 AIS. Based on the different alarm types, check T1/E1 carrier for the cause. Clears when the CARRIER_CLR_ALARM event is received.

Activity Manager Alarms

53249 (336) AM_COLD_START_NOT_SENT_CEM Activity_Manager.

53250 (337) AM_COLD_START_NOT_SENT_SWACT Activity_Manager.

UAS Logs/Faults available in Succession

- 53251 (338) AM_SWACT_FAILURE Critical Activity_Manager.
53252 (339) AM_ERM_FAILURE Critical Activity_Manager.
53253 (340) AM_ED SOCK_FAILURE Major Activity_Manager.
53254 (341) AM_CONFIG_ERROR_NOFILE Minor Activity_Manager.
53255 (342) AM_DATAFILE_ERROR_NOFILE Critical Activity_Manager.

Power Supply, Disk, and Fan Maintenance Alarms

- 61441 (345) COOLING_SYSTEM_RAISE_ALARM; Major/Critical. In the case of a cooling fault, this is due to a high temperature at air intake to the chassis. In the case of a Cooling alarm, it is due to an extremely high temperature at air intake to the chassis. Check air flow and cooling equipment. Clears upon receipt of a GlobalServer Equipment fault tag with a 'cleared' alarm condition.
- 59393 (344) POWER_SUPPLY_RAISE_ALARM; Major. HA Monitor received a Power Supply Fault Tag, and informed the PsFanMtc subsystem. This could be due to a faulty power supply system in the chassis that has gone down. Clears upon receipt of a Power Supply Fault tag with the "Power Good" bit set.
- 59393 POWER_SUPPLY_RAISE_ALARM; Major. HA Monitor received a Fan Fault Tag, and informed the PsFanMtc subsystem. This could be due to a faulty fan in the chassis that has gone down. Clears upon receipt of a Fan Fault tag with the "Fan Fault" bit unset.
- 63489 (346) DISKDRIVE_RAISE_ALARM Critical Hard_Disk ALARM: Problem detected on Domain %s %s disk drive, chassis peripheral %d, due to %s.

I/O Card Base-level Alarms

- 65537 (309) CD_SURPRISE_SLOT_POWER_OFF; Major. A surprise power off on a slot can be caused by a chassis hardware problem or by a software error. The problem may clear up after a reboot. Stop the applications and perform a reboot. If the problem does not clear up, then you may be able to workaroud the problem by moving the card to another slot. Refer to the appropriate card maintenance and configuration procedures. The alarm clears when power is restored to the slot.
- 65538 (310) CD_SURPRISE_CARD_EXTRACTION; Major. A card was improperly extracted from the specified slot. The applications will need to be restarted. Perform these actions: 1) stop the applications 2) reinsert the card 3) restart the applications. The alarm clears when the card is reinserted and the applications are restarted.
- 65539 (311) CD_LOAD_SCRIPT_FAILURE; Major. An attempt was made to load firmware onto the card in the specified slot. Stop the applications, reseal the card, and restart the applications. If the problem persists, then contact the Nortel support group. If reseating the card fixes the problem, then the alarm will clear when the applications are restarted.
- 65540 (312) CD_SLOT_VERIFY_SCRIPT_FAILURE; Major. An attempt was made to verify that the card contains the correct firmware version. Stop the applications, reseal the card, and restart the applications. If the problem persists, then contact the Nortel support group. If reseating the card fixes the problem, then the alarm will clear when the applications are restarted.

UAS Logs/Faults available in Succession

65541 (313) CD_GENERIC_CARD_ALARM; Major. A problem occurred with the card in the specified slot. A brief description of the problem is supplied. No action required; no clear condition.

Shelf Controller Alarms

67585 (309) SC_SURPRISE_SLOT_POWER_OFF Major Shelf Controller Surprise power off on slot %d.

67586 (310) SC_SURPRISE_CARD_EXTRACTION Major Shelf Controller Surprise card extraction on.

67587 (311) SC_LOAD_SCRIPT_FAILURE Major Shelf Controller Firmware load script failure on card in slot %d.

67588 (312) SC_SLOT_VERIFY_SCRIPT_FAILURE Major Shelf Controller Verify script failure on card in slot %d.

67589 (313) SC_GENERIC_CARD_ALARM Major Shelf Controller Problem with card in slot %d:

Hot Swap Controller Alarms

69633 (309) HS_SURPRISE_SLOT_POWER_OFF Major Hot Swap Controller Surprise power off on slot %d.

69634 (310) HS_SURPRISE_CARD_EXTRACTION Major Hot Swap Controller Surprise card extraction on slot %d.

69635 (311) HS_LOAD_SCRIPT_FAILURE Major Hot Swap Controller Firmware load script failure on card in slot %d.

69636 (312) HS_SLOT_VERIFY_SCRIPT_FAILURE Major Hot Swap Controller Verify script failure on card in slot %d.

69637 (313) HS_GENERIC_CARD_ALARM Major Hot Swap Controller Problem with card in slot %d:

SCSI Controller Base-level Alarms

71681 (309) SS_SURPRISE_SLOT_POWER_OFF; Major. A surprise power off on a slot can be caused by a chassis hardware problem or by a software error. The problem may clear up after a reboot. Stop the applications and perform a reboot. If the problem does not clear up, then you may be able to workaroud the problem by moving the card to another slot. Refer to the appropriate card maintenance and configuration procedures. The alarm clears when power is restored to the slot.

71682 (310) SS_SURPRISE_CARD_EXTRACTION; Major. A card was improperly extracted from the specified slot. The applications will need to be restarted. Perform these actions: 1) stop the applications 2) reinsert the card 3) restart the applications. The alarm clears when the card is reinserted and the applications are restarted.

71683 (311) SS_LOAD_SCRIPT_FAILURE Major SCSI_Controller Firmware load script failure on card in slot %d.

71684 (312) SS_SLOT_VERIFY_SCRIPT_FAILURE Major SCSI_Controller Verify script failure on card in slot %d.

71685 (313) SS_GENERIC_CARD_ALARM Major SCSI_Controller Problem with card in slot %d:

Chassis Even Manager Alarms

UAS Logs/Faults available in Succession

75783 (311) SS_LOAD_SCRIPT_FAILURE Major SCSI_Controller Firmware load script failure on card in slot %d.

75784 (312) SS_SLOT_VERIFY_SCRIPT_FAILURE Major SCSI_Controller Verify script failure on card in slot %d.

75785 (313) SS_GENERIC_CARD_ALARM Major SCSI_Controller Problem with card in slot %d:

Local Resource Manager Alarms

81921 (350) LRM_CPU_C Critical, LocalResourceManager cpu_overload_critical, The CPU is overloaded, critical alarm.

81922 (351) LRM_CPU_M Major, LocalResourceManager cpu_overload_major, The CPU is overloaded major alarm.

81923 (352) LRM_MEM_C Critical, LocalResourceManager, mem_usage_high_critical, Memory usage is high.

81924 (353) LRM_MEM_M Major, LocalResourceManager mem_usage_high_major, Memory usage is high

81925 (354) LRM_DISK_C Critical, LocalResourceManager disk_usage_critical, Disk usage is high.

81926 (355) LRM_DISK_M Major, LocalResourceManager disk_usage_major, Disk usage is high but less severe than critical where space is exhausted.

81927 (356) LRM_CONFIG_FILE_ERR Minor, LocalResourceManager, lrm_config_fileerror

Program Manager Alarms

83971 (357) c_FAILED_MALLOC Critical ProgramManager.

83974 (358) c_BAD_PARSE Critical ProgramManager.

83987 (359) c_BAD_FORK Critical ProgramManager.

83989 (360) c_BAD_EXEC Critical ProgramManager.

83998 (361) c_CRIT_DEATH Critical ProgramManager.

83999 (362) c_MAX_RETRIES Critical ProgramManager

84000 (363) c_MAX_RETRIES_NO_RESTART Minor ProgramManager.

84009 (364) c_FIFO_ERROR Critical ProgramManager.

84039 (365) c_RSM_FAILED_CONNECT Critical ProgramManager.

Clock Manager Alarms

90113 (367) PRIMARY_CLOCK_DOWN_ALARM Minor ClockManager Primary Clock Driver trunk %d on board %d is down.

90114 (368) SECONDARY_CLOCK_DOWN_ALARM Minor ClockManager Secondary Clock Driver trunk %d on board %d is down.

90115 (369) BOTH_CLOCK_DOWN_ALARM Critical ClockManager System has lost all external clocking.

UAS Logs/Faults available in Succession

- 90116 (370) PRIMARY_BOARD_CLOCK_DOWN_ALARM Minor ClockManager Board %d has lost its primary clock source.
- 90117 (371) SECONDARY_BOARD_CLOCK_DOWN_ALARM Minor ClockManager Board %d has lost its secondary clock source.
- 90118 (372) BOTH_BOARD_CLOCK_DOWN_ALARM Critical ClockManager Board %d has lost all external clocking.

Event Server Alarms

- 96257 (373) LOCAL_SRVSOCK_CREATION_FAILED Critical EventServer [es_alm_001] %s.
- 96258 (374) REMOTE_SRVSOCK_CREATION_FAILED Major, EventServer [es_alm_002] %s.
- 96259 (375) SYSTEM_RESOURCE_ERR Critical, EventServer [es_alm_003].
- 96260 (376) CONFIG_ERR EventServer [es_alm_004].
- 96261 (377) HAMODE_CHECK_FAILED Critical, EventServer [es_alm_005].
- 96262 (378) MATE_EVTSVR_CONN_LOST Minor, EventServer [es_alm_006].

UAS Logs

ATM logs	ASL001	General ATM log indicating an ATM interface card problem.
	ASL002	The ATM service has initialized successfully.
	ASL003	An ATM delete gateway request has failed.
	ASL004	An ATM delete gateway request has failed.
	ASL005	An ATM interface card port has failed to lock. The port has returned to its previous state.
	ASL006	An ATM interface card port has failed to lock. The port cannot return to its previous state.
	ASL007	An ATM Virtual Channel has experienced an AIS alarm.
	ASL008	An ATM Virtual Channel has experienced an RDI alarm.
	ASL009	An ATM Virtual Channel cleared the AIS alarm.
	ASL010	An ATM Virtual Channel cleared the RDI alarm.
	ASL013	The ATM port is configured with the wrong UNI version.
	ASL014	ILMI failure on the ATM port.
	ASL015	UNI failure on the ATM port.
	ASL016	ILMI is now ready on the ATM port.
	ASL017	UNI is now ready on the ATM port.
	ASL018	Invalid ATM SDP parameter received.
	ASL019	Invalid VCCI received in the incoming AAL2 SVC setup.
	ASL020	A specific ATM software error occurred as described in the log.

UAS Logs/Faults available in Succession

	ASL021	Failed to acquire a channel for the endpoint described in the log.
	ASL022	An error was reported by the NMS PA200 API.
	ASL023	ATM audit has started.
	ASL024	ATM audit has ended.
	ASL025	Audit has dropped a resource on the ATM board as described in the log.
	ASL026	Audit has established a resource on the board as described in the log.
	ASL027	Audit has found a missing resource on the board that can't be established. The resource is described in the log.
	APL001	The ATM interface port has initialized correctly.
UAS398		Indicates a raised alarm in a UAS device
UAS399		Indicates a cleared alarm in a UAS device

USP Logs/Faults in Succession

For detailed information on logs, refer to NN10275-909, *Succession Fault Management Log Reference*.

USP faults are available to the OSS via a third-party fault probe or fault collector. The fault probe/collector must reside somewhere on the OAM&P VLAN due to security rules for accessing the Succession network elements.

USP logs are available on the USP PC Client GUI.

USP supports SSV format. For details on this format, refer to the Performance section of the FCAPS documentation on USP, NN10137-711.



Operational measurements/performance measurements

Operating company personnel use operational measurements (OMs) and performance measurements (PMs) to obtain information on the performance and traffic load on a Succession Network. This data provides the information required for network planning and engineering.

For more complete details on OMs and PMs, refer to NN10264-709, *Operational Measurements Reference Manual*.

OM collection and delivery

OM information is collected for XA-Core and SPM (including the MG 4000, IW-SPM, and DPT-SPM) components. For network elements controlled by the XA-Core, OMs are collected at the network element level and transferred to the XA-Core. OM data can be viewed on the MAP by typing *OMSHOW* at the CI level. When using *OMSHOW* to view OM data, the active registers usually display zeros except for the last minute of the collection period. To view the active registers directly on an SPM network element, use *remlogin* to remotely log in and then change to directory *omutils* and use the CI command *print* to see the active OM data.

OMs can also be retrieved by the CS2K Core Manager (SDM functionality) OMD (OM Delivery) application, grouped into user-defined report elements, formatted into CSV (comma-separated value) format, and delivered to a customer OSS (operations support system). The OMD application delivers OMs/PMs only for the MG 4000, IW-SPM, DPT-SPM, SPM, and XA-Core.

PM collection and delivery

Other network elements (UAS, USP, and SAM21) have their own OM/PM viewers through their respective EMs (element managers).

Performance Monitoring Poller data collection output

The SNMP-based PM poller collects performance attributes from several Succession-based network elements (i.e., UAS, GWC, SSPFS platform). The data collected by the PM device pollers is output in CSV files to the `/data/oms` file output directory. The `oms` directory contains seven sub-directories (named 1- 7). Each of these sub-directories contains a day's

collection of CSV output files (i.e., one sub-directory each for the seven-day history the poller maintains). The current day's output files are always written to subdirectory '1'. File rotation occurs just prior to midnight every 24-hour period. When file rotation occurs, the files in sub-directory '7' are removed and contents of all subsequent sub-directories are moved up the directory chain (i.e., files in directory 6 are moved to directory 7, 5 to 6, etc.).

A separate file is created for each device during each profile polling interval. When creating the CSV files the poller adheres to the following naming conventions:

<NodeType>.<NodeName>.OMs.<Report
Name>.Year.Mon.Date_HR.MN_<TZ>.csv

where:

NodeType -> Node type (i.e, GWC, UAS, etc....)

NodeName -> A unique node name.

Report Name -> For the SSPFS poller this will correlate to the associated profile name.

TZ -> timezone (i.e., cst or cdt)

An example file name is provided below:

GWC.GWC-10_UNIT_1.OMs.GWC.2002.05.02_10.52_EDT.csv

Viewing CSV files

The CSV files can be viewed locally on the SSPFS platform by using a standard text editor. Alternately the SSPFS platform is configured with a snmp-poller ftp userid. A craftperson can utilize ftp to retrieve the CSV output data files for further analysis. When the snmp-poller ftp userid is used to ftp into the SSPFS server, the home directory for this account is the file **oms output directory**. For security reasons the snmp-poller ftp user only has access to the output directory and its sub-directories. Sample output files from the MIB-2 profile is provided in the following table:

Note 1: A device can reside in more than one profile.

Note 2: Keep in mind, however, that the CSV file format is not intended to be a user-friendly format for viewing the output in a standard text editor. Typically these files would be parsed by an editor that can format CSV files in a legible manner, or they would be parsed by a machine interface.

Note 3: The 'poller' ftp userid should be used to retrieve the PM poller output files. Contact your network administrator to obtain the associated password.

Sample CSV output file for profile MIB-2

```
$cat GWC.GWC6.OMs.MIB-2.2002.05.24_16.06_EDT
//MIB-2 - .iso.org.dod.internet.mgmt.mib-2.host.hrSystem
SCALAR_GROUP_BEGIN-hrSystemUptime,hrSystemDate,hrSystemProcesses,1
:2:18:51.85,"2002-5-24,20:7:42.0,+0:0",155
SCALAR_GROUP_END
//MIB-2 - .iso.org.dod.internet.mgmt.mib-2.snmp
SCALAR_GROUP_BEGIN-snmpInPkts,snmpOutPkts,snmpInBadVersions,snmpIn
nBadCommunityNames,snmpInBadCommunityUses,snmpInASNParseErrs,snmpIn
nTotalReqVars,snmpInTotalSetVars,snmpOutTraps,snmpSilentDrops,27608,2761
4,0,0,0,0,103010,772,7,80
SCALAR_GROUP_END
//MIB-2 - .iso.org.dod.internet.mgmt.mib-2.system
SCALAR_GROUP_BEGIN-sysDescr,"Nortel GateWay Controller GWC;
MCPN750 128MB AA01 AA01 0001af02da30; PGC08AP (VRTXsa 3303, SNMP
Research Agent 15.2.1.7)"
SCALAR_GROUP_END
//MIB-2 - .iso.org.dod.internet.mgmt.mib-2.host.hrDevice.hrProcessorTable.
hrProcessorEntry
TABLE_BEGIN-hrProcessorLoad
1
TABLE_END
//MIB-2 - .iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTable.
hrStorageEntry
TABLE_BEGIN-hrStorageIndex,hrStorageType,hrStorageAllocationUnits,hrStora
geSize,hrStorageUsed,hrStorageAllocationFailures
1,host.hrStorage.hrStorageTypes.hrStorageRam,66 Bytes,1023,13,0
2,host.hrStorage.hrStorageTypes.hrStorageRam,1532 Bytes,400,0,0
3,host.hrStorage.hrStorageTypes.hrStorageRam,1536 Bytes,1024,49,0
4,host.hrStorage.hrStorageTypes.hrStorageRam,52 Bytes,512,321,0
5,host.hrStorage.hrStorageTypes.hrStorageRam,1 Bytes,11912704,184672,0
6,host.hrStorage.hrStorageTypes.hrStorageRam,1 Bytes,2097152,1577296,0
TABLE_END
```


The following table shows sample output files from the GWC profile.

Sample CSV output file for profile GWC
<pre>//GWC - .iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceControl. legacyCallServer.lcsGateWayController.apgMeasurements SCALAR_GROUP_BEGIN-accState,apgInsertions,maxSimulApgCalls,apgCa llFailGWException,apgCallFailGWLost, active,0,0,0,0 SCALAR_GROUP_END //GWC - .iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceControl. legacyCallServer.lcsGateWayController.dptMeasurements SCALAR_GROUP_BEGIN-dptCallAttempts,dptCallFailResTimeout,dptCallF ailResError,dptCallFailAccOOS, 10,0,0,0 SCALAR_GROUP_END //GWC - .iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceControl. legacyCallServer.lcsGateWayController.gwcUnitStatusMIB.gwcUnitObjects.g wcUnitStatus SCALAR_GROUP_BEGIN-norUnitAdminStatus,norUnitOperStatus,norUnit Activity, unlocked,enabled,active SCALAR_GROUP_END //GWC - .iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceControl. legacyCallServer.lcsGateWayController.raMeasurements SCALAR_GROUP_BEGIN-raState,totalResourceCapacity,resourceRequestEr ror,inactive,0,0 SCALAR_GROUP_END</pre>

AMS Performance Measurements

Performance Measurements for the AudioCodes media servers are available through an SNMP interface and can be polled at scheduled intervals by an external poller. The media server will provide performance measurements in the form of two types:

- **Gauges:** Gauges represent the current state of activities on the media server. Gauges unlike counters can decrease in value and like counters, can

increase. The value of a gauge is the current value or a snapshot of the current activity on the media server at that moment.

- **Counters:** Counters always increase in value and are cumulative. Counters, unlike gauges, never decrease in value unless the server is reset and then the counters are zeroed.

The media server performance measurements will be provided by two AudioCodes MIBs (acPerfMediaGateway and acPerfMediaServices). The first mib is generic-type of PM mib. The second PM mib is media server specific.

The generic PM mib covers the control protocol, the RTP stream, and the system packets statistics. This AC PM enterprise mibs supports statistics which apply to the media server and other AC products like gateways.

Available OMs/ PMs in Succession

The OM/PM listings on the following pages are limited to the data accessible through OSS interfaces. These listings do not include those network elements that employ their own graphical user interfaces for delivery/viewing of OM/PM data.

AudioCodes media servers PMs in Succession

The media server performance measurements will be provided by two AudioCodes MIBs (acPerfMediaGateway and acPerfMediaServices). The first mib is generic-type of PM mib. The second PM mib is media server specific. The first table shows performance measurements related to control protocol, RTP stream, and system packet statistics mibs.

AMS Control Protocol, RTP, packet statistics PMs

OM Group or PM Name	Name	Description
Network Element: SAM21		
acPerfMediaGateway (new in SN07)	acPerfCpNumDupsForCompletedTransactions	Number of Duplicated Completed Transactions: The number of times a duplicate transaction request was received after the initial transaction had already been completed. In this case, the gateway resends the response for this transaction.
	acPerfCpNumDupsForOutstandingTransactions	Number of Duplicated Transactions Outstanding: The number of times a duplicate transaction request was received while the initial transaction was outstanding, that is, still in progress. In this case, the gateway ignores the duplicate request.

AMS Control Protocol, RTP, packet statistics PMs

OM Group or PM Name	Name	Description
	acPerfCpMessageSendSuccesses	Messages Send Successes: Number of times there was a success in sending a call control (H.248) message. Call control messages are sent using the system's socket library. This counter tracks successes in using the local socket services. It does not track successes in end-to-end message transfer between the gateway and the call agent.
	acPerfCpMessageSendErrors	Message Send Errors: Number of times there was a failure in sending a call control (H.248) message. The message is sent via a datagram using the system's socket library. Normally a failure on a socket send operation would be attributed to an internal system problem.
	acPerfCpMessageReceiveSuccesses	Message Receive Successes: Number of times there was a success in receiving a call control (H.248) message. Call control messages are received using the system's socket library. This counter tracks successes in using the local socket services. It does not track successes in end-to-end message transfer between the gateway and the call agent.
	acPerfCpMessageReceiveErrors	Message Receive Errors: Number of times there was a failure in receiving a call control (H.248) message. Call control messages are received using the system's socket library. A failure on the socket receive operation can be attributed to an internal system problem or with the call agent sending a message larger than what is supported by the gateway.
	acPerfCpProtocolSyntaxErrors	Protocol Syntax Errors:: Number of syntax errors detected in incoming call control (H.248) messages.
	acPerfCpMessageRetransmissions	Message Retransmissions: Each time the call engine times out waiting for an acknowledgement it retransmits the control protocol message, unless the number of max retransmissions is exceeded. This counter is incremented each time a message is retransmitted due to a timeout.
	acPerfCpMessageMaxRetransmissionsExceeded	Message Max Re-transmissions Exceeded: Number of times the call control message maximum retransmission count was exceeded. The gateway attempted several times to send a message to the call agent, but each time, an ack was not received. A failure of this type results in a failed call and is usually an indication that subsequent calls will fail. This problem is typically a result of the call agent being down or a result of a network problem

AMS Control Protocol, RTP, packet statistics PMs

OM Group or PM Name	Name	Description
	acPerfCpMessagesFromUntrustedSources	Messages From Untrusted Sources: Number of messages received from untrusted sources, that is from network nodes other than the node on which the call agent is running.
	acPerfRtpSenderPackets	RTP Sender Packets (Card): Total number of RTP packets sent by the system for this card.
	acPerfRtpSenderOctets	RTP Sending Octets (Card): Total number of non-header RTP octets sent by this card.
	acPerfRtpReceiverPackets	RTP Receiver Packets (Card): Total number of RTP packets received by the system for this card.
	acPerfRtpReceiverOctets	RTP Receiver Octets (Card): Total number of non-header RTP octets received by this card.
	acPerfRtpRcvrLostPackets	RTP Receiver Lost Packets (Card): Total number of RTP packets lost as observed by this card.
	acPerfRtpFailedDueToLackOfResources	RTP Failed Due to Lack of Resources: The number of times a rtp request was rejected due to lack of resources since the last application restart.
	acPerfRtpSimplexInSessionsCurrent	RTP Simplex In Sessions: Current number of simplex input RTP sessions.
	acPerfRtpSimplexOutSessionsTotal	RTP Simplex Out Session Total: Total number of simplex output RTP sessions.
	acPerfRtpSimplexOutSessionsCurrent	RTP Simplex Out Session Current: Current number of simplex output RTP sessions
	acPerfRtpDuplexSessionsTotal	RTP Duplex Sessions Total: Total number of duplex RTP sessions.
	acPerfRtpDuplexSessionsCurrent	RTP Duplex Sessions Current: Current number of duplex RTP sessions.
	acPerfSystemPacketEndpoints	System Packet Endpoints: Number of endpoints reserved for all packet network-related functions (conferencing, plays, etc.).

The second performance measurement mib is media server specific mib and contains statistics for these major categories:

- IVR – interactive voice response
- BCT – bearer channel tandeming

- CONF – Conferencing
- TT – Test Trunks

AMS IVR, BCT, CONF, and IT PMs

OM Group or PM Name	Name	Description
Network Element: SAM21		
acPerfMediaServices (new in SN07)	acPerflvrPlayRequests	Play Requests: The total number of announcement requests received from the call agent
	acPerflvrPlaySuccessful	Play Successes: Number of announcement requests processed successfully.
	acPerflvrPlayFailedDueToLackOfResources	Play Failures Due to Lack of Resources: Number of announcement requests which failed to be played because some resource was not available.
	acPerflvrPlayFailedDueToLackOfResources	Play In Progress: The number of announcement operations that are currently in progress.
	acPerflvrPlayDuration	Play Duration: The duration, in seconds, of all successful announcement requests. The average duration of all requests (average hold time) can be computed by dividing acPerfPlayDuration by acPerfPlaySuccessful.
	acPerflvrPlayFailedDueToProvMismatch	Play Failed Due to Provisioning Mismatch: Number of audio segments which failed to be played because of a provisioning mismatch.
	acPerflvrPlayCollectRequests	Play Collect Requests: The number of play collect requests.
	acPerflvrPlayCollectSuccessful	Play Collect Successful: Number of play collects completed successfully. A request is considered successful if the entire sequence, from initial prompt to success/failure prompt, is played out without a failure due to lack of resources, provisioning mismatch, or any other media server failure. The failure of the user to enter the proper digits is not a reason for failure of the request.
	acPerflvrPlayCollectFailedDueToLackOfResources	Play Collect Failure due to Lack of Resources: The number of play collect requests that failed due to lack of resources.
	acPerflvrPlayCollectFailedDueToProvMismatch	Play Collect Failed Due to Provisioning Mismatches: The number of play collect requests that failed due a provisioning mismatch.
	acPerflvrPlayCollectInProgress	Play Collect In Progress: The number of play collect operations that are currently in progress.

AMS IVR, BCT, CONF, and IT PMs

OM Group or PM Name	Name	Description
	acPerflvrPlayCollectDuration	Play Collect Duration in Seconds: The duration, in seconds, of all successful play collect requests. The average duration of all requests can be computed by dividing acPlayCollectDuration by acPlayCollectSuccessful.
	acPerflvrContDigitCollectRequests	Number of Continuous Digit Collection Requests: The number of continuous digit collect requests.
	acPerflvrContDigitCollectSuccessful	Number of Continuous Digit Collect Requests Successful: Number of continuous digit collects completed successfully.
	acPerflvrContDigitCollectFailedDueToLackOfResources	Number of Continuous Digit Collection request failed (no resources): The number of continuous digit collect requests that failed due to lack of resources.
	acPerflvrContDigitCollectInProgress	In Progress Continuous Digit Collection requests: The number of continuous digit collect operations that are currently in progress.
	acPerflvrContDigitCollectDuration	Successful Continuous Digit Collect Requests: The duration, in seconds, of all successful continuous digit collect requests. The average duration of all requests can be computed by dividing acDCCollectDuration by acDCCollectSuccessful.
	acPerfBctRequests	Total BCT Requests: The total number of BCT contexts opened since the media server initialized.
	acPerfBctSuccessful	Successful BCT requests: Number of BCT requests processed successfully.
	acPerfBctFailedDueToLackOfResources	Failed BCT requests: Number of BCT requests which failed to be played because a resource was not available.
	acPerfBctInProgress	In progress BCT requests: The number of BCT calls that are currently in progress.
	acPerfBctDuration	Duration of BCT contexts: The duration, in seconds, of all successful BCT contexts. The average duration of all contexts can be computed by dividing acPerfBCTDuration by acPerfBCTSuccessful.
	cPerfBctTotalParticipants	Total of BCT participants: The total number of BCT participants since the media server initialized.
	acPerfBctCurrentNumberOfParticipants	In progress BCT participants: The number of participants in all BCT calls that are currently in progress.

AMS IVR, BCT, CONF, and IT PMs

OM Group or PM Name	Name	Description
	acPerfConfRequests	Total number of conferences processed: The total number of conferences processed since the last application restart. This is the number of conferences created and not the number of members.
	acPerfConfSuccessful	Successful Conferences: Number of conference requests processed successfully.
	acPerfConfInProgress	In-progress Conferences: The number of conferences currently in progress.
	acPerfConfDuration	Conference Duration: The duration, in seconds, of all successful conference requests. The average duration of all requests can be computed by dividing acPerfConfDuration by acPerfConfSuccessful.
	acPerfConfFailedDueToLackOfResources	Conference Failures due to lack of resources: The number of times a conference request was rejected due to lack of resources since the last application restart.
	acPerfConfAddRequests	Requests to add a conferee: The number of requests to add a conferee to an existing conference.
	acPerfConfAddSuccessful	Conferee adds successful: The number of times a conferee was added successful to an existing conference.
	acPerfConfAddFailedDueToLackOfResources	Conferee Add Failures due to lack of resources: The number of times a conferee could not be added to an existing conference due to a lack of resources.
	acPerfConfPlays	Plays into Conference: The total number of plays made into conferences since the last application restart.
	acPerfConfPlayCollects	Play Collects in Conference: The total number of play collects made into conferences since the last application restart.
	acPerfConfTones	Play Tones into conference: The total number of Tones played into conferences since the last application restart.
	acPerfConfPortsUsed	Conference Ports Reserved: The total number of ports that were reserved for conferences since the last application restart.
	acPerfConfPortsReserved	Conference Port Reserved for monitor: A monitor port may be reserved by the call agent when setting up a conference. The monitor port can then be used by one or more listen-only conferees.

AMS IVR, BCT, CONF, and IT PMs

OM Group or PM Name	Name	Description
	acPerfTtRequests	Test Trunk Test Requests: The number of test trunk tests requested.
	acPerfTtSuccessful	Test Trunk Test Request Successes: The number of test trunk tests that were successfully setup and torn down. This PM is not a reflection on whether the test actually passed or failed.
	acPerfTtInProgress	In-Progress Test Trunk Tests: The number of test trunk tests that are currently in progress
	acPerfTtDuration	Test Trunk Test Duration: The duration, in seconds, of all successful test trunk requests. This number is the time between a test trunk test being initiated and completed. The average duration of all requests can be computed by dividing acPerfTtDuration by acPerfTtSuccessful.
	acPerfTtFailedDueToLackOfResources	Test Trunk failures due to lack of resources: The number of times a test trunk request was rejected due to lack of resources since the last application restart.

SAM21 OMs/PMs in Succession

The following table lists the operational measurements (OMs) and performance measurements (PMs) available from the SAM21 network element. The OMs/PMs are retrieved by the SNMP poller.

SAM21 OMs/PMs

OM Group or PM Name	New or Changed	Description
Network Element: SAM21		
IPOA MIB	New in SN05	Cell Drop Count: The number of cells dropped by the interface on the Shelf Controller Cell Drop Timestamp: The time stamp of last cell dropped by the interface on the Shelf Controller Total Bytes Sent: The combined number of bytes sent through all active SVCs on the Shelf Controller Bytes Sent per Second: The average number of bytes sent through all active SVCs on the Shelf Controller Total Bytes Received: The combined number of bytes received through all active SVCs on the Shelf Controller

SAM21 OMs/PMs

OM Group or PM Name	New or Changed	Description
		Bytes Received per Second: The average number of bytes received through all active SVCs on the Shelf Controller Oversized PDU Content: The combined number of Oversized PDUs sent through all active SVCs on the Shelf Controller Received Timeout Count: The combined number of timeouts received at the endnode of all active SVCs on the Shelf Controller

CS 2000 XA-Core OMs/PMs in Succession

The following table lists the operational measurements (OMs) and performance measurements (PMs) available from the Succession Call Server 2000 XA-Core network element.

CS 2000 XA-Core supports CSV and EADAS formats through SDM functionality. For details on EADAS, refer to the Performance section of CS 2000 FCAPS documentation, NN10149-711. For details on CSV format, refer to the previous two pages on “PM Poller data collection output.”

CS 2000 XA-Core OMs/PMs

OM Group or PM name	Registers	Description
Network Element: CS 2000 XA-Core		
AINTRAN AIN Transports group--new in SN07		
	INSCMSGO	Pegs Outgoing IN messages using SCTP
	INSCMSGI	Pegs Incoming IN messages using SCTP
	INSSNDFA	Pegs IN messages using SCTP for which send failed
	INSCDERR	Pegs IN messages which encountered errors at application data
	INSCTBIG	Pegs IN Messages which failed due to message length
	INSCTBMS	Pegs instances when buffer errors encountered while sending IN messages over SCTP
ATTAMA2 CAIN Triggers group (Applies only to DMS)--new in SN07		
Used for register overflows from the OM group ATTAMA, only when the BAS00023 SOC is ON, and only for registers AMANS and AMUNANS.		
	QUERYSCU	Added for Succession to count call attempts that are unsuccessful because switching equipment in another office handles too many calls.
	ISCONUCC	Added for Succession to count the number of times a CAIN call queries the SCU.

CS 2000 XA-Core OMs/PMs

OM Group or PM name	Registers	Description
CAINTRIG CAIN Triggers group		
	QUERYSCU	Added for Succession to count call attempts that are unsuccessful because switching equipment in another office handles too many calls.
	ISCONUCC	Added for Succession to count the number of times a CAIN call queries the SCU.
CP Call Processing Software Resources group		
	CPLOSZ	Added for Succession to count origination messages correctly attached to a call condense block.
	CINITC	Added for Succession to count call condense blocks that were in use at the time of a cold restart.
	WAKESZ	Added for Succession to count CPWAKEUP block seizures.
DCAMCEIA Dynamically Controlled Access Ineffective Attempts group		
	FR_TRUNK	Added for Succession to count the termination failures that the DCA considers ineffective attempts toward DNS for calls that come in from a trunk.
	TO_TRUNK	Added for Succession to count the termination failures that the DCA considers ineffective attempts toward DNS for calls that terminate to a trunk.
	TOTAL	Added for Succession to count the termination failures that the DCA considers ineffective attempts toward DNS.
	TRMT	Added for Succession to count the termination failures that the DCA considers ineffective attempts toward DNS.
	ISUP	Added for Succession to count the termination failures that the DCA considers ineffective attempts toward DNS.
FCDRTM1E (Applies only to DMS) Used for register overflows from the OM group FCDRTMP1, only when the UBFR0008 SOC is ON. This OM group provides 32 pre-defined tuples. Each register is associated with the CDR template being used for a CDR billing record. The CDR template index corresponds to the register number. This OM group supports indexes 0-31.		
FCDRTM2E (Applies only to DMS) Used for register overflows from the OM group FCDRTMP2, only when the UBFR0008 SOC is ON. This OM group provides 32 pre-defined tuples. Each register is associated with the CDR template being used for a CDR billing record. The CDR template index corresponds to the register number. This OM group supports indexes 32-63.		
FCDRALG2 (Applies only to DMS) Used for register overflows from the OM group FCDRALGR, only when the UBFR0008 SOC is ON. For these extension registers one count here is equal to 65535 counts of the same register in FCDRALGR..		

CS 2000 XA-Core OMs/PMs

OM Group	or PM name	Registers	Description
ISUPCONN			
ISUP Connection group			
	ISCONUCC		Added for Succession to count call attempts that are unsuccessful because there are no available idle circuits in another office to handle the call.
	ISCONUCE		Added for Succession to count call attempts that are unsuccessful because switching equipment in another office handles too many calls.
	ISCONUCF		Added for Succession to count call attempts that are unsuccessful because of a temporary fault in the far-end network.
NGSSOM			
Next Generation Session Server OM group			
	CS2ASOVF		Pegged when a CS2AS NGSS call is deflected because allowing the call would have caused the current CS2AS call count to exceed the SOC limit.
	CS2ASHWM		Keeps track of the maximum value reached for the CS2AS call counter.
	CS2CSOVF		Pegged when a CS2CS NGSS call is deflected because allowing the call would have caused the current CS2CS call count to exceed the SOC limit.
	CS2CSHWM		Keeps track of the maximum value reached for the CS2CS call counter.
NWMFRRCT			
Network Management Flexible Reroute group			
	FRRATTCT		Added for Succession to count calls that are rerouted to a Virtual Interworking Agent (VIA) route list. Required for ACC (Automatic Congestion Control).
	FRRFLCT		Added for Succession to count rerouted calls that fail to find an idle VIA route list. Required for ACC (automatic congestion control).
SPMOVLD			
Spectrum Overload Statistics group			
The new SPMOVLD group will have 18 OMs that give metrics on the SPM flow control system and the system overload control component. All OMs that apply to the system overload control component start with an 'S', all others apply to the flow control system. The actual peg counts and usage counts (accurate to one second) are accumulated on the peripheral and then uploaded to the OM group using the Spectrum OM Transfer System (SOTS).			
TONES			
	TONEATT		Added for Succession to count calls that the system routes to each tone generator.
TRNK2			
OM group to hold extension registers from TRK OM group			

CS 2000 XA-Core OMs/PMs

OM Group or PM name	Registers	Description
	TOTU2	Extension register of TOTU in TRK OM group
	INCATOT2	Extension register of INCATOT in TRK OM group
	TOTU2	Extension register of TOTU in TRK OM group
	INCATOT2	Extension register of INCATOT in TRK OM group
	NATTMPT2	Extension register of NATTMPT in TRK OM group
	DEFLDCA	Extension register of DEFLD in TRK OM group
	TRU2	Extension register of TRU in TRK OM group
	SBU2	Extension register of SBU in TRK OM group
	CONNECT2	Extension register of CONNECT in TRK OM group
	TANDEM2	Extension register of TANDEM in TRK OM group
	ANSWER2	Extension register of ANSWER in TRK OM group
UTR Universal Tone Receiver group		
	UTRSZRS	Added for Succession to count each time that the system supplies a UTR to a call in response to a request.
XACORE XA-Core hardware-related OMs		
	XAPE	PE (processor element) faults
	XARXPE	Routine exercise test (RXe) PE failures
	XASM	Critical shared memory (SM) faults
	XARXSM	Routine exercise test (RXe) SM failures
	XAIOP	Critical IOP (input/output processor) faults
	XARXIO	Routine exercise test (RXe) IOP failures
	XADISK	Disk faults
	XATAPE	Critical tape faults
	XARTIF	RTIF (reset terminal interface) packet faults
	XALOCP	Critical faults on a RTIF local port
	XAREMP	Critical faults on a RTIF remote port
	XACMIC	CMIC packet faults
	XACXABRT	Routine exercise (REx) test aborts
	XARXBASE	Routine exercise test on base hardware failures
	XARXFULL	Routine exercise test on all hardware failures
	XARXALL	Routine exercise test on all hardware failures
	XAMDI	Number of critical AMDI packet faults detected
	XAMDILNK	Number of critical AMDI link faults detected
	XETHR	Hardware faults on Ethernet packet
	XETHRPRT	Hardware faults on an Ethernet port

CS 2000 XA-Core OMs/PMs

OM Group or PM name	Registers	Description
	XETHRLNK	Hardware faults on an Ethernet link
XACSRVC	XA-Core service-related OMs	
	XAMDMAJU	Length of time (in 100 second increments) that an AMDI major alarm condition has existed
	XAMDCRIU	Length of time (in 100 second increments) that an AMDI critical alarm condition has existed
	XASSMPXU	Length of time (in 100 second increments) that a simplex SM condition has existed as a result of a system action
	XAMSMPXU	Length of time (in 100 second increments) that a simplex SM condition has existed as a result of a manual action
	XARXMPXU	Length of time (in 100 second increments) that a SM condition has existed as the result of a REx test
	XASMCRIU	Length of time (in 100 second increments) that a low SM critical alarm has existed
	XALKMAJU	Length of time (in 100 second increments) that an MScomm (message switch communication) major alarm has existed
	XETHRMJU	Major alarms on an Ethernet RM
	XETHRCRU	Minor alarms on an Ethernet RM
	XATRAPP	Trap interrupts
	XASWINI	Warm restarts as a result of a system action
	XAMWINI	Warm restarts as a result of a manual action
	XASCINI	Cold restarts as a result of a system action
	XAMCINI	Cold restarts as a result of a manual action
	XAPEMAJU	XACORE period of major alarm
	XAPECRIU	XACORE period of low processing power

DPT-SPM OMs/PMs in Succession

The following table lists the operational measurements (OMs) and performance measurements (PMs) available in Succession for the DPT-SPM network element.

DPT-SPM supports CSV format, and EADAS through SDM functionality. For details on EADAS, refer to the Performance section of DPT-SPM FCAPS

documentation NN10145-711 (IP). For details on CSV format, refer to “Performance Monitoring Poller data collection output” of this document.

DPT-SPM OMs

OM Group	Registers	Description
Network Element: DPT-SPM		
PM Peripheral Module group. The registers listed here are the only ones supported for SPM and MG4K applications.		
	PMERR	NOTE: This is an existing OM group. For details on the registers, see NTP 297-2621-814, available on Helmsman Express.
	PMFLT	
	PMMSBU	
	PMUMBU	
	PMSBP	
	PMMBP	
	PMMWXFR	
	PMMCXFR	
	PMINTEG	
PMTYP Peripheral Module Type group. The registers listed here are the only ones supported for SPM and MG4K applications.		
	PMTERR	NOTE: This is an existing OM group. For details on the registers, see NTP 297-2621-814, available on Helmsman Express.
	PMTFLT	
	PMTMSBU	
	PMTUSBU	
	PMTMMBU	
	PMTSBP	
	PMTMBP	
	PMTMWXFR	
	PMTMCXFR	
	PMTINTEG	
ENETPLNK ENET Peripheral Side Links group. The registers listed here are the only ones supported for SPM and MG4K applications.		
	ENSPCHER	NOTE: This is an existing OM group. For details on the registers, see NTP 297-2621-814, available on Helmsman Express.
	ENLKERR	
	ENLKFLT	
	ENSBLKU	
	ENMBLKU	
	ENLKPARU	

DPT-SPM OMs

OM Group	Registers	Description
	ENSLKPAR	
	ENMLKPAR	
	ENLNKISOU	
	ENSLKISO	
	ENMLKISO	
NMTCUNIT	Node Maintenance Unit Measurements group. The registers listed here are the only ones supported for SPM and MG4K applications.	
	NDUERR	NOTE: This is an existing OM group. For details on the
	NDUFLT	registers, see NTP 297-2621-814, available on
		Helmsman
	NDUMBP	Express.
	NDUMBU	
	NDUMCRST	
	NDUMRRST	
	NDUNAP	
	NDUSBP	
	NDUSBU	
	NDUNAU	
	NDUSWERR	
	NDUTRAP	
DPTNODE	Dynamic packet trunk node type (SPM or DPT), PM #, and node #	
	DPTGTAT	Get terminal attempts
	DPTGTAT2	Extension of DPTGTAT
	DPTGTFL	Get terminal failures
	DPTGTFO	Get terminal failures optimized
	DPTUSAG	Usage register
	DPTUSAG2	Extension of DPTUSAG
	DPTHWT	The high-water mark for terminal usage per transfer period.
DPTOFC	Dynamic packet trunk office events	
	DPTGTAT	Get terminal attempts
	DPTGTAT2	Extension register of DPGTAT incremented when DPGTAT reaches 65,535
	DPTGTFL	Get terminal failures per office (non-optimized)
	DPTGTFL2	Extension register of DPGTFL incremented when DPGTFL reaches 65,535
	DPTUSAG	Usage count

DPT-SPM OMs

OM Group	Registers	Description
	DPTUSAG2	Extension register of DPUSAG incremented when DPUSAG reaches 65,535
	DPTGTFLO	Get terminal failures (optimized)
	DPTGTFLO2	Extension register of DPGTFLO incremented when DPGTFLO reaches 65,535
	DPTHWT	High-water mark for terminal usage per transfer period.
	DPTHWT2	Extension register of DPHWT incremented when DPHWT reaches 65,535
	DPDPL	Number of attempts to get a DPT terminal that failed due to DPT port depletion
	DPDPL2	Extension register of DPDPL incremented when DPDPL reaches 65,535

IW-SPM OMs in Succession

The following table lists the operational measurements (OMs) and performance measurements (PMs) available in Succession for the IW-SPM network element.

IW-SPM supports CSV format, and EADAS through SDM functionality. For details on EADAS, refer to the Performance section of FCAPS documentation on IW-SPM, NN10143-711 (IP). For details on CSV format, refer to “Performance Monitoring Poller data collection output” of this document.

IW-SPM OMs

OM Group	Registers	Description
Network Element: IW-SPM		
IWBM	Interworking bridge manager events (associated with IW SPMs)	
	IWGBATT	Get bridge attempts
	IWGBATT2	Extension of IWGBATT
	IWGBFAIL	Get bridge attempt failures
	IWGGBABRT	Get bridge attempts aborted
	IWFBATT	Free bridge attempts
	IWFBATT2	Extension of IWFBATT
	IWFBFAIL	Free bridge attempt failures
	IWFBABRT	Free bridge attempts aborted
	IWONSET1	Total IW SPMs in use reached 70%
	IWONSET2	Total IW SPMs in use reached 90%
	IWABATE1	Total IW SPMs in use less than 65%
	IWABATE2	Total IW SPMs in use less than 85%

IW-SPM OMs

OM Group	Registers	Description
MNATM	MG 4000 interface performance statistics (Not applicable on IP IW SPM)	
MNATMA5	MG 4000 ATM PVC AAL5 interface performance statistics (Not applicable on IP IW SPM)	
MNATMVC	MG 4000 ATM PVC AAL5 interface performance statistics (Not applicable on IP IW SPM)	
TRNK2	(Not applicable on IP IW SPM)	

GWC OMs/PMs in Succession

The following table lists the operational measurements (OMs) and performance measurements (PMs) available in Succession for the GWC network element..

The GWC performance measurements support CSV format and support the CORBA interface. The PMs are not available for viewing on the EM GUI; to view them you must retrieve the CSV files. The GWC OMs are sent to the XA-Core and may be viewed through OMSHOW or a similar tool.

OM group	Register	Description
Network Element: GWC		
TRKQOS		records instances in which QOS threshold values have been exceeded for calls handled by a particular GWC-based TDM trunk group.
	PKTLOSS	Packet Loss. Counts the number of times that the packet loss threshold has been exceeded.
	JITTER	Jitter. Counts the number of times that the jitter threshold has been exceeded.
	DELAY	Delay (latency). Counts the number of times that the delay threshold has been exceeded.
N/A	Existing	As noted in the design document for 89007781 (PT-IP), the following data is reported by all gateways: packets sent; packets received; packet loss; octets sent; octets received; inter-arrival latency; jitter.

OM group	Register	Description
(Checking)		The OM's that feature 89008294 (UA-IP) will use already exist for the ATM solution, now extended to IP solutions. It includes the following OM counters: • Intra total number of channel allocation requests • Intra total number of failed channel allocation requests • Intra total number of failed channel allocation requests • Inter maximum simultaneous number of channels in use • Inter total number of channel allocation requests • Inter total number of failed channel allocation requests • Intra total number of channel allocation requests • Intra total number of failed channel allocation requests
DTSRPM Pegs originations and dialtone delays grouped by the type of line making the call (DP, DTMF, or Pphone).		
	DPLTOT	Dial Pulse Lines Total Originations. This value is always 0 for CS2K lines since no differentiation is made between DP and DGT.
	DPLDLY	Dial Pulse Line Delays. Counts DP lines which got dial tone after 3 seconds. Always 0 for CS2K.
	DGTTOT	Counts Digit Tone Line Total Originations.
	DGTDLY	Digit Tone Line Delays. Counts DGT lines which got dial tone after 3 seconds.
	KSTOT	Keyset (Pphone) Lines Total Originations.
	KSDLY	Keyset (Pphone) Lines which got dial tone after 3 seconds.
XPMOVL Collects statistics on XPM overload conditions. This is an existing OM group that functions the same as in TDM switches.		
XPMOCC Collects statistics on CPU occupancy in the GWC. This is an existing OM group that functions the same as in TDM switches.		

GWC Performance Measurements

OIDs	Description
The GWC supports collection of a subset of the Host Resources-MIB and the IF-MIB. The following table entries show the OIDs that are collected for each.	
Host-Resources-MIB	
host(25).hrSystem(1)	
25.1.hrSystemUptime(1)	System Uptime (distinct from sysUpTime)

GWC Performance Measurements

OIDs	Description
25.1.hrSystemDate(2)	System local DateAndTime
25.1.hrSystemInitialLoadParameters(4)	Load path/parameters used
25.1.hrSystemNumUsers(5)	Current number of "user sessions"
25.1.hrSystemProcesses(6)	Number of tasks
25.1.hrSystemMaxProcesses(7)	Maximum number of tasks
host(25).hrStorage(2)	
25.2.hrMemorySize(2)	Main memory DRAM size (KBytes)
25.2.hr.StorageTable(3)	Table describing storage and resource areas, including for each: Type, Description, AllocationUnits, Size, Used, and AllocationFailures. An entry in this table is planned for each of the resources currently registered in the Base Resource Monitor: - System Heap - VRTX Workspace - Segment Descriptors - IPC Buffers - Ethernet DCU Buffers
host(25).hrDevice(3)	
25.3.hrDeviceTable(2)	Table of hardware devices contained in host, including for each: Type, Description, "ID", Status, and Error counts. An entry is planned in this table for each of the devices listed on the PCI bus, plus the CPU.
25.3.hrProcessorTable(3)	Table of info on processors for this host, including a FirmwareID and CPU-Load (1min). There will be an entry for each processor in the hrDeviceTable (just 1 for now).
25.hrSWRun(4)	
25.4.hrSWOSIndex(1)	Index of the entry in the following table for the OS.
25.4.hrSWRunTable(2)	Table of software running on the host, and for each host, a Name, ProductID, Run Path and Parameters, Type, and Status. Status is implemented as READ-ONLY.
25.hrSWRunPerf(5)	
25.5.hrSWRunPerfTable(1)	Table of performance data for software in the hrSWRun table, which includes for each task the CPU and memory usage CPU and memory usage for each task that is available.

GWC Performance Measurements

OIDs	Description
IF-MIB	
interfaces(2)	
2.ifNumber(1)	Number of entries in ifTable
2.ifTable(2)	Table of interfaces to the device, where each entry is one “layer” or “sub-layer” of an interface. Each entry includes LOTS of columns, including: Descr, Type, MTU, Speed, PhysicalAddress, Administrative and Operational Status, In and Out Octets, Errors, Discards, etc (not all columns relevant to each) The GWC will include entries only for: - DEC Ethernet (Ia0) - DEC Ethernet loopback - Serial port - IP layer?
ifMIB(31)	
31.1.ifXTable(1)	An extension to the ifTable (same ifIndex), including Name, alternative High-speed octet and packet Counters, LinkUpDowntrapEnable, HighSpeed bandwidth estimate, an Alias, and PromiscuousMode and ConnectorPresent flags.
31.1.ifStacktable(2)	A table containing information on relationships between sub-layers of interfaces in the ifTable. Each row defines an “x on-top-of y” relationship.

MG9000 OMs/PMs in Succession

The following table lists the operational measurements (OMs) and performance measurements (PMs) available in Succession for the MG 9000 network element.

MG 9000 supports CSV format.

For details on CSV format, refer to “Performance Monitoring Poller data collection output” in this document.

MG 9000 OMs

OM Group	PM Name or OM Registers	Description
Network Element: MG 9000		
GWOVL0M This OM group will be incremented for every call connection request that is denied.		
	OVERLOAD	This register is incremented when a Media Gateway 9000 reaches an overload threshold and call connections are denied.

MG 9000 OMs

OM Group	PM Name or OM Registers	Description
The following OMs are maintained by the CMR FM application:		
	ADSI	No usage metering; no peg counts.
	BCLID	No usage metering; no peg counts.
	CID	Counts CID attempts and CID completions.
	CMWI	No usage metering; no peg counts.
	DSCWID	Counts DSCWID attempts.
	SCWID	Counts SCWID attempts.
Other OMs are:		
	Jitter	Jitter in a 15-minute interval (averaged)
	Latency	One-way delay in a 15-minute interval (averaged)
	numPktsSent	Total number of packets sent in a 15-minute interval.
	PktsLost	Percentage of packets lost
	numCalls	Total number of calls in a 15-minute interval
	numBadCalls	Number of bad calls that exceeded threshold values in a 15-minute interval.
For group-related and link-related OMs for the DS1-IMA application, refer to Appendix C "MG 9000 MIB OMs/PMs."		
Appendix C, "MG 9000 MIB OMs/PMs," contains the entire list of all OMs and PMs for MG 9000.		
NOTE: Entries in this table sometimes use the term UEMG, which came from a previous naming convention for the product and was made a part of the code in some instances.		

PVG/Media Gateway 15000 OMs/PMs in Succession and Passport 15000/Multiservice Switch OMs/PMs

Note: For SN07, the terms Packet Voice Gateway (PVG) and Passport 15000 have been rebranded as part of Nortel Networks' brand simplified naming format. The PVG is now referred to as Nortel Networks Media Gateway 15000. The Passport 15000 is now referred to as the Nortel Networks Multiservice Switch 15000.

For details on Media Gateway 15000 and Multiservice Switch 15000 performance measurements, refer to NTP NN10158-711

In SN07, the 5- and 30-minute performance measurements (PMs) now provide Internet protocol (IP) statistics. The IP statistics are available at a physical interface level. You can use IP statistics for operational monitoring and for

network planning and engineering. Also, you can obtain performance information from IP statistics, such as link bandwidth utilization, voice call volumes, and error conditions. These are key for monitoring the network using PMs. Within the Multiservice Switch in Succession context, performance measurements (PMs) are referred to as network traffic management (NTM) statistics.

IP interface statistics apply to all physical interfaces on Nortel Networks Multiservice Switch 15000 nodes that process layer 3 IP. This includes ports on the Ethernet-based Gigabit Ethernet (GE) function processors (FPs), the control processor (CP) operations, administration, and maintenance (OAM) Ethernet port, and the asynchronous transfer mode (ATM)-based OC-3, OC-12 and DS3 ports. PMs for these nodes now include an expanded range of values.

Statistics collection and data flow

The data collection system (DCS) on the node collects NTM statistics from the control and function processors, and ATM and IP interfaces, at 5-minute intervals. To collect the statistics, the DCS uses a real-time statistics stream (rtstats). Each node forwards these records to Nortel Networks Preside Multiservice Data Manager (MDM) servers.

On Nortel Networks Preside Multiservice Data Manager (MDM) servers, the Performance Measurements Stream Processor (PMSP) server application manages performance. NTM statistics originating from node processors flow to the PMSP server application. The PMSP server application converts the statistics into ASCII comma separated value (CSV) formatted 5-minute records. It also creates 30-minute data records by aggregating six 5-minute data records. These are referred to as 5-minute and 30-minute performance measurements (PMs).

The Preside MDM servers transfer the NTM data directly to the OSS applications, or to the CS2000 Core Manager running on the SDM, depending on the Succession Network configuration.

Accessing files through the SDM or MDM

NTM statistics data can be configured to be obtained from the SuperNode Data Manager (SDM). The PM file follows the file naming conventions of the Operational Measurement Delivery (OMD) application. The format of the file name is:

```
<name>.<date>.<time>.PP.<type>.CSV
```

The collected NTM statistics files are stored in the /omdata/closedNotSent directory. They are now available to the OSS application. The OSS application retrieves the files and moves them to the /omdata/closedSent directory. Upon the transfer of the files, the OMD automatically sets the retention period for

the files. The retention period for a file can be configured using the OMUI. It can range from one to fourteen days.

When NTM statistics data is configured to be obtained from Nortel Networks Preside Multiservice Data Manager (MDM) servers, the name of the file is similar to that used by SDM. However, the Host Group Directory Server (HGDS) group name or shelf name indicating the source of the NTM statistics data replaces the “PP” string found after the time stamp in the SDM file name. The format for the file name appears below.

<name>.<date>.<time>.<HGDS group or shelf name>.<type>.CSV

PMs for Media Gateway 15000

The following table lists the operational measurements (OMs) and performance measurements (PMs) available in Succession for the PVG/Media Gateway 15000 network element.

Note: The following performance measurements are applicable for VoIP when it uses ATM cards for network access, i.e., VoIP AAL5.

Network Element: PVG/Media Gateway 15000	
PM name/statistic	Description
Remote instance	Name of the remote instance.
provRate	Provisioned link rate.
actualRate	Actual measured link rate.
Tx Utilization	Tx link utilization of the link as percentage.
Rx Utilization	Rx link utilization of the link as percentage.
TxMinCellRate	Tx cell rate during the least busy minute over the collection interval.
TxMinCellRate	Rx cell rate during the least busy minute over the collection interval.
TxMinCellRateClp	Tx cell rate (CLP=1) during the least busy minute over the collection interval.
RxMinCellRateClp	Rx cell rate (CLP=1) during the least busy minute over the collection interval.
TxMaxCellRate	Tx cell rate during the busiest minute over the collection interval.
RxMaxCellRate	Rx cell rate during the busiest minute over the collection interval.
TxMaxCellRateClp	Tx cell rate (CLP=1) during the busiest minute over the collection interval.
RxMaxCellRateClp	Rx cell rate (CLP=1) during the busiest minute over the collection interval.
TxAvgCellRate	Average cell Tx rate over the collection interval.
RxAvgCellRate	Average cell Rx rate over the collection interval.

Network Element: PVG/Media Gateway 15000	
PM name/statistic	Description
TxAvgCellRateClp	Average cell Tx rate (CLP=1) over the collection interval.
RxAvgCellRateClp	Average cell Rx rate (CLP=1) over the collection interval.
TxCeIlDiscards	The number of Tx discarded cells.
RxCeIlDiscards	The number of Rx discarded cells.
TxCeIlDiscardsClp	The number of Tx discarded cells (CLP=1).
RxCeIlDiscardsClp	The number of Rx discarded cells (CLP=1).
TxFrAmDiscards	The number of Tx discarded frames.
RxFrAmDiscards	The number of Rx discarded frames.
TxFrAmDiscardsClp	The number of Tx discarded frames (CLP=1).
RxFrAmDiscardsClp	The number of Rx discarded frames (CLP=1).
Note: All of the listed statistics are provided as well per-service category (CBR, RTVBR, NTVBR, etc.). For detailed description refer to NTP 241-6001-806 MDM MDP Data Formats.	
CardNumber	Slot number.
CardStatus	Card status.
cpuUtilAvg	Average utilization.
cpuUtilAvgMin	Minimum average utilization.
cpuUtilAvgMax	Maximum average utilization.
MemoryCapacity	The processor's memory capacity (in kilobytes) for each memory type in the specified collection interval.
For the complete list of the LP statistics refer to NTP 241-6001-806 MDM MDP Data Formats.	

Line Provisioning OMs/PMs in Succession

The following table lists the operational measurements (OMs) and performance measurements (PMs) available in Succession for the Line Provisioning network element.

Network Element: Line Provisioning		
OM group or PM name	Register	Description
SCMP	SCMPTRF	If an SCMP line is found Callp busy, the SCMPTRF register will be pegged for that line.
	SCMPMNT	If an SCMP line is found maintenance busy or unavailable, the SCMPTRF register will be pegged for that line.

TOPS OMs/PMs in Succession

The following table lists the operational measurements (OMs) and performance measurements (PMs) available in Succession for TOPS.

OM group or PM name	Register	Description
IS41TOPS. This OM group is deleted in SN07, replaced by new OM groups WINTOPS and TC7WRLSS.		
SMSTOPS. This OM group records application-level events for the TOPS short message service.		
	SMSENT, SMSENT2	SMS sent
	SMSSUCC, SMSSUCC2	SMS success
	SMSFAIL, SMSFAIL2	SMS failure
	SMSTIME, SMSTIME2	SMS time-out
	SMSNETWK	SMS failure due to network problems
	SMSTERM	SMS failure due to terminal (cell phone) problems
	SMSRADIO	SMS failure due to radio interface problems
	SMSMISC	Miscellaneous SMS failure
WINTOPS. This OM group records application-level events for wireless ADACC with release. This group uses WIN in the name since wireless intelligent network capabilities are used to provide ADACC with release for both IS-41 and GSM.		
	WINBEGIN, WINBEGI2	IS-41 AnalyzedInformation or GSM InitialDP received.
	REQCONN, REQCONN2	IS-41 ConnectResource or GSM EstablishTemporaryConnection sent
	CONNECT, CONNECT2	IS-41 AnalyzedInformation or GSM Connect sent

OM group or PM name	Register	Description
	DISCONN, DISCONN2	IS-41 Analyzed Information with action code of "disconnect call" or GSM DisconnectTemporaryConnection sent. This event is not part of the normal IS-41 call flow, but it is part of the normal GSM call flow. If this is pegged for IS-41, it means ADACC with release was not provided.
	WINEND, WINEND2	GSM Application End received; no equivalent IS-41 message.
	ERRCONN	MSC could not connect to TOPS using TLDN
	ERRDISC	TOPS disconnected unexpectedly while providing operator assistance. IS-41 only; when this occurs in a GSM call, WINEND is pegged but not DISCONN or CONNECT.
	ERRSSFT	MSC's service switching function timer expired. Should not happen if TOPS Reset Timer is datafilled properly in Table ISUPTRK.
	ABANDON	Wireless caller disconnected prior to receiving ADACC with release.
	RESTIMR, RESTIMR2	ResetTimer sent (IS-41 and GSM)
	NOTLDNS	No TLDNs available in Table TOPSTLDN.
	NODATA	TOPS could not find EXT block associated with incoming TLDN call from MSC.
	RXLAFail	TOPS call could not obtain original called digits and defaulted to 411.
	SANTIMR	MSC did not release trunk to TOPS, or MSC did not send Application End.
	TLDNTIME	A TLDN was allocated for an MSC call which never arrived. The TLDN is allocated to a new call.
TC7WRLSS. This OM group records transport-level events such as types of TCAP messages sent and received, SS7 errors, etc. on TOPS wireless calls (SMS and WIN, as well as IS-41 and GSM).		

OM group or PM name	Register	Description
	INVOKES, INVOKES2	TCAP INVOKE sent
	INVOKER, INVOKER2	TCAP INVOKE receives
	RETRESS, RETRESS2	TCAP RETURN RESULT sent
	RETRESR, RETRESR2	TCAP RETURN RESULT received
	RETERRS	TCAP RETURN ERROR sent
	RETERRR	TCAP RETURN ERROR received
	REJECTS	TCAP REJECT sent
TC7WRLSS. This OM group records transport-level events such as types of TCAP messages sent and received, SS7 errors, etc. on TOPS wireless calls (SMS and WIN, as well as IS-41 and GSM).		
	INVOKES, INVOKES2	TCAP INVOKE sent
	INVOKER, INVOKER2	TCAP INVOKE receives
	RETRESS, RETRESS2	TCAP RETURN RESULT sent
	RETRESR, RETRESR2	TCAP RETURN RESULT received
	RETERRS	TCAP RETURN ERROR sent
	RETERRR	TCAP RETURN ERROR received
	REJECTS	TCAP REJECT sent
	REJECTR	TCAP REJECT received
	ABORTS	TCAP ABORT sent
	ABORTR	TCAP ABORT received
	NOTRIDS	No transaction identifiers
	MBFULL	Incoming message from MSC ignored due to heavy traffic

OM group or PM name	Register	Description
	RTFNOXLA	SCCP routing failure: No translation of such nature
	RTFNOXLS	SCCP routing failure: No translation for this specific address
	RTFSUBCG	SCCP routing failure: Subsystem congestion
	RTFSUBFL	SCCP routing failure: Subsystem failure
	RTFUNEQ	SCCP routing failure: Unequipped user
	RTFNETFL	SCCP routing failure: Network failure
	RTFNETCG	SCCP routing failure: Network congestion
	RTFMISCE	SCCP routing failure: Failure other than the above seven
	GTTFAIL	Global Title Translation failure
EXT -- The following register was added to the existing registers for the EXT OM group in TOPS19 -- IS41TOPS_EXT_BLK. There are other EXT OM group registers that are not mentioned here.		

UAS OMs/PMs in Succession

The following table lists the operational measurements (OMs) and performance measurements (PMs) available in Succession for the UAS network element.

UAS supports CSV format.

OM group or PM name	Description
Network Element: UAS	
CRC Count	A Minor alarm is raised when the CRC error count threshold is exceeded.
Plane Msg Count	A Minor alarm is raised when the plane message count threshold is exceeded.
norUasProtocolSyntaxErrors	Number of syntax errors detected in incoming call control (MGCP, H.248) messages.
norUasProtocolMessageValidationErrors	Number of times an incoming call control (MGCP, H.248) message had valid syntax, but failed validation

OM group or PM name	Description
norUasUdpSendErrors	Number of times there was a failure in sending a call control (MGCP, H.248) message. The message is sent via a datagram using the system's socket library. Normally a failure on a socket send operation would be attributed to an internal system problem.
norUasUdpReceiveErrors	Number of times there was a failure in receiving a call control (MGCP, H.248) message. Call control messages are received using the system's socket library. A failure on the socket receive operation can be attributed to an internal system problem or with the call agent sending a message larger than what is supported by the gateway.
norUasMgcpMessageRetransmissions	Number of retransmissions of media gateway control protocol messages. Media gateway control protocol is used in here in a generic sense to include both MGCP and H.248
norUasMgcpMessageRetransmissionFailures	Number of times a retransmitted media gateway control protocol message was not acknowledged. Media gateway control protocol is used in here in a generic sense to include both MGCP and H.248.
norUasAudioSegmentPlayed	Number of successful attempts to play audio. For the current number of play attempts, see norUasCurrentNumberOfPlays.
norUasAudioSegmentFailed	Number of failed attempts to play audio. Failures can occur for the following reasons: - call agent sent a bad audio segment id - the audio segment is not provisioned - there was an internal program error Examine the logs to determine the exact nature of the failure.
norUasAckfail	Number of negative acknowledgements (nacks) received. Nacks can be sent by the call agent in response to RSIP or NTFY messages.
norUasTimeout	Number of times the call engine timed out waiting for an acknowledgement.
norUasProterror	Number of call control protocol errors detected. Typical reasons for these errors are: - duplicate parameter - invalid range of parameter - mandatory parameter missing Examine the logs to determine the exact nature of the failure.

OM group or PM name	Description
norUasRestart	Number of abnormal restarts of one of two critical threads in the call processing process. The two threads are the event state machine thread and the maintenance state machine thread. Examine the logs to determine which thread failed.
norUasComperror	The number of times the call engine failed to build a response to a call agent message. Examine the logs to determine the exact nature of the failure.
norUasConndeleted	Number of times that the call engine receives a bad connection id from the call agent. This is normally a result of the call agent sending a message for a connection that has already been deleted.
norUasCallControlMessageSendFailures	Number of times the call control message maximum retransmission count was exceeded. The UAS attempted several times to send a message to the call agent, but each time, an ack was not received. A failure of this type results in a failed call and is usually an indication that subsequent calls will fail. This problem is typically a result of the call agent being down or a result of a network problem.
norUasEndpointsInUse	Number of endpoints that the call engine is currently using for all packet network-related functions (conferencing, plays, etc.).
norUasNumDupsForCompletedTransactions	The number of times a duplicate transaction request was received after the initial transaction had already been completed. In this case, the gateway resends the response for this transaction.
norUasNumDupsForOutstandingTransactions	The number of times a duplicate transaction request was received while the initial transaction was outstanding, that is, still in progress. In this case, the gateway ignores the duplicate request.
norUasConfTotal	The total number of conferences processed since the last application restart.
norUasConfLackOfResourceRejections	The number of times a conference request was rejected due to lack of resources since the last application restart.
norUasConfPlays	The total number of plays made into conferences since the last application restart.
norUasRequestsFailed	The number of resource requests for endpoints on this pool that failed.
norUasNumberOfPlayRecords	The total number of play record operations.
norUasNumberOfPlayRecordErrors	The total number of failed play record operations.

USP OMs/PMs in Succession

See Appendix D

Refer to Appendix D for a complete list of the operational measurements

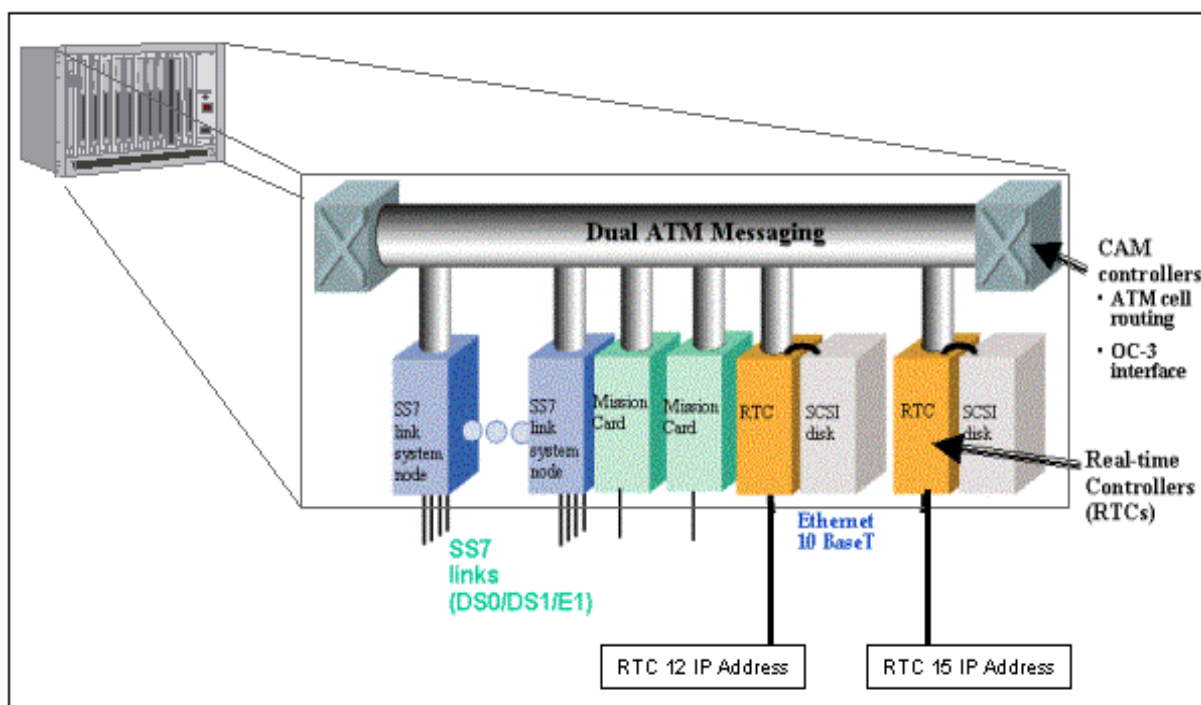
(OMs) and performance measurements (PMs) available in Succession for the USP network element.

USP supports SSV format. For details on this format, refer to the Performance section of the FCAPS documentation on USP, NN10137-711.

OM Export interface on USP

The OM Export interface on the Universal Signaling Point (USP) is provided to allow a customer Operation Support System (OSS) to periodically retrieve operational measurement (OM) performance data files via FTP.

Basic USP hardware and connectivity architecture



The OM data files are replicated to both Real Time Controller (RTC) SCSI disk's (as illustrated in the figure above). To establish a connection, the OSS would FTP to either IP address.

To allow the USP time to create the OM data files, the OSS should allow for a five-minute delay before an attempt is made to retrieve the specific OM interval data file. As an example, if you are retrieving the 12:05 five-minute OM data file, the OSS should establish its connection no earlier than 12:10. This five-minute delay is required to allow the RTC sufficient time to process the collected OM data from all of the system nodes in the USP. After all of the processing is completed, the OM data file is written to the SCSI disks on both RTCs.

In the event that the OSS is not able to connect to either RTC (i.e., an IP LAN network outage), the OM data files will be retained for a set amount of time. This is to allow for data file recovery for missed intervals when network connectivity is restored between the OSS and the USP.

OM data file retention periods

OM Data File Type	Retention Period
5-minute OM data files	6 files = 30 minutes
30-minute OM data files	12 files = 6 hours

The OM data files are stored in predetermined, static paths on each RTC SCSI disk:

5 minute OM data files: /ossinterface/oms/om05min

30 minute OM data files: /ossinterface/oms/om30min

Each of the above OM data directories may contain multiple OM data files. As illustrated in table 1, there may be up to six files in the 5-minute OM data directory and twelve files in the 30-minute OM data directory. The naming convention of the files may be used to determine the OM collection interval that is represented in each file.

5 minute files:

om05min<vv><hh><mm>

vv is the version number; it is currently 01

hh is hours from 00 to 23

mm is minutes 00,05,10,15,20,25, 30, 35, 40, 45, 50, 55

30 minute files:

om30min<vv><hh><mm>

vv is the version number; initially it is 01

hh is hours from 00 to 23

mm is minutes 00, 30

The time in the filename denotes the end of the OM collection period. For example, the OM file named om05min011205 would contain the OM data from 12:00 to 12:05.

OM Export file format

The OM export data files contain one OM register per line, with fields in each register delimited by semi-colons. A carriage return is used as a register delimiter. If there is no information for a given field, it will be left blank, but all delimiters will be present. Therefore, as a rule, every line in the OM data file will have eight fields as illustrated below.

```
<OM Type>;<Application>;<Element>;<RegText>;<Sub-Element>;<Start Time>;<End Time>;<RegisterValue>\r\n
```

OM file format field descriptions

Field Name	Field Description
OM Type	Accumulate (ACC), Maximum (MAX), Minimum (MIN), No Action* (NOA) *No Action indicates that the OM will only be present in the 5 minute data files.
Application	A high-level category, used to group related OM registers. Maximum length is 32 characters.
Element	The name of the element that the OM register value is pegged against, with a maximum length of 20 characters.
RegText	The name of the OM register. Maximum length is 32 characters.
Sub-Element	A sub-element is used to provide more granularity for a given element. This field is only used with Special Study OM's. Maximum length is 64 characters.
Start Time	OM collection interval start date and time with a 19-character capacity.
End Time	OM collection interval end date and time with a 19-character capacity.
Register Value	The OM register value. Maximum length is 10 characters.

A sample from the OM data file named "om30min010730" follows:

```
ACC;Linkset Utilization;LS:LON_PRI;TFP and TCP  
Transmitted Count;;05/09/2001 07:00:00;05/09/2001  
07:30:00;0
```

```
ACC;Linkset Utilization;LS:LON_PRI;TFP and TCP Received  
Count;;05/09/2001 07:00:00;05/09/2001 07:30:00;0
```



```
ACC;Linkset Utilization;LS:LON_PRI;TFR and TCR  
Transmitted Count;;05/09/2001 07:00:00;05/09/2001  
07:30:00;0
```

```
ACC;Linkset Utilization;LS:LON_PRI;TFR and TCR Received  
Count;;05/09/2001 07:00:00;05/09/2001 07:30:00;0
```

Implied OSS responsibilities

The following points should be considered in the design of the OSS application:

- The OSS FTP client application must use only the commands that are listed in the table below.
- All FTP retrieval of OM files will be performed via periodic “OSS pull.”
- In the event that the OSS cannot establish a FTP connection to RTC 12, it will try RTC 15.
- In the event that the OSS cannot establish a FTP connection to either RTC, it will try again after an appropriate delay (< 5 minutes).
- In the event of a prolonged network connectivity outage (> 5 minutes), the OSS will use the FTP “ls” command and the file naming conventions to identify OM data files that it may have missed during the outage.
- Although both date and time information are included for each register in an OM data file, the date is not used in the file naming convention. Therefore, if the OSS requires the date to aid in managing the retrieved OM data files, it will need to provide the date information or read it from one of the registers in the file itself.

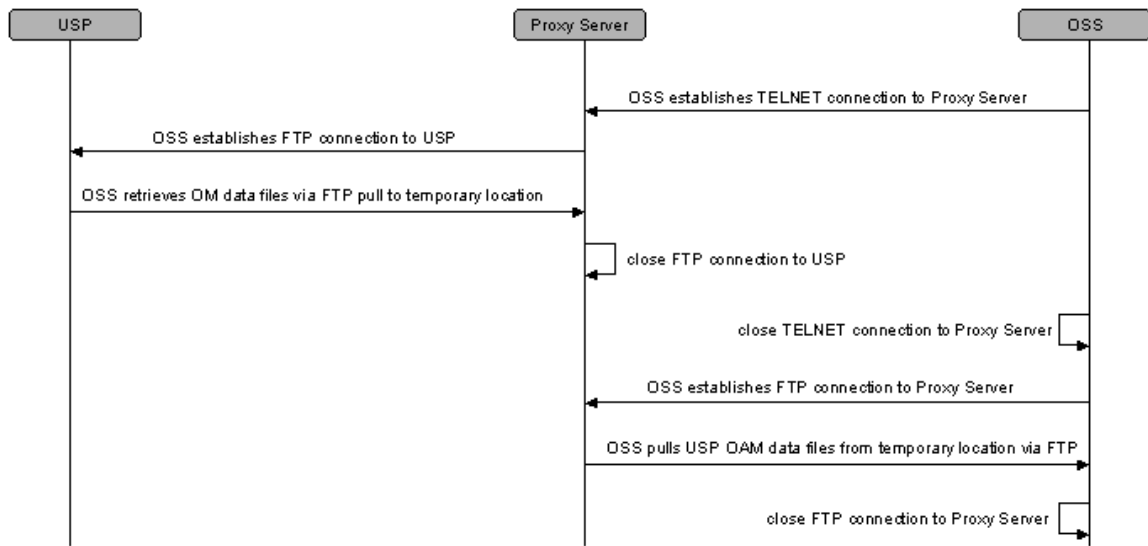
FTP base commands supported by the Vxworks FTP server running on the RTC

HELP USER PASS QUIT LIST NLST RETR STOR CWD TYPE PORT PWD STRU MODE ALLO ACCT PASV NOOP DELE

Using a 3-tier LAN architecture

In some cases it may be desirable to use an isolated three tier LAN architecture in order to satisfy network security requirements. In this configuration the OSS LAN does not have connectivity to the USP LAN. The OSS must make use of an intermediate proxy server to obtain FTP access to the USP.

In this scenario a combination of TELNET and FTP would need to be used in order to retrieve the USP OM files. The procedure is illustrated in the figure below.





SN07 IEMS Functionality

IEMS Northbound Interfaces

General Information

In SN07 the Integrated Element Management System (IEMS) at the central office level will:

- provide graphical topology and inventory relationships between the Network Elements (NEs) and EMS
- provide aggregation all of the EMS/NE fault data.
- provide integrated fault streams to the Network Management Layer (NML) through Integrated EMS.
- provide a customer choice of OSS fault interfaces (SCC2, SYSLOG, NT STD and SNMP)
- provide centralized performance management for network elements
- provide a centralized fault viewer with filtering capability
- provide context sensitive EMS launching, applications launching (ex TMM, LMM, and NPM) and NE CLUI launching.
- provide enhanced security through a more centralized administration of user accounts and passwords for EMS and NEs.

New or changed in SN07

SN07 IEMS Northbound Interface changes

Category	SN07 NB Interface Changes? Y/N	Backward Compatible w/SN06,6.2 Y/N/na	Section reference
Fault	Y	N	" IEMS Northbound Fault Interface"

Category	SN07 NB Interface Changes? Y/N	Backward Compatible w/SN06,6.2 Y/N/na	Section reference
Performance	Y	N/A (not available prior to SN07)	Please refer to Section “Northbound Performance Interface” on page 2568.
Inventory/Topology	Y	N/A (not available prior to SN07)	Please refer to Section “Inventory/Topology Interface” on page 2591.
Security	Y	Yes	Please refer to Section “Centralized Security Administration (Network Security)” on page 2591.

- The SN07 release adds NTSTD log format to the list of available Northbound fault feeds from IEMS. For more information see “Northbound NTSTD” on page 2534.
- The SN07 IEMS Northbound SNMP fault interface has been redefined based upon the IETF-compliant MIB. See “Northbound SNMP - IETF MIB specification” on page 2544 for detailed information.
- The IEMS Performance interface is new in SN07 and provides a common point of access for operational and performance data from integrated network elements.
- IEMS provides the ability to generate a snapshot of the entire network inventory and topology configuration to ACSII file for processing by downstream applications.
- Provide support for customer to centrally administer user accounts
- Provide Single Sign-on support - enables a user to log in once and access multiple Succession Network Elements, Applications, and features
- Customer Plug-ability - provides the ability for an OSS to plug-in it's own Authentication/Authorization and/or Single Sign-on solutions.

IEMS Northbound Fault Interface

User Setup, Administration, and Customization of Views

For information on initial setup and customization of the Northbound fault feed from IEMS see:

- IEMS Fault Management Guide - NN10334-911

Device Fault Mapping References for Northbound Interface

The following table shows the log identification criteria for each device, manager, and application supported by IEMS. Log references for table entries defined in *italics* can be found in:

NN10275-909 - Succession Fault Management Logs Reference (volumes 1-3)

See the table below for additional fault documentation

Fault Correlation for SN07 Devices

	NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
1	<i>“Audio Provisioning Server (APS)”</i>	Specific Problem	Specific Problem	Specific Problem	Specific Problem	NN10328-911 MS 2000 Series Fault Management
2	<i>“Call Agent Core”</i>	log name and log number	log name and log number	log name and log number	log name and log number	see “Fault documentation for Call Agent Core :”
3	<i>“Call Agent Platform”</i>	Logname and number	Logname and number	Logname and number	Logname and number	NN10087-911 Call Agent Fault Management
4	<i>CBM See “CS2000 Core Manager”</i>	log name and number	log name and number	log name and number	log name and number	See “CS2000 Core Manager”
5	<i>“Centrex IP Call Manager (CICM)”</i>	logname and number	logname and number	logname and number	logname and number	NN10233-911 CICM Fault Management
6	<i>“CS2000 Core Manager”</i>	log name and number	log name and number	log name and number	log name and number	NN10082-911 CS 2000 Core Manager Fault Management
7	<i>“Gateway Controller (GWC)”</i>	Logname and number	Logname and number	Logname and number	Logname and number	NN10090911 GWC Fault Management

	NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
8	“GWC Manager”	logname and number CMT 300,301	logname and number	logname and number	logname and number	PLN-07AT OSS SN07 OSS Guide (ATM) PLN-07IPOSS SN07 OSS Guide (IP)
9	“Media Application Server (MAS)”	Event Id	Event Id	Event Id	Event Id	NN10303-111 MCP 2.0 MAS Meetme Basics NN10297-111 MCP 2.0 MAS Adhoc Basics
10	“Multimedia Communication Server (MCS)”	logname and log number	logname and log number	logname and log number	logname and log number	NN10247-111 Multimedia Communication Server 5200 System Management Console User Guide
11	“Multi-Service Data Manager (MDM)”	log name and number	log name and number	log name and number	log name and number	NN10092-911 Passport 15000 and Preside MDM in Succession Networks Fault Management (PT-AAL1/UA-AAL1)
12	MDM for BSC see “Multi-Service Data Manager (MDM)”	log name and number	log name and number	log name and number	log name and number	see “Multi-Service Data Manager (MDM)”
13	MDM - carrier see “Multi-Service Data Manager (MDM)”	log name and number	log name and number	log name and number	log name and number	see “Multi-Service Data Manager (MDM)”

	NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
14	MDM Client-Server see “Multi-Service Data Manager (MDM)”	log name and number	log name and number	log name and number	log name and number	see “ Multi-Service Data Manager (MDM) ”
15	“MultiService Switch 7400, 15000, 20000”	log name and number	log name and number	log name and number	log name and number	NN10092-911 Passport 15000 and Preside MDM in Succession Networks Fault Management (PT-AAL1/UA-AAL1)
16	“Media Gateway 9000 (MG9000)”	Logname and number	Logname and number	Logname and number	Logname and number	NN10325-900 ATM/IP Fault Management
17	“MG9000 Manager”	logname and number	logname and number	logname and number	logname and number	NN10074-911 MG9000 Fault Management
18	“MS2000 Series Node”	logname and number	logname and number	logname and number	logname and number	NN10328-911 MS2000 Fault Management
19	“Network Patch Manager (NPM)”	logname and number	logname and number	logname and number	logname and number	N10084911 CS2000 Management Tools Fault Management
20	“Passport 8600”	logname and number	logname and number	logname and number	logname and number	241-6003-110 Preside Passport 8600 Device Integration Cartridge User Guide
21	“QoS Collector Application (QCA)”	logname and number	logname and number	logname and number	logname and number	NN10083-911 Communication Server 2000 Fault Management

	NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
22	“SAM21 Element Manager”	logname and number	logname and number	logname and number	logname and number	NN10089-911 SAM21 Shelf Controller Fault Management
23	“SAM21 Shelf Controller”	logname and number	logname and number	logname and number	logname and number	NN10089-911 SAM21 Shelf Controller Fault Management
24	“SDM Platform”	logname and number	logname and number	logname and number	logname and number	NN10081-911 SDM Fault Management
25	“Session Server Manager”	logname and number	logname and number	logname and number	logname and number	NN10332-911 Session Server Fault Management
26	“Succession Server Platform Foundation Software (SSPFS)”	logname and number	logname and number	logname and number	logname and number	NN10261- 450v2 Succession Network Volume 2 of 2
27	“Storage Manager (STORM)”	logname and number STM 800	logname and number	logname and number	logname and number	NN10088-911 Storm Fault Management
28	“Universal Audio Server (UAS)”	logname and number	logname and number	logname and number	logname and number	NN10275-909 v3 Succession Fault Management Logs Reference NN10073-911 UAS Fault Management

	NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
29	“Universal Signaling Point (USP)”	Specific Problem: Log Group=<text> & Log Number=<number> Note: Log GroupID is not used	Specific Problem: Log Group=<text> & Log Number=<number> Note: Log GroupID is not used	Specific Problem: Log Group=<text> & Log Number=<number> Note: Log GroupID is not used	Specific Problem: Log Group=<text> & Log Number=<number> Note: Log GroupID is not used	NN10071911 USP Fault Management
30	“XACore”	Logname and number	Logname and number	Logname and number	Logname and number	297-8991-510 XA-Core Maintenance Manual

IEMS Northbound Fault Specifications

In SN07, fault events are available from any of four Northbound interfaces. Log formats supported in this release are: NTSTD, SCC2, Syslog, and SNMP. A description of each of these interfaces is given in the sections that follow.

OSS clients can receive faults in **SCC2** and **NTSTD** formats from IEMS by initiating a TCP socket connection to designated ports on the IEMS server. When a connection attempt is made by a remote host, the IEMS validates the connecting OSS as an authorized client. It then forwards all logs that satisfy the configured filter criteria to the OSS. The port numbers and remote clients eligible to connect to these log streams are configured by the administrator.

Note: In legacy environments, the ECORE option was used to include the originating node name in the log header for SCC2 and NTSTD formats. This option is NOT supported with Nortel Networks Carrier VoIP solution. All references to ECORE in the following sections will assume this option is disabled.

Faults can be delivered to hosts via **SNMP** by configuring the IP address and port of the remote management application.

Note 1: By default, the following attribute values are used for configuring SNMP northbound fault feed. The administrator can change the above attribute values. Refer to the “Changing SNMP attributes for SNMP fault feeds” section to modify these values.

Note 2: • SNMP port: 8001

Note 3: • read community: public

Note 4: • **write community: public**

Note 5: • **SNMP version: v2c**

The standard **Syslog** interface can also be configured as a fault stream for remote management systems.

The following table summarizes the characteristics of the four Northbound fault feeds from IEMS.

IEMS Northbound Fault Stream Characteristics

Fault format	Port	OSS Connection	Stream type	IEMS Config required
NTSTD	8555	Incoming. IEMS waits for connection by remote host	ACSII stream over TCP, push	OSS IP address or hostname
SCC2	8556	Incoming. IEMS waits for connection by remote host	ACSII stream over TCP, push	OSS IP address or hostname
SNMP	user-defined on remote listener	IEMS forwards SNMP faults as SNMP traps to OSS. OSS can also query IEMS for active alarm data. By default, the following attribute values are used for configuring SNMP northbound fault feed. The administrator can change the attribute values. Default Settings: SNMP port: 8001 read community: public write community: public SNMP version: v2c	SNMP trap events (UDP), push	IP address and port of listener on OSS
Syslog	designated port for Syslog service (514)	IEMS forwards log events to remote host	ACSII data over UDP, push	syslog.conf requires forwarding entry for log facility Fault: local7.notice Audit: local0.notice Security: local3.notice

See *NN10321-111 - IEMS User Guide* for details on configuring these streams.

Each fault interface is discussed in the sections that follow.

Northbound SCC2 Specification

SCC2 is an ACSII stream delivered to a Northbound receiving application. The stream is delivered over a TCP socket and is configured by the administrator.

This section provides a detailed description of the SCC2 log format delivered by IEMS.

SCC2 Format Summary:

<Alarm Severity><Minute Indicator><Log Name><Log Number><Threshold>< Sequence Number><Event Type><Event Label><Equipment Identifier><Body Text>

SCC2 Header Formats

SCC2 Header format:

```

-----
12345678901234567890123456789012345678901234567890123456789012
3456789
-----|-----|-----|-----|-----|-----|
aabb\ccccdddeffff\gggg\h.../i.../j...
-----|-----|-----|-----|-----|-----|
-----

```

- 1 The backslash sign (\) signifies a space.
- 2 The forward slash sign (/) signifies a space that only appears if the preceding optional field exists.
- 3 The periods (...) signify variable length data.
- 4 The 'greater than' sign followed by periods (>...) signifies variable length indentation determined by the application.
- 5 The vertical lines do not appear on the actual report, they are used for presentation purposes in the above figure.
- 6 This notation only represents the header and does not include the application data area (i.e. the rest of the log report).

An example of a SCC2 log header is given below. It is also used in explaining the individual fields in the log header.

SCC2 Log Header Example:

```

* 03 PM 128+0417 TBL ISTB LIU7 348
      ISTb      From InSv

```

SCC2 Field Descriptions

Fld	Name	Description	Example
a	Alarm Severity	The severity level of the log report. This is a 2 character field left justified and padded with blanks. Possible values are: '*C' = critical alarm, '***' = major alarm, '* ' = minor alarm, ' ' = no alarm.	'**'
b	Minute Indicator	This value represents the minutes after the hour. It consists of 2 numeric characters, right justified and padded with zeroes. It ranges from 00 to 59.	'03'
c	Log Name	This value can be 2 to 4 non blank characters. Within this fixed 4 characters, it is left justified and padded with blanks.	'PM '
d	Log Number	This value is always 3 digits ranging from 000 to 999. It is right justified and padded with zeroes. For PROTOLOGs (i.e. TRAP, SWERR, INIT, INFO, and LOCK logs) it is a string of 3 spaces.	'128'
e	Threshold	Indicates whether a threshold was set for the given log report. A threshold can be temporarily set by using LOGUTIL. Thresholding will survive any restart by turning on the office parameter threshold_is_sampling in table OFCVAR and datafilling threshold value for individual log report in table LOGCLASS and RLOGCLAS on the CallServer. If THRESHOLD_IS_SAMPLING is on (Y), a log report is generated for every n-th instance of the log report generated. If threshold_is_sampling is off (N), every log report after the n-th report is generated. Possible values are: '+' = a threshold was set, ' ' = no threshold was set.	'+'
f	Sequence Number	This field defines the unique sequence for each log report. It is right justified and padded with zeroes. It represents 4 numeric characters ranging from 0000 to 9999.	'0417'

Fld	Name	Description	Example
g	Event Type	Log report event type which is a string of 4 uppercase characters, left justified and padded with blanks. This field is defined by the applications that generate the log report. Possible values include: ' ', 'CBSY', 'EXC ', 'FAIL', 'FLT ', 'INFO', 'INIT', 'LO ', 'MANB', 'OFFL', 'PASS', 'PBSY', 'RTS ', 'SUMM', 'SYSB', 'TBL ', 'TRAN', 'TRAP', 'UNEQ'.	'TBL '
h	Event Label	A variable length character string that represents application event description. It is an optional field.	'ISTB'
		<i>The following fields are defined by the applications that generate the log report. These fields are optional and independent of each other.</i>	
i	Equipment Identifier	A conditional equipment identifier determined by the application. It is a variable length character string.	'LIU7348'
j	Body Text	Application specific log body text starts here. This may contain several lines. Each new line is indented by eight spaces. Most log bodies start with a carriage return character so that none of it appears on the header line.	'ISTb From InSv'

Examples of Logs with SCC2 Header

The sample logs below are shown for example only. They are syntactically correct but field contents may vary.

1 Gateway Controller example

****14 GWC 307 7250 TBL GWC Fault**

Location: GWC-2-UNIT-0

NotificationID: 4

State: Raise

Category: Communications

Cause: Communications subsystem failure

Time: Jan 23 15:15:59 2004

Component Id: GWC=GWC-2-UNIT-0;Version=PGC92BA;Unit=unit_0;Software=NODE MTC

Specific Problem: EM not responding, provisioned data loaded from local Flash

Description: Element Manager communication failure.

2 Call Server example:

56 LINE138 3778 INFO TRMT

SLOA 21 1 02 01 DN 2145202111

TREATMENT SET = BUSY CALLED NO = 5202111

CALLID= 01BE 036D

Northbound NTSTD

NTSTD is an ACSII stream delivered to a Northbound receiving application. The stream is delivered over a TCP socket and is configured by the administrator.

This section provides a detailed description of the NTSTD log format delivered by IEMS.

NTSTD Format Summary:

<Office Identifier><Alarm Severity><Threshold><Log Name><Log Number><Time MMMMDD hh:mm:ss>< Sequence Number><Event Type><Event Label><Equipment Identifier><Body Text>

Standard Header Formats

ECORE Format OFF:

```
-----
-----
12345678901234567890123456789012345678901234567890123456789012
3456789
----- |----- |----- |----- |----- |----- |--
-----
a...#cccdeeeffff\ggghh\ii:jj:kk\llll\nnnn\o.../p.../q...
----- |----- |----- |----- |----- |----- |--
-----
```

Notes:

- 1 The placeholder represented by the pound sign (#) is non-existent if both office parameter log_office_id and ecore_format in table OFCVAR are turned off. The pound sign (#) represents a space in other cases (i.e. log_office_id is datafilled and ecore_format is turned off; and whenever ecore_format is turned on regardless of log_office_id).
- 2 The backslash sign (\) signifies a space.
- 3 The forward slash sign (/) signifies a space that only appears if the preceding optional field exists.
- 4 The periods (...) signify variable length data.

- 5 The vertical lines do not appear on the actual report, they are used for presentation purposes in the above figure.
- 6 This notation only represents the header and does not include the application data area (i.e. the rest of the log report).

An example of a standard log header is given below. It is also used in explaining the individual fields in the log header.

Standard log header example:

```
SCP2B *+ PM128 OCT20 10:03:42 0417 TBL ISTB LIU7 348
          ISTb      From InSv
```

NTSTD format field descriptions

FId	Name	Description	Example
a	Office Identifier	Identifies the switch generating the Identifier log. This is an optional field. It is output if the office parameter log_office_id in table OFCVAR on the CallServer is datafilled. It has variable length from 0 up to 12 characters.	'SCP2B'
b	Ecore Node Name	Originating node name where this log Node Name report is generated. It is an eight character field, its contents are left justified and padded with blanks. It is contained in the header if the office parameter ecore_format in table OFCVAR is turned on. As of SN07, this option is not supported	'CM'
c	Alarm Severity	The severity level of the log report. This is a 3 character field right justified and padded with blanks. Possible values are: '***' = critical alarm, ' **' = major alarm, ' *' = minor alarm, ' ' = no alarm.	' *'

Fld	Name	Description	Example
d	Threshold	Indicates whether a threshold was set for the given log report. A threshold can be temporarily set by using LOGUTIL. Thresholding will survive any restart by turning on the office parameter threshold_is_sampling in table OFCVAR and datafilling threshold value for individual log report in table LOGCLASS and RLOGCLAS on the CallServer. If threshold_is_sampling is on (Y), a log report is generated for every n-th instance of the log report generated. If threshold_is_sampling is off (N), every log report after the n-th report is generated. Possible values are: '+' = a threshold was set, ' ' = no threshold was set.	'+'
e	Log Name	This value can be 2 to 4 non blank characters. Within this fixed 4 characters, it is right justified and padded with blanks.	' PM'
f	Log Number	This value is always 3 digits ranging from 000 to 999. It is right justified and padded with zeroes. For PROTOLOGs, (ie. TRAP, SWERR, INIT, INFO and LOCK logs) it is a string of 3 spaces.	'128'
g	Month Indicator	Consists of 3 uppercase characters ranging from 'JAN' to 'DEC' that represent the month.	'OCT'
h	Day Indicator	Consists of 2 numeric characters ranging from 01 to 31 that represent the day of the month	'20'
i	Hour Indicator	Consists of 2 numeric characters ranging from 00 to 23 that represent the hour of the day.	'10'
j	Minute Indicator	Consists of 2 numeric characters ranging from 00 to 59 that represent the minute of the hour.	'03'
k	Second Indicator	Consists of 2 numeric characters ranging from 00 to 59 that represent the second of the minute.	'42'
l	Sequence Number	This field defines the unique sequence for each log report. It is right justified and padded left with zeroes. Represents 4 numeric characters ranging from 0000 to 9999.	'0417'

Fld	Name	Description	Example
n	Event Type	Log report event type which is a string of 4 uppercase characters, left justified and padded with blanks. This field is defined by the applications that generate the log report. Possible values include: ' ', 'CBSY', 'EXC ', 'FAIL', 'FLT ', 'INFO', 'INIT', 'LO ', 'MANB', 'OFFL', 'PASS', 'PBSY', 'RTS ', 'SUMM', 'SYSB', 'TBL ', 'TRAN', 'TRAP', 'UNEQ'.	'TBL'
o	Event Label	A variable length character string that represents application event description. This field is optional.	'ISTB'
		<i>The following fields are defined by the applications that generate the log report. These fields are optional and independent of each other.</i>	
p	Equipmnt Identifier	A conditional equipment identifier determined by the application. It is a variable length character string.	'LIU 7 348'
q	Body Text	Application specific log body text starts here. This may contain several lines. Each new line is indented by eight spaces. Most log bodies start with a carriage return character so that none of it appears on the header line.	'ISTb From InSv'

Examples of Logs with Standard Header

The sample logs below are shown for example only. They are syntactically correct but field contents may vary.

1 Gateway Controller example:

```

RTPU07BU  **  GWC307 Jan23 20:14:38 7250 TBL  GWC Fault
Location: GWC-2-UNIT-0
NotificationID: 4
State: Raise
Category: Communications
Cause: Communications subsystem failure
Time: Jan 23 15:15:59 2004
Component Id: GWC=GWC-2-UNIT-0;Version=PGC92BA;Unit=unit_0;Software=NODEMTC
Specific Problem: EM not responding, provisioned data loaded from local
Flash
Description: Element Manager communication failure.

```

2 Call Server example:

```

RTPU07BR      LINE138 Jan23 16:56:30 3778 INFO TRMT
SLOA 21 1 02 01      DN 2145202111
TREATMENT SET = BUSY   CALLED NO =                5202111
CALLID= 01BE 036D

```

Northbound Syslog

Syslog is a standardized UDP protocol defined by the IETF working group:
Syslog Protocol (RFC 3164): <http://www.ietf.org/rfc/rfc3164.txt>

This ACSII fault stream is delivered to a Northbound receiving Syslog host over the local 7 facility. On the IEMS server, Syslog routing is configured through the SSPFS command line interface. This interface manages any required changes to syslog.conf.

This section covers the vendor-specific information on the format and content of Syslog messages not covered under RFC3164.

The following shows a breakdown of the components of the MSG portion of a Syslog message provided by the IEMS Northbound interface:

```

<Time> <Host> IEMS:
_V2_~I=<NodeId>~H=<Host>~A=<ApplicationName>~S=<Seq.Number>
~~<LogName><LogNumber> <AlarmSeverity> <EventType> <Label> ^M
<LogBody>

```

The following Syslog message will be used to discuss the structure of Syslog messages from IEMS :

```

Feb 23 12:38:54 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=4317~~
MGEM302 NONE TBL MG9K InvalidEMIPAddress^M Location: MG9k EM
Comm Network^M Notification Id: 17180020453^M State:
Cleared^M Category: communications^M Cause: Communications
Subsystem Failure^M Invalid EM IP Address - An invalid EM IP
address has been set on the GW^M Component Id: MG9k EM Comm
Network^M specificProblem: Invalid EM IP Address - An invalid
EM IP address has be^M en set on the GW^M Description:
An invalid EM IP address has been set on the GW

```

Note: See “MG9000 Manager” for comparison of this log in all IEMS Northbound formats.

RFC3164 MSG Fields

Each Syslog message is prefixed by a timestamp and hostname. These fields are shown in *italics* in the example above. Section 4.1.2 of RFC3164 defines these fields as follows:

The **TIMESTAMP** field is the local time and is in the format of "Mmm dd

hh:mm:ss" (without the quote marks) where:

Mmm is the English language abbreviation for the month of the year with the first character in uppercase and the other two characters in lowercase. The following are the only acceptable values:

Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec

dd is the day of the month. If the day of the month is less than 10, then it **MUST** be represented as a space and then the number. For example, the 7th day of August would be represented as "Aug 7", with two spaces between the "g" and the "7".

hh:mm:ss is the local time. The hour (hh) is represented in a 24-hour format. Valid entries are between 00 and 23, inclusive. The minute (mm) and second (ss) entries are between 00 and 59 inclusive.

*A single space character **MUST** follow the **TIMESTAMP** field.*

The **HOSTNAME** field will contain only the hostname, the IPv4 address,

or the IPv6 address of the originator of the message. The preferred value is the hostname. If the hostname is used, the **HOSTNAME** field **MUST** contain the hostname of the device as specified in STD 13 [4].

It should be noted that this **MUST NOT** contain any embedded spaces.

The Domain Name **MUST NOT** be included in the **HOSTNAME** field. If the IPv4 address is used, it **MUST** be shown as the dotted decimal notation as used in STD 13 [5]. If an IPv6 address is used, any valid representation used in RFC 2373 [6] **MAY** be used.

*A single space character **MUST** also follow the **HOSTNAME** field.*

IEMS Header

After the timestamp and hostnames fields, the following constants can be found in the next two fields - separated by a space:

IEMS: Indicates the start of fault-specific information

V2 - Syslog format version

Immediately following this tag are several attributes specified as name-value pairs (NVPs). NVP tags are prefixed by a tilde '~' <tag>=<value> for easy identification by downstream parsers.

NVPs for IEMS Syslog message

Tag name	Description	example
~I	Node Identifier	~I=
~H	Host name of	~H=znc0s0jh
~A	Reporting Application name	~A=IEMS
~S	Log Sequence number	~S=4317
~~	Indicates start of formatted log header from originator. **Note: This indicator is NOT actually an NVP. It is followed by a single space character	~~ MGEM302 NONE TBL MG9K InvalidEMI PAddress

Parsing Conventions for Formatted Log Data:

The format of the log header and body follow a number of conventions to facilitate parsing by downstream applications:

- 1 Line feeds in message text are identified by the ^M character sequence (this denotes a sequence of the two printable characters: caret and upper case M).
- 2 The log header start can be identified by the ~~ sequence followed by a space. The header is delimited by the line feed indicator (discussed in the previous bullet).
- 3 The log body is separated into lines using ^M sequences defined in bullet 1. Each line is prefixed with eight (8) space characters.
- 4 Line length (including leading spaces) will not exceed 80 characters . See example log above.
- 5 All text in the log header and body will consist of printable ACSII characters.

- 6 Blank lines are not allowed in the formatted log message. This includes both header and body components.

Log Header

The log header consists of the following fields. These fields map to the corresponding fields defined in both SCC2 and NTSTD.

A typical log header will appear in the following format (' ' indicates a space character):

```
~~\<logname><lognumber>\<AlarmSeverity>\<EventType>\<Label>^M<LogBody>
```

Log Header fields in Syslog message

Name	Description	Example
Log Name	This value can be 2 to 4 non blank characters. Within this fixed 4 characters, it is right justified and padded with blanks.	' MGEM'
Log Number	This value is always 3 digits ranging from 000 to 999. It is right justified and padded with zeroes. For PROTOLOGs, (ie. TRAP, SWERR, INIT, INFO and LOCK logs) it is a string of 3 spaces.	'302'
Alarm Severity	This field defines the alarm severity and consists of one of the following text strings: NONE, MINOR, MAJOR, CRIT	'NONE'
Event Type	Log report event type which is a string of 4 uppercase characters, left justified and padded with blanks. This field is defined by the applications that generate the log report. Possible values include: ' ', 'CBSY', 'EXC ', 'FAIL', 'FLT ', 'INFO', 'INIT', 'LO ', 'MANB', 'OFFL', 'PASS', 'PBSY', 'RTS ', 'SUMM', 'SYSB', 'TBL ', 'TRAN', 'TRAP', 'UNEQ'.	'TBL '
Label	A variable length character string that represents application event description. This field is optional.	'MG9K InvalidEMIPAddress'

Name	Description	Example
Log Body	Application specific log body text starts here. This may contain several lines. Each new line is indented by eight spaces and delimited by the ^M (caret-M) character sequence.	<pre> Location: MG9k EMCommNetwork^M Notification Id: 17180020453^M State: Cleared^M Category: communications^M Cause: Communications SubsystemFailure^M Invalid EM IP Address - An invalid EM IP address has been set on the GW^M Component Id: MG9k EMCommNetwork^M specificProblem: Invalid EM IP Address - An invalid EM IP address has be^M en set on the GW^M Description: An invalid EM IP address has been set on the GW' </pre>

Notes on Log Body Text

The remainder of the message consists of the log body. The message text in this portion of the message is defined by the originating source. The presentation of this text is constrained only by the rules outlined in “[Parsing Conventions for Formatted Log Data:](#)” on page 2540.

Note: See Syslog Protocol (RFC 3164):

<http://www.ietf.org/rfc/rfc3164.txt> for full details on this specification.

Security and Audit logs

IEMS Security and Audit logs are managed through Syslog and can be forwarded to a remote Syslog host in the same way as fault events. Sample content of each follow:

Audit log sample (/var/log/auditlog):

```

Jan 16 10:37:55 sspfs_svr ID[SUNWcluster.pmf.1020]: "CorbaNotification" requested
Jan 16 10:38:06 sspfs_svr ID[SUNWcluster.pmf.1018]: "CorbaNotification" Failed to stay
up.
Jan 16 10:38:06 sspfs_svr ID[SUNWcluster.pmf.1019]: "CorbaNotification" restarting too
often ... sleeping 30 seconds.

```

```

Jan 16 10:38:36 sspfs_svr ID[SUNWcluster.pmf.1020]: "CorbaNotification" requeued
Jan 16 10:38:46 sspfs_svr ID[SUNWcluster.pmf.1018]: "CorbaNotification" Failed to stay
up.
Jan 16 10:38:46 sspfs_svr ID[SUNWcluster.pmf.1019]: "CorbaNotification" restarting too
often ... sleeping 30 seconds.
Jan 16 10:39:16 sspfs_svr ID[SUNWcluster.pmf.1020]: "CorbaNotification" requeued
Jan 16 10:41:42 sspfs_svr ID[SUNWcluster.pmf.1018]: "snmpp" Failed to stay up.
Jan 16 10:42:16 sspfs_svr ID[SUNWcluster.pmf.1018]: "omppush" Failed to stay up.
Jan 16 10:42:41 sspfs_svr ID[SUNWcluster.pmf.1018]: "CorbaNotification" Failed to stay
up.
Jan 16 10:42:41 sspfs_svr ID[SUNWcluster.pmf.1020]: "CorbaNotification" requeued
Jan 16 10:42:49 sspfs_svr ID[SUNWcluster.pmf.1018]: "PropServer" Failed to stay up.

```

Security log sample (/var/log/securitylog):

```

Feb  6 22:03:16 wnc0s0qh IEMS: IEMS class_security.ver01 STAT=SUCCESS SRC.USR=root
EVNT.TYPE =Authentication
Feb  6 22:03:16 wnc0s0qh last message repeated 1 time
Feb  9 14:34:33 wnc0s0qh IEMS: IEMS class_security.ver01 STAT=SUCCESS SRC.USR=root
EVNT.TYPE =Authentication
Feb  9 14:34:33 wnc0s0qh last message repeated 1 time
Feb  9 15:36:20 wnc0s0qh IEMS: IEMS class_security.ver01 STAT=SUCCESS SRC.USR=root
EVNT.TYPE =Authentication
Feb  9 15:36:20 wnc0s0qh last message repeated 1 time
Feb 11 10:15:53 wnc0s0qh IEMS: IEMS class_security.ver01 STAT=SUCCESS SRC.USR=root
EVNT.TYPE =Authentication
Feb 11 10:15:53 wnc0s0qh last message repeated 1 time

```

The following table shows a summary of all Syslog facilities used by IEMS.

Note: Only *Fault*, *Audit*, and *Security* streams are supported for use by downstream systems. Shaded entries are intended for support purposes only.

IEMS Northbound Syslog Facilities

Log Stream	Log file location on IEMS Server	Syslog facility
Fault	/var/log/iemsCustomerlog	local7
Audit	/var/log/auditlog	local0
Security	/var/log/securitylog	local3

Log Stream	Log file location on IEMS Server	Syslog facility
Customer log	/var/log/customerlog	local1
Debug	/var/log/debuglog	local2
SSPFS	/var/log/sspfslog	local4
NPM	/var/log/npm_designlog	local5

Northbound SNMP - IETF MIB specification

IEMS provides an SNMP interface that forwards faults in trap messages and responds to SNMP requests.

The SNMP Northbound interface is based on the IETF RFC 3877 standard which includes features such as alarm synchronization not available with NTSTD or SCC2.

This section provides a high-level description of how to support the IETF Alarm MIB draft defined in the DISMAN working group of the IETF. See the MIBs on the server in the locations specified in the table below. In this document, IEMS is the agent implementing the MIBs for the manager at the OSS level.

SN07 MIB Loading Sequence

In SN07, the MIB loading sequence for a manager application is as follows:

These MIBs are available on the IEMS server in the locations noted in the following table.

MIB Loading Sequence

Load Order	MIB Name	IEMS Server File location
1	SNMPv2-MIB	/opt/nortel/iems/current/mibs/ SNMPv2-MIB.txt
2	SNMP-FRAMEWORK-MIB	/opt/net-snmp/share/snmp/mibs/ SNMP-FRAMEWORK-MIB.txt
3	INET-ADDRESS-MIB	/opt/net-snmp/share/snmp/mibs/ INET-ADDRESS-MIB.txt
4	ALARM-MIB	/opt/nortel/iems/current/mibs/usp/ ALARM-MIB-disman-18.txt

Load Order	MIB Name	IEMS Server File location
5	IANA-ITU-ALARM-TC	/opt/nortel/iems/current/mibs/usp/ IANA-ITU-ALARM-TC-disman-18.txt
6	ITU-ALARM-TC	/opt/nortel/iems/current/mibs/usp/ ITU-ALARM-TC-disman-18.txt
7	ITU-ALARM-MIB	/opt/nortel/iems/current/mibs/usp/ ITU-ALARM-MIB-disman-18.txt
8	ITU-IANA-ALARM-TC	/opt/nortel/iems/current/mibs/usp/ ITU-IANA-ALARM-TC-disman-04.txt
9	NOTIFICATION-LOG-MIB	/opt/nortel/iems/current/mibs/usp/ NOTIFICATION-LOG-MIB-rfc3014.txt
10	NORTEL-MIB	/opt/nortel/iems/current/mibs/usp/nortel.mib
11	NORTEL-GENERIC-MIB	/opt/nortel/iems/current/mibs/usp/ nortelGenericMIBs-smi2.mib
12	ENTITY-MIB	/opt/nortel/iems/current/mibs/usp/ ENTITY-MIB-entmib-03.txt
13	ENTITY-STATE-MIB	/opt/nortel/iems/current/mibs/usp/ ENTITY-STATE-MIB-entmib-01.txt
14	NORTEL-ALARM-EXT-MIB	/opt/nortel/iems/current/mibs/usp/ nortel_alarm_ext_smi.txt
15	NORTEL-NMI-MIB	/opt/nortel/iems/current/mibs/usp/ nortelNMI-smi2.smi
16	NORTEL-NMI-ALARM-CLEAR-MIB	/opt/nortel/iems/current/mibs/usp/ nortelNMIalarmClear_smi.txt

Support for the IETF Alarm MIB is new to IETF in the SN07 release. The MIBs defined by the DISMAN working group of IETF are designed to allow surveillance of network elements. We have used this set of MIBs to present the state of our softswitch. The ALARM MIB presents a set of tables that contain

the current alarm information for the device. The alarm MIB does not prescribe the notifications used to set and clear alarms on the device.

Nortel has provided an extension MIB to allow a manager to monitor the system alarm changes through SNMP notifications. These notifications are the primary interface for monitoring faults in the Succession node.

Nortel Alarm Extension MIB

This MIB defines notifications used for alarm asserts and clears in addition to data type definitions and tables related to notifications that can be sent.

A complete listing and description of our fault management MIB may be found in “Appendix 2: Nortel Alarm Extension MIB”.

TABLE SUPPORT IN NORTEL ALARM EXTENSION MIB

The table `nnExtAlarmActiveTable` along with the `AlarmActiveTable` contains all the information required to resynchronize the northbound SNMP agent and to give the OSS a complete view of the active alarms within the scope of the Integrated EMS.

The `nnExtAlarmStateTable` is not supported at this time.

NOTIFICATION SUPPORT IN NORTEL ALARM EXTENSION MIB

All notifications defined in this MIB are supported. All OIDs defined within the notifications are also populated. The alarm notifications include sequence numbers so the SNMP manager can determine if a message is missed. Specific formats are supported as described in the following table.

Alarm Notifications Varbinds

Variable name	Format	OID
alarmActiveResourceId	OID	.1.3.6.1.2.1.118.1.2.2.1.10
alarmActiveDateAndTime	DateandTime	.1.3.6.1.2.1.118.1.2.2.1.2
alarmActiveDescription	Human readable string	1.3.6.1.2.1.118.1.2.2.1.11
nnExtAlarmActiveEventType	Enum	.1.3.6.1.4.1.562.29.6.1.1.1.1
nnExtAlarmActiveProbableCause	Enum	.1.3.6.1.4.1.562.29.6.1.1.1.2
nnExtAlarmActiveAdditionalText	String	.1.3.6.1.4.1.562.29.6.1.1.1.3
nnExtAlarmActiveDocumentation Pointer	String: up to 4 chars + 3 digits	.1.3.6.1.4.1.562.29.6.1.1.1.4

Variable name	Format	OID
nnExtAlarmActiveResourceDescription	compType=compname; subcompType=subcompName; for as many levels of hierarchy is required to identify the alarmed entity	.1.3.6.1.4.1.562.29.6.1.1.1.5
nnExtAlarmActiveManualClear	enum	.1.3.6.1.4.1.562.29.6.1.1.1.6
nnExtAlarmActiveSequenceNumber	Numeric	.1.3.6.1.4.1.562.29.6.1.1.1.7

These varbinds are included in all 5 of the alarm notifications supported by the Integrated EMS. As defined all notifications in SNMP, *sysUpTime* and the OID of the notification are included in the varbinds for all notification types (see the following table). Each of the notifications signifies a different severity of the specified alarm. Notifications are defined for critical, major, minor, warning and cleared alarms. The notifications are defined in the table below.

Trap OIDs and Alarm Severity

Trap OID	Severity
.1.3.6.1.4.1.562.29.6.1.0.306	nnExtAlarmMessage
.1.3.6.1.4.1.562.29.6.1.0.305	nnExtAlarmCritical
.1.3.6.1.4.1.562.29.6.1.0.304	nnExtAlarmMajor
.1.3.6.1.4.1.562.29.6.1.0.303	nnExtAlarmMinor
.1.3.6.1.4.1.562.29.6.1.0.302	nnExtAlarmWarning
.1.3.6.1.4.1.562.29.6.1.0.301	nnExtAlarmClear

The nnExtAlarmMessage notifications can be used to send informational messages from IEMS. Because these notifications are information, reliability is not addressed. As illustrated in the table below, we populate with information in the message header and bodytext of our NTSTD and CUSTLOG feeds.

Message Notification Varbinds

Variable name	Format	OID
nnExtAlarmMessageResource	OID	.1.3.6.1.4.1.562.29.6.1.3.1.1

Variable name	Format	OID
nnExtAlarmMessageResourceDescription	String	.1.3.6.1.4.1.562.29.6.1.3.1.2
nnExtAlarmMessageDateAndTime	DateAndTime	.1.3.6.1.4.1.562.29.6.1.3.1.3
nnExtAlarmMessageDocumentationPointer	String	.1.3.6.1.4.1.562.29.6.1.3.1.4
nnExtAlarmMessageInfo	String	.1.3.6.1.4.1.562.29.6.1.3.1.5
nnExtAlarmMessageResource	OID	.1.3.6.1.4.1.562.29.6.1.3.1.1

OTHER DEFINITIONS IN THIS MIB

This MIB also defines OSI state variables that are not defined in the IETF Entity State MIB. These variables and tables are not supported at this time.

IETF RFC 3877 MIB Tables

There are several tables introduced by the IETF Alarm MIB Model. This document will discuss each table and intended use.

ALARM MODEL TABLE

This table defines the notifications used by IEMS to express alarm events. Notifications to communicate alarm asserts and clears have been defined by NortelNetworks in a separate MIB. These new notifications are defined in “Nortel Alarm Extension MIB” on page 2546.

This table is not currently supported. This table is a static table and we will look to support this in some future release. This table provides model documentation to OSSes.

ALARM ACTIVE TABLE

This table contains a list of active alarms on IEMS and is supported. It, along with 2 other tables - the alarm active variable table and the Nortel Alarm Extension Table - provide a complete view of the active alarms within the scope of the Integrated EMS.

Indexes into this table are: *alarmListName*, *alarmActiveDateAndTime*, *alarmActiveIndex*. *AlarmListName* matches the index *nlnLogName* for *nlnLogTable* from RFC3014 (Notification Log MIB). For our Succession IEMS table we use the string "Nortel_fault".

The following table describes expected values for entries in this table.

IETF Alarm Active Entry

Sequence Field	Default Value
alarmListName	Nortel_fault
alarmActiveDateAndTime	none
alarmActiveIndex	Numerical index defined by agent, unique in table
alarmActiveEngineID	IEMS agent engine ID in SNMPv3; empty string in SNMPv2
alarmActiveEngineAddressType	Inet address type (IPv4)
alarmActiveEngineAddress	IPv4 address of active IEMS agent
alarmActiveContextName	""
alarmActiveVariables	12 = number of fields in our alarm set notifications + 2 mandatory entries per alarm
alarmActiveNotificationID	OID of notification sent for this alarm set
alarmActiveResourceID	OID that describes this entry in the Active Alarm Table
alarmActiveDescription	none
alarmActiveLogPointer	not implemented - default = 0.0
alarmActiveModelPointer	not implemented - default = 0.0
alarmActiveSpecificPointer	not implemented - default = 0.0

ALARM ACTIVE VARIABLE TABLE

Alarm Active variable table contains the varbinds for all the active alarm notifications. The indexes to the table are: *alarmListName*, *alarmActiveIndex*, *alarmVariableIndex*. For each alarm in the alarm active table there will be 12 entries in the alarm active variable table. The index *alarmVariableIndex* will be from 1 to 12 (also from 1 to *alarmActiveVariables* in the *alarmActiveTableEntry*). The notifications contain some varbinds that are not in the standard table so the OSS can index into this table to get the additional data. (Similarly, the OSS can index into the Nortel Extension Active Alarm Table for the additional information as well.)

Fields in this table for each alarm are as follows:

Alarm Active Variable Table

Alarm Active Variable Entry	Notification Varbind	Default Value
alarmActiveVariableIndex 1	sysUpTime	sysUpTime

Alarm Active Variable Entry	Notification Varbind	Default Value
alarmActiveVariableIndex 2	snmpTrapOID	snmpTrapOID
alarmActiveVariableIndex 3	alarmActiveResourceId	OID that describes this entry in the Active Alarm Table
alarmActiveVariableIndex 4	alarmActiveDescription	none
alarmActiveVariableIndex 5	alarmActiveDateAndTime	none
alarmActiveVariableIndex 6	nnExtAlarmActiveEventType	none
alarmActiveVariableIndex 7	nnExtAlarmActiveProbableCause	none
alarmActiveVariableIndex 8	nnExtAlarmActiveAdditionalText	none
alarmActiveVariableIndex 9	nnExtAlarmActiveDocumentationPointer	This is often logname & number
alarmActiveVariableIndex 10	nnExtAlarmActiveResourceDescription	none
alarmActiveVariableIndex 11	nnExtAlarmActiveManualClear	none
alarmActiveVariableIndex 12	nnExtAlarmActiveSequenceNumber	none

ALARM CLEAR TABLE

This table provides an interface for SNMP managers to clear alarms on devices which support this operation. Manual clears are performed with SNMP SET operations using the alarmActiveIndex of the alarm to be cleared. See section “Manual Clear” on page 2560 for details.

ACTIVE ALARM STATS TABLE

Not supported.

ITU ALARM ACTIVE TABLE

Not supported.

ITU ALARM ACTIVE VARIABLE TABLE

Not supported.

ITU ALARM ACTIVE STATS TABLE

Supported.

NLM LOG TABLE (RFC 3014)

NLM Log Table is defined in IETF RFC 3014. Implementation of the MIB is provided to support incremental resynchronization of the OSS. The OSS SNMP managers can reach into the `nlmLogTable` to get missed events. See [Notification Log MIB \(RFC 3014\)](http://www.ietf.org/rfc/rfc3014.txt?number=3014):
<http://www.ietf.org/rfc/rfc3014.txt?number=3014>.

The Notification Log MIB has 3 different MIB groups:

- configuration parameters dealing with log storage and reporting
- statistics of log reporting
- the actual history of notifications

Configuration

Configuration defines the size and the aging criteria of the *nlmLogTable*. Table *nlmConfigLogTable* also defines the named log entries supported in the *nlmLogTable*. We use a specific named log entry for allowing fault resync. This table also defines filtering of these logs.

Each entry in the config log table contains: *nlmLogName*, *nlmConfigLogFilterName*, *nlmConfigLogEntryLimit*, *nlmConfigLogAdminStatus*. This table enables Alarm notification resynchronization. The first and only entry in this table has an *nlmLogName* that matches the *alarmListName* index for the active alarm tables above. This index is "Nortel_fault."

nlmConfigLogFilterName is defined as "default". We do not support the correlation of this value to any specific data in the *snmpNotifyFilterTable* in the SNMP Notification MIB.

nlmConfigLogEntryLimit defines the size of the log table. This defines the number of alarm events that are available to the SNMP manager through the SNMP agent. Since there is only one entry in this table for Nortel_fault, this value is over-ridden by *nlmConfigGlobalEntryLimit*.

Note: It is recommended that *nlmConfigGlobalEntryLimit* be set to a minimum value as it maintains this history in memory. Do **not** set this value to zero. Setting this value to zero will lead to unlimited entries being saved and lead to potential resource issues in the system.

nlmConfigLogAdminStatus is set to enabled (1).

nlmConfigLogOperStatus is set to noFilter (3).

nlmConfigLogStorageType is a storageType OID. Data associated with this entry is considered volatile and will be lost when the agent is restarted.

SNMP sets for the configuration items in this table are not supported.

Statistics

The statistics group contains two scalars and a table. The table is required for the resync algorithm. The table *nlmStatsLogTable* augments the *nlmConfigLogTable* and has only two values in each entry: *nlmStatsLogNotificationsLogged* and *nlmStatsLogNotificationsBumped*. Because this table augments the *nlmConfigLogTable*, the index for these notifications uses the same key - "Nortel_fault"

nlmStatsLogNotifications for the named logs in Nortel_fault is the sequence number (*nnExtAlarmActiveSequenceNumber*) sent in Integrated EMS notifications of the faults. This also provides the secondary index into the *nlmLogTable* for notifications that have been missed - as detected through sequence numbers in those notifications.

It is the responsibility of the SNMP agent sending fault notifications to increment the *nlmStatsLogNotificationsLogged* and include the value in the varbinds of that notification as documented.

nlmStatsGlobalNotificationsBumped defines the number of logs that have been removed or "bumped" from the log table due to the limits imposed by the *nlmConfigGlobalEntryLimit* setting.

Log Table

The *nlmLogTable* contains the history of notifications sent to the manager. The indices are: *nlmLogName* and *nlmLogIndex*. *nlmLogName* is "Nortel_fault" and the *nlmLogIndex* is the sequence number in the proprietary notifications.

This section defines two tables: *nlmLogTable* and *nlmLogVariableTable*. The first provides the indices for retrieving missed notifications, and the second contains the varbinds for the notifications. We have 2 different size alarm notifications (in terms of number of varbinds)- alarm assert notifications are all the same size, and alarm clear notifications are slightly smaller (1 varbind). Only alarm notifications are stored in the log table, message notifications are not logged in this table.

The structure and implementation of the *nlmLogVariableTable* is the same as that of the *alarmActiveVariableTable* and is not described further.

Connecting to the NB feed:

The default SNMP Port in which the agent is listening is 8001. This port is configurable through the IEMS client. User can also disable the SNMP agent if he wishes. OSS has to register its SNMP manager host and port to which the traps are to be sent.

Connection Reliability

There are several scenarios which must be considered by an SNMP manager to ensure that the alarms presented at the OSS layer will be in sync with the actual alarms maintained on the device. Resynchronization will be required when either the OSS or the IEMS system goes through a restart, or when a lost trap is detected. See section “ Message Sequences and Manager Operations” on page 2558 for details on resynchronization of active alarms.

Lost Traps

If the OSS detects a lost trap via an out-of-order sequence number, the OSS must either try to recover the lost sequence numbers from the notification log table or re-synchronize from the the active alarm table. The notification log MIB will contain the last 25 traps sent. If the sequence number delta is within this range, the notification log table can be used to obtain missed traps. Otherwise, a read of the active alarm table must be used to determine the active alarms in the system.

Additionally, OSS can poll the sequence number of the last alarm or clear sent from the agent. The sequence number of last notification sent will be in the *nlmStatsLogNotifications* table in the *nlmStatsLogNotificationsLogged* variable in the “Nortel_fault” entry as described above.

Note: Since there is only one entry in this table, the scalar *nlmStatsGlobalNotificationsLogged* can also be used to obtain this value.

SNMP Alarm Events & Correlation

The *alarmActiveResourceID* uniquely identifies an alarm occurrence in the system. To correlate a clear notification to the appropriate assert, the *alarmActiveResourceID* must be used.

Event Types and ProbableCauses

Each alarm notification and record in the alarm table includes event type and probable cause. Values for these fields are define in the IANA-ITU-ALARM-TC MIB table. These values come from both the X.7xx and M.3100 series of standards.

Alarm Event Type Format:

IANAItuEventType - Valid values for this entry are provided here for convenience.

- other (1),
- communicationsAlarm (2),
- qualityOfServiceAlarm (3),
- processingErrorAlarm (4),
- equipmentAlarm (5),

environmentalAlarm (6),
integrityViolation (7),
operationalViolation (8),
physicalViolation (9),
securityServiceOrMechanismViolation (10),
timeDomainViolation (11)

Probable Cause Format:

IANAItuProbableCause - Valid values for this entry are provided here for convenience.

aIS (1), callSetUpFailure (2), degradedSignal (3),
farEndReceiverFailure (4), framingError (5), lossOfFrame (6),
lossOfPointer (7), lossOfSignal (8), payloadTypeMismatch (9),
transmissionError (10), remoteAlarmInterface (11), excessiveBER
(12), pathTraceMismatch (13), unavailable (14), signalLabelMismatch
(15), lossOfMultiFrame (16), receiveFailure (17), transmitFailure (18),
modulationFailure (19), demodulationFailure (20),
broadcastChannelFailure (21), connectionEstablishmentError (22),
invalidMessageReceived (23), localNodeTransmissionError (24),
remoteNodeTransmissionError (25), routingFailure (26),
backplaneFailure (51), dataSetProblem (52),
equipmentIdentifierDuplication (53), externalIFDeviceProblem (54),
lineCardProblem (55), multiplexerProblem (56),
nEIdentifierDuplication (57), powerProblem (58), processorProblem
(59), protectionPathFailure (60), receiverFailure (61),
replaceableUnitMissing (62), replaceableUnitTypeMismatch (63),
synchronizationSourceMismatch (64), terminalProblem (65),
timingProblem (66), transmitterFailure (67), trunkCardProblem (68),
replaceableUnitProblem (69), realTimeClockFailure (70),
antennaFailure (71), batteryChargingFailure (72), diskFailure (73),
frequencyHoppingFailure (74), iODeviceError (75),
lossOfSynchronisation (76), lossOfRedundancy (77),
powerSupplyFailure (78), signalQualityEvaluationFailure (79),
tranceiverFailure (80), protectionMechanismFailure (81),
protectingResourceFailure (82), airCompressorFailure (101),
airConditioningFailure (102), airDryerFailure (103),
batteryDischarging (104), batteryFailure (105),
commercialPowerFailure (106), coolingFanFailure (107),
engineFailure (108), fireDetectorFailure (109), fuseFailure (110),
generatorFailure (111), lowBatteryThreshold (112), pumpFailure
(113), rectifierFailure (114), rectifierHighVoltage (115),
rectifierLowFVvoltage (116), ventilationsSystemFailure (117),
enclosureDoorOpen (118), explosiveGas (119), fire (120), flood (121),
highHumidity (122), highTemperature (123), highWind (124),

iceBuildUp (125), intrusionDetection (126), lowFuel (127), lowHumidity (128), lowCablePressure (129), lowTemperature (130), lowWater (131), smoke (132), toxicGas (133), coolingSystemFailure (134), externalEquipmentFailure (135), externalPointFailure (136), storageCapacityProblem (151), memoryMismatch (152), corruptData (153), outOfCPUCycles (154), sfwrEnvironmentProblem (155), sfwrDownloadFailure (156), lossOfRealTime (157), applicationSubsystemFailure (158), configurationOrCustomisationError (159), databaseInconsistency (160), fileError (161), outOfMemory (162), softwareError (163), timeoutExpired (164), underlyingResourceUnavailable (165), versionMismatch (166), adapterError (500), applicationSubsystemFailure (501), bandwidthReducedX733 (502), callEstablishmentError (503), communicationsProtocolError (504), communicationsSubsystemFailure (505), configurationOrCustomizationError (506), congestionX733 (507), corruptData (508), cpuCyclesLimitExceeded (509), dataSetOrModemError (510), degradedSignalX733 (511), dteDceInterfaceError (512), enclosureDoorOpenX733 (513), equipmentMalfunction (514), excessiveVibration (515), fileErrorX733 (516), fireDetected (517), framingErrorX733 (518), heatingVentCoolingSystemProblem (519), humidityUnacceptable (520), inputOutputDeviceError (521), inputDeviceError (522), lanError (523), leakDetected (524), localNodeTransmissionErrorX733 (525), lossOfFrameX733 (526), lossOfSignalX733 (527), materialSupplyExhausted (528), multiplexerProblemX733 (529), outOfMemoryX733 (530), outputDeviceError (531), performanceDegraded (532), powerProblems (533), pressureUnacceptable (534), processorProblems (535), pumpFailureX733 (536), queueSizeExceeded (537), receiveFailureX733 (538), receiverFailureX733 (539), remoteNodeTransmissionErrorX733 (540), resourceAtOrNearingCapacity (541), responseTimeExcessive (542), retransmissionRateExcessive (543), softwareErrorX733 (544), softwareProgramAbnormallyTerminated (545), softwareProgramError (546), storageCapacityProblemX733 (547), temperatureUnacceptable (548), thresholdCrossed (549), timingProblemX733 (550), toxicLeakDetected (551), transmitFailureX733 (552), transmitterFailure (553), underlyingResourceUnavailable (554), versionMismatchX733 (555), -
- The following are defined in X.736 authenticationFailure (600), breachOfConfidentiality (601), cableTamper (602), delayedInformation (603), denialOfService (604), duplicateInformation (605), informationMissing (606), informationModificationDetected (607), informationOutOfSequence (608), keyExpired (609), nonRepudiationFailure (610), outOfHoursActivity (611), outOfService (612), proceduralError (613),

unauthorizedAccessAttempt (614), unexpectedInformation (615),
other (1024).

Northbound Fault Mapping

The following table shows the correlation between the fields of the supported Northbound fault feeds.

Northbound Fault Format Summary

Row#	IEMS Schema	SYSLOG	NTSTD	SCC2	SNMP
1.	Severity 1= critical 2 = major 3 = minor 4= warning 5 =clear 6 = info	Alarm Severity CRIT =1, MAJOR =2, MINOR =3, NONE =4,5,6 None	1 = '****' 2 = '*** ' 3 = '* ' 4,5,6 = ' ' 6 = ' '	1 = '*C' 2 = '***' 3 = '* ' 4,5,6 = ' ' 6 = ' '	Based on the severity the concerned alarm, appropriate notification will be sent. nnExtNotificationPrefix : .1.3.6.1.4.1.562.29.6.1.0 Alarm Events: nnExtAlarmCritical = 1 .1.3.6.1.4.1.562.29.6.1.0.30 5 nnExtAlarmMajor = 2 .1.3.6.1.4.1.562.29.6.1.0.30 4 nnExtAlarmMinor = 3 .1.3.6.1.4.1.562.29.6.1.0.30 3 nnExtAlarmWarning = 4 .1.3.6.1.4.1.562.29.6.1.0.30 2 nnExtAlarmClear = 5 .1.3.6.1.4.1.562.29.6.1.0.30 1 Non-alarm Events: nnExtAlarmMessage = 6 .1.3.6.1.4.1.562.29.6.1.0.30 6
2.	Time(long)	MMM DD hh:mm:ss -> UTC time	MMM DD hh:mm:ss UTC time	UTC -> Minute Indicator	Alarm event: alarmActiveDateAndTime .1.3.6.1.2.1.118.1.2.2.1.2 Non-alarm event: nnExtAlarmMessageDateAndTime .1.3.6.1.4.1.562.29.6.1.3.1.3

Northbound Fault Format Summary

Row#	IEMS Schema	SYSLOG	NTSTD	SCC2	SNMP
3.	LogName	Report Name	LogName	LogName	Log name&number shown in varbind Alarm event: nnExtAlarmActiveDocumentationPointer .1.3.6.1.4.1.562.29.6.1.1.1.4 Non-alarm event: nnExtAlarmMessageDocumentationPointer .1.3.6.1.4.1.562.29.6.1.3.1.4
4.	LogNumber	ReportNumber	LogNumber	LogNumber	Log name&number shown in varbind Alarm event: nnExtAlarmActiveDocumentationPointer .1.3.6.1.4.1.562.29.6.1.1.1.4 Non-alarm event: nnExtAlarmMessageDocumentationPointer .1.3.6.1.4.1.562.29.6.1.3.1.4
5.	Threshold	-	Threshold '+' set ' ' not set	Threshold '+' set ' ' not set	not supported
6.	ID(Integer)	NotificationID	NotificationID	NotificationID	last integer in the OID specified by: alarmActiveResourceID .12.78.111.114.116.101.108.95.102.97.117.108.116.25.50.48.48.52.45.49.45.56.44.51.58.50.49.58.53.55.46.49.44.43.48.53.58.51.48.10
7.	Sequence Number	Generated Sequence Number	Global Sequence Number (generated)	Global Sequence Number (generated)	Alarm event: nnExtAlarmActiveSequenceNumber .1.3.6.1.4.1.562.29.6.1.1.1.7
8.	EventType	EventType	EventType	EventType	Alarm event: not supported
9.	EventLabel	EventLabel	EventLabel	EventLabel	not supported

Northbound Fault Format Summary

Row#	IEMS Schema	SYSLOG	NTSTD	SCC2	SNMP
10.	Equipment Identifier	Location:	Location:	Location:	Alarm event: nnExtAlarmActiveResourceDescription .1.3.6.1.4.1.562.29.6.1.1.1.5 Non-alarm event: nnExtAlarmMessageResourceDescription .1.3.6.1.4.1.562.29.6.1.3.1.2
11.	Probable Cause	Cause	Cause	Cause	Alarm event: nnExtAlarmActiveProbableCause .1.3.6.1.4.1.562.29.6.1.1.1.2
12.	Category	Category:	Category:	Category:	Alarm event: nnExtAlarmActiveEventType .1.3.6.1.4.1.562.29.6.1.1.1.1
13.	Specific Problem	Specific Problem	Specific Problem	Specific Problem	Alarm event: alarmActiveDescription: .1.3.6.1.2.1.118.1.2.2.1.11
14.	NotificationID	not sent	not sent	non sent	not sent
15.	ComponentID	ComponentID	ComponentID	ComponentID	Alarm event: nnExtAlarmActiveResourceDescription .1.3.6.1.4.1.562.29.6.1.1.1.5 Non-alarm event: nnExtAlarmMessageResourceDescription .1.3.6.1.4.1.562.29.6.1.3.1.2
16.	BodyText	BodyText	BodyText	BodyText	Alarm event: alarmActiveDescription: .1.3.6.1.2.1.111.1.2.2.1.11 Non-alarm event: nnExtAlarmMessageInfo: .1.3.6.1.4.1.562.29.6.1.3.1.5

Message Sequences and Manager Operations

Raise Alarm

This sequence applies to the following alarm event types:

- nnAlarmWarning
- nnAlarmMinor

- nnAlarmMajor
 - nnAlarmCritical
- 1 IEMS forwards alarm from device. The trap contains references to the 12 varbinds depicted in Table , “Alarm Active Variable Table,” on page 2549.
 - 2 The OSS receives the alarm and notes the resource ID of the alarm event to allow correlation with a subsequent alarmClear event. IEMS adds the alarm entry to the *alarmActiveTable*, *alarmActiveVariableTable*, and *nnExtAlarmActiveTable*. The *nlmLogTable* and *nlmLogVariableTable* also maintain a rolling log of the last n alarm events received - where n is defined by the variable *nlmConfigGlobalEntryLimit*.

Clear Alarm

- 1 IEMS forwards clearAlarm event from device. The trap contains references to all varbinds listed in Please refer to “ Alarm Active Variable Table” on page 2549. except for *nnExtAlarmActiveManualClear* - which is not included in this message.
- 2 The OSS receives the clear event and matches its resource ID in **alarmActiveResourceId** against the ID of its corresponding alarm event in the *alarmActiveTable*.

The corresponding alarm entry is removed from all active alarm tables:

alarmActiveTable

alarmActiveVariableTable

nnExtAlarmActiveTable

An entry is made in the log notification tables for the CLEAR event.

nlmLogTable

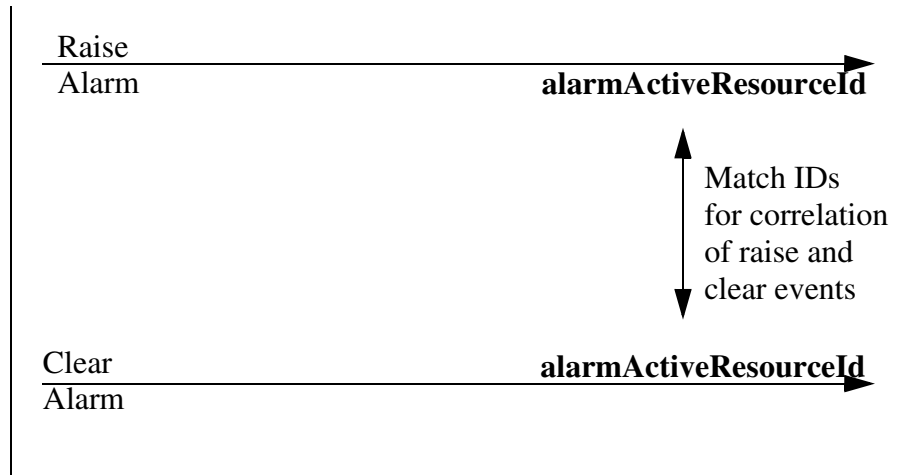
nlmLogVariableTable

Alarm Raise & Clear Correlation

IEMS

OSS

Alarm event forwarded to OSS



Manual Clear

Each alarm event contains information that indicates whether it can be manually cleared. The value in the varbind *nnExtAlarmActiveManualClear* makes this determination and can have the following values:

- other (1),
- forbidden (2),
- required (3),
- optional (4)

Note: Alarms with a value of *forbidden* in this field cannot be manually cleared.

Eligible alarms can be manually cleared by sending a SET request to the alarm clear interface variable *nortelNMIalarmClear* (.1.3.6.1.4.1.562.29.1.8.1) in the NORTEL_NMI-ALARM-CLEAR-MIB. The alarm to be cleared can be specified by using the *alarmActiveIndex* of the target alarm. The value of the *alarmActiveIndex* is stored as the last element in the *alarmActiveResourceId*.

Example: An alarm is generated and stored in the *alarmActiveTable* with the following values:

alarmsListName: **Nortel_fault**

alarmActiveDateAndTime: 2004-1-8,3:21:57.1,+05:30

alarmActiveIndex: **10**

The resulting *alarmActiveResourceId* will be:

alarmActiveResourceId.12.78.111.114.116.101.108.95.102.97.117.108.1
 16.25.50.48.48.52.45.49.45.56.44.51.58.50.49.58.53.55.46.49.44.43.48.5
 3.58.51.48.10

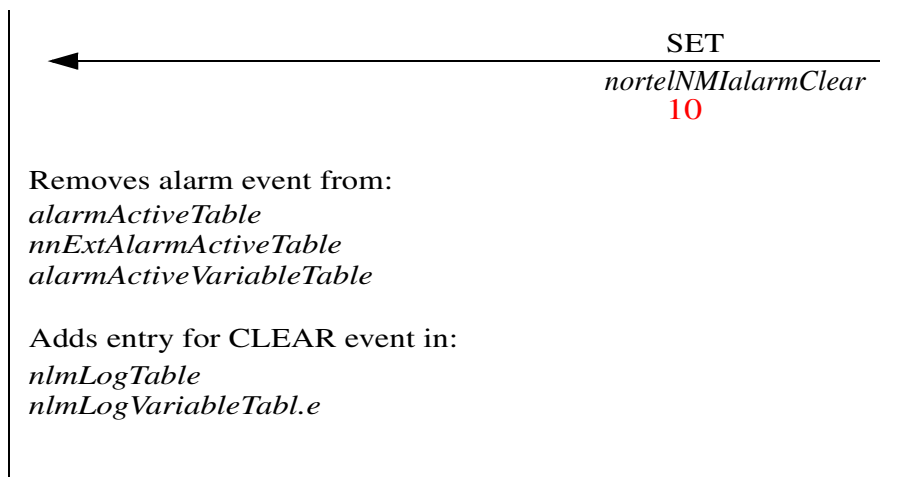
Note: *alarmActiveResourceId* is shown fully encoded.

The SET request will be sent with a value of 10. The corresponding alarm entry is removed from the *alarmActiveTable*, *alarmActiveVariableTable*, and *nnExtAlarmActiveTable*. A corresponding entry for the manual clear is then made in *nlmLogTable* and *nlmLogVariableTable*. See the following figure.

Manual Clear of Alarm Event

IEMS

OSS



Detecting System Restarts

Before an alarm event is forwarded to a downstream manager, the IEMS assigns the current system up-time of the server to the alarm contents. As discussed previously, it can be found in the *sysUpTime* varbind of the alarm. On restart of the IEMS server, this value is initialized to 0 to signal downstream systems of the event. The OSS can use *sysUptime* to monitor system restarts as follows:

Correlation with sequence numbers

Since *sysUpTime* will always increase with each sequential alarm event, restart conditions can be detected if the following condition is met:

$(sysUpTime \text{ of current event}) < (sysUpTime \text{ of previous event})$

Restart Recovery

When the OSS determines that IEMS has been restarted, it must perform a full reload of the active alarms in the system to synchronize its data with the agent. See [“Full Resync of Active Alarms” on page 2562](#) for details.

Detection of Missing Logs

Each alarm event generated by IEMS contains a unique sequence number that can be used to detect lost notifications. Once an OSS identifies a missing sequence number, it can be re-queried from the IEMS server if the following condition is met:

(sequence# of latest event) - (sequence# of missing event)

$\leq nlmConfigGlobalEntryLimit$ (default = 25)

If this condition is met, then the missing log can be recovered. See “Incremental Resync of missing logs”.

Otherwise, a full resynchronization of the alarm tables will be required. See [“Full Resync of Active Alarms” on page 2562](#).

Full Resync of Active Alarms

There are two scenarios for which an SNMP manager will be required to perform a complete reload of the active alarms from IEMS:

- on startup of the management application
- when missing alarm notifications are sufficiently old to have been rotated out of the *nlmLogTable*. This table maintains a snapshot of the most recent 25 alarm events. If the missing sequence number cannot be found in this table, then a reload of all active alarms is required.

Active alarm data resides in:

alarmActiveTable

nnExtAlarmActiveTable

A full table read must be performed on the varbinds in Please refer to “Required Varbinds for Active Alarm resync” on page 2562. to perform the resync:

Required Varbinds for Active Alarm resync

Varbind	OID
snmpTrapOID	.1.3.6.1.6.3.1.1.4.1
alarmActiveResourceId	.1.3.6.1.2.1.118.1.2.2.1.10
alarmActiveDateAndTime	.1.3.6.1.2.1.118.1.2.2.1.2
alarmActiveDescription	.1.3.6.1.2.1.118.1.2.2.1.11

Varbind	OID
nnExtAlarmActiveEventType	.1.3.6.1.4.1.562.29.6.1.1.1.1
nnExtAlarmActiveProbableCause	.1.3.6.1.4.1.562.29.6.1.1.1.2
nnExtAlarmActiveAdditionalText	.1.3.6.1.4.1.562.29.6.1.1.1.3
nnExtAlarmActiveDocumentationPointer	.1.3.6.1.4.1.562.29.6.1.1.1.4
nnExtAlarmActiveResourceDescription	.1.3.6.1.4.1.562.29.6.1.1.1.5
nnExtAlarmActiveManualClear	.1.3.6.1.4.1.562.29.6.1.1.1.6
nnExtAlarmActiveSequenceNumber	.1.3.6.1.4.1.562.29.6.1.1.1.7

Note: These varbinds are retrieved from the *alarmActiveVariableTable*

The manager can perform a full resync with the *alarmActiveTable* in a similar way to that used when performing an incremental resync from the *nmlLogVariableTable* (see “Incremental Resync of missing logs”). As stated earlier, each alarm entry in the *alarmActive* table has a corresponding entry for all of the alarm components in the *alarmActiveVariable* table. The complete set of alarm data can be retrieved for each alarm by first retrieving the *alarmActiveIndex* of the entry in the *alarmActiveTable*, and then using this index to request its corresponding entries from the *alarmActiveVariableTable*. These steps can be summarized as follows:

- 1 Poll the IEMS server for the latest sequence number. Issue a GET request on *nmlStatsLogNotificationsLogged*. Perform steps 2 to 3 until all alarms have been retrieved from IEMS.
- 2 Derive the list of indices to the *alarmActive* table by performing a series of GETNEXT requests on any one of its columns. The *alarmActiveIndex* for entries can be parsed from this data.
- 3 For each *alarmActiveIndex* derived in step 2, determine the alarm type perform a GET request on the *alarmActiveVariableTable* all index fields for the alarm type. The specific index fields requested will be based on the alarm type specified by the *snmpTrapOID* in index 2. See “Incremental Resync of missing logs” for a description of varbinds used in the different event types. This step essentially performs repeated incremental resync operations until complete.
- 4 Based on the alarm type determined in step 3, request all varbinds (GET) in the *alarmActiveVariableTable* for the constructed index

alarmListName = Nortel_fault

alarmActiveIndex = (derived in step 2)

alarmActiveVariableIndex (1-n) - depends on alarm type found in step 3

Note: The *alarmActiveVariableTable* and *nlmLogVariableTable* contain the same indexed alarm information and are accessed in similar ways. The main difference between the two is that *alarmActiveVariableTable* uses the *alarmActiveIndex* as one of its key components, whereas the *nlmLogVariableTable* uses the sequence number.

Incremental Resync of missing logs

An OSS can monitor sequence numbers from alarm events to detect missing notifications. If a missing notification is found (as described in “Detection of Missing Logs”), then it can be queried from the *nlmLogVariableTable* using the sequence number.

- 1 OSS detects missing sequence number
- 2 Missing alarm events can be recovered from the *nlmLogVariableTable* using the sequence number. Depending on the alarm event type, different numbers of varbinds will be present in the table for the entry.

The following table shows an example of the varbinds that would be used to recover a missing RAISE event with a sequence number of “1390”. RAISE events include the following alarm types:

nnExtAlarmWarning (.1.3.6.1.4.1.562.29.6.1.0.301)

nnExtAlarmMinor (.1.3.6.1.4.1.562.29.6.1.0.302)

nnExtAlarmMajor (.1.3.6.1.4.1.562.29.6.1.0.303)

nnExtAlarmCritical (.1.3.6.1.4.1.562.29.6.1.0.304)

Table , “nlmLogVariableTable varbinds for recovery of lost CLEAR notification,” on page 2566 shows an example of the varbinds that would be used to recover a missing CLEAR event with a sequence number of “1390”. CLEAR events are specified by the following OID:

nnExtAlarmClear (.1.3.6.1.4.1.562.29.6.1.0.301)

The alarm type can be determined by examining the value of the *snmpTrapOID* of the missed alarm. For both alarm types, this value is assigned index 2 of the *nlmLogVariable* table and can be queried with the OIDs shown in the following table. The alarm type will determine the mapping for the remaining fields in the notification message.

nImLogVariableTable varbinds for recovery of lost RAISE notification

nImLogVariableTable Index Variable	OID (nImLogName = "Nortel_fault" (encoded) Sequence# = 1390 Index = 1 - 12)	Notification Varbind Represented
nImLogVariableIndex 1	nImLogVariableTimeTicksVal.12.78.111.114.116.101.108.95.102.97.117.108.116.1390.1	sysUpTime
nImLogVariableIndex 2	nImLogVariableOidVal.12.78.111.114.116.101.108.95.102.97.117.108.116.1390.2	snmpTrapOID
nImLogVariableIndex 3	nImLogVariableOctetStringVal.12.78.111.114.116.101.108.95.102.97.117.108.116.1390.3	alarmActiveResourceId
nImLogVariableIndex 4	nImLogVariableOctetStringVal.12.78.111.114.116.101.108.95.102.97.117.108.116.1390.4	alarmActiveDescription
nImLogVariableIndex 5	nImLogVariableOctetStringVal.12.78.111.114.116.101.108.95.102.97.117.108.116.1390.5	alarmActiveDateAndTime
nImLogVariableIndex 6	nImLogVariableInteger32Val.12.78.111.114.116.101.108.95.102.97.117.108.116.1390.6	ituAlarmEventType
nImLogVariableIndex 7	nImLogVariableInteger32Val.12.78.111.114.116.101.108.95.102.97.117.108.116.1390.7	ituAlarmProbableCause
nImLogVariableIndex 8	nImLogVariableOctetStringVal.12.78.111.114.116.101.108.95.102.97.117.108.116.1390.8	ituAlarmAdditionalText
nImLogVariableIndex 9	nImLogVariableOctetStringVal.12.78.111.114.116.101.108.95.102.97.117.108.116.1390.9	nnItuAlarmActiveDocumentationPointer
nImLogVariableIndex 10	nImLogVariableOctetStringVal.12.78.111.114.116.101.108.95.102.97.117.108.116.1390.10	nnItuAlarmActiveResourceDescription

nImLogVariableTable varbinds for recovery of lost RAISE notification

nImLogVariableTable Index Variable	OID (nImLogName = "Nortel_fault" (encoded) Sequence# = 1390 Index = 1 - 12)	Notification Varbind Represented
nImLogVariableIndex 11	nImLogVariableInteger32Val .12.78.111.114.116.101.108 .95.102.97.117.108.116.139 0.11	nnItuAlarmActiveManualClear (not present in CLEAR events, see next table)
nImLogVariableIndex 12	nImLogVariableInteger32Val .12.78.111.114.116.101.108 .95.102.97.117.108.116.139 0.12	nnItuAlarmActiveSequenceNumber

nImLogVariableTable varbinds for recovery of lost CLEAR notification

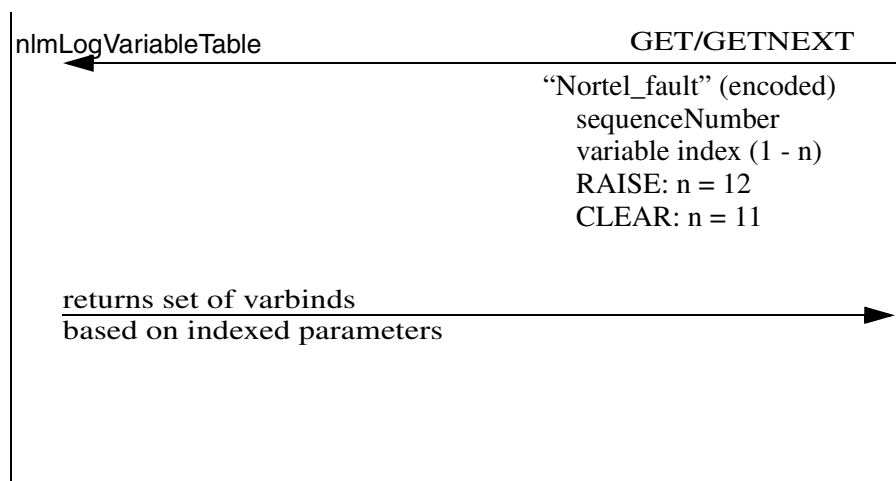
nImLogVariableTable Index Variable	OID (nImLogName = "Nortel_fault" (encoded) Sequence# = 1390 Index = 1 - 11)	Notification Varbind Represented
nImLogVariableIndex 1	nImLogVariableTimeTicksVal .12.78.111.114.116.101.108.95.102.97.117.108.116.1390. 1	sysUpTime
nImLogVariableIndex 2	nImLogVariableOidVal. 12.78.111.114.116.101.108.95.102.97.117.108.116.1390.2	snmpTrapOID
nImLogVariableIndex 3	nImLogVariableOctetStringVal. 12.78.111.114.116.101.108.95.102.97.117.108.116.1390.3	alarmActiveResourceId
nImLogVariableIndex 4	nImLogVariableOctetStringVal. 12.78.111.114.116.101.108.95.102.97.117.108.116.1390.4	alarmActiveDescription
nImLogVariableIndex 5	nImLogVariableOctetStringVal. 12.78.111.114.116.101.108.95.102.97.117.108.116.1390.5	alarmActiveDateAndTime
nImLogVariableIndex 6	nImLogVariableInteger32Val .12.78.111.114.116.101.108 .95.102.97.117.108.116.139 0.6	ituAlarmEventType

nImLogVariableTable Index Variable	OID (nImLogName = "Nortel_fault" (encoded) Sequence# = 1390 Index = 1 - 11)	Notification Varbind Represented
nImLogVariableIndex 7	nImLogVariableInteger32Val .12.78.111.114.116.101.108 .95.102.97.117.108.116.139 0.7	ituAlarmProbableCause
nImLogVariableIndex 8	nImLogVariableOctetStringVal .12.78.111.114.116.101.108.95.102.97.117.108.116.1390. 8	ituAlarmAdditionalText
nImLogVariableIndex 9	nImLogVariableOctetStringVal .12.78.111.114.116.101.108.95.102.97.117.108.116.1390. 9	nnItuAlarmActiveDocumentationPointer
nImLogVariableIndex 10	nImLogVariableOctetStringVal .12.78.111.114.116.101.108.95.102.97.117.108.116.1390. 10	nnItuAlarmActiveResourceDescription
nImLogVariableIndex 11	nImLogVariableInteger32Val .12.78.111.114.116.101.108 .95.102.97.117.108.116.139 0.11	nnItuAlarmActiveSequenceNumber

Recovery of missing alarm by sequence number

IEMS

OSS



Northbound Performance Interface

IEMS Performance Interface Specification

The Northbound performance interface is new to IEMS in SN07 and provides the customer a single reporting interface for the managed network. This has been achieved through the definition of a “Common Performance Record format” (CPR-F). The common format maps operational statistics from across network elements to a common set of metrics to provide a network-level view of performance.

The Common Performance Record format specification is defined using a standardized XML interface. It provides a full definition of the normalized containment hierarchy describing performance statistics for reporting network components. PM collection jobs configured in IEMS can report device metrics in either XML or CSV formats.

The following is a list of devices that support collection of performance data in the SN07 release, PP8600, STORM, MS2000, Session Server, CICM, CICM Mgr, MAS and MCS Mgr.

XML

If XML is selected as the output format, then the data is collected and saved as an ACSII file in the format defined by the CPR-F XML Schema Document. The format specification below provides a full description of the normalized representation of PM data for supported network elements.

Conversion to CSV

When CSV output is configured in the collection job, data is initially transformed to the XML format described above. An additional step then converts the XML file to its corresponding CSV representation. There is no loss of information during this process. Net content represented by each output is identical.

The next section defines the CPR-F in terms of its XML structure followed by a discussion of its *conversion* to CSV format.

Also, collected CSV and XML performance files can be transferred from IEMS to an OSS system by configuring a transfer job for the performance files. The transfer can be done using FTP or SFTP.

For more information on configuring, retrieving, and transferring performance measurements through IEMS, see NN10327-711 - IEMS Performance Management Guide.

The Common Performance Record Format

Overview

The Common Performance record is an XML document specified using an XML Schema Document (XSD).

There are two major aspects to encoding performance measurements – identifying the source of the measurements within the network and recording the measurement data itself.

The CPR-F uses an XML containment structure to indicate the source point in the network of the performance measurements. A typical performance measurement may have originated in an NE and then been passed up to an element management system (EMS). The EMS in turn may have passed the measurements along to an Operations Support System (OSS).

For this particular case, the common record would contain an XML element representing the management system (the OSS) which ultimately received the set of performance measurements. Within this OSS element would be an element representing the EMS which forwarded the measurements to the OSS.

And within this EMS element, there would be an XML element representing the NE (network element) from which the PMs were obtained. The NE element may itself contain another XML element representing the sub-component in the NE which generated the measurement.

The measurement data itself would also be encoded in one or more XML elements. These data elements would be contained within the sub-component element above.

XML Elements

The common performance record format uses thirteen major elements to encode performance information:

The *PMFile* element is the top-level element and contains all other elements.

The *System* element, *Entity* element and *SubEntity* element are used to relate the measurements to some origination point in the network and to capture their path through the management systems.

The *SingleValues* & *SingleValue* elements, the *GroupOfValues* & *GroupValue* elements and the *Table*, *Labels*, *Label*, *RowOfValues* & *RowValue* elements may all be used to capture the performance measurement information itself.

Encoding Source Identification for Performance Measurements

A performance measurement (PM) originates in some device in the network which records the measured value. This measurement may be combined with

other measurements within the device and forwarded to a management system. The management system may combine the PMs from many devices into a single grouping and may forward this grouping of PMs to some superior management system. Again this superior management system may combine groupings of measurements from many domains in the network and forward the combined package of measurements to yet another management system.

This path that PMs take as they move from the network device level to the management level is encoded in the CPR. Three elements are used to indicate this path:

System element

Entity element

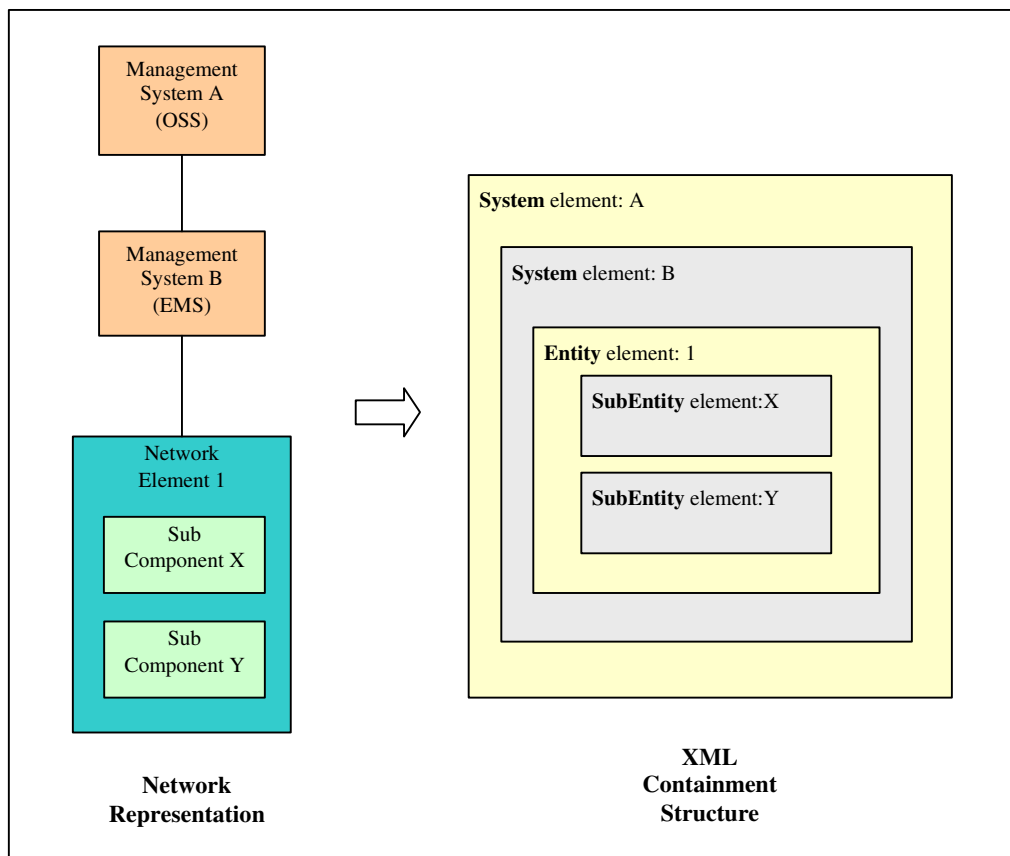
SubEntity element.

The intent of the Entity element is to represent the NE itself. What constitutes an NE and what device granularity determines an NE is an implementation choice for any particular product or technology. The System, Entity and SubEntity form a hierarchy. In this hierarchy, the Entity element may appear only once.

A Network Element may contain many sub-components and these sub-components may themselves contain sub-components and so on to some arbitrary level of decomposition. The SubEntity element represents a sub-component within the NE. A SubEntity element may contain other SubEntity elements to reflect the component structure within the NE. What constitutes a sub-component within an NE is, again, an implementation choice for any particular product or technology.

A set of performance measurements may traverse one or more management systems as it travels to some final destination system. Each of these intermediate management systems may be represented by a System element. A System element may contain another System element encoding the sequence of management systems which handle the performance measurement data.

The CPR may be emitted by a management system or by a network element. When an NE emits the record, the top-most XML element within the PMFile element will be an Entity element representing the NE which is sending the measurements. When a management system emits the CPR, the top-most XML element within the PMFile element will be a System element representing the management system.

OSS/EMS/NE hierarchy encoded in XML elements**Encoding the Performance Measurement Data****Measurement Descriptors**

In general, a performance measurement is some number which is bound to a measurement identifier such as: numberOfPackets = 23145. As well as these two items, a performance measurement may contain contextual information indicating the circumstances under which the measurement was taken or giving some further information as to the meaning of the measurement or its interpretation. The following information items are used in the common performance record format to describe measurement information:

Measurement Identifier: This is the name or label which uniquely identifies the measurement.

Measurement Value: This is (generally) the numerical value of the measurement (such as an integer or decimal number). Or it could be a string or some enumerated value

Measurement Kind: There are two kinds of performance measurement: 'snapshot' and 'period-based'.

A 'snapShot' measurement is one in which the measurement quantity (for example, some counter in a network device) is sampled at an instant in time and is being reported to the management system. There is no time significance attached to this sampled value. To derive information from a snapshot value, it may need to be compared to some previous snapshot of the counter or gauge and conclusions drawn about the change, if any, between the two values.

In contrast, a period-based measurement represents the value of some measurement quantity in the network device over a specified period of time. The measurement value relates only to activity which occurred within the measurement period.

Capture Time: This is the time at which the measurement value was captured. For a period-based measurement, this is the time at which measurement accrual stopped. For a snapshot measurement, it represents the time at which the measurement was sampled.

Interval Duration: This is the length of the time interval governing the performance measurement. For a period-based measurement, this interval is the duration between the time the measurement was started and the time the measurement was stopped. For a snapshot measurement, the interval indicates the duration between the time the current value was sampled and the time of the previous sample.

Last Record: If true this indicates that the performance measurement is the last value for the reporting time interval (indicated in IntervalDuration).

Reliability: This is an indicator of the quality or reliability of the measurement. It can take values such 'valid', 'invalid' and so on.

Unit: This names the unit in which the measurement is expressed (for example, packets, bytes and so on).

Value Type: This indicates the type of data contained in the Measurement Value. It can take on values such as 'integer', 'decimal', 'string' and so on).

Register Type: A register is the generic name given to the hardware or software capability in an NE which actually records the performance measurement. For numeric values the RegisterType property indicates whether the register behaves as a counter or a gauge or some other numeric register. (A counter is a register which accumulates a count of some defined event such as

the arrival of a packet. A gauge is a register which holds a state of usage sample – for example, the number of items in a queue).

Maximum Value: This property indicates the highest value the register can hold.

Reset Time: This is the register reset time. For numeric values this is the date/time when the register was last reset to zero.

Monitored Time: This indicates the actual duration of the period over which the measurements were taken. This property is used for cases where the actual measurement period is less than the period indicated in the Interval Duration value.

Intervals Covered: As an efficiency mechanism, it may be decided not to forward measurements when they have a value of zero at the end of the measurement period (for example, no events of interest occurred in the measurement period). This practice is called zero-suppression. In the case where a zero suppression representation is used, this attribute specifies the number of consecutive intervals over which a zero value was obtained for the measurement.

Table and Group Identifiers

Performance measurements may be stored within the common format as tables of values or as groups of values. The properties below are used to identify these tables and groups.

Table Identifier: This is the name or label for a particular table of measurements. This property is only used in the Table element.

KeyOfRow: This is a property specific to a column label used in representing tabular measurements. When it has a value of 'true' it indicates that this particular column of the table contains the key of the row of data values. The key is the identity of the object to which the row measurements pertain. This would generally refer to a sub-component in the network element.

Group Identifier: This is the name or label for a particular group of measurements. This property is only used in the GroupOfValues element.

Supplementary Identifiers

In many cases the identity of a network element, NE sub-component or performance measurement can be expressed in a single identifier. In other cases the identity will be contained in a number of individual identifiers. The approach taken in the common performance record format is to use supplementary identifiers to hold any additional identification information required in an element.

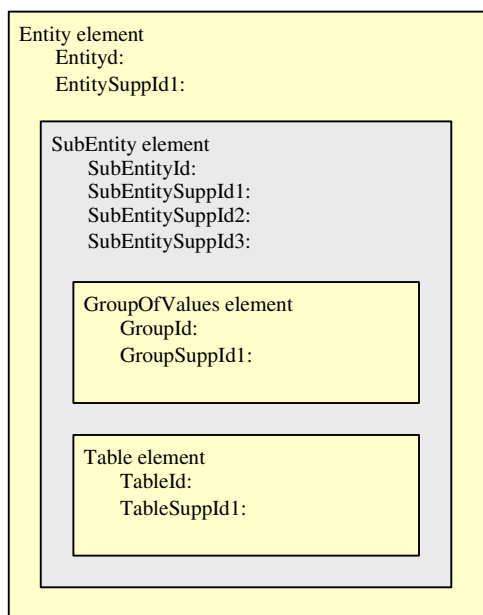
In the case of an *Entity* element (which is used to hold measurements for a particular NE), there are two identifiers: an EntityId (Entity Identifier) and an EntitySuppId (Entity Supplementary Identifier).

Likewise, the *SubEntity* element (which holds measurements for a sub-component of the NE) has a SubEntityId and three supplementary identifiers – SubEntitySuppId1, SubEntitySuppId2 and SubEntitySuppId3. Note that in the case of the *SubEntity* supplementary identifiers, it is not stipulated in which order or in which combination they are to be used. This is left as an implementation decision for any particular product/technology.

The performance measurement itself has a supplementary identifier – MeasureSuppId1. Both the *Table* element and *GroupOfValues* element also have a supplementary identifier – respectively TableSuppId1 and GroupSuppId1.

Some of these identifiers are mandatory and some are optional. See section “[Optionality](#)” on page 2579 for more information.

Example of Identifiers and Supplementary Identifiers



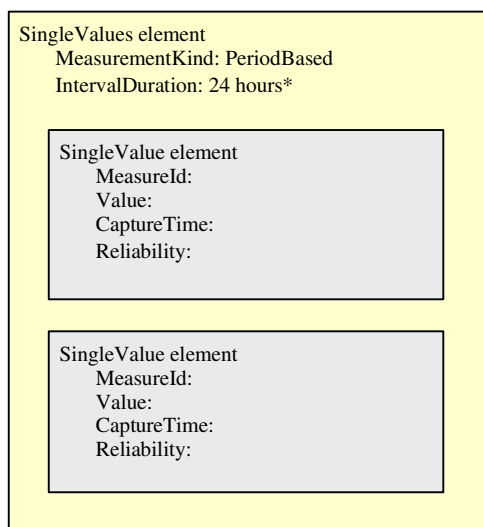
Measurement Elements

There are three ways to encode performance measurements in the common format – using a *SingleValues* approach, a *GroupOfValues* approach or a *Table* approach.

Single Values Approach

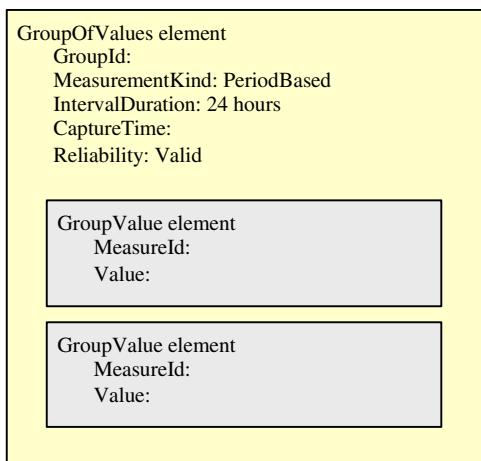
With this approach each performance measurement is considered as a standalone value with no explicit relationship to any other measurement value which may accompany it. Each measurement is encoded in a *SingleValue* element. One or more *SingleValue* elements are contained in a *SingleValues* element which specifies the kind of measurements contained within it (period-based or snapshot) and the interval duration for those measurements (for example, whether they are measurements for a 5-minute, 15-minute or 24-hour interval).

A SingleValues element containing two values



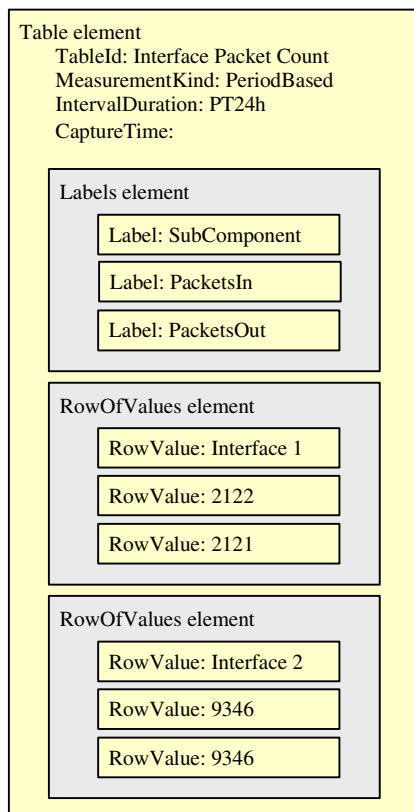
Group Values Approach

Like the *SingleValues* element, the *GroupOfValues* element contains one or more individual measurements. However, there is an explicit relationship between the measurements in the element. They are part of a group of measurements with a collective identity. The *GroupId* value contains the identity of the group. As with the *SingleValues* element, the *GroupOfValues* element specifies the kind of measurements it contains and their interval duration. In addition, many of the individual measurement properties such as *CaptureTime* and *Reliability* are common to the group and these are encoded once in the *GroupOfValues* element itself rather than being encoded for each measurement in the individual *GroupValue* element.

A GroupOfValues element containing two measurements**Table Approach**

The table approach encodes performance measurements in a tabular format. A Table element will contain a Labels element to hold the column headings for the table. The Table element will also contain one or more RowOfValues elements. Each RowOfValues element contains a row of individual data items with a one-to-one correspondence to the labels in the Labels element. One or more of the data items in a row may contain key information indicating the source of the measurements (that is, the data item will identify the sub-component from which the measurements were taken). This facet is indicated using the KeyOfRow property in the Label element.

A table may be explicitly identified using a TableId property or it may be an anonymous table with no name.

A Table element containing two rows of values**Interface Packet Count Table**

<u>SubComponent</u>	<u>PacketsIn</u>	<u>PacketsOut</u>
Interface 1	----	----

Top Level Properties

The performance measurements encoded in the common format constitute an XML string. This set of values will have high level properties in common. These are captured in the PMFile element. The term 'file' as used below is intended to designate the XML string containing the performance measurements.

MeasurementCategory: This property describes the type of measurements contained within the PM file (its value is always "PM" indicating the file contains performance measurements).

PMReportType: This describes the type of performance measurement report contained in the file (for example, this property could be used in the case where it is desired to distinguish between different types of PM reports).

FileCreationTime: This specifies the date/time when the PM file was created.

FileSchema: The FileSchema contains information which describes the format of a source non-CPR format PM file or the mapping file used to translate the source file into the common format.

FileSequenceNumber: The position of this file in some sequence of related PM files.

EarliestStartTime: This is set to the start time of the earliest measurement contained in the file.

LatestCaptureTime: This is set to the capture time of the latest measurement in the file.

PM File element contents

```
PMFile element
  MeasurementCategory:
  ReportType:
  FileCreationTime:
  FileSequenceNumber:
  EarliestStartTime:
  LatestCaptureTime:
  ValueTypeDefault:
  MaxValueDefault
  RegisterTypeDefault:
```

Default Values

ValueType, MaxValue and RegisterType are three properties which may be specified for a measurement (See Measurement Descriptors on page 11). It is possible to set defaults for these values in the file using the ValueTypeDefault, MaxValueDefault and RegisterTypeDefault properties in the top-level *PMFile* element. The scope of these default values is the entire PM file.

It is also possible to specify one or more of ValueType, MaxValue and RegisterType for each *SingleValue* element, each *GroupValue* element or each *Label* element (contained in a *Table* element). This local specification overrides the default value in *PMFile* for the particular element which contains the local specification.

If the property is not locally specified in the *SingleValue*, *GroupValue* or *Label* element, then the default value specified in the *PMFile* element is used.

If a default property is not specified in the *PMFile* element, then the following implicit default values are assumed. These implicit values function as if they were explicitly specified in *PMFile*.

RegisterTypeDefault: "counter"

ValueTypeDefault: "integer"

MaxValueDefault: 4,294,967,295 (that is, $2^{32} - 1$)

Optionality

It is possible to qualify a performance measurement with very many properties as shown above. Most of these properties are optional and are used in specific technologies or are needed to accommodate specific product performance management practices.

The following is the minimum set of properties required to identify a performance measurement. These are the required properties in a PM file:

PMFile Element: MeasurementCategory

System Element: SystemId

Entity: EntityId

SubEntity: SubEntityId

SingleValues Element: MeasurementKind

SingleValue Element: MeasureId; Value; CaptureTime

GroupOfValues Element: GroupId; CaptureTime; MeasurementKind

GroupValue Element: MeasureId; Value

Table Element: CaptureTime; MeasurementKind

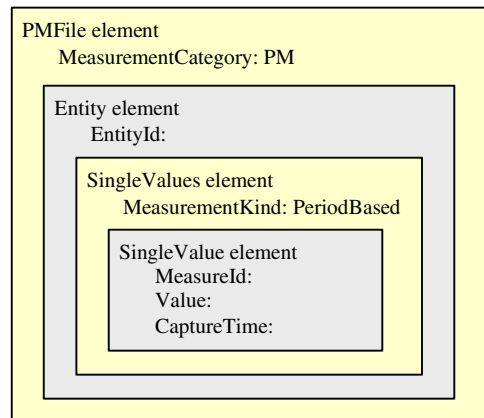
Labels Element: N/A

Label Element: N/A

RowOfValues Element: N/A

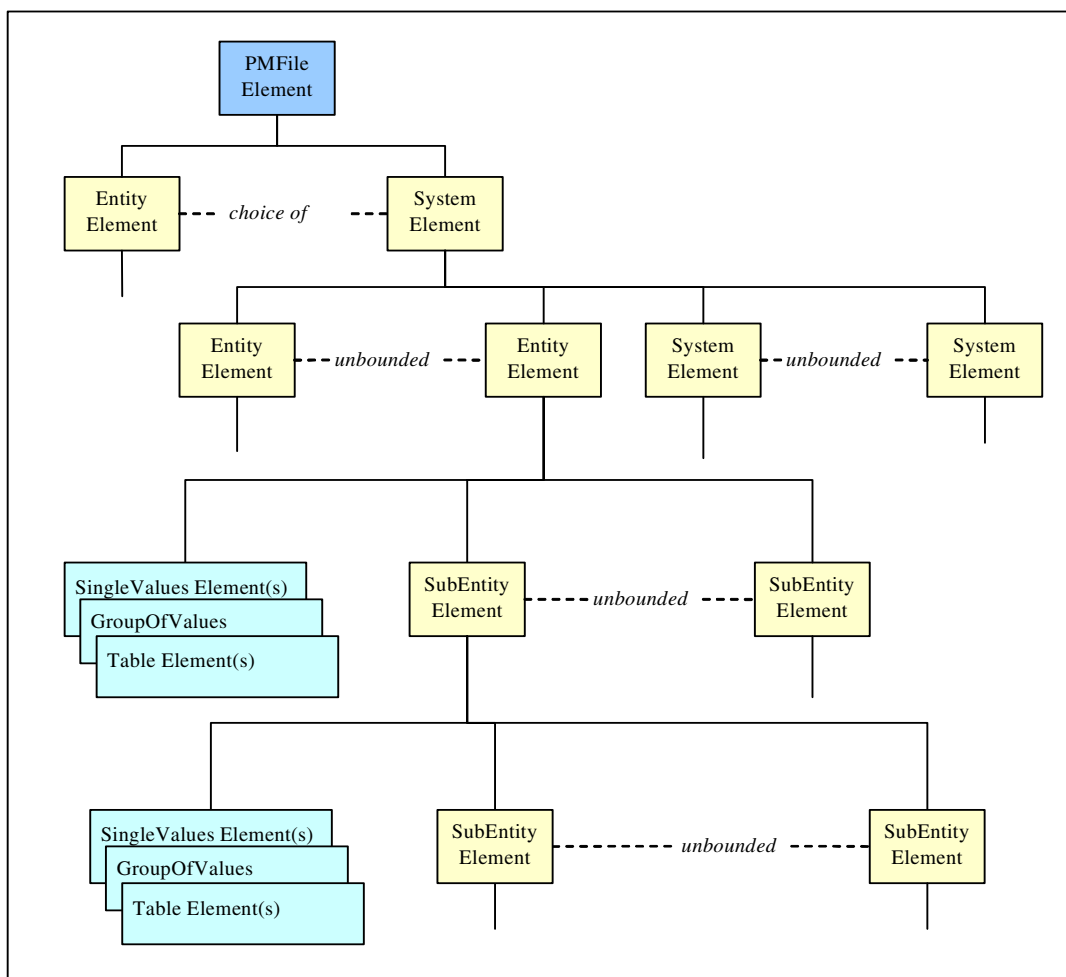
RowValue Element: Value

So a minimal CPR file would look like this:

Minimal Common Record Performance Record file

The figure below shows the hierarchical relationship of the major XML elements in the common performance record.

Hierarchy of the major XML elements



Attribute and Element Encoding

In the common performance record format some information is encoded as element data while other information is encoded using attributes. The approach followed is that attributes are used to encode metadata while elements are used for instance values.

Metadata is data which describes or qualifies some piece of information in terms of its class. So, in the common performance record, the *MeasurementKind* property differentiates between period-based measurements and snapshot measurements. This property is coded as an attribute.

Data which identifies or describes a specific instance of information rather than a class of information is encoded using an element. So the *CaptureTime*

property describes the time instant when a specific measurement was taken and so is not metadata. It is encoded as an element.

It also needs to be mentioned that the common performance record format adopts the approach of encoding the measurement name or label using an XML element. For instance:

Example 1: `<MeasureId> numberOfPackets </MeasureId>`

This is in contrast to the approach of directly coding the measurement name as an element tag:

Example 2: `<numberOfPackets> </numberOfPackets>`

The requirement for the common performance record format is to have standard fields for measurement information which could be used across all of Nortel (see the Performance Strategy requirements on page 5). This has been achieved using the current approach as shown in Example 1 above.

In order to use a direct coding of the measurement name as the element tag (Example 2 above) would require alignment across Nortel on the identification and semantics of all performance measurements which could possibly be encoded in the common performance record format. This alignment task has not been undertaken yet. It is envisaged that upon completion of such a convergence, the common performance record would be able to evolve to use measurement identifiers as tag names.

An additional concern is sometimes raised concerning the use of tables in the common performance record format. From a theoretical viewpoint, these tables are considered to constitute a lower quality of XML encoding than other means of encoding the data. However the common performance record format has opted to allow a tabular representation of data for pragmatic reasons. Tabular format measurement data has been the norm in most products for many years. Many operations systems expect their performance data to arrive in this customary format. In addition, industry standards for performance measurements such as 3GPP (Third Generation Partnership Project) mandate the use of tables for transporting performance data.

Layout of Elements and Attributes in the Common Format

The two figures below indicate which properties are expressed as elements and which are expressed via attributes. The figures represent one of many combinations of element types which are possible in the common performance record format. (Attributes are shown as *blue italicized* text. Elements are represented as boxes).

Layout of elements & attributes in the Common Performance Record**PMFile***MeasurementCategory= ;ReportType= ;*

FileCreationTime
FileSchema
FileSequenceNumber
EarliestStartTime
LatestCaptureTime
ValueTypeDefault
MaxValueDefault
RegisterTypeDefault

System*Type= ; Vendor= ;*

SystemId
SystemSuppId1
AuditSource

Entity*Type= ; Version= ; Vendor= ;*

EntityId
EntitySuppId1
EntityAddress

SubEntity*Type= ;*

SubEntityId
SubEntitySuppId1
SubEntitySuppId2
SubEntitySuppId3

SingleValues**GroupOfValues****Table**

Layout of elements & attributes in the CPR-F (cont'd)

SubEntity <i>Type= ;</i> <table border="1"> <tr><td>SubEntityId</td></tr> <tr><td>SubEntitySuppId1</td></tr> <tr><td>SubEntitySuppId2</td></tr> <tr><td>SubEntitySuppId3</td></tr> </table>		SubEntityId	SubEntitySuppId1	SubEntitySuppId2	SubEntitySuppId3										
SubEntityId															
SubEntitySuppId1															
SubEntitySuppId2															
SubEntitySuppId3															
SingleValues <i>MeasurementKind= ; IntervalDuration= ;</i> <table border="1"> <tr><td>LastRecord</td></tr> </table> <table border="1"> <tr> <td colspan="2"> SingleValue <i>Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i> <table border="1"> <tr><td>MeasureId</td></tr> <tr><td>Value</td></tr> <tr><td>CaptureTime</td></tr> <tr><td>MeasureSuppId1</td></tr> </table> <table border="1"> <tr><td>Reliability</td></tr> <tr><td>ResetTime</td></tr> <tr><td>IntervalsCovered</td></tr> <tr><td>MonitoredTime</td></tr> </table> </td> </tr> </table>		LastRecord	SingleValue <i>Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i> <table border="1"> <tr><td>MeasureId</td></tr> <tr><td>Value</td></tr> <tr><td>CaptureTime</td></tr> <tr><td>MeasureSuppId1</td></tr> </table> <table border="1"> <tr><td>Reliability</td></tr> <tr><td>ResetTime</td></tr> <tr><td>IntervalsCovered</td></tr> <tr><td>MonitoredTime</td></tr> </table>		MeasureId	Value	CaptureTime	MeasureSuppId1	Reliability	ResetTime	IntervalsCovered	MonitoredTime			
LastRecord															
SingleValue <i>Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i> <table border="1"> <tr><td>MeasureId</td></tr> <tr><td>Value</td></tr> <tr><td>CaptureTime</td></tr> <tr><td>MeasureSuppId1</td></tr> </table> <table border="1"> <tr><td>Reliability</td></tr> <tr><td>ResetTime</td></tr> <tr><td>IntervalsCovered</td></tr> <tr><td>MonitoredTime</td></tr> </table>		MeasureId	Value	CaptureTime	MeasureSuppId1	Reliability	ResetTime	IntervalsCovered	MonitoredTime						
MeasureId															
Value															
CaptureTime															
MeasureSuppId1															
Reliability															
ResetTime															
IntervalsCovered															
MonitoredTime															
GroupOfValues <i>MeasurementKind= ; IntervalDuration= ;</i> <table border="1"> <tr><td>GroupId</td></tr> <tr><td>GroupSuppId1</td></tr> <tr><td>CaptureTime</td></tr> <tr><td>LastRecord</td></tr> <tr><td>Reliability</td></tr> </table> <table border="1"> <tr> <td colspan="2"> GroupValue <i>Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i> <table border="1"> <tr><td>MeasureId</td></tr> <tr><td>Value</td></tr> </table> <table border="1"> <tr><td>MeasureSuppId1</td></tr> <tr><td>ResetTime</td></tr> </table> </td> </tr> </table>		GroupId	GroupSuppId1	CaptureTime	LastRecord	Reliability	GroupValue <i>Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i> <table border="1"> <tr><td>MeasureId</td></tr> <tr><td>Value</td></tr> </table> <table border="1"> <tr><td>MeasureSuppId1</td></tr> <tr><td>ResetTime</td></tr> </table>		MeasureId	Value	MeasureSuppId1	ResetTime			
GroupId															
GroupSuppId1															
CaptureTime															
LastRecord															
Reliability															
GroupValue <i>Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i> <table border="1"> <tr><td>MeasureId</td></tr> <tr><td>Value</td></tr> </table> <table border="1"> <tr><td>MeasureSuppId1</td></tr> <tr><td>ResetTime</td></tr> </table>		MeasureId	Value	MeasureSuppId1	ResetTime										
MeasureId															
Value															
MeasureSuppId1															
ResetTime															
Table <i>MeasurementKind= ; IntervalDuration= ;</i> <table border="1"> <tr><td>TableId</td></tr> <tr><td>CaptureTime</td></tr> <tr><td>LastRecord</td></tr> <tr><td>Reliability</td></tr> </table> <table border="1"> <tr> <td colspan="2"> Labels <table border="1"> <tr> <td>Label</td> <td><i>KeyOfRow= ; Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i></td> </tr> </table> </td> </tr> </table> <table border="1"> <tr> <td colspan="2"> RowOfValues <table border="1"> <tr> <td>RowValue</td> <td> <table border="1"> <tr> <td>Value</td> <td>ResetTime</td> </tr> </table> </td> </tr> </table> </td> </tr> </table>		TableId	CaptureTime	LastRecord	Reliability	Labels <table border="1"> <tr> <td>Label</td> <td><i>KeyOfRow= ; Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i></td> </tr> </table>		Label	<i>KeyOfRow= ; Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i>	RowOfValues <table border="1"> <tr> <td>RowValue</td> <td> <table border="1"> <tr> <td>Value</td> <td>ResetTime</td> </tr> </table> </td> </tr> </table>		RowValue	<table border="1"> <tr> <td>Value</td> <td>ResetTime</td> </tr> </table>	Value	ResetTime
TableId															
CaptureTime															
LastRecord															
Reliability															
Labels <table border="1"> <tr> <td>Label</td> <td><i>KeyOfRow= ; Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i></td> </tr> </table>		Label	<i>KeyOfRow= ; Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i>												
Label	<i>KeyOfRow= ; Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i>														
RowOfValues <table border="1"> <tr> <td>RowValue</td> <td> <table border="1"> <tr> <td>Value</td> <td>ResetTime</td> </tr> </table> </td> </tr> </table>		RowValue	<table border="1"> <tr> <td>Value</td> <td>ResetTime</td> </tr> </table>	Value	ResetTime										
RowValue	<table border="1"> <tr> <td>Value</td> <td>ResetTime</td> </tr> </table>	Value	ResetTime												
Value	ResetTime														

Common Performance Record Comma Separated Values (CSV) format

The following is an abbreviated generic description of the CPR CSV format. The CPR format is designed to be parsable into or from CPR XML format without loss of information.

The following elements are treated as 'blocks': PMFile, System, Entity, SubEntity, Table, GroupOfValues, SingleValues.

The start and end of these elements are marked or indicated in CSV with unique 'Begin' and 'End' markers. The format of an element block is as follows:

`{element_name}=Begin`

... CSV heading row for attributes & child text element nodes children of <element> ...

... CSV value row for attributes & child text element nodes of <element> ...

... recursive handling of all complex sub-elements (element children that are not text nodes) ...

`{element_name}=End`

For each element, a specific property (attribute or text element) has been selected as the identifier for that element. The identifier will always appear as the *first* of the comma separated values in the CSV representation of that element.

Values that contain commas are enclosed in double quotes in CSV format.

Element blocks and identifiers

Element	Block?	Identifier
PMFile	Y	MeasurementCategory
System	Y	SystemId
Entity	Y	EntityId
SubEntity	Y	SubEntityId
Table	Y	TableId
Labels	N	Label
RowOfValues	N	RowValue/Value

Element	Block?	Identifier
GroupOfValues	Y	GroupId
GroupValue	N	MeasureId
SingleValues	Y	MeasurementKind
SingleValue	N	MeasureId

As not all identifiers are in fact mandatory, when the identifier is not found in the XML being translated the value of `_Unnamed_` is used in the CSV output where the value of the identifier would normally appear.

For reference, “[Layout of elements & attributes in the Common Performance Record](#)” and “[Layout of elements & attributes in the CPR-F \(cont'd\)](#)” (which had been presented earlier) are shown below. The two figures indicate which properties are considered identifiers for each element, and therefore will always appear as the first comma separated value within a row. (Mandatory identifiers are shown in **red**. Optional identifiers are shown in **blue**. Attributes are shown as *italicized* text. Elements are represented as boxes.)

Layout of Elements & Attributes in the CPR-F**PMFile***MeasurementCategory= ;ReportType= ;*

FileCreationTime
FileSchema
FileSequenceNumber
EarliestStartTime
LatestCaptureTime
ValueTypeDefault
MaxValueDefault
RegisterTypeDefault

System*Type= ; Vendor= ;*

SystemId
SystemSuppId1
AuditSource

Entity*Type= ; Version= ; Vendor= ;*

EntityId
EntitySuppId1
EntityAddress

SubEntity*Type= ;*

SubEntityId
SubEntitySuppId1
SubEntitySuppId2
SubEntitySuppId3

SingleValues**GroupOfValues****Table**

Layout of elements & attributes in the CPR-F (cont'd)

SubEntity <i>Type= ;</i> <table border="1"> <tr><td>SubEntityId</td></tr> <tr><td>SubEntitySuppId1</td></tr> <tr><td>SubEntitySuppId2</td></tr> <tr><td>SubEntitySuppId3</td></tr> </table>	SubEntityId	SubEntitySuppId1	SubEntitySuppId2	SubEntitySuppId3							
SubEntityId											
SubEntitySuppId1											
SubEntitySuppId2											
SubEntitySuppId3											
SingleValues <i>MeasurementKind= ; IntervalDuration= ;</i> <table border="1"> <tr><td>LastRecord</td></tr> </table> <table border="1"> <tr> <td> SingleValue <i>Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i> <table border="1"> <tr><td>MeasureId</td></tr> <tr><td>Value</td></tr> <tr><td>CaptureTime</td></tr> <tr><td>MeasureSuppId1</td></tr> </table> <table border="1"> <tr><td>Reliability</td></tr> <tr><td>ResetTime</td></tr> <tr><td>IntervalsCovered</td></tr> <tr><td>MonitoredTime</td></tr> </table> </td></tr> </table>	LastRecord	SingleValue <i>Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i> <table border="1"> <tr><td>MeasureId</td></tr> <tr><td>Value</td></tr> <tr><td>CaptureTime</td></tr> <tr><td>MeasureSuppId1</td></tr> </table> <table border="1"> <tr><td>Reliability</td></tr> <tr><td>ResetTime</td></tr> <tr><td>IntervalsCovered</td></tr> <tr><td>MonitoredTime</td></tr> </table>	MeasureId	Value	CaptureTime	MeasureSuppId1	Reliability	ResetTime	IntervalsCovered	MonitoredTime	
LastRecord											
SingleValue <i>Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i> <table border="1"> <tr><td>MeasureId</td></tr> <tr><td>Value</td></tr> <tr><td>CaptureTime</td></tr> <tr><td>MeasureSuppId1</td></tr> </table> <table border="1"> <tr><td>Reliability</td></tr> <tr><td>ResetTime</td></tr> <tr><td>IntervalsCovered</td></tr> <tr><td>MonitoredTime</td></tr> </table>	MeasureId	Value	CaptureTime	MeasureSuppId1	Reliability	ResetTime	IntervalsCovered	MonitoredTime			
MeasureId											
Value											
CaptureTime											
MeasureSuppId1											
Reliability											
ResetTime											
IntervalsCovered											
MonitoredTime											
GroupOfValues <i>MeasurementKind= ; IntervalDuration= ;</i> <table border="1"> <tr><td>GroupId</td></tr> <tr><td>GroupSuppId1</td></tr> <tr><td>CaptureTime</td></tr> <tr><td>LastRecord</td></tr> <tr><td>Reliability</td></tr> </table> <table border="1"> <tr> <td> GroupValue <i>Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i> <table border="1"> <tr><td>MeasureId</td></tr> <tr><td>Value</td></tr> </table> <table border="1"> <tr><td>MeasureSuppId1</td></tr> <tr><td>ResetTime</td></tr> </table> </td></tr> </table>	GroupId	GroupSuppId1	CaptureTime	LastRecord	Reliability	GroupValue <i>Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i> <table border="1"> <tr><td>MeasureId</td></tr> <tr><td>Value</td></tr> </table> <table border="1"> <tr><td>MeasureSuppId1</td></tr> <tr><td>ResetTime</td></tr> </table>	MeasureId	Value	MeasureSuppId1	ResetTime	
GroupId											
GroupSuppId1											
CaptureTime											
LastRecord											
Reliability											
GroupValue <i>Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i> <table border="1"> <tr><td>MeasureId</td></tr> <tr><td>Value</td></tr> </table> <table border="1"> <tr><td>MeasureSuppId1</td></tr> <tr><td>ResetTime</td></tr> </table>	MeasureId	Value	MeasureSuppId1	ResetTime							
MeasureId											
Value											
MeasureSuppId1											
ResetTime											
Table <i>MeasurementKind= ; IntervalDuration= ;</i> <table border="1"> <tr><td>TableId</td></tr> <tr><td>CaptureTime</td></tr> <tr><td>LastRecord</td></tr> <tr><td>Reliability</td></tr> </table> <table border="1"> <tr> <td> Labels <table border="1"> <tr> <td>Label <i>KeyOfRow= ; Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i> </td></tr> </table> </td></tr> </table> <table border="1"> <tr> <td> RowOfValues <table border="1"> <tr> <td>RowValue</td> <td> <table border="1"> <tr><td>Value</td></tr> <tr><td>ResetTime</td></tr> </table> </td></tr> </table> </td></tr> </table>	TableId	CaptureTime	LastRecord	Reliability	Labels <table border="1"> <tr> <td>Label <i>KeyOfRow= ; Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i> </td></tr> </table>	Label <i>KeyOfRow= ; Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i>	RowOfValues <table border="1"> <tr> <td>RowValue</td> <td> <table border="1"> <tr><td>Value</td></tr> <tr><td>ResetTime</td></tr> </table> </td></tr> </table>	RowValue	<table border="1"> <tr><td>Value</td></tr> <tr><td>ResetTime</td></tr> </table>	Value	ResetTime
TableId											
CaptureTime											
LastRecord											
Reliability											
Labels <table border="1"> <tr> <td>Label <i>KeyOfRow= ; Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i> </td></tr> </table>	Label <i>KeyOfRow= ; Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i>										
Label <i>KeyOfRow= ; Unit= ; ValueType= ; MaxValue= ; RegisterType= ;</i>											
RowOfValues <table border="1"> <tr> <td>RowValue</td> <td> <table border="1"> <tr><td>Value</td></tr> <tr><td>ResetTime</td></tr> </table> </td></tr> </table>	RowValue	<table border="1"> <tr><td>Value</td></tr> <tr><td>ResetTime</td></tr> </table>	Value	ResetTime							
RowValue	<table border="1"> <tr><td>Value</td></tr> <tr><td>ResetTime</td></tr> </table>	Value	ResetTime								
Value											
ResetTime											

CSV Table example

```

PMFile=Begin
PM,commonFormat.xsd,2004-06-23T13:01:14EST

System=Begin
NortelNetworks/IEMS

Entity=Begin
47.165.168.120,CICM

Table=Begin
.iso.org.dod.internet.mgmt.mib-
  2.rmmon.usrHistory.usrHistoryControlTable.usrHistoryControlEntry,Snapshot,5
,2004-06-23T13:00:00EST
usrHistoryControlInterval,usrHistoryControlIndex,usrHistoryControlStatus,usrHi
storyControlOwner
900,5,1,CICM-120A
Table=End

Table=Begin
.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelPerfR
efMIB.nnPerfMetricReferenceTable.nnPerfMetricReferenceEntry,Snapshot,5,200
4-06-23T13:00:02EST
nnPerfMetricValue,nnPerfMetricSources,nnPerfMetricDataType,nnPerfMetricGroup,n
nPerfMetricName,nnPerfMetricRefIndex
0,2,1,CICM,ActiveConnections,5
0,2,1,CICM,PercentageCpuUsed,4
0,2,1,CICM,PercentageMemoryUsed,3
0,2,1,CICM,NumberOfLogs,2
0,2,1,CICM,ActiveSessions,1
Table=End
Entity=End
System=End
PMFile=End

```

Table attributes & text elements values

Labels attributes & text elements values

RowOfValues attributes & text elements

CSV SingleValues example

```

PMFile=Begin
PM,commonFormat.xsd,2004-06-23T17:30:21EST

System=Begin
NortelNetworks/IEMS

Entity=Begin
47.174.74.179,Session Server

SingleValues=Begin
Snapshot,5
sysDescr,2004-06-23T17:26:20EST,.iso.org.dod.internet.mgmt.mib-2.system,Linux sp2k-1
2.4.22-samxts #1 Thu May 13 01:48:09 EDT 2004 i686,Valid
snmpOutPkts,2004-06-23T17:26:20EST,.iso.org.dod.internet.mgmt.mib-2.snmp,8639,Valid
snmpInBadVersions,2004-06-23T17:26:21EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid
snmpInBadCommunityNames,2004-06-23T17:26:21EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,1,Valid
snmpInTotalReqVars,2004-06-23T17:26:21EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,9689,Valid
snmpOutTraps,2004-06-23T17:26:21EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid
snmpInBadCommunityUses,2004-06-23T17:26:21EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid
snmpInPkts,2004-06-23T17:26:21EST,.iso.org.dod.internet.mgmt.mib-2.snmp,8652,Valid
snmpInTotalSetVars,2004-06-23T17:26:21EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid
snmpInASNParseErrs,2004-06-23T17:26:21EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid
hrSystemDate,2004-06-23T17:26:22EST,.iso.org.dod.internet.mgmt.mib-
2.host.hrSystem,0,Valid
hrSystemUptime,2004-06-23T17:26:22EST,.iso.org.dod.internet.mgmt.mib-
2.host.hrSystem,1315598,Valid
hrSystemProcesses,2004-06-23T17:26:22EST,.iso.org.dod.internet.mgmt.mib-
2.host.hrSystem,170,Valid
snmpSilentDrops,2004-06-23T17:26:22EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid
SingleValues=End

Entity=End
System=End
PMFile=End

```

Note on CSV Examples

All CSV examples are with header information suppressed by default. This is the default behavior for all CSV performance reports in the SN07 release.

To have the header information included in the CSV performance reports, the user must change the “suppress-headers” option from “true” to “false”. The “suppress-headers” option is located in the cprxml2csv.properties file in the /opt/nortel/iems/current/resources directory.

CSV with header information example:

PMFile=Begin

MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime

PM,commonFormat.xsd,2004-06-23T12:45:04EST

System=Begin

SystemId

NortelNetworks/IEMS

Entity=Begin

EntityId,Type

47.165.168.120,CICM

Table=Begin

TableId,MeasurementKind,IntervalDuration,CaptureTime

.iso.org.dod.internet.mgmt.mib-
2.rmon.usrHistory.usrHistoryControlTable.usrHistoryControlEntry,Snapshot,5,2004-06-
23T12:40:00EST

Label,Label,Label,Label

usrHistoryControlInterval,usrHistoryControlIndex,usrHistoryControlStatus,usrHistoryControlOwner

Value,Value,Value,Value

900,5,1,CICM-120A

Table=End

Table=Begin

TableId,MeasurementKind,IntervalDuration,CaptureTime

.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelPerfRefMIB.nnPerf
MetricReferenceTable.nnPerfMetricReferenceEntry,Snapshot,5,2004-06-23T12:40:01EST

Label,Label,Label,Label,Label,Label

nnPerfMetricValue,nnPerfMetricSources,nnPerfMetricDataType,nnPerfMetricGroup,nnPerf
MetricName,nnPerfMetricRefIndex

```
Value,Value,Value,Value,Value,Value
0,2,1,CICM,ActiveConnections,5
0,2,1,CICM,PercentageCpuUsed,4
0,2,1,CICM,PercentageMemoryUsed,3
0,2,1,CICM,NumberOfLogs,2
2662732,2,1,CICM,ActiveSessions,1
Table=End
Entity=End
System=End
PMFile=End
```

Note: Collected performance files (in CSV and XML format) can be forwarded from the IEMS server to an OSS system by configuring an IEMS transfer job. Transfer jobs can be configured to forward these files using FTP or the secure SFTP protocols.

Inventory/Topology Interface

Overview

SN07 provides the ability to perform an ACSII dump of provisioned network inventory/topology information for use by 3rd party systems. The snapshot is initiated from the IEMS user interface and outputs full configuration details of the component hierarchy to the IEMS server as a text file. By default, the data is placed in the file `/opt/nortel/iems/current/logs/inventoryData.txt`. This information can then be retrieved and processed by third parties. For a full description of the format and content of these topology listings see the section titled “Dumping Inventory Details” in:

NN10330-511 - Integrated EMS Configuration Management

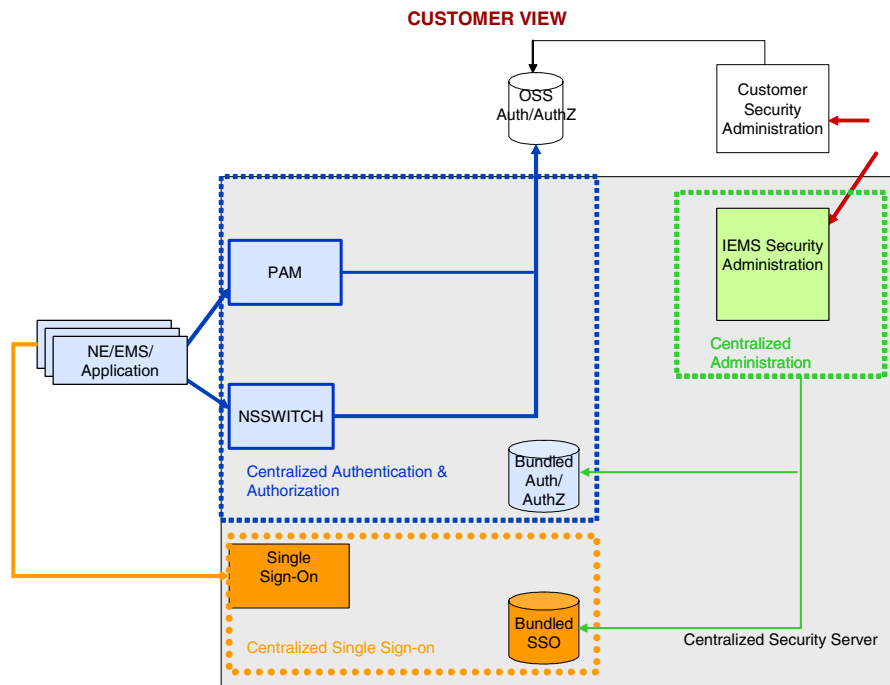
Network Security

Centralized Security Administration (Network Security)

Overview

The Integrated EMS provides a comprehensive security architecture based on PAM (Pluggable Authentication Module) and NSSwitch (Name Services Switch). The following figure shows the Nortel Networks VoIP Security Architecture.

Centralized Security Architecture



Features

This architecture provides the following features:

- Support for central administration of user accounts
- Support for central authentication: authentication of centrally administered user accounts is performed by the central security server(s)
- Support for central authorization: authorization information needed to support user access control is securely managed and provided by the central security server(s)
- Support for Single Sign-on (SSO)- This capability enables the user to access multiple network elements, applications, and features from a single login session. Session information for a user is shared between IEMS and network elements supporting SSO.
- Customer Plug-ability - provides the ability for third parties to plug-in its own Authentication/Authorization solutions.

The following table lists the SN07 devices and applications supporting these features:

Authentication and Authorization

Central Security Administration -Supported Devices

Network Element/EMS Platforms	Device Authentication Method	Device Reference Documentation
USP	HTTPS	NN10159-611 - USP Administration and Security
PP 8600	RADIUS	314724-B - Configuring and Managing Security
SSPFS Includes: CS2000 Management Tools (GWC Mgr, SAM21 Mgr, UAS Mgr, LMM,TMM,OSSGate, LTM,Trunk Provisioning, Line Provisioning, V5.2, Data Audit, Nodes Provisioning, Carrier EndPoint Provisioning, ADSL Flowthrough Provisioning, Batch Lines Provisioning) APS NPM MG9000 Manager, MG9000 Mid-Tier	PAM	NN10281-600 - ATM/IP Administration and Security
IEMS	HTTPS	NN10336-611 - IEMS Administration and Security
CICM Manager	HTTPS	NN10027-111 - CICM Series 2.5 Product and Technology Fundamentals

Network Elements and Applications can be configured to use Centralized Security Administration. To enable a device to use Centralized Security Administration, the device must be configured to use the IEMS central security server to authenticate users and access user profile information.

The IEMS Central Security Server uses PAM (Pluggable Authentication Module) to process the authentication requests and NSSwitch (Name Services Switch) to return user privilege and user profile information to Network Elements and Applications.

PAM Services

PAM provides authentication services for clients in the managed network. Customers have the option to use the PAM services that come pre-bundled

with the security server or to provide their own. See document: 0000007-24-1464 - *IEMS Installation Manual* for details on configuring PAM.

When a request is forwarded to the IEMS PAM SPI (PAM Service Provider), then authentication is performed against data provisioned and administered by the Security Administration application on the IEMS client.

Conversely, when a PAM services are provided by a customer, incoming authentication requests are forwarded to the customer SPI for resolution against their remote database.

NSSwitch Services

NSSwitch provides services to obtain group and profile information for users. Centralized access to network resources depends on the definition of a common set of user groups to map security access for each user. The Nortel Networks solution provides a number of predefined user groups to address the full range of OAM&P functions required across a managed network. For a full discussion of these user groups and their categorization, see *NN10281-600 - ATM/IP Administration and Security*.

Customers can configure NSSwitch to use the service pre-bundled with IEMS or, as with PAM services, provide their own service remotely. When the pre-bundled service is used, group and user profile information is administered from command-line Unix interface on the IEMS server. See *NN10336-611 - IEMS Administration and Security*.

If NSSwitch services are configured on a third party system, it is important to note that this security solution supports *only* the NSSwitch group and password databases. Although other database types may be defined in NSSwitch, they are not used by the central security feature.

See the References section for additional information on PAM and NSSwitch.

Single Sign-on (SSO)

The Single Sign-on feature allows users transparent access to multiple network elements and applications through a single login.

Once a user has been successfully authenticated for the first time (by user login), an SSO token is created by the IEMS security server that will be used to authenticate the same user on subsequent login attempts.

Network Elements and Applications use a Single Sign-On (SSO) interface on the Central Security Server to request SSO tokens whenever authentication is required.

For full details on the interface specification, see *NN10336-611 - IEMS Administration and Security*.

Configuring Security Administration

Managing Accounts

It is recommended practice that all user accounts be managed centrally with the following exceptions:

- accounts required to provide emergency access to a device.
- super user accounts (for example ‘root’ users)

There are two steps involved in adding a centrally managed user:

- 1 Add a user account on the Succession IEMS Security Server.
- 2 On the IEMS (security) server, add a user account and using Unix Administration tools.

Note: Detailed procedures for these steps can be found in *NN10336-611 - IEMS Administration and Security*.

Configuring Centralized Security Administration on NEs and EMS Platforms

An OSS must configure NEs and EMS Platforms to use centralized security administration. To enable centralized security administration on a device, the OSS must follow the procedures outlined for the device. For security configuration information for a specific device, look for its listing in the “Supported Devices” section of this document.

Note: Detailed procedures for these steps can be found in *NN10336-611 - IEMS Administration and Security*.

IEMS Suported Devices

The sections that follow contain a directory to provide customers a quick reference to device-specific information on faults, performance, interfaces, and other user documentation. The intended purpose is to allow customers to correlate IEMS Northbound interface events and behaviors with their originating source.

Each device in the listings below provide sample logs from all four Northbound fault streams: SCC2, NTSTD, Syslog, and SNMP. With the exception of the SNMP fault feed, these samples are shown as they appear from the Northbound interfaces.

Understanding SNMP Fault samples

Since SNMP has no inherent display format, each event is presented in a format that displays the short name of the MIB variables populated by the event:

<short MIB variable Name> => <value>

for example:

nnExtAlarmActiveResourceDescription =>
IEMS=ncOrtp2127.us.nortel.com-MS2000;

The following table provides a mapping of the displayed “short” variable name to its full form as well as its associated OID.

OID Short Name Mapping in SNMP Log Samples

Short name	sysUpTime
Long name	system.sysUpTime.0
OID	.1.3.6.1.2.1.1.3
Short name	snmpTrapOID.0
Long name	.iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTrap.snmpTrapOID.0
OID	.1.3.6.1.6.3.1.1.4.1
Short name	alarmActiveResourceId
Long name	alarmMIB.alarmObjects.alarmActive.alarmActiveTable.alarmActiveEntry.alarmActiveResourceId
OID	.1.3.6.1.2.1.111.1.2.2.1.10
Short name	alarmActiveDateAndTime

Long name	alarmMIB.alarmObjects.alarmActive.alarmActiveTable.alarmActiveEntry.alarmActiveDateAndTime
OID	.1.3.6.1.2.1.111.1.2.2.1.2
Short name	alarmActiveDescription
Long name	alarmMIB.alarmObjects.alarmActive.alarmActiveTable.alarmActiveEntry.alarmActiveDescription
OID	.1.3.6.1.2.1.111.1.2.2.1.11
Short name	nnExtAlarmActiveEventType
Long name	enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmActiveTable.nnExtAlarmActiveEntry.nnExtAlarmActiveEventType
OID	.1.3.6.1.4.1.562.29.6.1.1.1.1
Short name	nnExtAlarmActiveProbableCause
Long name	enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmActiveTable.nnExtAlarmActiveEntry.nnExtAlarmActiveProbableCause
OID	.1.3.6.1.4.1.562.29.6.1.1.1.2
Short name	nnExtAlarmActiveAdditionalText
Long name	enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmActiveTable.nnExtAlarmActiveEntry.nnExtAlarmActiveAdditionalText
OID	.1.3.6.1.4.1.562.29.6.1.1.1.3
Short name	nnExtAlarmActiveDocumentationPointer
Long name	enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmActiveTable.nnExtAlarmActiveEntry.nnExtAlarmActiveDocumentationPointer
OID	.1.3.6.1.4.1.562.29.6.1.1.1.4
Short name	nnExtAlarmActiveResourceDescription
Long name	enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmActiveTable.nnExtAlarmActiveEntry.nnExtAlarmActiveResourceDescription
OID	.1.3.6.1.4.1.562.29.6.1.1.1.5
Short name	nnExtAlarmActiveManualClear
Long name	enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmActiveTable.nnExtAlarmActiveEntry.nnExtAlarmActiveManualClear
OID	.1.3.6.1.4.1.562.29.6.1.1.1.6

Short name	nnExtAlarmActiveSequenceNumber
Long name	enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmActiveTable.nnExtAlarmActiveEntry.nnExtAlarmActiveSequenceNumber
OID	.1.3.6.1.4.1.562.29.6.1.1.1.7
Short name	nnExtAlarmMessageResource
Long name	.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmMessageTable.nnExtAlarmMessageEntry.nnExtAlarmMessageResource
OID	.1.3.6.1.4.1.562.29.6.1.3.1.1
Short name	nnExtAlarmMessageResourceDescription
Long name	iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmMessageTable.nnExtAlarmMessageEntry.nnExtAlarmMessageResourceDescription
OID	.1.3.6.1.4.1.562.29.6.1.3.1.2
Short name	nnExtAlarmMessageDateAndTime
Long name	iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmMessageTable.nnExtAlarmMessageEntry.nnExtAlarmMessageDateAndTime
OID	.1.3.6.1.4.1.562.29.6.1.3.1.3
Short name	nnExtAlarmMessageDocumentationPointer
Long name	iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmMessageTable.nnExtAlarmMessageEntry.nnExtAlarmMessageDocumentationPointer
OID	.1.3.6.1.4.1.562.29.6.1.3.1.4
Short name	nnExtAlarmMessageInfo
Long name	iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmMessageTable.nnExtAlarmMessageEntry.nnExtAlarmMessageInfo
OID	.1.3.6.1.4.1.562.29.6.1.3.1.5

Call Agent Core

This section contains IEMS Northbound log samples and device documentation references for the Call Agent Core.

Call Agent Core Fault Interface

Fault documentation for Call Agent Core :

- NN10275-909 - Succession fault Management logs Reference
- NN10083-911 - Communication Server 2000 Fault Management

DMS Standard (North America)

- 297-8021-840 - North American DMS100 Log Report Reference Manual Volumes 1 to 8

International Succession

- 297-9051-8401 - DMS100 Log Report Reference Manual Volumes 1 to 7

Fault Mapping for Call Agent Core

The following criteria can be used for looking up information on specific faults for Call Agent Core.

Fault Correlation for Call Agent Core

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
Call Agent Core	log name and log number	log name and log number	log name and log number	log name and log number	see section “ Fault documentation for Call Agent Core :”

Northbound Fault Formats for Call Agent Core

SCC2

The following is an example of a Call Agent Core log in SCC2 format:

```
56 LINE138 3778 INFO TRMT
      SLOA 21 1 02 01      DN 2145202111
TREATMENT SET = BUSY      CALLED NO =      5202111
CALLID= 01BE 036D
```

NTSTD

The following is an example of a Call Agent Core log in NTSTD format:

```
RTPU07BR      LINE138 Jan23 16:56:30 3778 INFO TRMT
              SLOA 21 1 02 01      DN 2145202111
              TREATMENT SET = BUSY   CALLED NO =                5202111
              CALLID= 01BE 036D
```

SNMP

The following is an example of a Call Agent Core log in SNMP format:

```
system.sysUpTime.0 => 19:51:46
snmpTrapOID.0 => nnExtAlarmMessage
nnExtAlarmMessageResource => .0.0
nnExtAlarmMessageResourceDescription => IEMS=wnc0y0m0.us.nortel.com-CS2K-Mgr;
nnExtAlarmMessageDateAndTime => 2004-1-23,11:56:30.0,
nnExtAlarmMessageDocumentationPointer => LINE138
nnExtAlarmMessageInfo => 56 LINE138 3778 INFO TRMT              SLOA 21 1 02 01
DN 2145202111
              TREATMENT SET = BUSY   CALLED NO =                5202111
              CALLID= 01BE 036D
```

Syslog

The following is an example of a Call Agent Core log in Syslog format:

```
Feb 23 11:57:27 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=3835~~ LINE138 NONE INFO
TRMT^M      SLOA 21 1 02 01      DN 2145202111 ^M      TREATMENT SET = BUSY   CALLED
NO =                5202111 ^M      CALLID= 01BE 036D
```

Performance

OM and PM Documentation references for Call Agent Core

- NN10149-711 - Communications Server 2000 Performance Management

DMS Standard (North America)

- 297-8021-814P1 - North American DMS-100 Operational Measurements Reference Manual Volumes 1 to 6

International Succession

- 297-9051-8141 - DMS-100 Family Operational Measurements Reference Manual Volumes 1 to 6

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

Performance measurements for Call Agent Core are available from the CS2K Core Manager. See NN10149-711 - Communications Server 2000 Performance Management for more information.

XML

The following is an example of Performance data for Call Agent Core in XML format:

***Note:** The IEMS northbound performance interface does not support this device..*

CSV

The following is an example of Performance data for Call Agent Core in CSV format:

***Note:** The IEMS northbound performance interface does not support this device..*

GUI/CLUI Documentation for Call Agent Core

The Call Agent Core provides both command-line and MAP-based interfaces accessed through the CS2000 Core Manager.

GUI/CLUI Launching and User procedures

- NN10018-111 - CS2000 Core Manager Basics
see section “Accessing the Core”

Related documents

- NN10197-111 - Communication Server 2000 Basics
- NN10193-511 - Communication Server 2000 Configuration Management
- NN10127-811 - Communication Server 2000 Accounting Management
- NN10171-611 - Communication Server 2000 Security and Administration
- 297-5051-921 - SuperNode Data Manager DDMS ASCII CI Gateway User Guide
- 297-5161-022P1 - Advanced Intelligent Network Service Enablers SIG Volumes 1 to 3
- 297-8021-350P1 - North American DMS-100 Translations Guide Volumes 1 to 25

- 297-8021-351P1 - DMS-100 Data Schema Reference Manual (volumes 1 to 12)
- 297-8021-801 - DMS-100 Feature Guide
- 297-8021-808P1 - DMS-100 SERVORD Reference Manual
- 297-8021-808P2 - DMS-100 SERVORD Reference Manual
- 297-8021-814P1 - DMS-100 Operational Measurements Reference Manual (volumes 1 to 6)
- 297-8021-840P1 - DMS-100 Logs Reference Manual (volumes 1 to 6)
- 297-8021-855P1 - DMS-100 Office Parameters Reference Manual (volumes 1 to 3)
- 297-8991-810 - XA-Core Reference Manual

Call Agent Platform

This section contains IEMS Northbound log samples and device documentation references for the Call Agent Platform.

Call Agent Platform Fault Interface

Fault documentation for Call Agent Platform :

- NN10087-911 - Call Agent Fault Management

Fault Mapping for Call Agent Platform

The following criteria can be used for looking up information on specific faults for Call Agent Platform.

Fault Correlation for Call Agent Platform

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
Call Agent Platform	logname and number	logname and number	logname and number	logname and number	NN10087-911 Call Agent Fault Management

Northbound Fault Formats for Call Agent Platform

SCC2

The following is an example of a Call Agent Platform log in SCC2 format:

```
* 41 CCA 355 6064 FLT Jam Inactive Unit
Unit Number : 0, ACTIVE
Description : Inactive JAMMED
```

NTSTD

The following is an example of a Call Agent Platform log in NTSTD format:

```
COMPACT06BT * CCA355 JAN21 18:41:14 1864 FLT Jam Inactive Unit
Unit Number : 0, ACTIVE
Description : Inactive JAMMED
```

SNMP

The following is an example of a Call Agent Platform log in SNMP format:

```
system.sysUpTime.0 => 1 day, 4:49:05
snmpTrapOID.0 => nnExtAlarmMinor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.49.44.54.58.52.49.58.49.52.46.48.44.8995
alarmActiveDateAndTime => 2004-1-21,6:41:14.0,
alarmActiveDescription => DeviceSpecificInfo=Unavailable;Unit Number : 0, ACTIVE
Description : Inactive JAMMED
nnExtAlarmActiveEventType => 5
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => CCA 355
nnExtAlarmActiveResourceDescription => IEMS=47.142.128.16-CS2K-Mgr;
nnExtAlarmActiveManualClear => 3
nnExtAlarmActiveSequenceNumber => 9104
```

Syslog

The following is an example of a Call Agent Platform log in Syslog format:

```
Jan 21 19:41:06 wnc0s0qh IEMS: _V2_~I=~H=wnc0s0qh~A=IEMS~S=2860~~ CCA355 MINOR FLT
Jam Inactive Unit^M Unit Number : 0, ACTIVE ^M Description : Inactive JAMMED
```

Performance

OM and PM Documentation references for Call Agent Platform

- NN10153-711 - Call Agent Performance Management

Northbound OM/PM Formats

Performance measurements for Call Agent Platform are available only from the Call Agent Manager interface. See NN10153-711 - Call Agent Performance Management for more information.

XML

The following is an example of Performance data for Call Agent Platform in XML format:

***Note:** The IEMS northbound performance interface does not support this device..*

CSV

The following is an example of Performance data for Call Agent Platform in CSV format:

***Note:** The IEMS northbound performance interface does not support this device..*

GUI/CLUI Documentation for Call Agent Platform

GUI Launching and User procedures

- NN10175-611 - Call Agent Administration and Security

Related documents

- NN10023-111 - Call Agent Basics
- NN10109-511 - Call Agent Configuration Management

Centrex IP Call Manager (CICM)

This section contains IEMS Northbound log samples and device documentation references for the CICM.

CICM Fault Interface

Fault documentation for CICM :

- NN10334-911 - IEMS Fault Management

Fault Mapping for CICM

The following criteria can be used for looking up information on specific faults for CICM.

Fault Correlation for CICM

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
CICM	logname and number	logname and number	logname and number	logname and number	NN10334-911 - IEMS Fault Management

Northbound Fault Formats for CICM

SCC2

The following is an example of a CICM log in SCC2 format:

* 02 CICM359 0001 FLT CICM Fault

Location: 47.165.168.120

Notification Id: 7

State: Raised

Category: equipment

Cause: equipmentMalfunction(15)

Time: Jun 17 09:02:08 2004

Component Id: CICM=CICM-120A;NodeType=Cicm;Component=Card;Card=7

Specific Problem: Card 7 has an alarm.

Description: Card Alarm

?

**02 CICM500 0002 FLT CICM Fault

Location: 47.165.168.120

Notification Id: 5

State: Raised

Category: equipment

Cause: unspecifiedReason(118)

Time: Jun 17 09:02:08 2004

Component Id: CICM=CICM-120A;NodeType=Cicm;Component=Chassis

Specific Problem: Chassis card state change report for slot 7 in state

1

Description: Chassis Card State Change

?

**02 CICM339 0003 FLT CICM Fault

Location: 47.165.168.120

Notification Id: 6

State: Raised

Category: equipment

Cause: IANError(25)

Time: Jun 17 09:02:13 2004

Component Id: CICM=CICM-120A;NodeType=Cicm

Specific Problem: Have not received a message from Node B for 1.5*ALARM
_POLL_PERIOD Seconds. CPU_CARD_DOMAIN_A

Description: No Message Received From B

NTSTD

The following is an example of a CICM log in NTSTD format:

```
test * CICM359 JUN17 09:02:08 0004 FLT CICM Fault
      Location: 47.165.168.120
      Notification Id: 7
      State: Raised
      Category: equipment
      Cause: equipmentMalfunction(15)
      Time: Jun 17 09:02:08 2004
      Component Id: CICM=CICM-120A;NodeType=Cicm;Component=Card;Card=7
      Specific Problem: Card 7 has an alarm.
      Description: Card Alarm
```

```
test  ** C1CM500 JUN17 09:02:08 0005 FLT  C1CM Fault
      Location: 47.165.168.120
      Notification Id: 5
      State: Raised
      Category: equipment
      Cause: unspecifiedReason(118)
      Time: Jun 17 09:02:08 2004
      Component Id: C1CM=C1CM-120A;NodeType=C1cm;Component=Chassis
      Specific Problem: Chassis card state change report for slot 7 in state
      1
      Description: Chassis Card State Change
```

```
test  ** C1CM339 JUN17 09:02:13 0006 FLT  C1CM Fault
      Location: 47.165.168.120
      Notification Id: 6
      State: Raised
      Category: equipment
      Cause: lANError(25)
      Time: Jun 17 09:02:13 2004
      Component Id: C1CM=C1CM-120A;NodeType=C1cm
      Specific Problem: Have not received a message from Node B for 1.5*ALARM
      _POLL_PERIOD Seconds. CPU_CARD_DOMAIN_A
      Description: No Message Received From B
```

SNMP

The following is an example of a C1CM log in SNMP format:

```
sysUpTime. => 19:40:36
snmpTrapOID. => nnExtAlarmClear
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.54.45.50.57.44.49.48.58.50.57.58.48.46.51.44.11927
alarmActiveDateAndTime => 2004-6-29,10:29:0.3
alarmActiveDescription => DeviceSpecificInfo=lANError(25);Location: 47.165.168.120
Notification Id: 6
State: Raised
Category: equipment
Cause: lANError(25)
Time: Jun 17 09:02:13 2004
```

Component Id: C1CM=C1CM-120A;NodeType=C1cm

Specific Problem: Have not received a message from Node B for 1.5*ALARM_POLL_PERIOD Seconds. CPU_CARD_DOMAIN_A

Description: No Message Received From B

nnExtAlarmActiveEventType => 4

nnExtAlarmActiveProbableCause => 118

nnExtAlarmActiveAdditionalText =>

nnExtAlarmActiveDocumentationPointer => C1CM339

nnExtAlarmActiveResourceDescription => IEMS=47.165.168.120-C1CM_Card_A;C1CM=C1CM-120A;NodeType=C1cm

nnExtAlarmActiveSequenceNumber => 1

sysUpTime. => 19:40:37

snmpTrapOID. => nnExtAlarmClear

alarmActiveResourceId =>

.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48.48.52.45.54.45.50.57.44.49.48.58.50.57.58.48.46.52.44.11925

alarmActiveDateAndTime => 2004-6-29,10:29:0.4

alarmActiveDescription => DeviceSpecificInfo=equipmentMalfunction(15);Location: 47.165.168.120

Notification Id: 7

State: Raised

Category: equipment

Cause: equipmentMalfunction(15)

Time: Jun 17 09:02:08 2004

Component Id: C1CM=C1CM-120A;NodeType=C1cm;Component=Card;Card=7

Specific Problem: Card 7 has an alarm.

Description: Card Alarm

nnExtAlarmActiveEventType => 4

nnExtAlarmActiveProbableCause => 118

nnExtAlarmActiveAdditionalText =>

nnExtAlarmActiveDocumentationPointer => C1CM359

nnExtAlarmActiveResourceDescription => IEMS=47.165.168.120-C1CM_Card_A;C1CM=C1CM-120A;NodeType=C1cm;Component=Card;Card=7

nnExtAlarmActiveSequenceNumber => 2

sysUpTime. => 19:40:37

snmpTrapOID. => nnExtAlarmClear


```
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.54.45.50.57.44.49.48.58.50.57.58.48.46.53.44.11926

alarmActiveDateAndTime => 2004-6-29,10:29:0.5

alarmActiveDescription => DeviceSpecificInfo=unspecifiedReason(118);Location:
47.165.168.120

Notification Id: 5

State: Raised

Category: equipment

Cause: unspecifiedReason(118)

Time: Jun 17 09:02:08 2004

Component Id: CICM=CICM-120A;NodeType=Cicm;Component=Chassis

Specific Problem: Chassis card state change report for slot 7 in state 1

Description: Chassis Card State Change


nnExtAlarmActiveEventType => 4
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => CICM500
nnExtAlarmActiveResourceDescription => IEMS=47.165.168.120-CICM_Card_A;CICM=CICM-
120A;NodeType=Cicm;Component=Chassis
nnExtAlarmActiveSequenceNumber => 3


sysUpTime. => 19:40:48

snmpTrapOID. => nnExtAlarmMinor

alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.18.50.48
.48.52.45.54.45.49.55.44.57.58.50.58.56.46.48.44.11934

alarmActiveDateAndTime => 2004-6-17,9:2:8.0

alarmActiveDescription => DeviceSpecificInfo=equipmentMalfunction(15);Location:
47.165.168.120

Notification Id: 7

State: Raised

Category: equipment

Cause: equipmentMalfunction(15)

Time: Jun 17 09:02:08 2004

Component Id: CICM=CICM-120A;NodeType=Cicm;Component=Card;Card=7

Specific Problem: Card 7 has an alarm.

Description: Card Alarm


nnExtAlarmActiveEventType => 4
```

```

nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => C1CM359
nnExtAlarmActiveResourceDescription => IEMS=47.165.168.120-C1CM_Card_A;C1CM=C1CM-
120A;NodeType=C1cm;Component=Card;Card=7
nnExtAlarmActiveManualClear => 1
nnExtAlarmActiveSequenceNumber => 4

```

Syslog

The following is an example of a C1CM log in Syslog format:

```

Jun 29 10:40:34 2004      ComponentId: 47.165.168.74-C1CM-Mgr_Card_B      Specific
Problem: Connection Lost      Description: IEMS Unable to communicate with managed device

Jun 29 10:50:40 2004      ComponentId: 47.165.168.120-C1CM_Card_A      Description: IEMS
regained communication with the managed device

```

Performance

OM and PM Documentation references for C1CM

- N10327-711 - IEMS Performance Management

Northbound OM/PM Formats

Performance measurements for C1CM are available only from the C1CM Manager interface. See N10327-711 - IEMS Performance Management for more information.

XML

The following is an example of Performance data for C1CM in XML format:

```

<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
_ <PMFile xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonFormat.xsd" MeasurementCategory="PM">
<FileCreationTime>2004-06-23T12:30:00EST</FileCreationTime>
_ <System>
<SystemId>NortelNetworks/IEMS</SystemId>
_ <Entity Type="C1CM">
<EntityId>47.165.168.120</EntityId>
_ <Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>.iso.org.dod.internet.mgmt.mib-
2.rmon.usrHistory.usrHistoryControlTable.usrHistoryControlEntry</TableId>
<CaptureTime>2004-06-23T12:25:01EST</CaptureTime>
_ <Labels>
<Label>usrHistoryControlInterval</Label>

```

```
<Label>usrHistoryControlIndex</Label>
<Label>usrHistoryControlStatus</Label>
<Label>usrHistoryControlOwner</Label>
</Labels>
_ <RowOfValues>
_ <RowValue>
<Value>900</Value>
</RowValue>
_ <RowValue>
<Value>5</Value>
</RowValue>
_ <RowValue>
<Value>1</Value>
</RowValue>
_ <RowValue>
<Value>CICM-120A</Value>
</RowValue>
</RowOfValues>
</Table>
</Entity>
</System>
</PMFile>
```

CSV

PMFile=Begin

PM,commonFormat.xsd,2004-06-23T13:01:14EST

System=Begin

NortelNetworks/IEMS

Entity=Begin

47.165.168.120,CICM

Table=Begin

.iso.org.dod.internet.mgmt.mib-
2.rmon.usrHistory.usrHistoryControlTable.usrHistoryControlEntry,Snapshot,
5,2004-06-23T13:00:00EST

usrHistoryControlInterval,usrHistoryControlIndex,usrHistoryControlStatus,u
srHistoryControlOwner

900,5,1,CICM-120A

Table=End

Table=Begin

.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelPerf
RefMIB.nnPerfMetricReferenceTable.nnPerfMetricReferenceEntry,Snapshot
,5,2004-06-23T13:00:02EST

nnPerfMetricValue,nnPerfMetricSources,nnPerfMetricDataType,nnPerfMetri
cGroup,nnPerfMetricName,nnPerfMetricRefIndex

0,2,1,CICM,ActiveConnections,5

0,2,1,CICM,PercentageCpuUsed,4

0,2,1,CICM,PercentageMemoryUsed,3

0,2,1,CICM,NumberOfLogs,2

0,2,1,CICM,ActiveSessions,1

Table=End

Entity=End

System=End

PMFile=End

GUI/CLUI Documentation for CICM

GUI Launching and User procedures

Related documents

Passport 8600

This section contains IEMS Northbound log samples and device documentation references for the Passport 8600.

Passport 8600 Fault Interface

Fault documentation for Passport 8600 :

- 241-6001-502 Preside MDM Device Alarms Reference Guide
- 241-6003-110 - Preside Passport 8600 Device Integration Cartridge User Guide

Fault Mapping for Passport 8600

The following criteria can be used for looking up information on specific faults for Passport 8600.

Fault Correlation for Passport 8600

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
Passport 8600	logname and number	logname and number	logname and number	logname and number	241-6003-110 - Preside Passport 8600 Device Integration Cartridge User Guide

Northbound Fault Formats for Passport 8600

SCC2

The following is an example of a Passport 8600 log in SCC2 format:

```
**03 PP 398 5831 TBL PP Fault
Location: 47.142.130.66
State: Raise
Specific Problem: Generic Link Status
Description: Link Down: ifIndex = 175 ( AdminStatus = down OpeationStatu
s = down )
```

NTSTD

The following is an example of a Passport 8600 log in NTSTD format:

```

znc0s0jh  **    PP398 Feb04 22:58:46 3203 TBL  PP Fault
Location: 47.142.130.66
State: Raise
Specific Problem: Generic Link Status
Description: Link Down: ifIndex = 175 ( AdminStatus = down OpeationStatu
s = down )

```

SNMP

The following is an example of a Passport 8600 log in SNMP format:

```

sysUpTime.0 => 2:55:28
snmpTrapOID.0 => nnExtAlarmMajor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48
.48.52.45.50.45.52.44.53.58.53.56.58.52.54.46.54.44.90024
alarmActiveDateAndTime => 2004-2-4,5:58:46.6
alarmActiveDescription => DeviceSpecificInfo=;Link Down: ifIndex = 175 ( AdminStatus
= down OpeationStatus = down )
nnExtAlarmActiveEventType => 5
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => PP 398
nnExtAlarmActiveResourceDescription => IEMS=47.142.130.66-PP8600;3
nnExtAlarmActiveSequenceNumber => 2709

```

Syslog

The following is an example of a Passport 8600 log in Syslog format:

```

Feb  4 11:31:57 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=1459~~ PP398 MAJOR TBL
PP Fault^M      Location: 47.142.130.66^M      State: Raise ^M      Specific
Problem: Generic Link Status^M      Description: Link Down: ifIndex = 133 ( AdminStatus
= up OpeationStatus ^M      = down )

```

Performance

OM and PM Documentation references for Passport 8600

Not available at time of publication

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of Performance for Passport 8600 in XML format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
_ <PMFile xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonFormat.xsd" MeasurementCategory="PM">
<FileCreationTime>2004-06-23T17:35:01EST</FileCreationTime>
_ <System>
<SystemId>NortelNetworks/IEMS</SystemId>
_ <Entity Type="PP8600">
<EntityId>47.142.130.66</EntityId>
_ <SingleValues MeasurementKind="Snapshot" IntervalDuration="5">
_ <SingleValue>
<CaptureTime>2004-06-23T17:30:01EST</CaptureTime>
<MeasureId>snmpInvalidMsgs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.snmpV2.snmpModules.snmpMPDMIB.snmpMPDMI
BObjects.snmpMPDStats</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:30:01EST</CaptureTime>
<MeasureId>snmpOutPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>311026</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:30:01EST</CaptureTime>
<MeasureId>snmpOutTraps</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
```

```
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:30:01EST</CaptureTime>
<MeasureId>snmpInTotalSetVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>15</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:30:02EST</CaptureTime>
<MeasureId>snmpInPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>320467</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:30:03EST</CaptureTime>
<MeasureId>snmpInTotalReqVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>1412075</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:30:03EST</CaptureTime>
<MeasureId>snmpInASNParseErrs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>2</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:30:03EST</CaptureTime>
<MeasureId>snmpInBadVersions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
```



```
- <SingleValue>
<CaptureTime>2004-06-23T17:30:04EST</CaptureTime>
<MeasureId>snmpInBadCommunityUses</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
</SingleValues>
</Entity>
</System>
</PMFile>
```

CSV

The following is an example of Performance for Passport 8600 in CSV format:

```
PMFile=Begin
PM,commonFormat.xsd,2004-06-23T17:25:00EST

System=Begin
NortelNetworks/IEMS

Entity=Begin
47.142.130.66,PP8600

Table=Begin
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcStat.rcStatTable.rcStat
Entry,Snapshot,5,2004-06-23T17:20:15EST
rcStatFrameTooShorts,rcStatStgForwardTransitions,rcStatRouteInDiscards,rcStatBridgeI
nDiscards
0,0,0,0
0,0,0,0
253,0,0,0
0,0,0,0
74,0,0,0
0,0,0,0
0,0,0,0
560,0,0,0
591,0,0,0
```

544,0,0,0

0,0,0,0

0,0,0,0

0,0,0,0

566,0,0,0

0,0,0,0

0,0,0,0

208,0,0,0

698,0,0,0

586,0,0,0

0,0,0,0

547,0,0,0

537,0,0,0

582,0,0,0

553,0,0,0

28,0,0,0

582,0,0,0

173,0,0,0

574,0,0,0

544,0,0,0

544,0,0,0

0,0,0,0

0,0,0,0

563,0,0,0

558,0,0,0

589,0,0,0

513,0,0,0

575,0,0,0

350,0,0,0

0,0,0,0

45,0,0,0

0,0,0,0

552,0,0,0

0,0,0,904

0,0,0,577

8,0,0,0

0,0,0,0

0,0,0,0

0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,1678
669,0,0,0
0,0,0,0
0,0,0,0
0,0,0,30614
1,0,0,15253
0,0,0,0
0,0,0,0
0,0,0,0
13,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
17,0,0,0
0,0,0,0
49,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,1911
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0

```
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
556,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
0,0,0,0
283,0,0,0
Table=End
```

```
Table=Begin
```

```
.iso.org.dod.internet.mgmt.mib-2.ospf.ospfIfTable.ospfIfEntry,Snapshot,5,2004-06-23T17:20:14EST
```

```
ospfIfEvents
```

```
9
```

```
1
```

```
3
```

```
1
```

```
5
```

```
1
```

```
1
```

```
Table=End
```

```
Table=Begin
```

```
.iso.org.dod.internet.mgmt.mib-2.ospf.ospfNbrTable.ospfNbrEntry,Snapshot,5,2004-06-23T17:20:14EST
```

```
ospfNbrEvents,ospfNbrIpAddress
```

```
5,47.142.130.67
```

```
Table=End
```

```
SingleValues=Begin
Snapshot,5
snmpInvalidMsgs,2004-06-
23T17:20:13EST,.iso.org.dod.internet.snmpV2.snmpModules.snmpMPDMIB.snmpMPDMIBObjects
.snmpMPDStats,0,Valid
snmpOutPkts,2004-06-23T17:20:13EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,310853,Valid
snmpOutTraps,2004-06-23T17:20:13EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid
snmpInTotalSetVars,2004-06-23T17:20:13EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,15,Valid
snmpInPkts,2004-06-23T17:20:13EST,.iso.org.dod.internet.mgmt.mib-2.snmp,320294,Valid
snmpInTotalReqVars,2004-06-23T17:20:13EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,1411445,Valid
snmpInASNParseErrs,2004-06-23T17:20:14EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,2,Valid
snmpInBadVersions,2004-06-23T17:20:14EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid
snmpInBadCommunityUses,2004-06-23T17:20:14EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid
rcSysBufferUtilPeakTime,2004-06-
23T17:20:14EST,.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcSystem,0
,Valid
rcSysSwitchFabricUtil,2004-06-
23T17:20:14EST,.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcSystem,0
,Valid
rcSysNVRamUsed,2004-06-
23T17:20:14EST,.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcSystem,0
,Valid
rcSysBufferUtilPeak,2004-06-
23T17:20:14EST,.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcSystem,0
,Valid
rcSysCpuUtil,2004-06-
23T17:20:14EST,.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcSystem,9
,Valid
rcSysBufferUtil,2004-06-
23T17:20:14EST,.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcSystem,0
,Valid
SingleValues=End

Entity=End

System=End

PMFile=End
```

GUI/CLUI Documentation for Passport 8600

GUI Launching and User procedures

- 316341-B Rev 00 - Installing and Using Device Manager
- 314723-B - Configuring Network Management

Related documentation

- 314724-B - Configuring and Managing Security
- 314997-B - Read Me for Security
- 316341-A - Installing and Using Device Manager
- 313189-C - Getting Started
- 315545-B - Managing Platform Operations and Using Diagnostics Tools
- 314723-B - Configuring Network Management
- 314721-B - Configuring BGP Services
- 316433-B - Configuring QoS and IP Filtering
- 314720-C - Configuring IP Routing Operations
- 314725-B - Configuring Layer 2 Operations: "VLANs," Spanning "Tree," Multilink Trunking
- 314719-B - Configuring IP Multicast Routing Protocols
- 316343-A - Configuring IGMP for User Authentication (IGAP)
- 314722-A - Configuring IPX Routing Operations
- 314995-A - Configuring the Web Switching Module with Device Manager
- 316350-A - Using the SSL acceleration module with the Web switching module for the 8600 Series switch
- 315015-B - System Messaging Platform Reference Guide
- 315023-B - Using the Packet Capture Tool

Gateway Controller (GWC)

This section contains IEMS Northbound log samples and device documentation references for the GWC.

GWC Fault Interface

Fault documentation for GWC :

- NN10090-911 - GWC Fault Management

Fault Mapping for GWC

The following criteria can be used for looking up information on specific faults for GWC.

Fault Correlation for GWC

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
GWC	logname and number	logname and number	logname and number	logname and number	NN10090-911 GWC Fault Management

Northbound Fault Formats for GWC

SCC2

The following is an example of a GWC log in SCC2 format:

```
**14 GWC 307 7250 TBL GWC Fault
Location: GWC-2-UNIT-0
NotificationID: 4
State: Raise
Category: Communications
Cause: Communications subsystem failure
Time: Jan 23 15:15:59 2004
Component Id: GWC=GWC-2-UNIT-0;Version=PGC92BA;Unit=unit_0;Software=NODE
MTC
Specific Problem: EM not responding, provisioned data loaded from local
Flash
Description: Element Manager communication failure.
```

NTSTD

The following is an example of a GWC log in NTSTD format:

```
COMPACT06BT ** GWC307 Jan23 20:14:38 7250 TBL GWC Fault
Location: GWC-2-UNIT-0
NotificationID: 4
State: Raise
Category: Communications
Cause: Communications subsystem failure
```

```

Time: Jan 23 15:15:59 2004
Component Id: GWC=GWC-2-UNIT-0;Version=PGC92BA;Unit=unit_0;Software=NODE
MTC
Specific Problem: EM not responding, provisioned data loaded from local
Flash
Description: Element Manager communication failure.

```

SNMP

The following is an example of a GWC log in SNMP format:

```

system.sysUpTime.0 => 23:10:15
snmpTrapOID.0 => nnExtAlarmMajor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.51.44.51.58.49.52.58.51.56.46.48.44.42848
alarmActiveDateAndTime => 2004-1-23,3:14:38.0,
alarmActiveDescription => DeviceSpecificInfo=;Location: GWC-2-UNIT-0 NotificationID:
4
State: Raise
Category: Communications
Cause: Communications subsystem failure
Time: Jan 23 15:15:59 2004
Component Id: GWC=GWC-2-UNIT-0;Version=PGC92BA;Unit=unit_0;Software=NODEMTC
Specific Problem: EM not responding, provisioned data loaded from local Flash
Description: Element Manager communication failure.
nnExtAlarmActiveEventType => 5
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => GWC 307
nnExtAlarmActiveResourceDescription => IEMS=znc0s0j6;GWC=GWC-2-UNIT-
0;Version=PGC92BA;Unit=unit_0;Software=NODE
nnExtAlarmActiveManualClear => 0
nnExtAlarmActiveSequenceNumber => 9028

```

Syslog

The following is an example of a GWC log in Syslog format:

```

Feb 23 15:15:56 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=7307~~ GWC307 MAJOR TBL
GWC Fault^M          Location: GWC-2-UNIT-0^M          NotificationID: 4^M          State:

```

Raise^M failure^M	Category: Communications^M Time: Jan 23 15:15:59 2004^M	Cause: Communications subsystem Component Id: GWC=GWC-2-UNIT- 0;Version=PGC92BA;Unit=unit_0;Software=NODE^M
not responding, provisioned data loaded from local^M	MTC^M	Specific Problem: EM
Element Manager communication failure.^M	Flash^M	Description:

Performance

OM and PM Documentation references for GWC

- NN10156-711 - GWC Performance Management

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of performance data for GWC in XML format:

***Note:** The IEMS northbound performance interface does not support this device..*

CSV

The following is an example of performance data for GWC in CSV format:

***Note:** The IEMS northbound performance interface does not support this device..*

GUI/CLUI Documentation for GWC

GUI Launching and User procedures

- NN10026-111 - GWC Basics
- NN10112-511 - GWC Configuration Management
- NN10178-611 - GWC Security and Administration

Related documents

Media Application Server (MAS)

MAS Fault Interface

This section will provide references to customer documentation for Fault, Performance, Topology, GUI/CLUI, and Security for MAS.

Fault documentation for MAS :

- NN10303-111 - MCP 2.0 MAS Meetme Basics
- NN10297-111 - MCP 2.0 MAS Adhoc Basics

Fault Mapping for MAS

The following criteria can be used for looking up information on specific faults for MAS.

Fault Correlation for MAS

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
MAS	Event Id Logname and Log number	Event Id Logname and Log number	Event Id Logname and Log number	Event Id Logname and Log number	NN10303-111 MCP 2.0 MAS Meetme Basics NN10297-111 MCP 2.0 MAS Adhoc Basics

Northbound Fault Formats for MAS

SCC2

The following is an example of a MAS log in SCC2 format:

```
*C00 MAS 330 2515 FLT Fault
Location: 47.104.11.120
Notification Id: 1001
State: Raised
Category: processingError
Cause: applicationSubsystemFailure
Time: Mar 23 10:46:51 2004
Component Id: MediaServer_CStore
Specific Problem: MAS;330
Description: Component Shutdown
```

NTSTD

The following is an example of a MAS log in NTSTD format:

```
RTPU07CAPT *** MAS330 MAR23 17:00:18 2310 FLT Fault
```

```
Location: 47.104.11.120
```

```
Notification Id: 1001
```

```
State: Raised
```

```
Category: processingError
```

```
Cause: applicationSubsystemFailure
```

```
Time: Mar 23 10:46:51 2004
```

```
Component Id: MediaServer_CStore
```

```
Specific Problem: MAS;330
```

```
Description: Component Shutdown
```

SNMP

The following is an example of a MAS log in SNMP format:

```
sysUpTime.0 => 1:52:16
```

```
snmpTrapOID.0 => nnExtAlarmCritical
```

```
alarmActiveResourceId =>
```

```
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48  
.48.52.45.51.45.50.51.44.48.58.48.58.49.56.46.54.44.
```

```
2572
```

```
alarmActiveDateAndTime => 2004-3-23,0:0:18.6
```

```
alarmActiveDescription => Location: 47.104.11.120
```

```
Notification Id: 1001
```

```
State: Raised
```

```
Category: processingError
```

```
Cause: applicationSubsystemFailure
```

```
Time: Mar 23 10:46:51 2004
```

```
Component Id: MediaServer_CStore
```

```
Specific Problem: MAS;330
```

```
Description: Component Shutdown
```

```
nnExtAlarmActiveEventType => 3
```

```
nnExtAlarmActiveProbableCause => 2
```

```
nnExtAlarmActiveAdditionalText =>
```

```
nnExtAlarmActiveDocumentationPointer => MAS 330
```

```
nnExtAlarmActiveResourceDescription => IEMS=47.104.11.120-MAS;MediaServer_CStore
```

```
nnExtAlarmActiveManualClear => 1
```

```
nnExtAlarmActiveSequenceNumber => 1
```

Syslog

The following is an example of a MAS log in Syslog format:

```
Mar 23 12:00:19 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=3629~~ MAS330 CRIT FLT
Fault^M      Location: 47.104.11.120^M      Notification Id: 1001^M      State:
Raised^M      Category: processingError^M Cause: applicationSubsystemFailure^M
Time: Mar 23 10:46:51 2004^M      Component Id: MediaServer_CStore^M      Specific
Problem: MAS;330^M      Description: Component Shutdown
```

Performance

OM and PM Documentation references for MAS

- NN10303-111 - MCP 2.0 MAS Meetme Basics
- NN10297-111 - MCP 2.0 MAS Adhoc Basics

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of Performance data for MAS in XML format:

Not available at time of publication

CSV

The following is an example of Performance data for MAS in CSV format:

PMFile=Begin

MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime

PM,commonFormat.xsd,2004-07-02T05:55:54EST

System=Begin

SystemId

NortelNetworks/IEMS

Entity=Begin

EntityId,Type

47.104.11.120,MAS

SingleValues=Begin

MeasurementKind,IntervalDuration

Snapshot,5

MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability

CreateConf,2004-07-02T05:13:44EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:44EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:45EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:45EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:46EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:46EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:47EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:47EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:48EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:48EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:49EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:49EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:50EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:50EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:51EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:51EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:52EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:52EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:53EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:53EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:54EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:54EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:55EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:55EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:56EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:56EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:57EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:57EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:58EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:58EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:13:59EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:59EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:00EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:00EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:01EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:01EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:02EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:02EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:03EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:03EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:04EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:04EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:05EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:05EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:06EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:06EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:07EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:07EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:08EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:08EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:09EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:09EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:10EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:10EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:11EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:11EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:12EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:12EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:13EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:13EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:14EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:14:14EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:15EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:15EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:16EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:16EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:17EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:17EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:18EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:18EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:19EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:19EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:20EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:20EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:21EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:21EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:22EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:22EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:23EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:23EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:24EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:24EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:25EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:25EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:26EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:26EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:27EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:27EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:28EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:28EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:29EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:29EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:14:30EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:30EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:31EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:31EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:32EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:32EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:33EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:33EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:34EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:34EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:35EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:35EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:36EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:36EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:37EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:37EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:38EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:38EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:39EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:39EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:40EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:40EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:41EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:41EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:42EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:42EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:43EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:43EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:44EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:44EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:45EST,ConfMP,40,Valid

CreateConf,2004-07-02T05:14:45EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:46EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:46EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:47EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:47EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:48EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:48EST,ConfMP,40,Valid
SingleValues=End
Entity=End
System=End
PMFile=End

GUI/CLUI Documentation for MAS

GUI Launching and User procedures

- NN10303-111 - MCP 2.0 MAS Meetme Basics

Related Documents

None

Multimedia Communication Server (MCS)

MCS Fault Interface

This section will provide references to customer documentation for Fault, Performance, Topology, GUI/CLUI, and Security for MCS.

Fault documentation for MCS :

- NN10030-111 - Multimedia Communication Server 5200 Management Module Basics
- NN10303-111 - MCP 2.0 MAS Meetme Basics
- NN10297-111 - MCP 2.0 MAS Adhoc Basics

Fault Mapping for MCS

The following criteria can be used for looking up information on specific faults for MCS.

Fault Correlation for MCS

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
MCS	logname and log number	logname and log number	logname and log number	logname and log number	NN10247-111 Multimedia Communication Server 5200 System Management Console User Guide

Northbound Fault Formats for MCS**SCC2**

The following is an example of a MCS log in SCC2 format:

```

**55 LAM 102 0447 FLT  Fault
    Location: 47.104.23.117
    Notification Id: 1199
    State: Raised
    Category: communications
    Cause: communicationsSubsystemFailure
    Time: Mar 23 11:55:13 2004
    Component Id: Site=MgmtSite;Server=AppSvr;System.Sites.MgmtSite.Servers.
    Appsvr.Services.appsvr.BillingTransferAgent.BtaPrimaryConnectToAmLost
    Specific Problem: LAM;102
    Description: severity=MAJOR;probableCause=communications subsystem failure;
    addedText=Communication Error : Primary stream cannot connect to CAM;

```

NTSTD

The following is an example of a MCS log in NTSTD format:

```

RTPU07CAPT  **  LAM102 MAR23 16:55:13 0242 FLT  Fault
    Location: 47.104.23.117
    Notification Id: 1199
    State: Raised
    Category: communications
    Cause: communicationsSubsystemFailure
    Time: Mar 23 11:55:13 2004
    Component Id: Site=MgmtSite;Server=AppSvr;System.Sites.MgmtSite.Servers.
    Appsvr.Services.appsvr.BillingTransferAgent.BtaPrimaryConnectToAmLost

```

Specific Problem: LAM;102

Description: severity=MAJOR;probableCause=communications subsystem failure;
addedText=Communication Error : Primary stream cannot connect to CAM;

SNMP

The following is an example of a MCS log in SNMP format:

```
sysUpTime.0 => 2:19:58
snmpTrapOID.0 => nnExtAlarmMajor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.21.50.48
.48.52.45.51.45.50.51.44.49.49.58.53.53.58.49.51.46.
48.44.2616
alarmActiveDateAndTime => 2004-3-23,11:55:13.0
alarmActiveDescription => Location: 47.104.23.117
Notification Id: 1199
State: Raised
Category: communications
Cause: communicationsSubsystemFailure
Time: Mar 23 11:55:13 2004
Component Id:
Site=MgmtSite;Server=AppSvr;System.Sites.MgmtSite.Servers.Appsvr.Services.appsvr.Bil
lingTransferAgent.BtaPrimaryConnectToAmLost
Specific Problem: LAM;102
Description: severity=MAJOR;probableCause=communications subsystem
failure;addedText=Communication Error : Primary stream cannot connect to CAM;

nnExtAlarmActiveEventType => 1
nnExtAlarmActiveProbableCause => 6
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => LAM 102
nnExtAlarmActiveResourceDescription => IEMS=47.104.23.117-
CSE;Site=MgmtSite;Server=AppSvr;System.Sites.MgmtSite.Servers.Appsvr.Services.appsvr
.BillingTransferAge
nt.BtaPrimaryConnectToAmLost
nnExtAlarmActiveManualClear => 1
nnExtAlarmActiveSequenceNumber => 533
```

Syslog

The following is an example of a MCS log in Syslog format:

```
Mar 23 12:17:08 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=1558~~ LAM102 MAJOR FLT
Fault^M Location: 47.104.23.117^M Notification Id: 1199^M State:
Raised^M Category: communications^M Cause: communicationsSubsystemFailure^M
Time: Mar 23 11:55:13 2004^M Component Id:
```

```
Site=MgmtSite;Server=AppSvr;System.Sites.MgmtSite.Servers.^M
Appsvr.Services.appsvr.BillingTransferAgent.BtaPrimaryConnectToAmLost^M
Specific Problem: LAM;102^M      Description:
severity=MAJOR;probableCause=communications subsystem failu^M
re;addedText=Communication Error : Primary stream cannot connect to CAM;
```

Performance

OM and PM Documentation references for MCS

- NN10030-111 - Multimedia Communication Server 5200 Management Module Basics
- NN10247-111 - Multimedia Communication Server 5200 System

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of Performance data for MCS in XML format:

Not available at time of publication

CSV

The following is an example of Performance data for MCS in CSV format:

Not available at time of publication

GUI/CLUI Documentation for MCS

GUI Launching and User procedures

- NN10247-111 - Multimedia Communication Server 5200 System Management Console User Guide

Related Documents

None

Media Gateway 9000 (MG9000)

This section contains IEMS Northbound log samples and device documentation references for the MG9000.

MG 9000 Fault Interface

Fault documentation for MG 9000 :

- NN10074-911 MG9000 Fault Management

- NN10325-900 ATM/IP Fault Management

Fault Mapping for MG 9000

The following criteria can be used for looking up information on specific faults for MG 9000.

Fault Correlation for MG 9000

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
MG 9000	logname and number	logname and number	logname and number	logname and number	NN10325-900 ATM/IP Fault Management

Northbound Fault Formats for MG 9000

SCC2

The following is an example of a MG 9000 log in SCC2 format:

```
* 37 SWLN302 4259 TBL MG9K NorLineFault
Location: Port.frame0.shelf1.slot5.WL32.port21
Notification Id: 330712652810
State: UnAcknowledged
Category: processingError
Cause: Underlying Resource Unavailable
      NorLineFault - Line Protection Fault
Component Id: Port.frame0.shelf1.slot5.WL32.port21
specificProblem: NorLineFault - Line Protection Fault
Description: Line Protection HighVoltageError      : 0,1,5,21 [suspect b
ad LineCard]
```

NTSTD

The following is an example of a MG 9000 log in NTSTD format:

```
RTPU07BU * SWLN302 Jan23 17:37:31 4259 TBL MG9K NorLineFault
Location: Port.frame0.shelf1.slot5.WL32.port21
Notification Id: 330712652810
State: UnAcknowledged
```

```

Category: processingError
Cause: Underlying Resource Unavailable
      NorLineFault - Line Protection Fault
Component Id: Port.frame0.shelf1.slot5.WL32.port21
specificProblem: NorLineFault - Line Protection Fault
Description: Line Protection HighVoltageError      : 0,1,5,21 [suspect b
ad LineCard]

```

SNMP

The following is an example of a MG 9000 log in SNMP format:

```

system.sysUpTime.0 => 17:59:11
snmpTrapOID.0 => nnExtAlarmClearalarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48
.48.52.45.49.45.50.51.44.49.48.58.52.58.50.46.54.44.41817
alarmActiveDateAndTime => 2004-1-23,10:4:2.6,
alarmActiveDescription => Underlying Resource Unavailable
      NorLineFault - Line Protection Fault

nnExtAlarmActiveEventType => 3
nnExtAlarmActiveProbableCause => 56
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => SWLN302
nnExtAlarmActiveResourceDescription => IEMS=CC07;Port.frame0.shelf1.slot5.WL32.port21
nnExtAlarmActiveSequenceNumber => 7240

```

Syslog

The following is an example of a MG 9000 log in Syslog format:

```

Feb 23 12:40:26 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=4323~~ SWLN302 NONE TBL
MG9K NorLineFault^M      Location: Port.frame0.shelf1.slot5.WL32.port21^M
Notification Id: 330712652810^M      State: Cleared^M      Category:
processingError^M      Cause: Underlying Resource Unavailable^M
NorLineFault - Line Protection Fault^M      Component Id:
Port.frame0.shelf1.slot5.WL32.port21^M      specificProblem: NorLineFault - Line
Protection Fault^M      Description: Line Protection HighVoltageError      : 0,1,5,21
[suspect b^M      ad LineCard]

```

Performance

OM and PM Documentation references for MG 9000

- NN10140-711 MG9000 Performance Management

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of Performance data for MG 9000 in XML format:

Note: The IEMS northbound performance interface does not support this device..

CSV

The following is an example of Performance data for MG 9000 in CSV format:

Note: The IEMS northbound performance interface does not support this device..

GUI/CLUI Documentation for MG 9000

GUI Launching and User procedures

- NN10096-511 MG9000 Configuration Management

Related documents

- NN10276-500 ATM/IP Configuration Management

MultiService Switch 7400, 15000, 20000

This section contains IEMS Northbound log samples and device documentation references for the MSS 7400, 15000, 20000.

Information for this device is covered in MDM documentation. *Please refer to Section “ Multi-Service Data Manager (MDM)” on page 2716.* for more details.

MSS 7400, 15000, 20000 Fault Interface

Fault documentation for MSS 7400, 15000, 20000 :

Please refer to Section “ Fault documentation for MDM:” on page 2716.

Fault Mapping for MSS 7400, 15000, 20000

Please refer to Section “ Fault Mapping for MDM” on page 2716.

Northbound Fault Formats for MSS 7400, 15000, 20000

SCC2

The following is an example of a MSS 7400, 15000, 20000 log in SCC2 format:

```
19 PPEM302 8013 TBL
  time: 2004 01 27 14 19 53
  event: message
  compId: EM PP04 LP 8
  severity: indeterminate
  faultcode: 70560000
  alarmType: other
  commentData: 1-7-200
  0000
  1;DBG_WARNING:R:21-L:18 stats timeout.
```

NTSTD

The following is an example of a MSS 7400, 15000, 20000 log in NTSTD format:

```
RTPU07BU      PPEM302 Jan27 19:19:53 7467 TBL
  time: 2004 01 27 14 19 53
  event: message
  compId: EM PP04 LP 8
  severity: indeterminate
  faultcode: 70560000
  alarmType: other
  commentData: 1-7-200
  0000
  1;DBG_WARNING:R:21-L:18 stats timeout.
```


SNMP

The following is an example of a MSS 7400, 15000, 20000 log in SNMP format:

```
system.sysUpTime.0 => 3 days, 1:02:10
snmpTrapOID.0 => nnExtAlarmMessage
nnExtAlarmMessageResource => .0.0
nnExtAlarmMessageResourceDescription => IEMS=47.142.116.75-MDM-Mgr_PP04;EM PP04 LP 8
nnExtAlarmMessageDateAndTime => 2004-1-21,6:41:14.0,
nnExtAlarmMessageDocumentationPointer => PPEM302
nnExtAlarmMessageInfo => 19 PPEM302 8013 TBL time: 2004 01 27 14 19 53
event: message
compId: EM PP04 LP 8
severity: indeterminate
faultcode: 70560000
alarmType: other
commentData: 1-7-200
0000
1;DBG_WARNING:R:21-L:18 stats timeout.
```

Syslog

The following is an example of a MSS 7400, 15000, 20000 log in Syslog format:

```
Feb 27 13:19:58 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=2202~~ PPEM302 NONE TBL ^M
time: 2004 01 27 14 19 53^M event: message^M compId: EM PP04 LP 8^M
severity: indeterminate^M faultcode: 70560000^M alarmType: other^M
commentData: 1-7-200^M 0000 ^M 1;DBG_WARNING:R:21-L:18 stats timeout.
```

Performance

OM and PM Documentation references for MSS 7400, 15000, 20000

Please refer to Section “ OM and PM Documentation references for MDM” on page 2719.

Northbound OM/PM Formats

Performance measurements for MSS 7400, 15000, 20000 are available only from the MDM directly. *Please refer to Section “ Northbound OM/PM Formats” on page 2719.*

XML

The following is an example of Performance data for MSS 7400, 15000, 20000 in XML format:

***Note:** The IEMS northbound performance interface does not support this device..*

CSV

The following is an example of Performance data for MSS 7400, 15000, 20000 in CSV format:

***Note:** The IEMS northbound performance interface does not support this device..*

GUI/CLUI Documentation for MSS 7400, 15000, 20000

GUI Launching and User procedures

Please refer to *[“GUI/CLUI Documentation for MDM” on page 2720.](#)*

- NN10600-030 - Nortel Networks Multiservice Switch 7400/15000/20000 Overview
- 241-5701-045 - Passport "7400," "15000," 20000 Management System User Interface Guide
- NN10600-050 - Nortel Networks Multiservice Switch 7400/15000/20000 Commands Reference
- NN10600-053 - Nortel Networks Multiservice Switch 7400/15000/20000 Commands Job Aid

Related documents

Please refer to *[“Related documents” on page 2720.](#)*

- NN10600-001 - Nortel Networks Multiservice Switch 7400/15000/20000 Using the Documentation
- NN10600-002 - Nortel Networks Multiservice Switch 7400/15000/20000 Using Task-based Documentation Job Aid
- NN10600-005 - Nortel Networks Multiservice Switch 7400/15000/20000 Terminology
- NN10600-030 - Nortel Networks Multiservice Switch 7400/15000/20000 Overview
- NN10600-270 - Nortel Networks Multiservice Switch 7400/15000/20000 Software Installation

- NN10600-271 - Nortel Networks Multiservice Switch 7400/15000/20000 Network Management Connectivity
- NN10600-272 - Nortel Networks Multiservice Switch 7400/15000/20000 Upgrading Software
- NN10600-300 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: SNMP
- 241-5701-400 - Passport "7400," "15000," 20000 Networking Overview
- NN10600-405 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Call Server
- NN10600-410 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Call Redirection Server
- NN10600-415 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Hunt Group Server
- NN10600-420 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Trunking
- NN10600-425 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Dynamic Packet Routing System
- NN10600-435 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Path-Oriented Routing System
- NN10600-440 - Nortel Networks Multiservice Switch 7400 Operations: Frame Relay Managed Cut-through Switching
- NN10600-445 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Multiprotocol Label Switching
- NN10600-500 - Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference
- NN10600-510 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Trace System
- NN10600-520 - Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting
- NN10600-581 - Nortel Networks Multiservice Switch 7400/15000/20000 IP VPN Technology Fundamentals
- NN10600-582 - Nortel Networks Multiservice Switch 7400/15000/20000 IP VPN Configuration Management
- NN10600-550 - Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures
- NN10600-561 - Nortel Networks Multiservice Switch 7400/15000/20000 Data Management

- NN10600-551 - Nortel Networks Multiservice Switch 7400/15000/20000 FP Configuration Reference
- NN10600-560 - Nortel Networks Multiservice Switch 7400/15000/20000 Accounting
- NN10600-700 - Nortel Networks Multiservice Switch 7400/15000/20000 ATM Technology Fundamentals
- NN10600-702 - Nortel Networks Multiservice Switch 7400/15000/20000 ATM Routing and Signaling Fundamentals
- NN10600-705 - Nortel Networks Multiservice Switch 7400/15000/20000 ATM Traffic Management Fundamentals
- NN10600-706 - Nortel Networks Multiservice Switch 7400/15000/20000 ATM Traffic Shaping and Policing Fundamentals
- NN10600-707 - Nortel Networks Multiservice Switch 7400/15000/20000 ATM Queuing and Scheduling Fundamentals
- NN10600-708 - Nortel Networks Multiservice Switch 7400/15000/20000 ATM CAC and Bandwidth Fundamentals
- NN10600-710 - Nortel Networks Multiservice Switch 7400/15000/20000 ATM Configuration Management
- NN10600-715 - Nortel Networks Multiservice Switch 7400/15000/20000 ATM Fault and Performance Management
- NN10600-720 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: AAL1 Circuit Emulation
- NN10600-730 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Inverse Multiplexing for ATMe
- NN10600-780 - Nortel Networks Media Gateway 7480/15000 Technology Fundamentals
- NN10600-781 - Nortel Networks Media Gateway 7480/15000 Non-switched Service Configuration Management
- NN10600-782 - Nortel Networks Media Gateway 7480/15000 Switched Service Configuration Management
- NN10600-800 - Nortel Networks Multiservice Switch 7400/15000/20000 IP Technology Fundamentals
- NN10600-801 - Nortel Networks Multiservice Switch 7400/15000/20000 IP Configuration Management
- NN10600-580 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Ethernet Service
- NN10600-120 - Nortel Networks Multiservice Switch 15000/20000 Hardware Description

- NN10600-130 - Nortel Networks Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade
- NN10600-170 - Nortel Networks Multiservice Switch 7400 Hardware Description
- NN10600-130 - Nortel Networks Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade
- NN10600-172 - Nortel Networks Multiservice Switch 7400 FP Cabling Reference
- NN10600-745 - Nortel Networks Multiservice Switch 7400 Operations: MPANL
- NN10600-750 - Nortel Networks Multiservice Switch 7400 Operations: Voice Transport
- NN10600-755 - Nortel Networks Multiservice Switch 7400 Operations: Voice Networking
- NN10600-765 - Nortel Networks Multiservice Switch 7400 Operations: Remote Server Agent
- NN10600-605 - Passport MDM Network Security: Operations
- NN10600-606 - Passport MDM Network Security: User Access Configuration
- NN10600-607 - Passport MDM Network Security: Secure Communications Configuration
- 241-6001-309 - Preside MDM Management Data Provider User Guide
- 241-6001-806 - Preside MDM MDP Data Formats Reference Guide
- NN10600-060 - Nortel Networks Multiservice Switch 7400/15000/20000 Components Reference

MS2000 Series Node

This section contains IEMS Northbound log samples and device documentation references for the MS2000 Series Node.

MS2000 Series Node Fault Interface

Fault documentation for MS2000 Series Node :

- NN10328-911 MS2000 Fault Management

Fault Mapping for MS2000 Series Node

The following criteria can be used for looking up information on specific faults for MS2000 Series Node.

Fault Correlation for MS2000 Series Node

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
MS2000 Series Node	logname and number	logname and number	logname and number	logname and number	NN10328-911 MS2000 Fault Management

Northbound Fault Formats for MS2000 Series Node

SCC2

The following is an example of a MS2000 Series Node log in SCC2 format:

34 AMS 501 0035 INFO MS2000 FAULT

Location: 47.142.134.127

State: Cleared

Time: 1086806097963

**34 AMS 501 0036 FLT MS2000 FAULT

Location: 47.142.134.127

State: Raised

Category: processingError

Cause: 71

Time: 1086806097964

Component Id: System#0

Trap Name: 6

Description: Network element admin state change alarm. Gateway is locked

NTSTD

The following is an example of a MS2000 Series Node log in NTSTD format:

Nortel-JH ** AMS501 JUN10 09:21:12 5707 FLT MS2000 FAULT

Location: 47.142.134.127

State: Raised
Category: processingError
Cause: 71
Time: 1086873672171
Component Id: System#0
Trap Name: 6
Description: Network element admin state change alarm. Gateway is shuttingDown

Nortel-JH AMS501 JUN10 09:21:12 5708 INFO MS2000 FAULT

Location: 47.142.134.127
State: Cleared
Time: 1086873672172

Nortel-JH ** AMS501 JUN10 09:21:12 5709 FLT MS2000 FAULT

Location: 47.142.134.127
State: Raised
Category: processingError
Cause: 71
Time: 1086873672174
Component Id: System#0
Trap Name: 6
Description: Network element admin state change alarm. Gateway is locked

Nortel-JH AMS501 JUN10 09:21:25 5710 INFO MS2000 FAULT

Location: 47.142.134.127
State: Cleared
Time: 1086873685240

SNMP

The following is an example of a MS2000 Series Node log in SNMP format:

sysUpTime. => 1 day, 19:19:22
snmpTrapOID. => nnExtAlarmMessage
nnExtAlarmMessageResource => .0.0

```
nnExtAlarmMessageResourceDescription => IEMS=Unknown Device;  
nnExtAlarmMessageDateAndTime => 2004-6-9,3:4:5.0  
nnExtAlarmMessageDocumentationPointer => IEMS601  
nnExtAlarmMessageInfo => 04 IEMS601 3350 INFO
```

Location: 10.5.0.17

Event: .1.3.6.1.6.3.1.1.5.3

Varbind0: .1.3.6.1.2.1.2.2.1.1.0: 132

Varbind1: .1.3.6.1.2.1.2.2.1.7.0: 1

Varbind2: .1.3.6.1.2.1.2.2.1.8.0: 2

```
sysUpTime. => 1 day, 19:19:25  
snmpTrapOID. => nnExtAlarmMessage  
nnExtAlarmMessageResource => .0.0  
nnExtAlarmMessageResourceDescription => IEMS=Unknown Device;  
nnExtAlarmMessageDateAndTime => 2004-6-9,3:4:7.9  
nnExtAlarmMessageDocumentationPointer => IEMS601  
nnExtAlarmMessageInfo => 04 IEMS601 3351 INFO
```

Location: 10.5.0.17

Event: .1.3.6.1.6.3.1.1.5.4

Varbind0: .1.3.6.1.2.1.2.2.1.1.0: 132

Varbind1: .1.3.6.1.2.1.2.2.1.7.0: 1

Varbind2: .1.3.6.1.2.1.2.2.1.8.0: 1

Syslog

The following is an example of a MS2000 Series Node log in Syslog format:


```
Jun  9 14:31:41 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=9643~~ AMS501 MAJOR FLT
MS2000 FAULT      Location: 47.142.134.127      State: Raised      Category:
processingError   Cause: 71      Time: 1086805901311      Component Id: System#0
Trap Name: 6      Description: Network element admin state change alarm. Gateway is
shuttingDown
```

```
Jun  9 14:31:41 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=9644~~ AMS501 NONE INFO
MS2000 FAULT      Location: 47.142.134.127      State: Cleared      Time:
1086805901313
```

```
Jun  9 14:31:41 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=9645~~ AMS501 MAJOR FLT
MS2000 FAULT      Location: 47.142.134.127      State: Raised      Category:
processingError   Cause: 71      Time: 1086805901314      Component Id: System#0
Trap Name: 6      Description: Network element admin state change alarm. Gateway is
locked
```

```
Jun  9 14:31:41 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=9646~~ IEMS601 NONE
```

Resetting board

Performance

OM and PM Documentation references for MS2000 Series Node

- NN10320-100 - ATM Solutions Basics
- NN10300-100 - IP Solutions Basics

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided.

XML

The following is an example of Performance data for MS2000 Series Node in XML format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
_ <PMFile xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonFormat.xsd" MeasurementCategory="PM">
<FileCreationTime>2004-06-23T17:40:01EST</FileCreationTime>
_ <System>
<SystemId>NortelNetworks/IEMS</SystemId>
_ <Entity Type="MS2000">
<EntityId>47.142.92.107</EntityId>
_ <SingleValues MeasurementKind="Snapshot" IntervalDuration="5">
```

```
- <SingleValue>
<CaptureTime>2004-06-23T17:35:01EST</CaptureTime>
<MeasureId>sysDescr</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.system</MeasureSuppId1>
<Value>Product: IPMedia 3000;SW Version: 4.30.380.12</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:35:01EST</CaptureTime>
<MeasureId>snmpOutPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>4858</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:35:01EST</CaptureTime>
<MeasureId>snmpInBadVersions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:35:01EST</CaptureTime>
<MeasureId>snmpInBadCommunityNames</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:35:02EST</CaptureTime>
<MeasureId>snmpInTotalReqVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>9089</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
```

```
<CaptureTime>2004-06-23T17:35:02EST</CaptureTime>
<MeasureId>snmpOutTraps</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>15</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:35:02EST</CaptureTime>
<MeasureId>snmpInBadCommunityUses</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:35:02EST</CaptureTime>
<MeasureId>snmpInPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>4844</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:35:02EST</CaptureTime>
<MeasureId>snmpInTotalSetVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>4</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:35:03EST</CaptureTime>
<MeasureId>snmpInASNParseErrs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:35:03EST</CaptureTime>
```

```
<MeasureId>tcpOutSegs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.tcp</MeasureSuppId1>
<Value>3531</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:35:03EST</CaptureTime>
<MeasureId>tcpInSegs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.tcp</MeasureSuppId1>
<Value>4359</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:35:03EST</CaptureTime>
<MeasureId>udpOutDatagrams</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.udp</MeasureSuppId1>
<Value>438175</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:35:03EST</CaptureTime>
<MeasureId>udpInDatagrams</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.udp</MeasureSuppId1>
<Value>107768</Value>
<Reliability>Valid</Reliability>
</SingleValue>
</SingleValues>
</Entity>
</System>
</PMFile>
```

CSV

The following is an example of Performance data for MS2000 Series Node in CSV format:

PMFile=Begin

PM,commonFormat.xsd,2004-06-23T17:25:50EST

System=Begin

NortelNetworks/IEMS

Entity=Begin

47.142.92.104,MS2000

SingleValues=Begin

Snapshot,5

snmpOutPkts,2004-06-23T17:24:09EST,.iso.org.dod.internet.mgmt.mib-2.snmp,368,Valid

snmpInBadVersions,2004-06-23T17:24:10EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid

snmpInBadCommunityNames,2004-06-23T17:24:10EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid

snmpInTotalReqVars,2004-06-23T17:24:10EST,.iso.org.dod.internet.mgmt.mib-2.snmp,959,Valid

snmpOutTraps,2004-06-23T17:24:10EST,.iso.org.dod.internet.mgmt.mib-2.snmp,13,Valid

snmpInBadCommunityUses,2004-06-23T17:24:10EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid

snmpInPkts,2004-06-23T17:24:10EST,.iso.org.dod.internet.mgmt.mib-2.snmp,356,Valid

snmpInTotalSetVars,2004-06-23T17:24:10EST,.iso.org.dod.internet.mgmt.mib-2.snmp,12,Valid

snmpInASNParseErrs,2004-06-23T17:24:10EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid

tcpOutSegs,2004-06-23T17:24:11EST,.iso.org.dod.internet.mgmt.mib-2.tcp,195,Valid

tcpInSegs,2004-06-23T17:24:11EST,.iso.org.dod.internet.mgmt.mib-2.tcp,13675,Valid

udpOutDatagrams,2004-06-23T17:24:11EST,.iso.org.dod.internet.mgmt.mib-2.udp,27702,Valid

udpInDatagrams,2004-06-23T17:24:11EST,.iso.org.dod.internet.mgmt.mib-2.udp,14797,Valid

snmpSilentDrops,2004-06-23T17:24:11EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid

acPerfCpMessageSendErrors,2004-06-23T17:24:11EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp,0,Valid

acPerfCpNumDupsForCompletedTransactions,2004-06-23T17:24:11EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp,0,Valid

acPerfCpMessageMaxRetransmissionsExceeded,2004-06-23T17:24:11EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp,0,Valid

acPerfCpMessageReceiveErrors,2004-06-23T17:24:12EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp,0,Valid

acPerfCpMessageRetransmissions,2004-06-23T17:24:13EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp,18,Valid

acPerfCpNumDupsForOutstandingTransactions,2004-06-23T17:24:13EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp,0,Valid

acPerfCpMessagesFromUntrustedSources,2004-06-23T17:24:13EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp,0,Valid

acPerfCpProtocolSyntaxErrors,2004-06-23T17:24:13EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp,0,Valid

acPerfRtpRcvrLostPackets,2004-06-23T17:24:13EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfRtp,0,Valid

acPerfRtpFailedDueToLackOfResources,2004-06-23T17:24:13EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfRtp,0,Valid

acPerfIvrPlayCollectRequests,2004-06-
23T17:24:14EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerf
ormances.acPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrPlayRequests,2004-06-
23T17:24:15EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerf
ormances.acPerfMediaServices.acPerfIvr,88,Valid

acPerfBctRequests,2004-06-
23T17:24:16EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerf
ormances.acPerfMediaServices.acPerfBct,0,Valid

acPerfIvrPlayCollectFailedDueToLackOfResources,2004-06-
23T17:24:15EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerf
ormances.acPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrPlaySegmentFailedDueToProvMismatch,2004-06-
23T17:24:15EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerf
ormances.acPerfMediaServices.acPerfIvr,9,Valid

acPerfIvrContDigitCollectRequests,2004-06-
23T17:24:15EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerf
ormances.acPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrPlayFailedDueToLackOfResources,2004-06-
23T17:24:15EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerf
ormances.acPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrPlayCollectFailedDueToProvMismatch,2004-06-
23T17:24:16EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerf
ormances.acPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrContDigitCollectFailedDueToLackOfResources,2004-06-
23T17:24:16EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerf
ormances.acPerfMediaServices.acPerfIvr,0,Valid

acPerfBctFailedDueToLackOfResources,2004-06-
23T17:24:16EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerf
ormances.acPerfMediaServices.acPerfBct,0,Valid

acPerfConfRequests,2004-06-
23T17:24:16EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerf
ormances.acPerfMediaServices.acPerfConf,11,Valid

acPerfConfPlays,2004-06-
23T17:24:16EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerf
ormances.acPerfMediaServices.acPerfConf,36,Valid

acPerfConfAddFailedDueToLackOfResources,2004-06-23T17:24:16EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaServices.acPerfConf,0,Valid

acPerfConfFailedDueToLackOfResources,2004-06-23T17:24:17EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaServices.acPerfConf,0,Valid

acPerfTtFailedDueToLackOfResources,2004-06-23T17:24:17EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaServices.acPerfTt,0,Valid

acPerfTtRequests,2004-06-23T17:24:17EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaServices.acPerfTt,0,Valid

acPerfSystemPacketEndpointsInUse,2004-06-23T17:24:17EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfSystem,0,Valid

SingleValues=End

Entity=End

System=End

PMFile=End

GUI/CLUI Documentation for MS2000 Series Node

GUI Launching and User procedures

- NN10323-111 MS2000 Basics

Related documents

- NN10340-511 MS2000 Configuration
- NN10337-611 MS2000 Security

Session Server Manager

This section contains IEMS Northbound log samples and device documentation references for the Session Server Manager.

Session Server Manager Fault Interface

This section will provide references to customer documentation for Fault, Performance, Topology, GUI/CLUI, and Security for Session Server Manager.

Fault documentation for Session Server Manager:

- NN10322-911 - Session Server Manager Fault Management

Fault Mapping for Session Server Manager

The following criteria can be used for looking up information on specific faults for Session Server Manager.

Fault Correlation for Session Server Manager

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
Session Server Manager	logname and number	logname and number	logname and number	logname and number	NN10322-911 Session Server Manager Fault Management

Northbound Fault Formats for Session Server Manager

SCC2

The following is an example of a Session Server Manager log in SCC2 format:

```
**57 SIPM302 2080 FLT SIPM Fault
Location: 47.142.123.43
Notification Id: 111
State: Raised
Category: communications
Cause: applicationSubsystemFailure
Time: Apr 12 21:57:55 2004
Component Id: NCGL=RTPF-SIP0;Unit=0;
Specific Problem: SIP Gateway Application State Not Synced With Mate
Description: SIP Gateway Application Mtc Out Of Sync
```

NTSTD

The following is an example of a Session Server Manager log in NTSTD format:

```
znc0s0jh ** SIPM302 APR12 21:57:55 2080 FLT SIPM Fault
Location: 47.142.123.43
Notification Id: 111
State: Raised
Category: communications
Cause: applicationSubsystemFailure
```

Time: Apr 12 21:57:55 2004
 Component Id: NCGL=RTPF-SIP0;Unit=0;
 Specific Problem: SIP Gateway Application State Not Synced With Mate
 Description: SIP Gateway Application Mtc Out Of Sync

SNMP

The following is an example of a Session Server Manager log in SNMP format:

```
sysUpTime.0 => 2:34:22
snmpTrapOID.0 => nnExtAlarmMajor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.
20.50.48.48.52.45.52.45.49.50.44.57.58.53.55.58.53.53.46.48.44.3070
alarmActiveDateAndTime => 2004-4-12,9:57:55.0
alarmActiveDescription => Location: 47.142.123.43
Notification Id: 111
State: Raised
Category: communications
Cause: applicationSubsystemFailure
Time: Apr 12 21:57:55 2004
Component Id: NCGL=RTPF-SIP0;Unit=0;
Specific Problem: SIP Gateway Application State Not Synced With Mate
Description: SIP Gateway Application Mtc Out Of Sync

nnExtAlarmActiveEventType => 1
nnExtAlarmActiveProbableCause => 2
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => SIPM302
nnExtAlarmActiveResourceDescription => IEMS=47.142.123.48-SP2000-Unit-0;NCGL=RTPF-
SIP0;Unit=0;
nnExtAlarmActiveManualClear => 2
nnExtAlarmActiveSequenceNumber => 35
```

Syslog

The following is an example of a Session Server Manager log in Syslog format:

```
Apr 12 22:13:03 znc0s0jh IEMS: V2_~I=~H=znc0s0jh~A=IEMS~S=6213~~ SIPM302 MAJOR FLT
SIPM Fault^M      Location:47.142.123.43^M      Notification Id: 111^M      State:
Raised^M      Category: communications^M      Cause: applicationSubsystemFailure^M
Time: Apr 12 21:57:55 2004^M      Component Id: NCGL=RTPF-SIP0;Unit=0;^M      Specific
Problem: SIP Gateway Application State Not Synced With Mate^M      Description: SIP
Gateway Application Mtc Out Of Sync
```

Performance

OM and PM Documentation references for Session Server Manager

- NN10342-711 Session Server Manager Performance Management

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of Performance for Session Server Manager in XML format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
_ <PMFile xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonFormat.xsd" MeasurementCategory="PM
```

```
<MeasureId>snmpInBadVersions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:35:01EST</CaptureTime>
<MeasureId>snmpInBadCommunityNames</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>1</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:35:01EST</CaptureTime>
<MeasureId>snmpInTotalReqVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>9899</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:35:01EST</CaptureTime>
<MeasureId>snmpOutTraps</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:35:01EST</CaptureTime>
<MeasureId>snmpInBadCommunityUses</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:35:02EST</CaptureTime>
<MeasureId>snmpInPkts</MeasureId>
```

```
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>8692</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:35:02EST</CaptureTime>
<MeasureId>snmpInTotalSetVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:35:02EST</CaptureTime>
<MeasureId>snmpInASNParseErrs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:35:02EST</CaptureTime>
<MeasureId>hrSystemDate</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.host.hrSystem</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:35:03EST</CaptureTime>
<MeasureId>hrSystemUptime</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.host.hrSystem</MeasureSuppId1>
<Value>1316119</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:35:03EST</CaptureTime>
<MeasureId>hrSystemProcesses</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.host.hrSystem</MeasureSuppId1>
```

```
<Value>170</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T17:35:03EST</CaptureTime>
<MeasureId>snmpSilentDrops</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
</SingleValues>
</Entity>
</System>
</PMFile>
```

CSV

The following is an example of Performance for Session Server Manager in CSV format:

PMFile=Begin

PM,commonFormat.xsd,2004-06-23T20:35:30EST

System=Begin

NortelNetworks/IEMS

Entity=Begin

47.174.74.179,Session Server

SingleValues=Begin

Snapshot,5

sysDescr,2004-06-23T20:30:01EST,.iso.org.dod.internet.mgmt.mib-2.system,Linux sp2k-1 2.4.22-samxts #1 Thu May 13 01:48:09 EDT 2004 i686,Valid

snmpOutPkts,2004-06-23T20:30:01EST,.iso.org.dod.internet.mgmt.mib-2.snmp,9342,Valid

snmpInBadVersions,2004-06-23T20:30:02EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid

snmpInBadCommunityNames,2004-06-23T20:30:02EST,.iso.org.dod.internet.mgmt.mib-2.snmp,1,Valid

snmpInTotalReqVars,2004-06-23T20:30:02EST,.iso.org.dod.internet.mgmt.mib-2.snmp,13190,Valid

snmpOutTraps,2004-06-23T20:30:02EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid

snmpInBadCommunityUses,2004-06-23T20:30:02EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid

snmpInPkts,2004-06-23T20:30:03EST,.iso.org.dod.internet.mgmt.mib-2.snmp,9355,Valid

snmpInTotalSetVars,2004-06-23T20:30:03EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid

snmpInASNParseErrs,2004-06-23T20:30:03EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid

hrSystemDate,2004-06-23T20:30:04EST,.iso.org.dod.internet.mgmt.mib-2.host.hrSystem,0,Valid

hrSystemUptime,2004-06-23T20:30:04EST,.iso.org.dod.internet.mgmt.mib-2.host.hrSystem,1326620,Valid

hrSystemProcesses,2004-06-23T20:30:04EST,.iso.org.dod.internet.mgmt.mib-2.host.hrSystem,170,Valid

SingleValues=End

Entity=End

System=End

PMFile=End

GUI/CLUI Documentation for Session Server Manager

GUI Launching and User procedures

- NN10333-111 Session Server Manager Basics

Related documents

- NN10338-511 - Session Server Manager configuration
- NN10346-611 - Session Server Manager Security and Administration

SAM21 Shelf Controller

This section contains IEMS Northbound log samples and device documentation references for the SAM21 Shelf Controller.

SAM21 Shelf Controller Fault Interface

Fault documentation for SAM21 Shelf Controller :

- NN10089-911 - SAM21 Shelf Controller Fault Management

Fault Mapping for SAM21 Shelf Controller

The following criteria can be used for looking up information on specific faults for SAM21 Shelf Controller.

Fault Correlation for SAM21 Shelf Controller

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
SAM21 Shelf Controller	logname and number	logname and number	logname and number	logname and number	NN10089-911 SAM21 Shelf Controller Fault Management

Northbound Fault Formats for SAM21 Shelf Controller

SCC2

The following is an example of a SAM21 Shelf Controller log in SCC2 format:

```
**37 SCU 350 0009 FLT Alarm Raised
Location: SAM21 1:CSAM01-01:sled 3
Time:      Wed Jan 14 13:55:52 EST 2004
Reason:    Temperature in Sled 3 is high
```


NTSTD

The following is an example of a SAM21 Shelf Controller log in NTSTD format:

```
COMPACT06BT  **  SCU350 Jan15 00:37:17 0009 FLT Alarm Raised
Location: SAM21 1:CSAM01-01:sled 3
Time:      Wed Jan 14 13:55:52 EST 2004
Reason:    Temperature in Sled 3 is high
```

SNMP

The following is an example of a SAM21 Shelf Controller log in SNMP format:

```
sysUpTime.0 => 9:14:20
snmpTrapOID.0 => nnExtAlarmMajor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.49.44.54.58.52.49.58.49.52.46.48.44.8995
alarmActiveDateAndTime => 2004-1-21,6:41:14.0,
alarmActiveDescription => DeviceSpecificInfo=;Location: SAM21 1:CSAM01-01:sled 3
Time:      Wed Jan 14 13:57:48 EST 2004
Reason:    Temperature in Sled 3 is high
nnExtAlarmActiveEventType => 5
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => SCU 350
nnExtAlarmActiveResourceDescription => IEMS=wnc0y0kz.us.nortel.com-SAM21-Mgr;
nnExtAlarmActiveManualClear => 2
nnExtAlarmActiveSequenceNumber => 1
```

Syslog

The following is an example of a SAM21 Shelf Controller log in Syslog format:

```
Feb 12 18:30:19 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=7929~~ SCU350 MAJOR FLT
Alarm Raised^M Location: SAM21 1:CSAM01-01:sled 3^M Time: Mon Jan 12
12:49:06 EST 2004^M Reason: Temperature in Sled 3 is high
```

Performance

OM and PM Documentation references for SAM21 Shelf Controller

- There are no OMs or PMs associated with this device

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of performance data for SAM21 Shelf Controller in XML format:

Note: The IEMS northbound performance interface does not support this device.

CSV

The following is an example of performance data for SAM21 Shelf Controller in CSV format:

Note: The IEMS northbound performance interface does not support this device.

GUI/CLUI Documentation for SAM21 Shelf Controller

GUI Launching and User procedures

- NN10025-111 - SAM21 Shelf Controller Basics
- NN10089-911 - SAM21 Shelf Controller Fault Management
- NN10111-511 - SAM21 Shelf Controller Configuration Management
- NN10177-611 - SAM21 Shelf Controller Administration and Security
- NN10155-711 - SAM21 Shelf Controller Performance Management

Related documents

- NN10320-100 - ATM Solutions Basics
- NN10300-100 - IP Solutions Basics

Storage Manager (STORM)

This section contains IEMS Northbound log samples and device documentation references for the STORM.

STORM Fault Interface

Fault documentation for STORM :

- NN10024-111 - STORM Basics
- NN10088-911 - STORM Fault Management

Fault Mapping for STORM

The following criteria can be used for looking up information on specific faults for STORM.

Fault Correlation for STORM

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
STORM	logname and number eg: STM 800	logname and number	logname and number	logname and number	NN10088-911 STORM Fault Management

Northbound Fault Formats for STORM

SCC2

The following is an example of a STORM log in SCC2 format:

Sample Clear:

```
19 STM 801 0595 INFO
  Location: 47.166.56.10
  Notification Id: 13
  State: Cleared
  Time: Jan 24 19:19:49 2004
```

Sample Raise:

```
**19 STM 801 0596 FLT  STM Fault
  Location: 47.166.56.10
  Notification Id: 14
  State: Raised
  Category: qualityOfService
  Cause: thresholdCrossed
  Time: Jan 24 19:19:49 2004
  Component Id: STORMIA=langley1
  Specific Problem:
```

Description: Status: Alarm raised. Used memory percentage is 18.24. Major alarm threshold value is 6.00.

NTSTD

The following is an example of a STORM log in NTSTD format:

Sample Clear:

```
RTPU07BR      STM801 Jan25 00:19:49 0041 INFO
Location: 47.166.56.10
Notification Id: 13
State: Cleared
Time: Jan 24 19:19:49 2004
```

Sample Raise:

```
RTPU07BR  **  STM801 Jan25 00:19:49 0042 FLT  STM Fault
Location: 47.166.56.10
Notification Id: 14
State: Raised
Category: qualityOfService
Cause: thresholdCrossed
Time: Jan 24 19:19:49 2004
Component Id: STORMIA=langley1
Specific Problem:
Description: Status: Alarm raised. Used memory percentage is 18.24. Major alarm threshold value is 6.00.
```

SNMP

The following is an example of a STORM log in SNMP format:

Sample Clear:

```
system.sysUpTime.0 => 8:01:55
snmpTrapOID.0 => nnExtAlarmClear
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.52.44.55.58.49.57.58.52.57.46.48.44.312
alarmActiveDateAndTime => 2004-1-21,6:41:14.0,
alarmActiveDescription => DeviceSpecificInfo=;Status: Alarm cleared. A new alarm with
higher severity will be raised.
nnExtAlarmActiveEventType => 2
nnExtAlarmActiveProbableCause => 118
```

```

nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => STM 801
nnExtAlarmActiveResourceDescription => IEMS=zmdhh0jk.europe.nortel.com-
STORM;STORMIA=langley1
nnExtAlarmActiveSequenceNumber => 24

```

Sample Raise:

```

system.sysUpTime.0 => 7:01:55
snmpTrapOID.0 => nnExtAlarmMajor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.52.44.55.58.49.57.58.52.57.46.48.44.329
alarmActiveDateAndTime => 2004-1-21,6:41:14.0,
alarmActiveDescription => Status: Alarm raised. Used memory percentage is 18.24. Major
alarm threshold value is 6.00.
nnExtAlarmActiveEventType => 2
nnExtAlarmActiveProbableCause => 51
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => STM 801
nnExtAlarmActiveResourceDescription => IEMS=zmdhh0jk.europe.nortel.com-
STORM;STORMIA=langley1
nnExtAlarmActiveManualClear => 2
nnExtAlarmActiveSequenceNumber => 25

```

Syslog

The following is an example of a STORM log in Syslog format:

Sample Clear:

```

Feb 24 19:19:43 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=0618~~ STM801 NONE INFO
^M      Location: 47.166.56.10^M      Notification Id: 13^M      State: Cleared^M
Time: Jan 24 19:19:49 2004

```

Sample Raise:

```

Feb 24 19:19:43 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=0619~~ STM801 MAJOR FLT
STM Fault^M      Location: 47.166.56.10^M      Notification Id: 14^M      State:
Raised^M      Category: qualityOfService^M      Cause: thresholdCrossed^M      Time:
Jan 24 19:19:49 2004^M      Component Id: STORMIA=langley1^M      Specific Problem:
^M      Description: Status: Alarm raised. Used memory percentage is 18.24. Majo^M
r alarm threshold value is 6.00.

```

Performance

OM and PM Documentation references for STORM

The SNMP based attributes that can be collected from the STORM device are documented in:

- NN10054-711 - STORM Performance Management Customer Document

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided.

XML

The following is an example of Performance data for STORM in XML format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
_ <PMFile xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonFormat.xsd" MeasurementCategory="PM">
<FileCreationTime>2004-06-23T21:30:00EST</FileCreationTime>
_ <System>
<SystemId>NortelNetworks/IEMS</SystemId>
_ <Entity Type="STORM">
<EntityId>47.166.56.10</EntityId>
_ <SingleValues MeasurementKind="Snapshot" IntervalDuration="5">
_ <SingleValue>
<CaptureTime>2004-06-23T21:25:01EST</CaptureTime>
<MeasureId>sysDescr</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.system</MeasureSuppId1>
<Value>Linux langley40 2.4.19-xfs #1 SMP Fri Nov 7 11:18:05 EST 2003 i686</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T21:25:02EST</CaptureTime>
<MeasureId>snmpOutPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>2790</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
```

```
<CaptureTime>2004-06-23T21:25:03EST</CaptureTime>
<MeasureId>snmpInBadVersions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T21:25:03EST</CaptureTime>
<MeasureId>snmpInBadCommunityNames</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>1</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T21:25:04EST</CaptureTime>
<MeasureId>snmpInTotalReqVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>8880</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T21:25:04EST</CaptureTime>
<MeasureId>snmpOutTraps</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>69</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T21:25:04EST</CaptureTime>
<MeasureId>snmpInBadCommunityUses</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T21:25:05EST</CaptureTime>
```

```
<MeasureId>snmpInPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>2739</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T21:25:05EST</CaptureTime>
<MeasureId>snmpInTotalSetVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T21:25:06EST</CaptureTime>
<MeasureId>snmpInASNParseErrs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T21:25:07EST</CaptureTime>
<MeasureId>snmpSilentDrops</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T21:25:08EST</CaptureTime>
<MeasureId>hrSystemDate</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.host.hrSystem</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T21:25:09EST</CaptureTime>
<MeasureId>hrSystemUptime</MeasureId>
```



```
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.host.hrSystem</MeasureSuppId1>
<Value>6603666</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2004-06-23T21:25:09EST</CaptureTime>
<MeasureId>hrSystemProcesses</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.host.hrSystem</MeasureSuppId1>
<Value>73</Value>
<Reliability>Valid</Reliability>
</SingleValue>
</SingleValues>
</Entity>
</System>
</PMFile>
```

CSV

The following is an example of Performance data for STORM in CSV format:

```
PMFile=Begin
PM,commonFormat.xsd,2004-06-23T21:30:00EST

System=Begin
NortelNetworks/IEMS

Entity=Begin
47.166.56.10,STORM

SingleValues=Begin
Snapshot,5
sysDescr,2004-06-23T21:25:01EST,.iso.org.dod.internet.mgmt.mib-2.system,Linux
langley40 2.4.19-xfs #1 SMP Fri Nov 7 11:18:05 EST 2003 i686,Valid
snmpOutPkts,2004-06-23T21:25:02EST,.iso.org.dod.internet.mgmt.mib-2.snmp,2790,Valid
snmpInBadVersions,2004-06-23T21:25:03EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid
snmpInBadCommunityNames,2004-06-23T21:25:03EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,1,Valid
```

```
snmpInTotalReqVars,2004-06-23T21:25:04EST,.iso.org.dod.internet.mgmt.mib-  
2.snmp,8880,Valid  
snmpOutTraps,2004-06-23T21:25:04EST,.iso.org.dod.internet.mgmt.mib-2.snmp,69,Valid  
snmpInBadCommunityUses,2004-06-23T21:25:04EST,.iso.org.dod.internet.mgmt.mib-  
2.snmp,0,Valid  
snmpInPkts,2004-06-23T21:25:05EST,.iso.org.dod.internet.mgmt.mib-2.snmp,2739,Valid  
snmpInTotalSetVars,2004-06-23T21:25:05EST,.iso.org.dod.internet.mgmt.mib-  
2.snmp,0,Valid  
snmpInASNParseErrs,2004-06-23T21:25:06EST,.iso.org.dod.internet.mgmt.mib-  
2.snmp,0,Valid  
snmpSilentDrops,2004-06-23T21:25:07EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid  
hrSystemDate,2004-06-23T21:25:08EST,.iso.org.dod.internet.mgmt.mib-  
2.host.hrSystem,0,Valid  
hrSystemUptime,2004-06-23T21:25:09EST,.iso.org.dod.internet.mgmt.mib-  
2.host.hrSystem,6603666,Valid  
hrSystemProcesses,2004-06-23T21:25:09EST,.iso.org.dod.internet.mgmt.mib-  
2.host.hrSystem,73,Valid  
SingleValues=End  
Entity=End  
System=End  
PMFile=End
```

GUI/CLUI Documentation for STORM

GUI Launching and User procedures

- NN10024-111 (STORM Basics)

Related documents

- NN10066-461 (Understanding STORM)
- NN10110-511 (STORM Configuration)
- NN10054-711 (STORM Performance)
- NN10176-611 (STORM Administration and Security)

Universal Audio Server (UAS)

This section contains IEMS Northbound log samples and device documentation references for the UAS.

UAS Fault Interface

Fault documentation for UAS :

- NN10073-911 UAS Fault Management

Fault Mapping for UAS

The following criteria can be used for looking up information on specific faults for UAS.

Fault Correlation for UAS

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
UAS	logname and number	logname and number	logname and number	logname and number	NN10073-911 UAS Fault Management

Northbound Fault Formats for UAS

SCC2

The following is an example of a UAS log in SCC2 format:

```
*C59 UAS 301 0723 TBL UAS Fault
Location: UAS12_Test
NotificationID: 2109441
State: Raise
Category: Processing Error
Cause: Software error
Time: Jan 22 15:41:28 2004
Component Id: UAS;UASUnit=MATTA-2;Software=Call_Engine_1
Specific Problem: 12289
Description: CallEngine test alarm critical number 1
```

NTSTD

The following is an example of a UAS log in NTSTD format:

```
COMPACT506BT *** UAS301 Jan22 20:59:00 1149 TBL UAS Fault
Location: UAS12_Test
```

```

NotificationID: 2109441
State: Raise
Category: Processing Error
Cause: Software error
Time: Jan 22 15:41:28 2004
Component Id: UAS;UASUnit=MATTA-2;Software=Call_Engine_1
Specific Problem: 12289
Description: CallEngine test alarm critical number 1

```

SNMP

The following is an example of a UAS log in SNMP format:

```

sysUpTime.0 => 3:21:08
snmpTrapOID.0 => nnExtAlarmCritical
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.11
6.19.50.48.48.52.45.49.45.50.50.44.51.58.53.57.58.48.46.52.44.28556
alarmActiveDateAndTime => 2004-1-22,3:59:0.4,
alarmActiveDescription => DeviceSpecificInfo=Unavailable;Location: UAS12_Test
NotificationID: 2109441
State: Raise
Category: Processing Error
Cause: Software error
Time: Jan 22 15:41:28 2004
Component Id: UAS;UASUnit=MATTA-2;Software=Call_Engine_1
Specific Problem: 12289
Description: CallEngine test alarm critical number 1

```

Syslog

The following is an example of a UAS log in Syslog format:

```

Jan 22 15:59:00 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=3086~~ UAS301 CRIT TBL UAS
Fault^M      Location: UAS12_Test^M      NotificationID: 2109441^M      State:
Raise^M      Category: Processing Error^M      Cause: Software error^M      Time:
Jan 22 15:41:28 2004^M      Component Id: UAS;UASUnit=MATTA-
2;Software=Call_Engine_1^M      Specific Problem: 12289^M      Description:
CallEngine test alarm critical number 1

```

Performance

OM and PM Documentation references for UAS

- NTP NN10139-001 UAS Performance

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided
each of the Northbound formats provided

XML

The following is an example of performance data for UAS in XML format:

Note: The IEMS northbound performance interface does not support this device.

CSV

The following is an example of performance data for UAS in CSV format:

Note: The IEMS northbound performance interface does not support this device.

GUI/CLUI Documentation for UAS

GUI Launching and User procedures

- NTP NN10047-461 UAS Basics

Related documents

- NTP NN10095-511 UAS Configuration
- NTP NN10161-611 UAS Security
- NTP NN10047-461 UAS Upgrades

Universal Signaling Point (USP)

This section contains IEMS Northbound log samples and device documentation references for the USP.

USP Fault Interface

Fault documentation for USP :

- NN10071911 - USP Fault Management
- NN10072911 - USP-Compact Fault Management

Fault Mapping for USP

The following criteria can be used for looking up information on specific faults for USP.

Fault Correlation for USP

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
USP	Specific Problem: Log Group=<text> & Log Number=<number> Note: Log GroupID is not used	Specific Problem: Log Group=<text> & Log Number=<number> Note: Log GroupID is not used	Specific Problem: Log Group=<text> & Log Number=<number> Note: Log GroupID is not used	Specific Problem: Log Group=<text> & Log Number=<number> Note: Log GroupID is not used	NN10071911 USP Fault Management

Northbound Fault Formats for USP

SCC2

The following is an example of a USP log in SCC2 format:

```
**10 USP 398 0022 FLT  USP Fault
Location: 47.135.60.201
Notification Id: 526
State: Raised
Category: processingError
Cause: applicationSubsystemFailure(2)
Time: Jan 20 07:10:29 2004
Component Id: USP=autoimage;Shelf=0;Slot=15;ContextID=0x0
Specific Problem: Log GroupID=13;Log Group=System Node Maintenance;Log Number=3
Description: Transition to DISABLED Operational State.
```

NTSTD

The following is an example of a USP log in NTSTD format:

```
COMPACT06BT  ** USP398 Jan20 12:10:29 0022 FLT  USP Fault
    Location: 47.135.60.201
    Notification Id: 526
    State: Raised
    Category: processingError
    Cause: applicationSubsystemFailure(2)
    Time: Jan 20 07:10:29 2004
    Component Id: USP=autoimage;Shelf=0;Slot=15;ContextID=0x0
    Specific Problem: Log GroupID=13;Log Group=System Node Maintenance;Log Number=3
    Description: Transition to DISABLED Operational State.
```

SNMP

The following is an example of a USP log in SNMP format:

```
sysUpTime.0 => 2:58:15
snmpTrapOID.0 => nnExtAlarmMajor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.48.44.55.58.49.48.58.50.57.46.48.44.36582
alarmActiveDateAndTime => 2004-1-20,7:10:29.0,
alarmActiveDescription =>
DeviceSpecificInfo=applicationSubsystemFailure(2);Transition to DISABLED Operational
State.
nnExtAlarmActiveEventType => 3
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => USP 398
nnExtAlarmActiveResourceDescription => IEMS=usp_germany-1321-Unit-
0;USP=autoimage;Shelf=0;Slot=15;ContextID=0x0
nnExtAlarmActiveManualClear => 0
nnExtAlarmActiveSequenceNumber => 21
```

Syslog

The following is an example of a USP log in Syslog format:

```
Feb 22 01:50:39 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=0088~~ USP398 MAJOR FLT
USP Fault^M      Location: 47.135.60.201^M      Notification Id: 526^M      State:
Raised^M      Category: processingError^M      Cause:
applicationSubsystemFailure(2)^M      Time: Jan 20 07:10:29 2004^M      Component
Id: USP=autoimage;Shelf=0;Slot=15;ContextID=0x0^M      Specific Problem: Log
GroupID=13;Log Group=System Node Maintenance;Log N^M      umber=3^M      Description:
Transition to DISABLED Operational State.
```

Performance

OM and PM Documentation references for USP

- NN10137711 - USP Performance Management
- NN10138711 - USP-Compact Performance Management
- USP Logs & OMs - USP Logs and OMs

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of performance data for USP in XML format:

***Note:** The IEMS northbound performance interface does not support this device.*

CSV

The following is an example of performance data for USP in CSV format:

***Note:** The IEMS northbound performance interface does not support this device.*

GUI/CLUI Documentation for USP

GUI Launching and User procedures

- NN10093511 - USP Configuration Management
- NN10094511 - USP-Compact Operation Configuration
- NN10159611 - USP Administration and Security
- NN10160611 - USP-Compact Administration and Security

Related documents

- NN10008111 - USP Basics
- NN10045461 - Upgrading the USP

- NN10009111 - USP-Compact Product and Technology Fundamentals

XACore

This section contains IEMS Northbound log samples and device documentation references for the XACore.

XACore Fault Interface

Fault documentation for XACore :

- 297-8991-510 - XA-Core Maintenance Manual
- 297-8991-511 - XA-Core Maintenance Guide
- NN10275-909 - Succession fault Management logs Reference
- NN10083-911 - Communication Server 2000 Fault Management

DMS Standard (North America)

- 297-8021-840P1 - North American DMS100 Log Report Reference Manual Volume 1 of 8
- 297-8021-840P2 - North American DMS100 Log Report Reference Manual Volume 2 of 8
- 297-8021-840P3 - North American DMS100 Log Report Reference Manual Volume 3 of 8
- 297-8021-840P4 - North American DMS100 Log Report Reference Manual Volume 4 of 8
- 297-8021-840P5 - North American DMS100 Log Report Reference Manual Volume 5 of 8
- 297-8021-840P6 - North American DMS100 Log Report Reference Manual Volume 6 of 8
- 297-8021-840P7 - North American DMS100 Log Report Reference Manual Volume 7 of 8
- 297-8021-840P8 - North American DMS100 Log Report Reference Manual Volume 8 of 8

International Succession

- 297-9051-8401 - DMS100 Log Report Reference Manual Volume 1 of 7
- 297-9051-8402 - DMS100 Log Report Reference Manual Volume 2 of 7

- 297-9051-8403 - DMS100 Log Report Reference Manual Volume 3 of 7
- 297-9051-8404 - DMS100 Log Report Reference Manual Volume 4 of 7
- 297-9051-8405 - DMS100 Log Report Reference Manual Volume 5 of 7
- 297-9051-8406 - DMS100 Log Report Reference Manual Volume 6 of 7
- 297-9051-8407 - DMS100 Log Report Reference Manual Volume 7 of 7

Fault Mapping for XACore

The following criteria can be used for looking up information on specific faults for XACore.

Fault Correlation for XACore

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
XACore	log name and log number	log name and log number	log name and log number	log name and log number	297-8991-510 - XA-Core Maintenance Manual

Northbound Fault Formats for XACore

SCC2

The following is an example of a XACore log in SCC2 format:

```
* 47 XAC 305 0114 FLT RTIF (Reset Terminal Interface)
DESCRIPTION: State has changed from INSV to SYSB by FAULT action
PORT: Type State Site FL Row Bay Shf/Slt/Pk/Pt EqPEC/Serial
RTIF SYSB HOST 01 A00 DPCC:00 00 15R U 1 NTLX08AA/ NNTM17205KR8
REASON: Device Fault: RTIF IPC Protocol Error.
FAULT RECORD ID: 880166C7
```

NTSTD

The following is an example of a XACore log in NTSTD format:

```
COMPACT06BT * XAC305 Feb15 00:47:43 0114 FLT RTIF (Reset Terminal Interface)
DESCRIPTION: State has changed from INSV to SYSB by FAULT action
PORT: Type State Site FL Row Bay Shf/Slt/Pk/Pt EqPEC/Serial
RTIF SYSB HOST 01 A00 DPCC:00 00 15R U 1 NTLX08AA/ NNTM17205KR8
REASON: Device Fault: RTIF IPC Protocol Error.
```

FAULT RECORD ID: 880166C7

SNMP

The following is an example of a XACore log in SNMP format:

```
sysUpTime. => 0:28:39
snmpTrapOID. => nnExtAlarmMinor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.54.45.50.52.44.51.58.53.51.58.52.49.46.48.44.5248
alarmActiveDateAndTime => 2004-6-24,3:53:41.0
alarmActiveDescription => DeviceSpecificInfo=localTransmissionError;time: 2004 06 24
15 53 41
event: set
compId: EM MANTEO LP 3 SONET 2
severity: minor
faultcode: 70115203
alarmType: communications
commentData: Far end has raised a Line Remote Failure Indication alarm (rxRfiAlarm).
Check the operational attributes of the far-end.

nnExtAlarmActiveEventType => 1
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => PPEM300
nnExtAlarmActiveResourceDescription => IEMS=wnc0y0m3.us.nortel.com-MDM-Mgr;EM MANTEO
LP 3 SONET 2
nnExtAlarmActiveManualClear => 1
nnExtAlarmActiveSequenceNumber => 1375

sysUpTime. => 0:28:47
snmpTrapOID. => nnExtAlarmMinor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.54.45.50.52.44.51.58.53.51.58.52.56.46.48.44.5249
alarmActiveDateAndTime => 2004-6-24,3:53:48.0
alarmActiveDescription => time: 2004 06 24 15 53 48
event: set
compId: EM MANTEO LP 3 SONET 2
severity: minor
```

```

faultcode: 70115210
alarmType: communications
commentData: Far end line: Entering unavailable state (10 consecutive SESs).
Check the provisioning or the hardware on the local and far end.

nnExtAlarmActiveEventType => 1
nnExtAlarmActiveProbableCause => 12
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => PPEM300
nnExtAlarmActiveResourceDescription => IEMS=wnc0y0m3.us.nortel.com-MDM-Mgr;EM MANTEO
LP 3 SONET 2
nnExtAlarmActiveManualClear => 1
nnExtAlarmActiveSequenceNumber => 1376

```

Syslog

The following is an example of a XACore log in Syslog format:

```

Feb 14 19:47:43 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=9773~~ XAC305 MINOR FLT
RTIF (Reset Terminal Interface)^M node CM ^M DESCRIPTION: State
has changed from INSV to SYSB by FAULT action^M PORT: Type State Site FL Row
Bay Shf/Slt/Pk/Pt EqPEC/Serial^M RTIF SYSB HOST 01 A00 DPCC:00 00
15R U 1 NTLX08AA/ NNTM17205KR8^M REASON: Device Fault: RTIF IPC Protocol
Error. ^M FAULT RECORD ID: 880166C7

```

Performance

OM and PM Documentation references for XACore

- 297-8991-810 - XA-Core Reference Manual
- NN10149-711 - Communications Server 2000 Performance Management

DMS Standard (North America)

- 297-8021-814P1 - North American DMS-100 Operational Measurements Reference Manual Volume 1 of 6
- 297-8021-814P2 - North American DMS-100 Operational Measurements Reference Manual Volume 2 of 6
- 297-8021-814P3 - North American DMS-100 Operational Measurements Reference Manual Volume 3 of 6
- 297-8021-814P4 - North American DMS-100 Operational Measurements Reference Manual Volume 4 of 6

- 297-8021-814P5 - North American DMS-100 Operational Measurements Reference Manual Volume 5 of 6
- 297-8021-814P6 - North American DMS-100 Operational Measurements Reference Manual Volume 6 of 6

International Succession

- 297-9051-8141 - DMS-100 Family Operational Measurements Reference Manual Volume 1 of 6
- 297-9051-8142 - DMS-100 Family Operational Measurements Reference Manual Volume 2 of 6
- 297-9051-8143 - DMS-100 Family Operational Measurements Reference Manual Volume 3 of 6
- 297-9051-8144 - DMS-100 Family Operational Measurements Reference Manual Volume 4 of 6
- 297-9051-8145 - DMS-100 Family Operational Measurements Reference Manual Volume 5 of 6
- 297-9051-8146 - DMS-100 Family Operational Measurements Reference Manual Volume 6 of 6

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

Performance measurements for XACore are available from the CS2K Core Manager. See NN10149-711 - Communications Server 2000 Performance Management for more information.

XML

The following is an example of Performance data for XACore in XML format:

***Note:** The IEMS northbound performance interface does not support this device.*

CSV

The following is an example of Performance data for XACore in CSV format:

***Note:** The IEMS northbound performance interface does not support this device.*

GUI/CLUI Documentation for XACore

The XACore provides both command-line and MAP-based interfaces accessed through the CS2000 Core Manager.

GUI/CLUI Launching and User procedures

- NN10018-111 - CS2000 Core Manager Basics
see section “Accessing the Core”

Related documents

- NN10197-111 - Communication Server 2000 Basics
- NN10193-511 - Communication Server 2000 Configuration Management
- NN10127-811 - Communication Server 2000 Accounting Management
- NN10171-611 - Communication Server 2000 Security and Administration
- 297-5051-921 - SuperNode Data Manager DDMS ASCII CI Gateway User Guide
- 297-5161-022P1 - Advanced Intelligent Network Service Enablers SIG Volume 1 of 3
- 297-5161-022P2 - Advanced Intelligent Network Service Enablers SIG Volume 2 of 3
- 297-5161-022P3 - Advanced Intelligent Network Service Enablers SIG Volume 3 of 3
- 297-8021-350P1 - North American DMS-100 Translations Guide Volume 1 of 25
- 297-8021-350P2 - North American DMS-100 Translations Guide Volume 2 of 25
- 297-8021-350P3 - North American DMS-100 Translations Guide Volume 3 of 25
- 297-8021-350P4 - North American DMS-100 Translations Guide Volume 4 of 25
- 297-8021-350P5 - North American DMS-100 Translations Guide Volume 5 of 25
- 297-8021-350P6 - North American DMS-100 Translations Guide Volume 6 of 25
- 297-8021-350P7 - North American DMS-100 Translations Guide Volume 7 of 25
- 297-8021-350P8 - North American DMS-100 Translations Guide Volume 8 of 25
- 297-8021-350P9 - North American DMS-100 Translations Guide Volume 9 of 25
- 297-8021-350P10 - North American DMS-100 Translations Guide Volume 10 of 25

- 297-8021-350P11 - North American DMS-100 Translations Guide
Volume 11 of 25
- 297-8021-350P12 - North American DMS-100 Translations Guide
Volume 12 of 25
- 297-8021-350P13 - North American DMS-100 Translations Guide
Volume 13 of 25
- 297-8021-350P14 - North American DMS-100 Translations Guide
Volume 14 of 25
- 297-8021-350P15 - North American DMS-100 Translations Guide
Volume 15 of 25
- 297-8021-350P16 - North American DMS-100 Translations Guide
Volume 16 of 25
- 297-8021-350P17 - North American DMS-100 Translations Guide
Volume 17 of 25
- 297-8021-350P18 - North American DMS-100 Translations Guide
Volume 18 of 25
- 297-8021-350P19 - North American DMS-100 Translations Guide
Volume 19 of 25
- 297-8021-350P20 - North American DMS-100 Translations Guide
Volume 20 of 25
- 297-8021-350P21 - North American DMS-100 Translations Guide
Volume 21 of 25
- 297-8021-350P22 - North American DMS-100 Translations Guide
Volume 22 of 25
- 297-8021-350P23 - North American DMS-100 Translations Guide
Volume 23 of 25
- 297-8021-350P24 - North American DMS-100 Translations Guide
Volume 24 of 25
- 297-8021-350P25 - North American DMS-100 Translations Guide
Volume 25 of 25
- 297-8021-351P1 - DMS-100 Data Schema Reference Manual
- 297-8021-351P2 - DMS-100 Data Schema Reference Manual
- 297-8021-351P3 - DMS-100 Data Schema Reference Manual
- 297-8021-351P4 - DMS-100 Data Schema Reference Manual
- 297-8021-351P5 - DMS-100 Data Schema Reference Manual
- 297-8021-351P6 - DMS-100 Data Schema Reference Manual
- 297-8021-351P7 - DMS-100 Data Schema Reference Manual

- 297-8021-351P8 - DMS-100 Data Schema Reference Manual
- 297-8021-351P9 - DMS-100 Data Schema Reference Manual
- 297-8021-351P10 - DMS-100 Data Schema Reference Manual
- 297-8021-351P11 - DMS-100 Data Schema Reference Manual
- 297-8021-351P12 - DMS-100 Data Schema Reference Manual
- 297-8021-801 - DMS-100 Feature Guide
- 297-8021-808P1 - DMS-100 SERVORD Reference Manual
- 297-8021-808P2 - DMS-100 SERVORD Reference Manual
- 297-8021-814P1 - DMS-100 Operational Measurements Reference Manual
- 297-8021-814P2 - DMS-100 Operational Measurements Reference Manual
- 297-8021-814P3 - DMS-100 Operational Measurements Reference Manual
- 297-8021-814P4 - DMS-100 Operational Measurements Reference Manual
- 297-8021-814P5 - DMS-100 Operational Measurements Reference Manual
- 297-8021-814P6 - DMS-100 Operational Measurements Reference Manual
- 297-8021-840P1 - DMS-100 Logs Reference Manual
- 297-8021-840P2 - DMS-100 Logs Reference Manual
- 297-8021-840P3 - DMS-100 Logs Reference Manual
- 297-8021-840P4 - DMS-100 Logs Reference Manual
- 297-8021-840P5 - DMS-100 Logs Reference Manual
- 297-8021-840P6 - DMS-100 Logs Reference Manual
- 297-8021-840P7 - DMS-100 Logs Reference Manual
- 297-8021-840P8 - DMS-100 Logs Reference Manual
- 297-8021-855P1 - DMS-100 Office Parameters Reference Manual
- 297-8021-855P2 - DMS-100 Office Parameters Reference Manual
- 297-8021-855P3 - DMS-100 Office Parameters Reference Manual
- 297-8991-810 - XA-Core Reference Manual

Platforms

SDM Platform

This section contains IEMS Northbound log samples and device documentation references for the SDM Platform.

SDM Platform Fault Interface

Fault documentation for SDM Platform :

- NN10081-911 SDM Fault Management

Fault Mapping for SDM Platform

The following criteria can be used for looking up information on specific faults for SDM Platform.

Fault Correlation for SDM Platform

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
SDM (Platform) - AIX	logname and number	logname and number	logname and number	logname and number	NN10081-911 SDM Fault Management

Northbound Fault Formats for SDM Platform

SCC2

The following is an example of a SDM Platform log in SCC2 format:

```
* 52 SDM 317 0162 TBL
    node SDM          SDM Base Maintenance
DCE problem detected
Reason: SEC Master Server 47.142.94.49 is down.
```

NTSTD

The following is an example of a SDM Platform log in NTSTD format:

```
COMPACT06BT * SDM 317 Feb15 00:52:49 0162 TBL
    node SDM          SDM Base Maintenance
```

DCE problem detected

Reason: SEC Master Server 47.142.94.49 is down.

SNMP

The following is an example of a SDM Platform log in SNMP format:

```
sysUpTime.0 => 9:27:56
snmpTrapOID.0 => nnExtAlarmMinor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.49.44.54.58.52.49.58.49.52.46.48.44.8995
alarmActiveDateAndTime => 2004-1-14,7:52:49.1
alarmActiveDescription => DeviceSpecificInfo=Unavailable; node SDM      SDM Base
Maintenance
DCE problem detected
Reason: SEC Master Server 47.142.94.49 is down.

nnExtAlarmActiveEventType => 5
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => SDM 317
nnExtAlarmActiveResourceDescription => IEMS=wnc0y0m0.us.nortel.com-SDM;
nnExtAlarmActiveManualClear => 2
nnExtAlarmActiveSequenceNumber => 35
```

Syslog

The following is an example of a SDM Platform log in Syslog format:

```
Feb 14 19:52:49 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=9821~~ SDM317 MINOR TBL
^M      node SDM      SDM Base Maintenance^M      DCE problem detected^M      Reason:
SEC Master Server 47.142.94.49 is down.
```

Performance

OM and PM Documentation references for SDM Platform

- NN10147-711 SDM Performance Management

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of performance data for SDM Platform in XML format:

***Note:** The IEMS northbound performance interface does not support this device.*

CSV

The following is an example of performance data for SDM Platform in CSV format:

***Note:** The IEMS northbound performance interface does not support this device.*

GUI/CLUI Documentation for SDM Platform

SDM Platform has a command line user interface that can be accessed via a secure shell.

GUI/CLUI Launching and User procedures

- NN10017-111 SDM Basics (see User Interfaces Overview)

Related documents

- NN10059-461 Upgrading the SDM
- NN10103-511 SDM Configuration Management
- NN10125-811 SDM Accounting
- NN10169-611 SDM Security and Administration

Succession Server Platform Foundation Software (SSPFS)

This section contains IEMS Northbound log samples and device documentation references for the SSPFS platform.

SSPFS Fault Interface

Fault documentation for SSPFS

- NN10261-450v2 - Succession Network Volume 2 of 2

Fault Mapping for SSPFS

The following criteria can be used for looking up information on specific faults for SSPFS.

Fault Correlation for SSPFS

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
SSPFS	logname and number	logname and number	logname and number	logname and number	NN10261- 450v2 Succession Network Volume 2 of 2

Northbound Fault Formats for SSPFS

The SSPFS SNMP interface is not implemented yet.

SCC2

The following is an example of a SSPFS log in SCC2 format:

Not available at time of publication

NTSTD

The following is an example of a SSPFS log in NTSTD format:

Not available at time of publication

SNMP

The following is an example of a SSPFS log in SNMP format:

Not available at time of publication

Syslog

The following is an example of a SSPFS log in Syslog format:

Not available at time of publication

Performance

OM and PM Documentation references for SSPFS

The SSPFS platform does not generate and OMs or PMs, but it does collect such information from other network elements. For more information see:

- NN10276-500 - ATM/IP Configuration Management (Configuration of SNMP Poller)

- Succession Network Volume 2 of 2, NN10261-450v2.

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of performance data for SSPFS platform in XML format:

***Note:** The IEMS northbound performance interface does not support this device.*

CSV

The following is an example of performance data for SSPFS platform in CSV format:

***Note:** The IEMS northbound performance interface does not support this device.*

GUI/CLUI Documentation for SSPFS

GUI Launching and User procedures

- NN10276-500 - ATM/IP Configuration Management

***Note:** Contains information on the SSPFS CLI interface*

Related documents

- NN10281-600 - ATM/IP Administration and Security

Element Managers

CS2000 Core Manager

This section contains IEMS Northbound log samples and device documentation references for the CS2K Core Manager.

CS2K Core Manager Fault Interface

Fault documentation for CS2000 Core Manager :

- NN10275-909 - Succession fault Management logs Reference
- NN10082-911 - CS 2000 Core Manager Fault Management

Fault Mapping for CS2000 Core Manager

The following criteria can be used for looking up information on specific faults for CS2000 Core Manager.

Fault Correlation for CS2000 Core Manager

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
CS2000 Core Manager	log name and number	log name and number	log name and number	log name and number	NN10275-909 Succession fault Management logs Reference NN10082-911 CS 2000 Core Manager Fault Management

Northbound Fault Formats for CS2000 Core Manager

SCC2

The following is an example of a CS2000 Core Manager log in SCC2 format:

```
* 06 SDM 550 1506 INFO Node Status Change
Node:   SDM 0
Status: ** ISTb      from  ** ISTb
```

Reason: Application alarm set. SDM_ETA.eta

NTSTD

The following is an example of a CS2000 Core Manager log in NTSTD format:

```
COMPACT506BT    * SDM550 Feb15 03:07:00 1520 INFO Node Status Change
Node:          SDM 0
Status:        InSv          from    * ISTb
Reason:        Application alarm cleared. SDM_ETA.eta
```

SNMP

The following is an example of a CS2000 Core Manager log in SNMP format:

```
sysUpTime. => 1 day, 19:19:26
snmpTrapOID. => nnExtAlarmMessage
nnExtAlarmMessageResource => .0.0
nnExtAlarmMessageResourceDescription => IEMS=wnc0y0m0.us.nortel.com-CS2K-Mgr;
nnExtAlarmMessageDateAndTime => 2004-6-9,3:4:9.1
nnExtAlarmMessageDocumentationPointer => PM 610
nnExtAlarmMessageInfo => 04 PM 610 3352 INFO ABI XPM C-side Link State Change
```

Node: SMA2 0 Link: 0 Plane: 0 Port: 0

From: SYSB To: INSV

Reason: Link opened by MG9K/ABI

```
sysUpTime.0 => 1 day, 19:19:27
snmpTrapOID.0 =>
alarmActiveResourceId => .0.0
alarmActiveDateAndTime => 2004-6-9,3:4:9.3
alarmActiveDescription => DeviceSpecificInfo=Unavailable;
Node:          SDM 0
Status:        ** ISTb          from    ** ISTb
Reason:        Application alarm set. SDM_ETA.eta
```


Syslog

The following is an example of a CS2000 Core Manager log in Syslog format:

```
Feb 14 22:06:01 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=1165~~ SDM550 MINOR INFO
Node Status Change^M          node CM          ^M          Node:   SDM 0^M          Status:  **
ISTb          from  ** ISTb      ^M          Reason: Application alarm set. SDM_ETA.eta
```

Performance

OM and PM Documentation references for CS2000 Core Manager

- NN10148-711 - CS 2000 Core Manager Performance Management

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of performance data for CS2000 Core Manager in XML format:

***Note:** Northbound performance interface not supported for this component.*

CSV

The following is an example of performance data for CS2000 Core Manager in CSV format:

***Note:** Northbound performance interface not supported for this component.*

GUI/CLUI Documentation for CS2000 Core Manager

The CS2000 Core Manager provides both command-line and MAP-based interfaces.

GUI/CLUI Launching and User procedures

- NN10018-111 - CS2000 Core Manager Basics

Related documents

- NN10060-461 - Upgrading the CS 2000 Core Manager
- NN10082-911 - CS 2000 Core Manager Fault Management
- NN10104-511 - CS 2000 Core Manager Configuration Management
- NN10126-811 - CS 2000 Core Manager Accounting

- NN10170-611 - CS 2000 Core Manager Administration and Security

Centrex IP Call Manager (CICM Manager)

This section contains IEMS Northbound log samples and device documentation references for the CICM Manager.

CICM Fault Interface

Fault documentation for CICM Manager:

- NN10334-911 - IEMS Fault Management

Fault Mapping for CICM Manager

The following criteria can be used for looking up information on specific faults for CICM Manager.

Fault Correlation for CICM Manager

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
CICM Mgr	logname and number	logname and number	logname and number	logname and number	NN10334-911 - IEMS Fault Management

Northbound Fault Formats for CICM Manager

SCC2

The following is an example of a CICM Manager log in SCC2 format:

?

```
44 IEMS399 0011 FLT Communication Regained
Location: 47.142.106.223
NotificationID: 0
State: Cleared
Category: Communications
Time: Jun 30 15:44:06 2004
ComponentId: 47.165.168.74-CICM-Mgr_Card_B
Description: IEMS regained communication with the managed device
```

?

```
*C44 IEMS398 0012 FLT Communication Lost
      Location: 47.142.106.223
      NotificationID: 0
      State: Raised
      Category: Communications
      Cause: Communications subsystem failure
      Time: Jun 30 15:44:15 2004
      ComponentId: 47.165.168.74-CICM-Mgr_Card_B
      Specific Problem: Connection Lost
      Description: IEMS Unable to communicate with managed device
```

NTSTD

The following is an example of a CICM Manager log in NTSTD format:

```
test IEMS399 JUN30 15:44:06 0011 FLT Communication Regained
      Location: 47.142.106.223
      NotificationID: 0
      State: Cleared
      Category: Communications
      Time: Jun 30 15:44:06 2004
      ComponentId: 47.165.168.74-CICM-Mgr_Card_B
      Description: IEMS regained communication with the managed device
```

```
test *** IEMS398 JUN30 15:44:15 0012 FLT Communication Lost
      Location: 47.142.106.223
      NotificationID: 0
      State: Raised
      Category: Communications
      Cause: Communications subsystem failure
      Time: Jun 30 15:44:15 2004
      ComponentId: 47.165.168.74-CICM-Mgr_Card_B
      Specific Problem: Connection Lost
      Description: IEMS Unable to communicate with managed device
```

SNMP

The following is an example of a CICM Manager log in SNMP format:

```
sysUpTime. => 1 day, 18:18:50
snmpTrapOID. => nnExtAlarmClear
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.54.45.51.48.44.51.58.51.53.58.49.50.46.51.44.2
alarmActiveDateAndTime => 2004-6-30,3:35:12.3
alarmActiveDescription => DeviceSpecificInfo=transmitFailure(54);Location:
47.165.168.252
Notification Id: 13
State: Raised
Category: communications
Cause: transmitFailure(54)
Time: Jun 29 08:30:47 2004
Component Id: CICM=CICMEM-070-B;NodeType=Platform
Specific Problem: Syslog failure for securitylog stream.
Description: Syslog Failure.
nnExtAlarmActiveEventType => 1
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => CICM301
nnExtAlarmActiveResourceDescription => IEMS=47.165.168.252-CICM-
Mgr_Card_A;CICM=CICMEM-070-B;NodeType=Platform
nnExtAlarmActiveSequenceNumber => 7

sysUpTime. => 1 day, 18:19:00
snmpTrapOID. => nnExtAlarmMinor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.54.45.50.57.44.56.58.51.48.58.52.55.46.48.44.2965
alarmActiveDateAndTime => 2004-6-29,8:30:47.0
alarmActiveDescription => DeviceSpecificInfo=transmitFailure(54);Location:
47.165.168.252
Notification Id: 13
State: Raised
Category: communications
Cause: transmitFailure(54)
Time: Jun 29 08:30:47 2004
Component Id: CICM=CICMEM-070-B;NodeType=Platform
Specific Problem: Syslog failure for securitylog stream.
Description: Syslog Failure.
nnExtAlarmActiveEventType => 1
```

```

nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => C1CM301
nnExtAlarmActiveResourceDescription => IEMS=47.165.168.252-C1CM-
Mgr_Card_A;C1CM=C1CMEM-070-B;NodeType=Platform
nnExtAlarmActiveManualClear => 1
nnExtAlarmActiveSequenceNumber => 8

```

Syslog

The following is an example of a C1CM Manager log in Syslog format:

```

Jun 30 15:44:06 2004      ComponentId: 47.165.168.74-C1CM-Mgr_Card_B      Description:
IEMS regained communication with the managed device

Jun 30 15:44:15 znc0s0tm IEMS: _V2_~I=~H=znc0s0tm~A=IEMS~S=6162~~ IEMS398 CRIT FLT
Communication Lost      Location: 47.142.106.223      NotificationID: 0      State:
Raised      Category: Communications      Cause: Communications subsystem failure
Time:

Jun 30 15:44:15 2004      ComponentId: 47.165.168.74-C1CM-Mgr_Card_B      Specific
Problem: Connection Lost      Description: IEMS Unable to communicate with managed
device

```

Performance

OM and PM Documentation references for C1CM Manager

- NN10327-711 - IEMS Performance Management

Northbound OM/PM Formats

Performance measurements for C1CM Manager are available only from the C1CM Manager interface. See NN10327-711 - IEMS Performance Management for more information.

XML

The following is an example of Performance data for C1CM Manager in XML format:

```

<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
_ <PMFile xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonFormat.xsd" MeasurementCategory="PM">
<FileCreationTime>2004-06-23T13:36:04EST</FileCreationTime>
_ <System>
<SystemId>NortelNetworks/IEMS</SystemId>
_ <Entity Type="C1CM Mgr">
<EntityId>47.165.168.120</EntityId>

```

```

<Table MeasurementKind="Snapshot" IntervalDuration="5">
  <TableId>.iso.org.dod.internet.mgmt.mib-
2.rmon.usrHistory.usrHistoryControlTable.usrHistoryControlEntry</TableId>
  <CaptureTime>2004-06-23T13:35:01EST</CaptureTime>
  <Labels>
    <Label>usrHistoryControlInterval</Label>
    <Label>usrHistoryControlIndex</Label>
    <Label>usrHistoryControlStatus</Label>
    <Label>usrHistoryControlOwner</Label>
  </Labels>
  <RowOfValues>
    <RowValue>
      <Value>900</Value>
    </RowValue>
    <RowValue>
      <Value>5</Value>
    </RowValue>
    <RowValue>
      <Value>1</Value>
    </RowValue>
    <RowValue>
      <Value>CICM-120A</Value>
    </RowValue>
  </RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
  <TableId>.iso.org.dod.internet.mgmt.mib-
2.rmon.usrHistory.usrHistoryControlTable.usrHistoryControlEntry</TableId>
  <CaptureTime>2004-06-23T13:35:58EST</CaptureTime>
  <Labels>
    <Label>usrHistoryControlInterval</Label>
    <Label>usrHistoryControlIndex</Label>
    <Label>usrHistoryControlStatus</Label>
    <Label>usrHistoryControlOwner</Label>
  </Labels>
  <RowOfValues>
```

```
  <RowValue>
  <Value>900</Value>
</RowValue>
  <RowValue>
  <Value>5</Value>
</RowValue>
  <RowValue>
  <Value>1</Value>
</RowValue>
  <RowValue>
  <Value>CICM-120A</Value>
</RowValue>
</RowOfValues>
</Table>
  <Table MeasurementKind="Snapshot" IntervalDuration="5">
  <TableId>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelPerfRefMIB
.nnPerfMetricReferenceTable.nnPerfMetricReferenceEntry</TableId>
  <CaptureTime>2004-06-23T13:35:02EST</CaptureTime>
  <Labels>
  <Label>nnPerfMetricValue</Label>
  <Label>nnPerfMetricSources</Label>
  <Label>nnPerfMetricDataType</Label>
  <Label>nnPerfMetricGroup</Label>
  <Label>nnPerfMetricName</Label>
  <Label>nnPerfMetricRefIndex</Label>
  </Labels>
  <RowOfValues>
  <RowValue>
  <Value>0</Value>
  </RowValue>
  <RowValue>
  <Value>2</Value>
  </RowValue>
  <RowValue>
  <Value>1</Value>
  </RowValue>
```

```
<RowValue>
<Value>CICM</Value>
</RowValue>
<RowValue>
<Value>ActiveConnections</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>CICM</Value>
</RowValue>
<RowValue>
<Value>PercentageCpuUsed</Value>
</RowValue>
<RowValue>
<Value>4</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>2</Value>
```



```
</RowValue>
_ <RowValue>
<Value>1</Value>
</RowValue>
_ <RowValue>
<Value>CICM</Value>
</RowValue>
_ <RowValue>
<Value>PercentageMemoryUsed</Value>
</RowValue>
_ <RowValue>
<Value>3</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>0</Value>
</RowValue>
_ <RowValue>
<Value>2</Value>
</RowValue>
_ <RowValue>
<Value>1</Value>
</RowValue>
_ <RowValue>
<Value>CICM</Value>
</RowValue>
_ <RowValue>
<Value>NumberOfLogs</Value>
</RowValue>
_ <RowValue>
<Value>2</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
```

```
<Value>0</Value>
</RowValue>
_ <RowValue>
<Value>2</Value>
</RowValue>
_ <RowValue>
<Value>1</Value>
</RowValue>
_ <RowValue>
<Value>CICM</Value>
</RowValue>
_ <RowValue>
<Value>ActiveSessions</Value>
</RowValue>
_ <RowValue>
<Value>1</Value>
</RowValue>
</RowOfValues>
</Table>
</Entity>
</System>
</PMFile>
```

CSV

The following is an example of Performance data for CICM Manager in CSV format:

PMFile=Begin

PM,commonFormat.xsd,2004-06-23T13:45:00EST

System=Begin

NortelNetworks/IEMS

Entity=Begin

47.165.168.120,CICM Mgr

Table=Begin

.iso.org.dod.internet.mgmt.mib-
2.rmon.usrHistory.usrHistoryControlTable.usrHistoryControlEntry,Snapshot,
5,2004-06-23T13:40:01EST

usrHistoryControlInterval,usrHistoryControlIndex,usrHistoryControlStatus,u
srHistoryControlOwner

900,5,1,CICM-120A

Table=End

Table=Begin

.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelPerf
RefMIB.nnPerfMetricReferenceTable.nnPerfMetricReferenceEntry,Snapshot
,5,2004-06-23T13:40:02EST

nnPerfMetricValue,nnPerfMetricSources,nnPerfMetricDataType,nnPerfMetri
cGroup,nnPerfMetricName,nnPerfMetricRefIndex

0,2,1,CICM,ActiveConnections,5

0,2,1,CICM,PercentageCpuUsed,4

0,2,1,CICM,PercentageMemoryUsed,3

0,2,1,CICM,NumberOfLogs,2

0,2,1,CICM,ActiveSessions,1

Table=End

Entity=End

System=End

PMFile=End

GUI/CLUI Documentation for CICM Manager

GUI Launching and User procedures

Related documents

GWC Manager

This section contains IEMS Northbound log samples and device documentation references for the GWC Manager.

GWC Manager Fault Interface

Fault documentation for GWC Mgr :

- NN10325-900 - ATM/IP Fault Management

Fault Mapping for GWC Mgr

The following criteria can be used for looking up information on specific faults for GWC Mgr.

Fault Correlation for GWC Mgr

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
GWC Mgr	logname and number	logname and number	logname and number	logname and number	PLN-07AT OSS SN07 OSS Guide (ATM) PLN-07IPOSS SN07 OSS Guide (IP)

Northbound Fault Formats for GWC Mgr

SCC2

The following is an example of a GWC Mgr log in SCC2 format:

```
*C14 CMT 301 7248 TBL CMT Fault
Location: gwcem
NotificationID: 700
```

State: Raise
Category: Processing Error
Cause: Corrupt data
Time: Jan 23 15:14:38 2004
Component Id: SESM=GWCEMalarm;GWCEM=Recovery;GWC=GWC-2-UNIT-0
Specific Problem: FTP Problem
Description: Problem detected in GWC Recovery Subsystem

NTSTD

The following is an example of a GWC Mgr log in NTSTD format:

```
COMPACT06BT *** CMT301 Jan23 20:14:38 7248 TBL CMT Fault
Location: gwcem
NotificationID: 700
State: Raise
Category: Processing Error
Cause: Corrupt data
Time: Jan 23 15:14:38 2004
Component Id: SESM=GWCEMalarm;GWCEM=Recovery;GWC=GWC-2-UNIT-0
Specific Problem: FTP Problem
Description: Problem detected in GWC Recovery Subsystem
```

SNMP

The following is an example of a GWC Mgr log in SNMP format:

```
system.sysUpTime.0 => 23:10:15
snmpTrapOID.0 => nnExtAlarmCritical
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.51.44.51.58.49.52.58.51.56.46.48.44.42847
alarmActiveDateAndTime => 2004-1-23,3:14:38.0,
alarmActiveDescription => DeviceSpecificInfo=;Location: gwcem
NotificationID: 700
State: Raise
Category: Processing Error
Cause: Corrupt data
Time: Jan 23 15:14:38 2004
Component Id: SESM=GWCEMalarm;GWCEM=Recovery;GWC=GWC-2-UNIT-0
```

Specific Problem: FTP Problem

Description: Problem detected in GWC Recovery Subsystem

nnExtAlarmActiveEventType => 5

nnExtAlarmActiveProbableCause => 118

nnExtAlarmActiveAdditionalText =>

nnExtAlarmActiveDocumentationPointer => CMT 301

nnExtAlarmActiveResourceDescription =>

IEMS=znc0s0j6;SESM=GWCeMalarm;GWCeM=Recovery;GWC=GWC-2-UNIT-0

nnExtAlarmActiveManualClear => 0

nnExtAlarmActiveSequenceNumber => 9027

Syslog

The following is an example of a GWC Mgr log in Syslog format:

```
Feb 23 15:15:56 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=7305~~ CMT301 CRIT TBL CMT
Fault^M      Location: gwcem^M      NotificationID: 700^M      State: Raise^M
Category: Processing Error^M      Cause: Corrupt data^M      Time: Jan 23 15:14:38
2004^M      Component Id: SESM=GWCeMalarm;GWCeM=Recovery;GWC=GWC-2-UNIT-0^M
Specific Problem: FTP Problem^M      Description: Problem detected in GWC Recovery
Subsystem^M
```

Performance

OM and PM Documentation references for GWC Mgr

GWC Mgr has no operational or performance measurements.

- See NN10156-711 - GWC Performance Management for PM information.

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of performance data for GWC Mgr in XML format:

***Note:** Northbound performance interface not supported for this component.*

CSV

The following is an example of performance data for GWC Mgr in CSV format:

***Note:** Northbound performance interface not supported for this component.*

GUI/CLUI Documentation for GWC Mgr

GUI Launching and User procedures

- NN10320-100 - ATM Solutions Basics
- NN10300-100 - IP Solutions Basics
- NN10276-500 - ATM/IP Configuration Management
- NN10281-600 - ATM/IP Administration and Security
- NN10325-900 - ATM/IP Fault Management

Related documents

Integrated Element Management System (IEMS)

This section contains IEMS Northbound log samples and device documentation references for the IEMS.

IEMS Fault Interface

Fault documentation for IEMS :

- NN10334-911 - IEMS Fault Management

Fault Mapping for IEMS

The following criteria can be used for looking up information on specific faults for IEMS.

Fault Correlation for IEMS

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
IEMS	logname and logNumber	logname and logNumber	logname and logNumber	logname and logNumber	NN10334-911 IEMS Fault Management Guide

Northbound Fault Formats for IEMS

SCC2

The following is an example of a IEMS log in SCC2 format:

36 IEMS603 0001 INFO Missed Notifications

Location: 47.142.122.202

Component Id: IEMS=wnc0y0m0.us.nortel.com-CS2K-Mgr

Time: Feb 14 19:36:32 2004

Description: Notification(s) missed in ML 5050 - 5149

NTSTD

The following is an example of a IEMS log in NTSTD format:

RTPU07BU IEMS603 Feb15 00:36:32 0001 INFO Missed Notifications

Location: 47.142.122.202

Component Id: IEMS=wnc0y0m0.us.nortel.com-CS2K-Mgr

Time: Feb 14 19:36:32 2004

Description: Notification(s) missed in ML 5050 - 5149

SNMP

The following is an example of a IEMS log in SNMP format:

sysUpTime.0 => 9:34:06

snmpTrapOID.0 => nnExtAlarmMessage

nnExtAlarmMessageResource => .0.0

nnExtAlarmMessageResourceDescription => IEMS=wnc0y0m0.us.nortel.com-CS2K-Mgr;

nnExtAlarmMessageDateAndTime => 2004-1-14,7:58:59.2

nnExtAlarmMessageDocumentationPointer => IEMS603

nnExtAlarmMessageInfo => 58 IEMS603 0234 INFO Missed Notifications

Location: 47.142.122.202

Component Id: IEMS=wnc0y0m0.us.nortel.com-CS2K-Mgr

Time: Feb 14 19:58:59 2004

Description: Notification(s) missed in ML 5050 - 5149

Syslog

The following is an example of a IEMS log in Syslog format:

Feb 14 18:42:42 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=9198~~ IEMS603 NONE INFO
Missed Notifications^M Location: 47.142.122.202^M Component Id:
IEMS=wnc0y0m0.us.nortel.com-CS2K-Mgr^M Time: Feb 14 18:42:41 2004^M
Description: Notification(s) missed in ML 5050 - 5149

Performance

OM and PM Documentation references for IEMS

- NN10327-711 IEMS Performance Monitoring
- NN10321-111 - IEMS User Guide

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of performance data for IEMS in XML format:

***Note:** Northbound performance interface not supported for this component.*

CSV

The following is an example of performance data for IEMS in CSV format:

***Note:** Northbound performance interface not supported for this component.*

GUI/CLUI Documentation for IEMS

GUI Launching and User procedures

- NN10329-111 - IEMS Basics

Related documents

- NN10336-611 - IEMS Administration and Security
- NN10330-511 - IEMS Operational Configuration
- NN10326-461 - IEMS Upgrades

MG9000 Manager

This section contains IEMS Northbound log samples and device documentation references for the MG9000 Mgr.

MG9000 Mgr Fault Interface

Fault documentation for MG9000 Mgr :

- NN10074-911 MG9000 Fault Management

- NN10325-900 ATM/IP Fault Management
- NN10275-909 Succession Fault Management Logs Reference

Fault Mapping for MG9000 Mgr

The following criteria can be used for looking up information on specific faults for MG9000 Mgr.

Fault Correlation for MG9000 Mgr

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
MG9000 Mgr	logname and number	logname and number	logname and number	logname and number	NN10074-911 MG9000 Fault Management

Northbound Fault Formats for MG9000 Mgr

SCC2

The following is an example of a MG9000 Mgr log in SCC2 format:

```
49 MGEM302 4260 TBL MG9K InvalidEMIPAddress
  Location: MG9k EM Comm Network
  Notification Id: 17180020453
  State: Cleared
  Category: communications
  Cause: Communications Subsystem Failure
      Invalid EM IP Address - An invalid EM IP address has been set on the GW
  Component Id: MG9k EM Comm Network
  specificProblem: Invalid EM IP Address - An invalid EM IP address has be
en set on the GW
  Description: An invalid EM IP address has been set on the GW
```

NTSTD

The following is an example of a MG9000 Mgr log in NTSTD format:

```
RTPU07BR      MGEM302 Jan20 06:49:09 4260 TBL MG9K InvalidEMIPAddress
  Location: MG9k EM Comm Network
  Notification Id: 17180020453
```

```

State: Cleared
Category: communications
Cause: Communications Subsystem Failure
      Invalid EM IP Address - An invalid EM IP address has been set on the GW
Component Id: MG9k EM Comm Network
specificProblem: Invalid EM IP Address - An invalid EM IP address has be
en set on the GW
Description: An invalid EM IP address has been set on the GW

```

SNMP

The following is an example of a MG9000 Mgr log in SNMP format:

```

system.sysUpTime.0 => 20:33:14
iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTrap.snmpTrapOID.0 => nnExtAlarmClear
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48
.48.52.45.49.45.50.48.44.49.58.52.57.58.57.46.51.44.37279
alarmActiveDateAndTime => 2004-1-20,1:49:9.3,
alarmActiveDescription => Communications Subsystem Failure
Invalid EM IP Address - An invalid EM IP address has been set on the GW

nnExtAlarmActiveEventType => 1
nnExtAlarmActiveProbableCause => 6
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => MGEM302
nnExtAlarmActiveResourceDescription => IEMS=cco4;MG9k EM Comm Network
nnExtAlarmActiveSequenceNumber => 7768

```

Syslog

The following is an example of a MG9000 Mgr log in Syslog format:

```

Feb 23 12:38:54 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=4317~~ MGEM302 NONE TBL
MG9K InvalidEMIPAddress^M      Location: MG9k EM Comm Network^M      Notification
Id: 17180020453^M      State: Cleared^M      Category: communications^M      Cause:
Communications Subsystem Failure^M      Invalid EM IP Address - An invalid EM IP
address has been set on the GW^M      Component Id: MG9k EM Comm Network^M
specificProblem: Invalid EM IP Address - An invalid EM IP address has be^M      en
set on the GW^M      Description: An invalid EM IP address has been set on the GW

```

Performance

OM and PM Documentation references for MG9000 Mgr

There are no OM's or PM's associated with this component.

GUI/CLUI Documentation for MG9000 Mgr

GUI Launching and User procedures

- NN10096-511 MG9000 Configuration Management

Related documents

- NN10221105 VoA OSS Guide
- NN10162-611 MG9000 Administration and Security
- NN10048-461 Upgrading the MG9000
- NN10276-500 ATM/IP Configuration Management
- NN10325-900 ATM/IP Fault Management

Multi-Service Data Manager (MDM)

This section contains IEMS Northbound log samples and device documentation references for the MDM.

Information in this section also applies to the following Media Gateways : MSS 7400, 15000, 20000. All these devices are closely related and are covered by the same set of customer documentation.

MDM Fault Interface

Fault documentation for MDM:

- 241-6001-011 - Preside MDM Fault Management User Guide
- NN10092-911 - Passport 15000 and Preside MDM in Succession Networks Fault Management
- NN10600-500 - Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference
- 241-6001-501 - Preside MDM Proxy Alarms Reference Guide

Fault Mapping for MDM

The following criteria can be used for looking up information on specific faults for MDM.

MDM and Media Gateway devices (6400, 7480, 15000, 20000) use fault code to identify different alarms. Fault codes are eight digits or letters and are grouped by type (first four digits of fault code). Documentation for each fault code group is provided in the following table.

Fault Documentation for MDM

Fault Code Group	Document Reference
0000	NN10600-500 - Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference
1100	NN10600-500 - Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference
70xx	NN10600-500 - Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference
0999	241-6001-501 - Preside MDM Proxy Alarms Reference Guide
301x	241-6001-501 - Preside MDM Proxy Alarms Reference Guide
50xx	241-6001-501 - Preside MDM Proxy Alarms Reference Guide
600x	241-6001-501 - Preside MDM Proxy Alarms Reference Guide
A0xx	241-6001-501 - Preside MDM Proxy Alarms Reference Guide
B000	241-6001-501 - Preside MDM Proxy Alarms Reference Guide
CDxx	241-6001-501 - Preside MDM Proxy Alarms Reference Guide

The faults that are fed northbound from the IEMS use log name and number for distinction. The mapping between log name/number and fault code can be found in the Succession Solution document.

- NN10092-911 - Passport 15000 and Preside MDM in Succession Networks Fault Management (PT-AAL1/UA-AAL1).

Fault Correlation for MDM

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
Multi-Service Data manager (MDM)	log name and number	log name and number	log name and number	log name and number	NN10092-911 Passport 15000 and Preside MDM in Succession Networks Fault Management (PT-AAL1/UA-AAL1)

Northbound Fault Formats for MDM**SCC2**

The following is an example of a MDM log in SCC2 format:

```
*C22 MDM 303 7891 TBL
time: 2004 01 25 09 22 32
event: set
compId: EM PP14
severity: critical
faultcode: 09990001
alarmType: equipment
commentData: FMDR_SURV@rtipmdm has lost connection to EM PP14. Please in
vestigate.
```

NTSTD

The following is an example of a MDM log in NTSTD format:

```
RTPU07BU *** MDM303 Jan25 14:22:32 7345 TBL
time: 2004 01 25 09 22 32
event: set
compId: EM PP14
severity: critical
faultcode: 09990001
alarmType: equipment
commentData: FMDR_SURV@rtipmdm has lost connection to EM PP14. Please in
vestigate.
```

SNMP

The following is an example of a MDM log in SNMP format:

```
system.sysUpTime.0 => 3 days, 0:41:03
snmpTrapOID.0 => nnExtAlarmCritical
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.53.44.57.58.50.50.58.51.50.46.48.44.13270
alarmActiveDateAndTime => 2004-1-21,6:41:14.0,
alarmActiveDescription => DeviceSpecificInfo=equipmentFailure;FMDR_SURV@rtipmdm has
lost connection to EM PP14. Please investigate.

nnExtAlarmActiveEventType => 4
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => MDM 303
nnExtAlarmActiveResourceDescription => IEMS=47.142.116.75-MDM-Mgr_PP14;EM PP14
nnExtAlarmActiveManualClear => 1
nnExtAlarmActiveSequenceNumber => 17433
```

Syslog

The following is an example of a MDM log in Syslog format:

```
Feb 27 11:16:54 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=0402~~ MDM303 CRIT TBL ^M
time: 2004 01 27 11 15 32^M          event: set^M          compId: EM PP14^M          severity:
critical^M          faultcode: 09990001^M          alarmType: equipment^M          commentData:
FMDR_SURV@rtipmdm has lost connection to EM PP14. Please in^M          vestigate.
```

Performance

OM and PM Documentation references for MDM

- 241-6001-806 - Preside MDM MDP Data Formats Reference Guide

Northbound OM/PM Formats

Performance measurements for MDM are available only from the MDM directly. For more information on MDM, MSS 7000, and MSS 15000 OMs, see 241-6001-806 - Preside MDM MDP Data Formats Reference Guide

XML

The following is an example of Performance data for MDM in XML format:

***Note:** The IEMS northbound performance interface does not support this device.*

CSV

The following is an example of Performance data for MDM in CSV format:

***Note:** The IEMS northbound performance interface does not support this device.*

GUI/CLUI Documentation for MDM

GUI Launching and User procedures

The following documents provide specific details about the various user interfaces provided by the MDM.

- 241-6001-801 - Preside MDM Overview
- 241-6001-011 - Preside MDM Fault Management User Guide
- 241-6001-013 - Preside MDM Remote Network Communication System User Guide
- 241-6001-015 - Preside MDM Network Model Administrator Guide
- 241-6001-022 - Preside MDM Network Reporting System User Guide
- 241-6001-023 - Preside MDM Configuration Management for Passport User Guide
- 241-6001-030 - Preside MDMWeb User Guide
- 241-6001-031 - Preside MDM Performance Management User Guide
- 241-6001-040 - Preside MDM Security User Guide

Related documents

Numerous documents are available on MDM installation, configuration, and planning. All the documents in the **241-6001-xxx** series are related to the MDM and its operations.

- NN10028-111 - Passport 15000 and Preside MDM in Succession Networks Product and Technology Fundamentals (PT-AAL1/U)
- NN10070-461 - Passport 15000 and Preside MDM in Succession Networks Upgrade Guide (PT-AAL1/UA-AAL1)
- NN10092-911 - Passport 15000 and Preside MDM in Succession Networks Fault Management Overview (PT-AAL1/UA-AAL1)
- NN10114-511 - Passport 15000 and Preside MDM in Succession Networks Configuration Overview (PT-AAL1/UA-AAL1)
- NN10158-711 - Passport 15000 and Preside MDM in Succession Networks Performance (PT-AAL1/UA-AAL1)

- NN10180-611 - Passport 15000 and Preside MDM in Succession Networks Security and Administration (PT-AAL1/UA-AAL1)
- NN10185-461 - Preside MDM in Succession Networks Upgrade Guide (PT-AAL1/UA-AAL1)
- NN10198-912 - Passport 15000 and Preside MDM in Succession Networks Fault Management Troubleshooting (PT-AAL1/UA-A)
- NN10225-512 - Passport 15000 and Preside MDM in Succession Networks Configuration Attribute Summary (PT-AAL1/UA-AA

SAM21 Element Manager

This section contains IEMS Northbound log samples and device documentation references for the SAM21 EM.

SAM21 EM Fault Interface

Fault documentation for SAM21 EM :

The SAM 21 Manager reports faults for the SAM 21 Shelf Controller. Please refer to the SAM 21 SC documents below for details about SAM 21 faults.

- NN10089-911 - SAM21 Shelf Controller Fault Management

Fault Mapping for SAM21 EM

The following criteria can be used for looking up information on specific faults for SAM21 EM.

Fault Correlation for SAM21 EM

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
SAM21 Mgr	logname and number	logname and number	logname and number	logname and number	NN10089-911 SAM21 Shelf Controller Fault Management

Northbound Fault Formats for SAM21 EM

SCC2

The following is an example of a SAM21 EM log in SCC2 format:

```
**37 SCU 350 0009 FLT Alarm Raised
Location: SAM21 1:CSAM01-01:sled 3
Time:      Wed Jan 14 13:55:52 EST 2004
Reason:    Temperature in Sled 3 is high
```

NTSTD

The following is an example of a SAM21 EM log in NTSTD format:

```
COMPACT06BT ** SCU350 Jan15 00:37:17 0009 FLT Alarm Raised
Location: SAM21 1:CSAM01-01:sled 3
Time:      Wed Jan 14 13:55:52 EST 2004
Reason:    Temperature in Sled 3 is high
```

SNMP

The following is an example of a SAM21 EM log in SNMP format:

```
sysUpTime.0 => 9:14:20
snmpTrapOID.0 => nnExtAlarmMajor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.51.44.51.58.49.52.58.51.56.46.48.44.42847
alarmActiveDateAndTime => 2004-1-23,3:14:38.0,
alarmActiveDescription => DeviceSpecificInfo=;Location: SAM21 1:CSAM01-01:sled 3
Time:      Wed Jan 14 13:57:48 EST 2004
Reason:    Temperature in Sled 3 is high

nnExtAlarmActiveEventType => 5
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => SCU 350
nnExtAlarmActiveResourceDescription => IEMS=wnc0y0kz.us.nortel.com-SAM21-Mgr;
nnExtAlarmActiveManualClear => 2
nnExtAlarmActiveSequenceNumber => 1
```

Syslog

The following is an example of a SAM21 EM log in Syslog format:

```
Feb 12 18:30:19 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=7929~~ SCU350 MAJOR FLT
Alarm Raised^M Location: SAM21 1:CSAM01-01:sled 3^M Time: Mon Jan 12
12:49:06 EST 2004^M Reason: Temperature in Sled 3 is high
```

Performance

OM and PM Documentation references for SAM21 EM

SAM21 EM has no operational or performance measurements.

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of performance data for SAM21 EM in XML format:

Note: Northbound performance interface not supported for this component.

CSV

The following is an example of performance data for SAM21 EM in CSV format:

Note: Northbound performance interface not supported for this component.

GUI/CLUI Documentation for SAM21 EM

GUI Launching and User procedures

- NN10320-100 - ATM Solutions Basics
- NN10300-100 - IP Solutions Basics
- NN10281-600 - ATM/IP Administration and Security

Related documents

- NN10089-911 - SAM21 Shelf Controller Fault Management
- NN10325-900 - ATM/IP Fault Management
- NN10276-500 - ATM/IP Configuration Management

Applications

Audio Provisioning Server (APS)

This section contains IEMS Northbound log samples and device documentation references for the APS.

APS Fault Interface

Fault documentation for APS :

- NN10328-911 - MS 2000 Series Fault Management

Fault Mapping for APS

The following criteria can be used for looking up information on specific faults for APS.

Fault Correlation for APS

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
APS	SpecificProblem	SpecificProblem	SpecificProblem	SpecificProblem	NN10328-911 MS 2000 Series Fault Management

Northbound Fault Formats for APS

SCC2

The following is an example of a APS log in SCC2 format:

```
*C02 APS 398 2759 TBL APS Fault
Location: rtp2aps
Notification Id: 28673
State: Raise
Category: communications
Cause: softwareError
Time: Jan 27 07:02:30 2004
Component Id: APS;APSUnit=nc0rtp170;Software=Audio_Management_0
Specific Problem: 28673
Description: DB is not available, or the user cannot get a connection to
```

the DB

NTSTD

The following is an example of a APS log in NTSTD format:

```
RTPU07BR *** APS398 Jan27 12:02:30 2207 TBL APS Fault
Location: rtp2aps
Notification Id: 28673
State: Raise
Category: communications
Cause: softwareError
Time: Jan 27 07:02:30 2004
Component Id: APS;APSUnit=nc0rtp170;Software=Audio_Management_0
Specific Problem: 28673
Description: DB is not available, or the user cannot get a connection to
the DB
```

SNMP

The following is an example of a APS log in SNMP format:

```
sysUpTime.0 => 2 days, 18:44:37
snmpTrapOID.0 => nnExtAlarmCritical
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.18.50.48
.48.52.45.49.45.50.55.44.5
5.58.49.58.54.46.48.44.11202
alarmActiveDateAndTime => 2004-1-27,7:1:6.0
alarmActiveDescription => DeviceSpecificInfo=;DB is not available, or the user cannot
get a connection to
nnExtAlarmActiveEventType => 5
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => APS 398
nnExtAlarmActiveResourceDescription => IEMS=znc0s0j6-SSPFS-Unit-
0;APS;APSUnit=nc0rtp170;Software=Audio_Management_0
nnExtAlarmActiveManualClear => 4
nnExtAlarmActiveSequenceNumber => 13458
```

Syslog

The following is an example of a APS log in Syslog format:

```
Feb 27 07:02:24 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=6645~~ APS398 CRIT TBL APS
Fault^M      Location: rtp2aps^M      NotificationID: 28673^M      State: Raise^M
Category: Communications^M      Cause: Software error^M      Time: Jan 27 07:02:30
2004^M      Component Id: APS;APSUnit=nc0rtp170;Software=Audio_Management_0^M
Specific Problem: 28673^M      Description: DB is not available, or the user cannot
get a connection to^M      the DB^M
```

Performance

OM and PM Documentation references for APS

- NN10331-711 - MS 2000 Series Performance Monitoring

Northbound OM/PM Formats

XML

The following is an example of performance data for APS in XML format:

Note: Northbound performance interface not supported for this component.

CSV

The following is an example of performance data for APS in CSV format:

Note: Northbound performance interface not supported for this component.

GUI/CLUI Documentation for APS

GUI Launching and User procedures

- NN10340-511 - MS 2000 Series Configuration Management

Related documents

- NN10320-100 - ATM Solutions Basics
- NN10300-100 - IP Solutions Basics

Line Maintenance Manager (LMM)

This section contains IEMS Northbound log samples and device documentation references for LMM.

LMM Fault Interface

Fault documentation for LMM :

There are no faults or logs associated with this application.

Fault Mapping for LMM

There are no faults or logs associated with this application.

Performance

There are no OMs or PMs associated with this application.

GUI/CLUI Documentation for LMM

GUI Launching and User procedures

- NN10320-100 - ATM Solutions Basics
- NN10300-100 - IP Solutions Basics
- NN10321-111 - IEMS User Guide

Related documents

Network Patch Manager (NPM)

This section contains IEMS Northbound log samples and device documentation references for the Network Patch Manager (NPM).

NPM Fault Interface

Fault documentation for NPM :

- NN10325-900 - ATM/IP Fault Management

Fault Mapping for NPM

The following criteria can be used for looking up information on specific faults for NPM.

Fault Correlation for NPM

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
NPM	logname and number	logname and number	logname and number	logname and number	NN10325-900 ATM/IP Fault Management

Northbound Fault Formats for NPM

SCC2

The following is an example of an NPM log in SCC2 format:

```
38 NPM 360 6012 INFO Alarm Raised
Alarm ACT_NOT_APP has been raised.
Alarm Description: Activatable patches not applied.
```

NTSTD

The following is an example of an NPM log in NTSTD format:

```
RTPU07BU      NPM360 Jan27 15:38:44 5466 INFO Alarm Raised
Alarm ACT_NOT_APP has been raised.
Alarm Description: Activatable patches not applied.
```

SNMP

The following is an example of an NPM log in SNMP format:

```
system.sysUpTime.0 => 2 days, 22:22:15
snmpTrapOID.0 => nnExtAlarmMessage
nnExtAlarmMessageResource => .0.0
nnExtAlarmMessageResourceDescription => IEMS=znc0s0j6-SSPFS-Unit-0;
nnExtAlarmMessageDateAndTime => 2004-1-27,10:38:44.0
nnExtAlarmMessageDocumentationPointer => NPM 360
nnExtAlarmMessageInfo => 38 NPM 360 6012 INFO Alarm Raised           Alarm
ACT_NOT_APP has been raised.

Alarm Description: Activatable patches not applied.
```

Syslog

The following is an example of an NPM log in Syslog format:

```
Feb 27 10:40:03 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=0201~~ NPM360 NONE INFO
Alarm Raised^M           Alarm ACT_NOT_APP has been raised.^M           Alarm Description:
Activatable patches not applied.
```


Performance

OM and PM Documentation references for NPM

There are no OMs or PMs associated with this application.

GUI/CLUI Documentation for NPM

GUI Launching and User procedures

- NN10320-100 - ATM Solutions Basics
- NN10300-100 - IP Solutions Basics
- NN10276-500 - ATM/IP Configuration Management

Related documents

- NN10281-600 - ATM/IP Administration and Security
- NN10261-450 - Upgrading the Succession Network

OSSGate

This section contains IEMS Northbound log samples and device documentation references for the OSSGate.

OSSGate Fault Interface

Fault documentation for OSSGate :

There are no faults or logs associated with this application.

Fault Mapping for OSSGate

There are no faults or logs associated with this application.

Performance

OM and PM Documentation references for OSSGate

There are no OMs or PMs associated with this application.

Northbound OM/PM Formats

There are no OMs or PMs associated with this application.

GUI/CLUI Documentation for OSSGate

GUI Launching and User procedures

- NE10004-512 OSSGate User's Guide

Related documents

- 297-9051-8081 SERVORD Reference Manual Vol 1 of 2
- 297-9051-8082 SERVORD Reference Manual Vol 2 of 2

QoS Collector Application (QCA)

This section contains IEMS Northbound log samples and device documentation references for the QCA.

QCA Fault Interface

Fault documentation for QCA :

The QoS Collector reports faults as part of the CS2K Management Tools suite. The documents below contain information about QoS Collector faults.

- NN10083-911 - Communication Server 2000 Fault Management

Fault Mapping for QCA

The following criteria can be used for looking up information on specific faults for QCA.

Fault Correlation for QCA

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
QCA	logname and number	logname and number	logname and number	logname and number	NN10083-911 Communication Server 2000 Fault Management

Northbound Fault Formats for QCA

SCC2

The following is an example of a QCA log in SCC2 format:

```
*C34 QCA 310 0052 TBL wnc0y0kz
Location: wnc0y0kz
NotificationID : 49
State : Raise
Category : Processing Error
```

Cause : storageCapacityProblem
Time : Jan 22 16:34:19 2004
Component Id: /data/qca
Specific Problem: checkDiskSpace() has shown that there is less than
104857600 bytes available on the local disk.
Description : More Disk space is required immediately.

NTSTD

The following is an example of a QCA log in NTSTD format:

```
COMPACT06BT *** QCA 310 Jan22 21:34:19 0052 TBL wnc0y0kz
Location: wnc0y0kz
NotificationID : 49
State : Raise
Category : Processing Error
Cause : storageCapacityProblem
Time : Jan 22 16:34:19 2004
Component Id: /data/qca
Specific Problem: checkDiskSpace() has shown that there is less than
104857600 bytes available on the local disk.
Description : More Disk space is required immediately.
```

SNMP

The following is an example of a QCA log in SNMP format:

```
system.sysUpTime.0 => 0:28:36
snmpTrapOID.0 => nnExtAlarmCritical
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.50.44.52.58.51.52.58.50.48.46.48.44.37495
alarmActiveDateAndTime => 2004-1-22,4:34:20.0,
alarmActiveDescription => DeviceSpecificInfo=;Location: wnc0y0kz
NotificationID : 49
State : Raise
Category : Processing Error
Cause : storageCapacityProblem
Time : Jan 22 16:34:19 2004
Component Id: /data/qca
```

Specific Problem: checkDiskSpace() has shown that there is less than 104857600 bytes available on the local disk.

Description : More Disk space is required immediately.

```
nnExtAlarmActiveEventType => 5
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => QCA 310
nnExtAlarmActiveResourceDescription => IEMS=wnc0y0kz-QOS;/data/qca
nnExtAlarmActiveManualClear => 4
nnExtAlarmActiveSequenceNumber => 3
```

Syslog

The following is an example of a QCA log in Syslog format:

```
Feb 22 16:34:19 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=0062~~ QCA310 CRIT TBL
wnc0y0kz^M      Location: wnc0y0kz^M      NotificationID : 49^M      State :
Raise^M      Category : Processing Error^M      Cause : storageCapacityProblem^M
Time : Jan 22 16:26:49 2004^M      Component Id: /data/qca^M      Specific Problem:
checkDiskSpace() has shown that there is less than^M      104857600 bytes available
on the local disk.^M      Description : More Disk space is required immediately.^M
```

Performance

OM and PM Documentation references for QCA

- There are no OMs or PMs associated with QCA.

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of Performance data for QCA in XML format:

Note: Northbound performance interface not supported for this component.

CSV

The following is an example of Performance data for QCA in CSV format:

Note: Northbound performance interface not supported for this component.

GUI/CLUI Documentation for QCA

GUI Launching and User procedures

- NN10320-100 - ATM Solutions Basics
- NN10300-100 - IP Solutions Basics
- NN10281-600 - ATM/IP Administration and Security
- NN10325-900 - ATM/IP Fault Management
- NN10276-500 - ATM/IP Configuration Management

Related documents

Trunk Maintenance Manager (TMM)

This section contains IEMS Northbound log samples and device documentation references for TMM.

TMM Fault Interface

Fault documentation for TMM :

There are no faults or logs associated with this application.

Fault Mapping for TMM

There are no faults or logs associated with this application.

Performance

OM and PM Documentation references for TMM

There are no OM's or PM's associated with this application.

GUI/CLUI Documentation for TMM

GUI Launching and User procedures

- NN10320-100 - ATM Solutions Basics
- NN10300-100 - IP Solutions Basics
- NN10321-111 - IEMS User Guide

Related documents

Non-Topology Elements

This section contains references to applications that do not appear in the IEMS topology, but still report faults to the Northbound log streams.

Data Audit System

This section contains IEMS Northbound log samples and device documentation references for the Data Audit System.

Data Audit System Fault Interface

Fault documentation for Data Audit System :

- NN10325-900 - ATM/IP Fault Management

Fault Mapping for Data Audit System

The following criteria can be used for looking up information on specific faults for Data Audit System.

Fault Correlation for Data Audit System

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
Data Audit System	logname and number	logname and number	logname and number	logname and number	NN10325-900 ATM/IP Fault Management

Northbound Fault Formats for Data Audit System

SCC2

The following is an example of a Data Audit System log in SCC2 format:

```
*C43 CMT 300 5341 TBL CMT Fault
  Location: Audit
  NotificationID: 1001
  State: Raise
  Category: Processing Error
  Cause: Corrupt data
  Time: Jan 23 13:43:37 2004
  Component Id: SESM=AuditSystem;Audit=CS2K Data Integrity Audit
  Specific Problem: Data mismatches detected
  Description: The SESM audit: CS2K Data Integrity Audit, has 59 unresolved problems. To view and correct the problems, open the audit problem report from the Audit System found under the SESM Maintenance menu item.
```

NTSTD

The following is an example of a Data Audit System log in NTSTD format:

```
COMPACT06BT *** CMT300 Jan23 18:43:37 5341 TBL CMT Fault
Location: Audit
NotificationID: 1001
State: Raise
Category: Processing Error
Cause: Corrupt data
Time: Jan 23 13:43:37 2004
Component Id: SESM=AuditSystem;Audit=CS2K Data Integrity Audit
Specific Problem: Data mismatches detected
Description: The SESM audit: CS2K Data Integrity Audit, has 59 unresolv
d problems. To view and correct the problems, open the audit problem rep
ort from the Audit System found under the SESM Maintenance menu item.
```

SNMP

The following is an example of a Data Audit System log in SNMP format:

```
system.sysUpTime.0 => 21:39:13
snmpTrapOID.0 => nnExtAlarmCritical
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.51.44.49.58.52.51.58.51.55.46.48.44.42485
alarmActiveDateAndTime => 2004-1-23,1:43:37.0,
alarmActiveDescription => DeviceSpecificInfo=;Event from Unknown Syslog Device
nnExtAlarmActiveEventType => 5
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => CMT 300
nnExtAlarmActiveResourceDescription => IEMS=znc0s0j6;SESM=AuditSystem;Audit=CS2K Data
Integrity Audit
nnExtAlarmActiveManualClear => 0
nnExtAlarmActiveSequenceNumber => 8390
```

Syslog

The following is an example of a Data Audit System log in Syslog format:

```
Feb 23 13:44:54 wnc0s0pf IEMS: _V2_-I=~H=wnc0s0pf~A=IEMS~S=5398~~ CMT300 CRIT TBL CMT
Fault^M Location: Audit^M NotificationID: 1001^M State: Raise^M Category: Processing
Error^M Cause: Corrupt data^M Time: Jan 23 13:43:37 2004^M Component Id:
SESM=AuditSystem;Audit=CS2K Data Integrity Audit^M Specific Problem: Data mismatches
detected^M Description: The SESM audit: CS2K Data Integrity Audit, has 59 unresolve^M
d problems. To view and correct the problems, open the audit problem rep^M ort from
the Audit System found under the SESM Maintenance menu item.^M
```


Performance

OM and PM Documentation references for Data Audit System

There are no OMs or PMs associated with this application.

Northbound OM/PM Formats

There are no OMs or PMs associated with this application.

GUI/CLUI Documentation for Data Audit System

GUI Launching and User procedures

- NN10320-100 - ATM Solutions Basics
- NN10300-100 - IP Solutions Basics
- NN10276-500 - ATM/IP Configuration Management
- NN10325-900 - ATM/IP Fault Management

Related documents

IW-SPM IP

This section contains IEMS Northbound log samples and device documentation references for the IW-SPM IP.

IW-SPM IP Fault Interface

Fault documentation for IW-SPM IP :

- NN10078-911 - IW SPM IP Fault Management
- NN10275-909 - Succession Fault Management Logs Reference

Fault Mapping for IW-SPM IP

The following criteria can be used for looking up information on specific faults for IW-SPM IP.

Fault Correlation for IW-SPM IP

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
IW-SPM IP	Logname and number	Logname and number	Logname and number	Logname and number	NN10078-911 IW SPM IP Fault Management

Northbound Fault Formats for IW-SPM IP

SCC2

The following is an example of a IW-SPM IP log in SCC2 format:

```
**17 SPM 313 4488 TBL Fault
      SPM    0 CEM    0 : A                               Time: 12:16:13.890
      Source: None           State: Insv           Type: None
      Reason:      Loadname mismatch.
      Diagnostic: Autonomous fault detection
      Comp:MCM           RegAddr:0           Exp:0           Act:0
```

NTSTD

The following is an example of a IW-SPM IP log in NTSTD format:

```
RTPU07BU ** SPM313 Feb28 00:06:14 9091 TBL Fault
      SPM    0 CEM    1 : A                               Time: 19:05:14.820
      Source: None           State: Insv           Type: None
      Reason:      SYNC OOSpec: prim. ref. NA.
      Diagnostic: Autonomous fault detection
      Comp:TIC           RegAddr:0           Exp:0           Act:0
```

SNMP

The following is an example of a IW-SPM IP log in SNMP format:

```
system.sysUpTime.0 => 3 days, 6:54:40
snmpTrapOID.0 => nnExtAlarmMajor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.50.45.50.55.44.55.58.49.50.58.50.55.46.54.44.14023
alarmActiveDateAndTime => 2004-2-27,7:12:27.6
alarmActiveDescription => DeviceSpecificInfo=Unavailable;SPM 0 CEM 0 : A
Time: 19:11:31.010
Source: None           State: Insv           Type: None
Reason:      SYNC OOSpec: prim. ref. NA.
Diagnostic: Autonomous fault detection
Comp:TIC           RegAddr:0           Exp:0           Act:0
```

```

nnExtAlarmActiveEventType => 5
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => SPM 313
nnExtAlarmActiveResourceDescription => IEMS=wnc0y0m0.us.nortel.com-CS2K-Mgr;
nnExtAlarmActiveManualClear => 3
nnExtAlarmActiveSequenceNumber => 18489

```

Syslog

The following is an example of a IW-SPM IP log in Syslog format:

```

Feb 28 12:11:09 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=7983~~ SPM313 MAJOR TBL
Fault^M      SPM  0 CEM  1 : I      Time: 12:10:11.080^M      Source:
None      State: Insv      Type: None ^M      Reason:      No frame pulse from
DS-512 #0 ^M      Diagnostic: Autonomous fault detection ^M      Comp:TIC
RegAddr:0      Exp:0      Act:0

```

Performance

OM and PM Documentation references for IW-SPM IP

- NN10144-711 - IW SPM IP Performance Management

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of Performance data for IW-SPM IP in XML format:

***Note:** The IEMS northbound performance interface does not support this device.*

CSV

The following is an example of Performance data for IW-SPM IP in CSV format:

***Note:** The IEMS northbound performance interface does not support this device.*

GUI/CLUI Documentation for IW-SPM IP

GUI Launching and User procedures

- NN10015-111 - IW SPM IP Basics

Related documents

- NN10056-461 - Upgrading the IW SPM IP
- NN10100-511 - IW SPM IP Configuration Management
- NN10166-611 - IW SPM IP Administration and Security

MG9000 Manager Mid-Tier

This section contains IEMS Northbound log samples and device documentation references for the MG9000 Mgr Mid-Tier.

MG9000 Mgr Mid-Tier Fault Interface

Fault documentation for MG9000 Mgr Mid-Tier :

All MG9000 Mgr Mid-Tier faults are delivered via MG9000 Mgr. See document(s)

- NN10074-911 MG9000 Fault Management
- NN10325-900 ATM/IP Fault Management
- NN10275-909 Succession Fault Management Logs Reference

Fault Mapping for MG9000 Mgr Mid-Tier

The following criteria can be used for looking up information on specific faults for MG9000 Mgr Mid-Tier.

Fault Correlation for MG9000 Mgr Mid-Tier

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
MG9K Mid-Tier	log name and number	log name and number	log name and number	log name and number	NN10074-911 MG9000 Fault Management

Northbound Fault Formats for MG9000 Mgr Mid-Tier

SCC2

The following is an example of a MG9000 Mgr Mid-Tier log in SCC2 format:

```
52 MGEM703 0193 INFO Shutdown_Event
Status: Shutting MG 9K Midtier Server down ...
```

NTSTD

The following is an example of a MG9000 Mgr Mid-Tier log in NTSTD format:

```
RTPU07BT      MGEM703 Feb02 20:52:08 0197 INFO Shutdown_Event
Status: Shutting MG 9K Midtier Server down ...
```

SNMP

The following is an example of a MG9000 Mgr Mid-Tier log in SNMP format:

```
sysUpTime.0 => 1:30:14
snmpTrapOID.0 => nnExtAlarmMessage
nnExtAlarmMessageResource => .0.0
nnExtAlarmMessageResourceDescription => IEMS=wnc0y0nr.us.nortel.com-SSPFS-Unit-0;
nnExtAlarmMessageDateAndTime => 2004-2-2,3:52:8.0
nnExtAlarmMessageDocumentationPointer => MGEM703
nnExtAlarmMessageInfo => 52 MGEM703 0193 INFO Shutdown_Event      Status:
Shutting MG 9K Midtier Server down ...
```

Syslog

The following is an example of a MG9000 Mgr Mid-Tier log in Syslog format:

```
Mar  4 15:27:47 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=0682~~ MGEM703 NONE INFO
Shutdown_Event
Status: Shutting MG 9K Midtier Server down ...
```

Performance

OM and PM Documentation references for MG9000 Mgr Mid-Tier

There are no OMs or PMs associated with this component.

GUI/CLUI Documentation for MG9000 Mgr Mid-Tier

GUI Launching and User procedures

The MG9000 Mgr Mid-Tier is an application that runs on an SSPFS machine. See SSPFS platform for client launch details.

- NN10096-511 MG9000 Configuration Management

Related documents

- NN10221105 VoA OSS Guide
- NN10048-461 Upgrading the MG9000
- NN10276-500 ATM/IP Configuration Management
- NN10325-900 ATM/IP Fault Management
- NN10162-611 MG9000 Administration and Security

OM Collector

OM Collector Fault Interface

This section contains IEMS Northbound log samples and device documentation references for the OM Collector.

Fault documentation for OM Collector :

- NN10074-911 MG9000 Fault Management

Fault Mapping for OM Collector

- NN10074-911 MG9000 Fault Management

The following criteria can be used for looking up information on specific faults for OM Collector.

Fault Correlation for OM Collector

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
OM Collector	logname and number	logname and number	logname and number	logname and number	NN10074-911 MG9000 Fault Management

Northbound Fault Formats for OM Collector

SCC2

The following is an example of a OM Collector log in SCC2 format:

```
27 OMC 700 0470 INFO Startup_Event
Status: OMCLTR_Process: OMCollector Process was started with PSID 17585
```

NTSTD

The following is an example of a OM Collector log in NTSTD format:

```
RTPU07BR      OMC700 Jan28 21:27:53 9923 INFO Startup_Event
Status: OMCLTR_Process: OMCollector Process was started with PSID 17585
```

SNMP

The following is an example of a OM Collector log in SNMP format:

```
system.sysUpTime.0 => 4 days, 4:10:00
snmpTrapOID.0 => nnExtAlarmMessage
nnExtAlarmMessageResource => .0.0
nnExtAlarmMessageResourceDescription => IEMS=wnc0s0kq.us.nortel.com-SSPFS-Unit-0;
nnExtAlarmMessageDateAndTime => 2004-1-28,4:27:53.0
nnExtAlarmMessageDocumentationPointer => OMC 700
nnExtAlarmMessageInfo => 27 OMC 700 0470 INFO Startup_Event
Status: OMCLTR_Process: OMCollector Process was started with PSID 17585
```

Syslog

The following is an example of a OM Collector log in Syslog format:

```
Feb 28 16:27:48 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=4656~~ OMC700 NONE INFO
Startup_Event^M      Status: OMCLTR_Process: OMCollector Process was started with
PSID 17585
```

Performance

OM and PM Documentation references for OM Collector

There are no OMs or PMs associated with this application. For MG9000 performance information see:

- NN10140-711 MG9000 Performance Management

Northbound OM/PM Formats

There are no OMs or PMs associated with this application.

GUI/CLUI Documentation for OM Collector

GUI Launching and User procedures

- NN10140-711 MG9000 Performance Management
- NN10096-511 MG9000 Configuration Management

Related documents

- NN10276-500 ATM/IP Configuration Management

V5.2 Data Audit

This section contains IEMS Northbound log samples and device documentation references for the V5.2 Data Audit.

V5.2 Data Audit Fault Interface

Fault documentation for V5.2 Data Audit :

The V5.2 Data Integrity Audit Module of V5.2 Data Audit will raise CMT300 faults, and it will be covered in **DataAudit**'s Fault Management.

The Data Audit system will generate CMT300 logs when problems are found during any of its audits. The component ID of the log can be used to identify the specific audit that encountered a problem.

- NN10275-909 - Succession Fault Management Logs Reference
- NN10325-900 - ATM/IP Fault Management

Fault Mapping for V5.2 Data Audit

The following criteria can be used for looking up information on specific faults for V5.2 Data Audit.

Fault Correlation for V5.2 Data Audit

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
V5.2 Data Audit	log name and log number. Seen as component ID in generic CMT300 Audit log. example: componentid = SESM=AuditSystem;Audit=V5.2 Data Integrity Audit	log name and log number. Seen as component ID in generic CMT300 Audit log. example: componentid = SESM=AuditSystem;Audit=V5.2 Data Integrity Audit	log name and log number. Seen as component ID in generic CMT300 Audit log. example: componentid = SESM=AuditSystem;Audit=V5.2 Data Integrity Audit	log name and log number. Seen as component ID in generic CMT300 Audit log. example: componentid = SESM=AuditSystem;Audit=V5.2 Data Integrity Audit	NN10275-909 Succession Fault Management Logs Reference

Northbound Fault Formats for V5.2 Data Audit**SCC2**

The following is an example of a V5.2 Data Audit log in SCC2 format:

```
*C12 CMT 300 0002 TBL CMT Fault
Location: Audit
NotificationID: 1002
State: Raise
Category: Processing Error
Cause: Corrupt data
Time: Feb 14 23:12:48 2004
Component Id: SESM=AuditSystem;Audit=V5.2 Data Integrity Audit
Specific Problem: Data mismatches detected
Description: The SESM audit: V5.2 Data Integrity Audit, has 5 unresolved
problems. To view and correct the problems, open the audit problem report
from the Audit System found under the SESM Maintenance menu item.
```

NTSTD

The following is an example of a V5.2 Data Audit log in NTSTD format:

```
COMPACT06BT *** CMT300 Feb15 07:12:48 0002 TBL CMT Fault
```

Location: Audit
 NotificationID: 1002
 State: Raise
 Category: Processing Error
 Cause: Corrupt data
 Time: Feb 14 23:12:48 2004
 Component Id: SESM=AuditSystem;Audit=V5.2 Data Integrity Audit
 Specific Problem: Data mismatches detected
 Description: The SESM audit: V5.2 Data Integrity Audit, has 5 unresolved problems. To view and correct the problems, open the audit problem report from the Audit System found under the SESM Maintenance menu item.

SNMP

The following is an example of a V5.2 Data Audit log in SNMP format:

```

system.sysUpTime.0 => 3:05:01
snmpTrapOID.0 => nnExtAlarmCritical
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.49.44.54.58.52.49.58.49.52.46.48.44.8995
alarmActiveDateAndTime => 2004-1-21,6:41:14.0,
alarmActiveDescription => DeviceSpecificInfo=;Event from Unknown Syslog Device
nnExtAlarmActiveEventType => 5
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => CMT 300
nnExtAlarmActiveResourceDescription => IEMS=zsups228;SESM=AuditSystem;Audit=V5.2 Data
Integrity Audit
nnExtAlarmActiveManualClear => 2
nnExtAlarmActiveSequenceNumber => 1
  
```

Syslog

The following is an example of a V5.2 Data Audit log in Syslog format:

```

Feb 14 23:12:50 zsups228 IEMS: _V2_~I=~H=zsups228~A=IEMS~S=0008~~ CMT300 CRIT TBL CMT
Fault^M      Location: Audit^M      NotificationID: 1002^M      State: Raise^M
Category: Processing Error^M      Cause: Corrupt data^M      Time: Feb 14 23:12:48
2004^M      Component Id: SESM=AuditSystem;Audit=V5.2 Data Integrity Audit^M
Specific Problem: Data mismatches detected^M      Description: The SESM audit: V5.2
Data Integrity Audit, has 5 unresolved^M      problems. To view and correct the
  
```

problems, open the audit problem repository from the Audit System found under the SESM Maintenance menu item.

Performance

OM and PM Documentation references for V5.2 Data Audit

- There are no performance measurements for V5.2 Data Audit V5.2 Data Audit

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of Performance data for V5.2 Data Audit in XML format:

***Note:** Northbound performance interface not supported for this component.*

CSV

The following is an example of Performance data for V5.2 Data Audit in CSV format:

***Note:** Northbound performance interface not supported for this component.*

GUI/CLUI Documentation for V5.2 Data Audit

GUI Launching and User procedures

- NN10320-100 - ATM Solutions Basics
- NN10300-100 - IP Solutions Basics

Related documents

- NN10083-911 - CS2000 Fault Management
- NN10281-600 - ATM/IP Administration and Security
- NN10276-500 - ATM/IP Configuration Management
- NIS V208-1 - DMS-100 International Switching V5: CS2K Interface Specification to Support V5.2 Protocol

References

Fault Specifications

- [1] Syslog Protocol (RFC 3164): <http://www.ietf.org/rfc/rfc3164.txt>
- [2] Alarm MIB (draft): <http://www.ietf.org/html.charters/disman-charter.html>
- [3] Notification Log MIB (RFC 3014):
<http://www.ietf.org/rfc/rfc3014.txt?number=3014>

OAM&P Security

- [4] NN10281-600 - ATM/IP Administration and Security

Network Engineering

- [5] <SN07 SEB number> - IAC Engineering Guidelines
- [6] <SN07 SEB number> - IAW Engineering Guidelines
- [7] <SN07 SEB number> - UAIP Engineering Guidelines
- [8] <SN07 SEB number> - PT-IP Engineering Guidelines
- [9] <SN07 SEB number> - VoATM Engineering Guidelines
- [10] <SN07 SEB number> - TRIMODAL Engineering Guidelines

Industry Standards

PAM

- [11] Introduction to PAM: <http://docs.sun.com/db/doc/805-7229/6j6q8svdi?q=pam.conf&a=view>
- [12] PAM RFC from OpenGroup: <http://www.opengroup.org/tech/rfc/mirror-rfc/rfc86.0.txt>
- [13] pam.conf (Solaris 8): <http://docs.sun.com/db/doc/806-0633/6j9vn6q5t?q=pam.conf&a=view>

NSSwitch

- [14] Solaris Name Services: <http://docs.sun.com/db/doc/806-1387/6jam6926b?q=nsswitch&a=view>
- [15] nsswitch.conf (Solaris 8): <http://docs.sun.com/db/doc/806-0633/6j9vn6q5m?q=nsswitch&a=view>

Secure Shell (SSH)

- [16] Secure Shell (secsh) Internet Drafts: <http://www.ietf.org/html.charters/secsh-charter.html>
- [17] OpenSSH: <http://www.openssh.org>

SNMP V3/USM

- [18] An Architecture for Describing SNMP Management Frameworks (RFC3411): <http://www.ietf.org/rfc/rfc3411.txt?number=3411>
- [19] User-based Security Model (RFC3414): <http://www.ietf.org/rfc/rfc3414.txt?number=3414>
- [20] View-based Access Control Model (RFC3415): <http://www.ietf.org/rfc/rfc3415.txt?number=3415>

HTTPS

- [21] The SSL Protocol V3.0: <http://wp.netscape.com/eng/ssl3/ssl-toc.html>
- [22] Transport Layer Security (TLS) Extensions (RFC2246): <http://www.ietf.org/rfc/rfc3546.txt>
- [23] HTTP over TLS (RFC 2818): <http://www.ietf.org/rfc/rfc2818.txt>
- [24] OpenSSL: <http://www.openssl.org>

Appendix 1: Northbound OSS Configurations

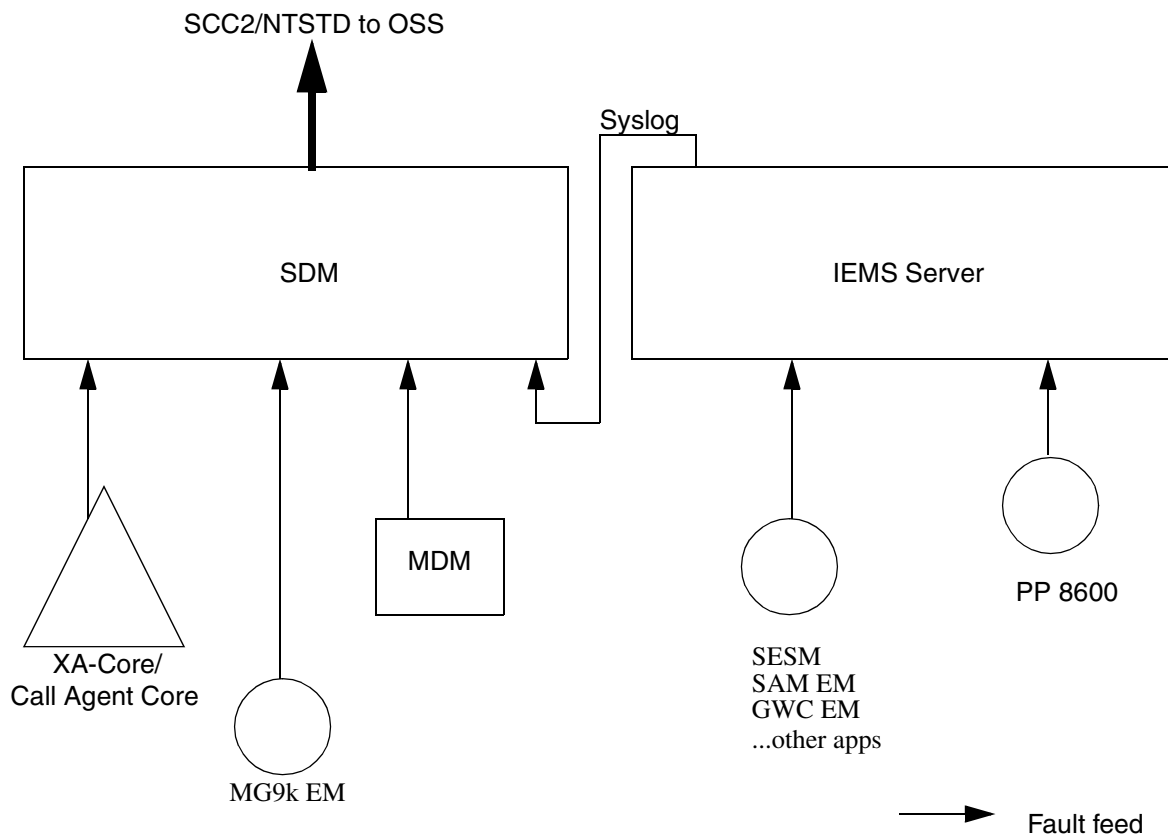
Depending on customer requirements, a single-source OSS interface can be provided from either the IEMS server or the SDM platform. In either scenario, one system is configured as the primary and the other a subordinate log source .

For existing Nortel Networks ATM customers, the SDM provides the external interface to third party OSSs. The IEMS is configured to forward all of its collected faults to the SDM through its Syslog interface. The SDM then aggregates all incoming faults and forwards them to the standard SCC2 and NTSTD interfaces used by customers. See figure .

Conversely, for Nortel Networks Carrier VoIP customers, IEMS provides the single Northbound interface using the SDM as a one of several subordinate fault collectors/forwarders in the network. See figure .

Using the SDM as a Northbound Fault Feed

As an OAM&P requirement, fault information must be available from the existing SDM northbound interfaces. In order to support that, the IEMS can be configured to send its northbound information to the SDM.

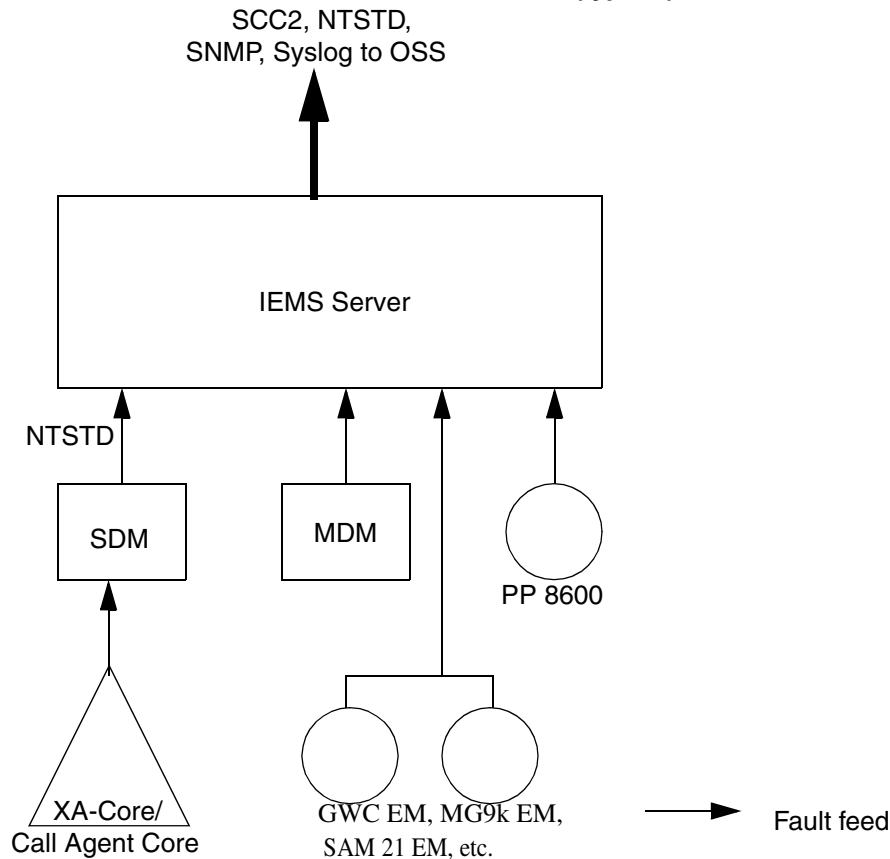
Fault flow with SDM as Northbound interface (ATM Market only)

Note: The IEMS northbound Syslog stream is sent on local7.notice. The SDM syslog.conf file will need to be configured to accept this stream.

The following figure shows the fault feeds that are used in the ATM market to provide a single source feed for all devices. In this case, the SDM serves as the Northbound fault interface.

The MDM and MG9000 Manager send their information to the SDM. This information is sent by the SDM northbound along with the CS2k core information (XA-Core as illustrated or Call Agent Core).

Additional data comes to the IEMS server from the CS2000 Manager applications and element managers (GWC-EM, NPM, SAM 21 EM, etc.). The IEMS then sends this data to the SDM via its Syslog facility. In this way, the IEMS acts as a mediator for devices that cannot directly send events to the SDM.

Fault flow with IEMS as Northbound interface (typical)

Note: The SDM SCC2 and NTSTD logroute streams must be configured for SCC2_old or NTstd_old in SN07. This is a change from SN06.2

This figure shows the fault flows in an office where the IEMS will be the northbound interface. In this configuration, all the devices that have been implemented in IEMS forward their fault information to IEMS. The SDM will only be responsible for forwarding core faults to the IEMS.

Note: The SDM logroute stream must be configured from tcpin.

Appendix 2: Nortel Alarm Extension MIB

-- Draft Version

NORTEL-ALARM-EXT-MIB

DEFINITIONS ::= BEGIN

IMPORTS

nortelGenericMIBs FROM NORTEL-GENERIC-MIB
alarmActiveEntry, alarmActiveResourceId, alarmActiveDescription,
ResourceId, alarmActiveDateAndTime

FROM ALARM-MIB

IANAItuEventType, IANAItuProbableCause

FROM IANA-ITU-ALARM-TC

AdminState, OperState, UsageState,

AlarmStatus, StandbyStatus FROM ENTITY-STATE-MIB

nlnLogName, nlnLogIndex FROM NOTIFICATION-LOG-MIB

NOTIFICATION-GROUP FROM SNMPv2-CONF

DateAndTime, DisplayString FROM SNMPv2-TC

SnmpAdminString FROM SNMP-FRAMEWORK-MIB

MODULE-IDENTITY, OBJECT-IDENTITY,

OBJECT-TYPE, NOTIFICATION-TYPE,

Unsigned32

FROM SNMPv2-SMI;

nnExtAlarmMIB MODULE-IDENTITY

LAST-UPDATED "200401270000Z"

ORGANIZATION "Nortel Networks"

CONTACT-INFO

" Nortel Networks
8200 Dixie Road
Brampton, Ontario L6T 5P6
Canada

1-800-4Nortel

www.nortelnetworks.com "

```
DESCRIPTION
    "This module contains objects that extend the IETF Alarm MIB, including
    notifications."

-- Revision history

REVISION "200401270000Z"
DESCRIPTION
    " Initial version"

::= { nortelGenericMIBs 6 }

nnExtAlarmObjects OBJECT IDENTIFIER ::= { nnExtAlarmMIB 1 }
nnExtAlarmConformance OBJECT IDENTIFIER ::= { nnExtAlarmMIB 2 }
nnExtAlarmCompliances OBJECT IDENTIFIER ::= { nnExtAlarmConformance 1 }
nnExtAlarmGroups OBJECT IDENTIFIER ::= { nnExtAlarmConformance 2 }

-- Textual Conventions

NnAvailabilityStatus ::= TEXTUAL-CONVENTION
    STATUS current
    DESCRIPTION
        "Represents the availability status"
    SYNTAX INTEGER {
        notSupported (1),
        inTest (2),
        failed (3),
        powerOff (4),
        offLine (5),
        offDuty (6),
        dependency (7),
        degraded (8),
        notInstalled (9),
        logFull (10)
    }

NnControlStatus ::= TEXTUAL-CONVENTION
    STATUS current
```

```
DESCRIPTION
    "Represents the control status"
SYNTAX INTEGER {
    notSupported (1),
    subjectToTest (2),
    partOfServiceLocked (3),
    reservedForTest (4),
    suspended (5)
}

NnProceduralStatus ::= TEXTUAL-CONVENTION
    STATUS          current
    DESCRIPTION
        "Represents the procedural status"
    SYNTAX INTEGER {
        notSupported (1),
        initializationRequired (2),
        notInitialized (3),
        initializing (4),
        reporting (5),
        terminating (6)
    }

NnUnknownStatus ::= TEXTUAL-CONVENTION
    STATUS          current
    DESCRIPTION
        "The unknown status attribute is used to indicate that
        the state of the resource represented by the managed object
        is unknown. When the unknown status attribute value is
        true, the value of the state attributes may not reflect
        the actual state of the resource."
    SYNTAX          INTEGER {
        false(1),
        true(2)
    }

-- Nortel Extended Active Alarm Table
```

nnExtAlarmActiveTable OBJECT-TYPE

SYNTAX SEQUENCE OF NnExtAlarmActiveEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"This table contains additional information about active alarms than what is found in the IETF Alarm MIB."

::= { nnExtAlarmObjects 1 }

nnExtAlarmActiveEntry OBJECT-TYPE

SYNTAX NnExtAlarmActiveEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"An active alarm entry"

AUGMENTS { alarmActiveEntry }

::= { nnExtAlarmActiveTable 1 }

NnExtAlarmActiveEntry ::= SEQUENCE {

nnExtAlarmActiveEventType IANAItuEventType,

nnExtAlarmActiveProbableCause IANAItuProbableCause,

nnExtAlarmActiveAdditionalText SnmpAdminString,

nnExtAlarmActiveDocumentationPointer SnmpAdminString,

nnExtAlarmActiveResourceDescription SnmpAdminString,

nnExtAlarmActiveManualClear INTEGER,

nnExtAlarmActiveSequenceNumber Integer32

}

nnExtAlarmActiveEventType OBJECT-TYPE

SYNTAX IANAItuEventType

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"Represents the per active alarm instance event type values."

REFERENCE

"ITU Recommendation M.3100, 'Generic Network Information Model', 1995

```
ITU Recommendation X.733, 'Information Technology - Open
Systems Interconnection - System Management: Alarm
Reporting Function', 1992
ITU Recommendation X.736, 'Information Technology - Open
Systems Interconnection - System Management: Security
Alarm Reporting Function', 1992"
::= { nnExtAlarmActiveEntry 1 }
```

nnExtAlarmActiveProbableCause OBJECT-TYPE

```
SYNTAX      IANAItuProbableCause
MAX-ACCESS  read-write
STATUS      current
```

DESCRIPTION

"Per active alarm instance ITU probable cause values."

REFERENCE

```
"ITU Recommendation M.3100, 'Generic Network Information
Model', 1995
ITU Recommendation X.733, 'Information Technology - Open
Systems Interconnection - System Management: Alarm
Reporting Function', 1992
ITU Recommendation X.736, 'Information Technology - Open
Systems Interconnection - System Management: Security
Alarm Reporting Function', 1992"
::= { nnExtAlarmActiveEntry 2 }
```

nnExtAlarmActiveAdditionalText OBJECT-TYPE

```
SYNTAX      SnmpAdminString
MAX-ACCESS  read-write
STATUS      current
```

DESCRIPTION

"Represents the per active alarm instance additional text field."

REFERENCE

```
"ITU Recommendation M.3100, 'Generic Network Information
Model', 1995
```

```
ITU Recommendation X.733, 'Information Technology - Open
Systems Interconnection - System Management: Alarm
Reporting Function', 1992"
::= { nnExtAlarmActiveEntry 3 }
```

nnExtAlarmActiveDocumentationPointer OBJECT-TYPE

SYNTAX SnmpAdminString

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This object services as a pointer to documentation related to this problem.

If there is no specific document pointer for this alarm, this object is a null length string."

```
::= { nnExtAlarmActiveEntry 4 }
```

nnExtAlarmActiveResourceDescription OBJECT-TYPE

SYNTAX SnmpAdminString

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a textual description of the resource under under alarm.

The format of the string is as follows:

```
NEtype=NEname;componentType=componentInstanceId;subcompType=subcompInstanceId;....
```

With NE as the root, the entire containment with the list of Relative Distinguished Names (RDNs) is presented upto the point where the alarming component is clearly identified. Semicolon is the delimiter between a 'category=value' pair. The string can only contain alphanumeric characters and underscores. No commas, spaces, slashes, hyphens, or dollar signs are allowed

"

```
::= { nnExtAlarmActiveEntry 5 }
```


nnExtAlarmActiveManualClear OBJECT-TYPE

```
SYNTAX      INTEGER {
    other (1),
    forbidden (2),
    required (3),
    optional (4)
}
```

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This object provides guidance to a mid-level manager on the handling of this alarm. A value of forbidden indicates that a mid-level manager MUST NOT allow this alarm to be manually cleared. A value of required indicates that this alarm has no corresponding clear so MUST always be manually cleared. A value of optional indicates that this alarm does have a corresponding clear, but that is MAY also be cleared manually. A value of other indicates that the manual clear status is either unknown or not one of the specified values."

::= { nnExtAlarmActiveEntry 6 }

nnExtAlarmActiveSequenceNumber OBJECT-TYPE

```
SYNTAX      Integer32
```

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The sequence number of this notification. This object MUST have a value of 0 for notifications without sequence numbers or solutions that don't support sequence numbers."

DEFVAL { 0 }

::= { nnExtAlarmActiveEntry 7 }

-- Nortel Extended Alarm State Information

nnExtAlarmStateTable OBJECT-TYPE

```
SYNTAX      SEQUENCE OF NnExtAlarmStateEntry
```

```
MAX-ACCESS    not-accessible
STATUS        current
DESCRIPTION
    "This table contains state information about active alarms than
    what is found in the IETF Alarm MIB."
 ::= { nnExtAlarmObjects 2 }
```

nnExtAlarmStateEntry OBJECT-TYPE

```
SYNTAX        NnExtAlarmStateEntry
MAX-ACCESS    not-accessible
STATUS        current
DESCRIPTION
    "An active alarm state entry"
AUGMENTS { alarmActiveEntry }
 ::= { nnExtAlarmStateTable 1 }
```

NnExtAlarmStateEntry ::= SEQUENCE {

```
    nnExtAlarmStateAdministrative    AdminState,
    nnExtAlarmStateOperational       OperState,
    nnExtAlarmStateUsage              UsageState,
    nnExtAlarmStateAlarm              AlarmStatus,
    nnExtAlarmStateAvailability       NnAvailabilityStatus,
    nnExtAlarmStateControl            NnControlStatus,
    nnExtAlarmStateProcedural         NnProceduralStatus,
    nnExtAlarmStateStandby            StandbyStatus,
    nnExtAlarmStateUnknown            NnUnknownStatus
}
```

nnExtAlarmStateAdministrative OBJECT-TYPE

```
SYNTAX        AdminState
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION
    " "
 ::= { nnExtAlarmStateEntry 1 }
```

nnExtAlarmStateOperational OBJECT-TYPE

```
SYNTAX        OperState
```

```
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION
    " "
 ::= { nnExtAlarmStateEntry 2 }
```

```
nnExtAlarmStateUsage OBJECT-TYPE
    SYNTAX      UsageState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        " "
    ::= { nnExtAlarmStateEntry 3 }
```

```
nnExtAlarmStateAlarm OBJECT-TYPE
    SYNTAX      AlarmStatus
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        " "
    ::= { nnExtAlarmStateEntry 4 }
```

```
nnExtAlarmStateAvailability OBJECT-TYPE
    SYNTAX      NnAvailabilityStatus
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        " "
    ::= { nnExtAlarmStateEntry 5 }
```

```
nnExtAlarmStateControl OBJECT-TYPE
    SYNTAX      NnControlStatus
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        " "
    ::= { nnExtAlarmStateEntry 6 }
```

nnExtAlarmStateProcedural OBJECT-TYPE

SYNTAX NnProceduralStatus

MAX-ACCESS read-only

STATUS current

DESCRIPTION

" "

::= { nnExtAlarmStateEntry 7 }

nnExtAlarmStateStandby OBJECT-TYPE

SYNTAX StandbyStatus

MAX-ACCESS read-only

STATUS current

DESCRIPTION

" "

::= { nnExtAlarmStateEntry 8 }

nnExtAlarmStateUnknown OBJECT-TYPE

SYNTAX NnUnknownStatus

MAX-ACCESS read-only

STATUS current

DESCRIPTION

" "

::= { nnExtAlarmStateEntry 9 }

-- Table of Information related to Messages

nnExtAlarmMessageTable OBJECT-TYPE

SYNTAX SEQUENCE OF NnExtAlarmMessageEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A table of information on messages. Entries are added to this table when their corresponding notifications have been sent. Entries will be removed from this table as outlined in the Notification Log MIB [RFC3014]. Implementations that do not support the Notification Log MIB should provide behaviour for nlmLogName, nlmLogIndex and

```
        this table as if they did."
 ::= { nnExtAlarmObjects 3 }
```

nnExtAlarmMessageEntry OBJECT-TYPE

```
SYNTAX      NnExtAlarmMessageEntry
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
    "An alarm message entry."
INDEX       { nlmLogName, nlmLogIndex }
 ::= { nnExtAlarmMessageTable 1 }
```

```
NnExtAlarmMessageEntry ::= SEQUENCE {
    nnExtAlarmMessageResource      ResourceId,
    nnExtAlarmMessageResourceDescription SnmpAdminString,
    nnExtAlarmMessageDateAndTime    DateAndTime,
    nnExtAlarmMessageDocumentationPointer SnmpAdminString,
    nnExtAlarmMessageInfo           SnmpAdminString
}
```

nnExtAlarmMessageResource OBJECT-TYPE

```
SYNTAX      ResourceId
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "This object identifies the resource that this message pertains to

    If there is no corresponding resource, then
    the value of this object MUST be 0.0."
 ::= { nnExtAlarmMessageEntry 1 }
```

nnExtAlarmMessageResourceDescription OBJECT-TYPE

```
SYNTAX      SnmpAdminString
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "This is a textual description of the resource this message
    pertains to."
```

The format of the string is as follows:

```
NType=NName;componentType=componentInstanceId;subcompType=subcompInstanceId;....
```

With NE as the root, the entire containment with the list of Relative Distinguished Names (RDNs) is presented upto the point where the messaging component is clearly identified. Semicolon is the delimiter between a 'category=value' pair. The string can only contain alphanumeric characters and underscores. No commas, spaces, slashes, hyphens, or dollar signs are allowed

```
"
 ::= { nnExtAlarmMessageEntry 2 }
```

nnExtAlarmMessageDateAndTime OBJECT-TYPE

SYNTAX DateAndTime

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"The local date and time when the message originated.

Implementations MUST include the offset from UTC, if available. Implementation in environments in which the UTC offset is not available is NOT RECOMMENDED."

```
::= { nnExtAlarmMessageEntry 3 }
```

nnExtAlarmMessageDocumentationPointer OBJECT-TYPE

SYNTAX SnmpAdminString

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This object services as a pointer to documentation related to this problem.

If there is no specific document pointer for this alarm, this object is a null length string."

```
 ::= { nnExtAlarmMessageEntry 4 }

nnExtAlarmMessageInfo OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "A textual discription of the event that has occurred,
        suitable to display to an operator. "
 ::= { nnExtAlarmMessageEntry 5 }

-- all notification OIDs would be prefixed with a zero OID to
-- facilitate snmp v1<->v2 conversion

nnExtNotificationPrefix OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION
        "This OID represents the prefix branch for all Nortel ITU
        Alarm Notifications.
        The last but one sub identifier in the OID of
        any Notification must have the value zero to facilitate
        v2<-->v1 conversion."
 ::= {nnExtAlarmObjects 0 }

-- Alarm Notifications

nnExtAlarmClear NOTIFICATION-TYPE
    OBJECTS { alarmActiveResourceId,
              alarmActiveDateAndTime,
              alarmActiveDescription,
              nnExtAlarmActiveEventType,
              nnExtAlarmActiveProbableCause,
              nnExtAlarmActiveAdditionalText,
              nnExtAlarmActiveDocumentationPointer,
              nnExtAlarmActiveResourceDescription,
              nnExtAlarmActiveSequenceNumber
            }
}
```

STATUS current

DESCRIPTION

"This notification indicates that one or more previously reported alarms have been cleared and the previously reported alarms are identified via the correlation id list field. The varbinds include alarm context via the ComponentId field and other additional useful information."

::= { nnExtNotificationPrefix 301 }

nnExtAlarmWarning NOTIFICATION-TYPE

```
OBJECTS { alarmActiveResourceId,
           alarmActiveDateAndTime,
           alarmActiveDescription,
           nnExtAlarmActiveEventType,
           nnExtAlarmActiveProbableCause,
           nnExtAlarmActiveAdditionalText,
           nnExtAlarmActiveDocumentationPointer,
           nnExtAlarmActiveResourceDescription,
           nnExtAlarmActiveManualClear,
           nnExtAlarmActiveSequenceNumber
        }
```

STATUS current

DESCRIPTION

"This notification indicates that an alarm of 'Warning' severity has been raised on a NE. The varbinds include alarm context via the ComponentId field and other additional useful information on the alarm condition."

::= { nnExtNotificationPrefix 302 }

nnExtAlarmMinor NOTIFICATION-TYPE

```
OBJECTS { alarmActiveResourceId,
           alarmActiveDateAndTime,
```



```
        alarmActiveDescription,
        nnExtAlarmActiveEventType,
        nnExtAlarmActiveProbableCause,
        nnExtAlarmActiveAdditionalText,
        nnExtAlarmActiveDocumentationPointer,
        nnExtAlarmActiveResourceDescription,
        nnExtAlarmActiveManualClear,
        nnExtAlarmActiveSequenceNumber
    }

STATUS    current
DESCRIPTION
    "This notification indicates that an alarm of 'Minor' severity
    has been raised on a NE.

    The varbinds include alarm context via the ComponentId field
    and other additional useful information on the alarm condition."

::= { nnExtNotificationPrefix 303 }

nnExtAlarmMajor NOTIFICATION-TYPE
    OBJECTS { alarmActiveResourceId,
        alarmActiveDateAndTime,
        alarmActiveDescription,
        nnExtAlarmActiveEventType,
        nnExtAlarmActiveProbableCause,
        nnExtAlarmActiveAdditionalText,
        nnExtAlarmActiveDocumentationPointer,
        nnExtAlarmActiveResourceDescription,
        nnExtAlarmActiveManualClear,
        nnExtAlarmActiveSequenceNumber
    }

STATUS    current
DESCRIPTION
    "This notification indicates that an alarm of 'Major' severity
    has been raised on a NE.

    The varbinds include alarm context via the ComponentId field
```

and other additional useful information on the alarm condition."

```
::= { nnExtNotificationPrefix 304 }
```

nnExtAlarmCritical NOTIFICATION-TYPE

```
    OBJECTS { alarmActiveResourceId,  
              alarmActiveDateAndTime,  
              alarmActiveDescription,  
              nnExtAlarmActiveEventType,  
              nnExtAlarmActiveProbableCause,  
nnExtAlarmActiveAdditionalText,  
              nnExtAlarmActiveDocumentationPointer,  
              nnExtAlarmActiveResourceDescription,  
              nnExtAlarmActiveManualClear,  
nnExtAlarmActiveSequenceNumber  
    }
```

STATUS current

DESCRIPTION

"This notification indicates that an alarm of 'Critical' severity has been raised on a NE.

The varbinds include alarm context via the ComponentId field and other additional useful information on the alarm condition."

```
::= { nnExtNotificationPrefix 305 }
```

nnExtAlarmMessage NOTIFICATION-TYPE

```
    OBJECTS {  
nnExtAlarmMessageResource,  
nnExtAlarmMessageResourceDescription,  
nnExtAlarmMessageDateAndTime,  
nnExtAlarmMessageDocumentationPointer,  
nnExtAlarmMessageInfo  
    }
```

STATUS current

DESCRIPTION

```
"An informational message. This notification does not
correspond to an alarm so would not be stored in the
active alarm table and it does not have a corresponing
clear."

::= { nnExtNotificationPrefix 306 }

-- Notification group definitions

nnExtAlarmNotificationsGroup NOTIFICATION-GROUP

    NOTIFICATIONS {
        nnExtAlarmClear,
        nnExtAlarmWarning,
        nnExtAlarmMinor,
        nnExtAlarmMajor,
        nnExtAlarmCritical
    }

    STATUS    current
    DESCRIPTION
        " Nortel alarm notification group."
    ::= { nnExtAlarmGroups 1}

nnExtAlarmGroup OBJECT-GROUP

    OBJECTS {
        nnExtAlarmActiveEventType,
        nnExtAlarmActiveProbableCause,
        nnExtAlarmActiveAdditionalText,
        nnExtAlarmActiveDocumentationPointer,
        nnExtAlarmActiveResourceDescription,
        nnExtAlarmActiveManualClear,
        nnExtAlarmActiveSequenceNumber
    }

    STATUS    current
    DESCRIPTION
        " Nortel alarm group."
    ::= { nnExtAlarmGroups 2}

nnExtAlarmStateGroup OBJECT-GROUP
```

```
OBJECTS {
    nnExtAlarmStateAdministrative,
nnExtAlarmStateOperational,
    nnExtAlarmStateUsage,
    nnExtAlarmStateAlarm,
    nnExtAlarmStateAvailability,
    nnExtAlarmStateControl,
    nnExtAlarmStateProcedural,
    nnExtAlarmStateStandby,
    nnExtAlarmStateUnknown
}

STATUS    current
DESCRIPTION
    " Nortel  alarm state group."
 ::= { nnExtAlarmGroups 3}

nnExtAlarmMessageGroup OBJECT-GROUP
OBJECTS {
    nnExtAlarmMessageResource,
    nnExtAlarmMessageInfo,
    nnExtAlarmMessageDocumentationPointer,
    nnExtAlarmMessageDateAndTime,
    nnExtAlarmMessage
}

STATUS    current
DESCRIPTION
    " Nortel  alarm message group."
 ::= { nnExtAlarmGroups 4}

-- Compliance
nnExtAlarmCompliance MODULE-COMPLIANCE
STATUS current
DESCRIPTION
    "The compliance statement for entities which implement
    the Nortel Alarm MIB."
MODULE    -- this module
MANDATORY-GROUPS {
    nnExtAlarmGroup
```

```
    }  
    ::= { nnExtAlarmCompliances 1}  
END
```


Appendix A: Passport 8600 Performance Metrics

<u>Performance Metric Identifier</u>	<u>MIB Name</u>	<u>Description</u>	<u>Default Succession IEMS Collection Interval</u>
RFC1213-MIB			
sysDescr	RFC1213-MIB	A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software. It is mandatory that this only contain printable ASCII characters.	Every 30 mins
sysObjectID	RFC1213-MIB	The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router'.	Every 30 mins
sysUpTime	RFC1213-MIB	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.	Every 30 mins
sysName	RFC1213-MIB	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name.	Every 30 mins
sysLocation	RFC1213-MIB	The physical location of this node (e.g., 'telephone closet, 3rd floor').	Every 30 mins
ifInOctets	RFC1213-MIB	The total number of octets received on the interface, including framing characters.	Every 5 and 30 mins
ifInDiscards	RFC1213-MIB	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.	Every 30 mins
ifInErrors	RFC1213-MIB	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.	Every 30 mins
ifOutOctets	RFC1213-MIB	The total number of octets transmitted out of the interface, including framing characters.	Every 5 and 30 mins
ifOutDiscards	RFC1213-MIB	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.	Every 30 mins
ifOutErrors	RFC1213-MIB	The number of outbound packets that could not be transmitted because of errors.	Every 30 mins
ipInReceives	RFC1213-MIB	The total number of input datagrams received from interfaces, including those received in error.	Every 5 and 30 mins
ipInDiscards	RFC1213-MIB	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.	Every 30 mins
ipOutRequests	RFC1213-MIB	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.	Every 5 and 30 mins
ipOutDiscards	RFC1213-MIB	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.	Every 30 mins
RFC1271-MIB			
etherStatsCRCAlignErrors	RFC1271-MIB	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but were not an integral number of octets in length or had a bad Frame Check Sequence (FCS).	Every 30 mins

<u>Performance Metric Identifier</u>	<u>MIB Name</u>	<u>Description</u>	<u>Default Succession</u>
			<u>IEMS Collection</u> <u>Interval</u>
etherStatsUndersizePkts	RFC1271-MIB	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.	Every 30 mins
etherStatsOversizePkts	RFC1271-MIB	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.	Every 30 mins
etherStatsFragments	RFC1271-MIB	The total number of packets received that were not an integral number of octets in length or that had a bad Frame Check Sequence (FCS), and were less than 64 octets in length (excluding framing bits but including FCS octets).	Every 30 mins
etherStatsJabbers	RFC1271-MIB	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and were not an integral number of octets in length or had a bad Frame Check Sequence (FCS).	Every 30 mins
etherStatsCollisions	RFC1271-MIB	The best estimate of the total number of collisions on this Ethernet segment.	Every 30 mins
etherHistoryCRCAlignErrors	RFC1271-MIB	The number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but were not an integral number of octets in length or had a bad Frame Check Sequence (FCS).	Every 30 mins
etherHistoryUndersizePkts	RFC1271-MIB	The number of packets received during this interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.	Every 30 mins
etherHistoryOversizePkts	RFC1271-MIB	The number of packets received during this interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.	Every 30 mins
etherHistoryFragments	RFC1271-MIB	The total number of packets received during this sampling interval that were not an integral number of octets in length or that had a bad Frame Check Sequence (FCS), and were less than 64 octets in length (excluding framing bits but including FCS octets).	Every 30 mins
etherHistoryJabbers	RFC1271-MIB	The number of packets received during this interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and were not an integral number of octets in length or had a bad Frame Check Sequence (FCS).	Every 30 mins
etherHistoryCollisions	RFC1271-MIB	The best estimate of the total number of collisions on this Ethernet segment during this interval.	Every 30 mins
OSPF-MIB			
ospfIfEvents	OSPF-MIB	The number of times this OSPF interface has changed its state, or an error has occurred.	Every 30 mins
OSPF-MIB			
ospfNbrIpAddr	OSPF-MIB	The IP address this neighbor is using in its IP Source Address. Note that, on addressless links, this will not be 0.0.0.0, but the address of another of the neighbor's interfaces.	Every 30 mins
ospfNbrEvents	OSPF-MIB	The number of times this neighbor relationship has changed state, or an error has occurred.	Every 30 mins
SNMP-FRAMEWORK-MIB			
snmplnInvalidMsgs	SNMP-FRAMEWORK-MIB	The total number of packets received by the SNMP engine which were dropped because there were invalid or inconsistent components in the SNMP message.	Every 30 mins
SNMP-FRAMEWORK-MIB			
snmplnPkts	SNMP-FRAMEWORK-MIB	The total number of Messages delivered to the SNMP entity from the transport service.	Every 30 mins
snmpOutPkts	SNMP-FRAMEWORK-MIB	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.	Every 30 mins
snmplnBadVersions	SNMP-FRAMEWORK-MIB	The total number of SNMP Messages which were delivered to the SNMP protocol entity and were for an unsupported SNMP version.	Every 30 mins
snmplnBadCommunityUses	SNMP-FRAMEWORK-MIB	The total number of SNMP Messages delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the Message.	Every 30 mins
snmplnASNParseErrs	SNMP-FRAMEWORK-MIB	The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding received SNMP Messages.	Every 30 mins

<u>Performance Metric Identifier</u>	<u>MIB Name</u>	<u>Description</u>	<u>Default Succession</u>
			<u>IEMS Collection</u> <u>Interval</u>
snmplnTotalReqVars	SNMP-FRAMEWORK-MIB	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.	Every 30 mins
snmplnTotalSetVars	SNMP-FRAMEWORK-MIB	The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.	Every 30 mins
snmpOutTraps	SNMP-FRAMEWORK-MIB	The total number of SNMP Trap PDUs which have been generated by the SNMP protocol entity.	Every 30 mins
VRRP-MIB			
vrrpStatsBecomeMaster	VRRP-MIB	The total number of times that this virtual router's state has transitioned from BACKUP to MASTER.	Every 30 mins
RAPID-CITY			
rcSysBufferUtil	RAPID-CITY	Buffer utilization as a percentage of the total amount of buffer space in the system. A high value indicates congestion.	Every 30 mins
rcSysBufferUtilPeak	RAPID-CITY	The largest buffer utilization since sysUpTime.	Every 30 mins
rcSysBufferUtilPeakTime	RAPID-CITY	Timestamp for rcSysPeakBandwidth.	Every 30 mins
rcSysNVRamUsed	RAPID-CITY	Non-volatile RAM in use in Kbytes.	Every 30 mins
rcSysCpuUtil	RAPID-CITY	Percentage of CPU utilization.	Every 30 mins
rcSysSwitchFabricUtil	RAPID-CITY	Percentage of Switching Fabric utilization.	Every 30 mins
rcStatFrameTooShorts	RAPID-CITY	The total number of frames that are too short that were encountered on this interface.	Every 30 mins
rcStatBridgeInDiscards	RAPID-CITY	The total number of frames that were discarded by the bridging entity.	Every 30 mins
rcStatRouteInDiscards	RAPID-CITY	The total number of frames that were discarded by the routing entity.	Every 30 mins
rcStatStgForwardTransitions	RAPID-CITY	The number of times this port has transitioned from the Learning state to the Forwarding state.	Every 30 mins
rcStatGigLinkFailures	RAPID-CITY	The total number of link failures encountered on this interface.	Every 30 mins
rcStatGigPacketErrors	RAPID-CITY	The total number of packet errors encountered on this interface.	Every 30 mins
rcStatGigCarrierErrors	RAPID-CITY	The total number of carrier errors encountered on this interface.	Every 30 mins
rcStatGigLinkInactiveErrors	RAPID-CITY	The total number of link inactive errors encountered on this interface.	Every 30 mins
rcStatSmltStDownCnt	RAPID-CITY	Counters that counts how the session between the two peering switches has done down since last boot.	Every 30 mins
rcStatSmltSmltDownTxMsgCnt	RAPID-CITY	Counters that counts the tx Smlt Down msg.	Every 30 mins
rcStatSmltSmltDownRxMsgCnt	RAPID-CITY	Counters that counts the rx Smlt Down msg.	Every 30 mins
rcStatSmltSmltUpTxMsgCnt	RAPID-CITY	Counters that counts the tx Smlt Up msg.	Every 30 mins
rcStatSmltSmltUpRxMsgCnt	RAPID-CITY	Counters that counts the rx Smlt Up msg.	Every 30 mins
rc2kAtmPortStatsInDroppedPkts	RAPID-CITY	Number of AAL5 CPCS PDUs dropped due to resource exhaustion.	Every 30 mins
rc2kAtmPortStatsOutDroppedPkts	RAPID-CITY	Number of AAL5 CPCS PDUs dropped because the transmitter closed the channel.	Every 30 mins
rc2kAtmVPortStatsInOctets	RAPID-CITY	AAL5 CPCS PDU octets received from ATM interface	Every 5 and 30 mins
rc2kAtmVPortStatsOutOctets	RAPID-CITY	AAL5 CPCS PDU octets transmitted out of ATM interface	Every 5 and 30 mins
rc2kAtmVPortStatsInErrors	RAPID-CITY	AAL5 CPCS PDUs received with errors from ATM interface. These errors include CRC-32 errors,SAR time-out errors and oversized SDU errors.	Every 30 mins
rc2kAtmVPortStatsOutErrors	RAPID-CITY	Number of AAL5 CPCS PDUs that couldn't be transmitted due to errors.	Every 30 mins
rc2kAtmVPortStatsInDiscards	RAPID-CITY	Number of received AAL5 CPCS PDUs discarded.	Every 30 mins
rc2kAtmVPortStatsOutDiscards	RAPID-CITY	Number of AAL5 CPCS PDUs which are to be transmitted but discarded.	Every 30 mins
rcStgPortForwardTransitions	RAPID-CITY	The number of times this port has transitioned from the Learning state to the Forwarding state.	Every 30 mins

OMs collected via CSV for OSS
Not supported at Performance Browser
New in SN07

Appendix B: MG 9000 MIB OMs/PMs

OM Name	Type	Duration	Description	EM PM Browser Section	Browser Tab	Browser Name	MIB Table Name	MIB Name	For OSS	Release	Test Procedures
NORTEL-UEMG-NODE-MIB norNodeAlarmsTable											
norNodeAlarmsCritical	Counter32	count goes up and down, does not rollover	Number of Critical Alarms currently on this Node	ITP, OC3, IMA, ITX, and DS1 Card	Card Alarm Statistics : Current data	Number of Critical alarms currently on this card	norNodeAlarmsTable	NORTEL-UEMG-NODE-MIB	No	SN04	Generate any Critical Alarm (See Fault test procedures) and see that the alarm counts match between the MG9K and the MG9K EM display for that MG9K
norNodeAlarmsMajor	Counter32	count goes up and down, does not rollover	Number of Major Alarms currently on this Node	ITP, OC3, IMA, ITX, and DS1 Card	Card Alarm Statistics : Current data	Number of Critical alarms currently on this card	norNodeAlarmsTable	NORTEL-UEMG-NODE-MIB	No	SN04	Generate any Major Alarm (See Fault test procedures) and see that the alarm counts match between the MG9K and the MG9K EM display for that MG9K
norNodeAlarmsMinor	Counter32	count goes up and down, does not rollover	Number of Minor Alarms currently on this Node	ITP, OC3, IMA, ITX, and DS1 Card	Card Alarm Statistics : Current data	Number of Critical alarms currently on this card	norNodeAlarmsTable	NORTEL-UEMG-NODE-MIB	No	SN04	Generate any Minor Alarm (See Fault test procedures) and see that the alarm counts match between the MG9K and the MG9K EM display for that MG9K
NORTEL-UEMG-CARRIER-MIB norCarrSonetMediumCurrentTable											
norCarrSonetMedCurrentOpt	Unsigned32	count goes up and down, does not rollover	Optical Power Transmitted. This is interpreted as a Percentage	OC3 Port	Sonet Medium Statistics : Current data	Optical Tx Power (%)	norCarrSonetMediumCurrentTable	NORTEL-UEMG-CARRIER-MIB	No	SN04	On the MG9K EM Performance Browser collect this particular OM. For an operational OC3 interface the value will be non-zero.
norCarrSonetMedCurrentLBC	Unsigned32	count goes up and down, does not rollover	Laser Bias Current.	OC3 Port	Sonet Medium Statistics : Current data	Laser Bias Current (%)	norCarrSonetMediumCurrentTable	NORTEL-UEMG-CARRIER-MIB	No	SN04	On the MG9K EM Performance Browser collect this particular OM. For an operational OC3 interface the value will be non-zero.
norCarrSonetMediumIntervalTable											
norCarrSonetMedCurrentOpt	Unsigned32	count goes up and down, does not rollover	Optical Power Transmitted. This is interpreted as a Percentage	OC3 Port	Sonet Medium Statistics : History data	Optical Tx Power (%)	norCarrSonetMediumIntervalTable	NORTEL-UEMG-CARRIER-MIB	Yes	SN04	On the MG9K EM Performance Browser collect all 96 intervals of this particular OM. For an operational OC3 interface the values will be non-zero.
norCarrSonetMedIntervalLBC	Unsigned32	count goes up and down, does not rollover	Laser Bias Current.	OC3 Port	Sonet Medium Statistics : History data	Laser Bias Current (%)	norCarrSonetMediumIntervalTable	NORTEL-UEMG-CARRIER-MIB	Yes	SN04	On the MG9K EM Performance Browser collect all 96 intervals of this particular OM. For an operational OC3 interface the values will be non-zero.
NORTEL-UEMG-MEGACO-MIB nnMegacoOMMedGwyIntervalTable											
nnMegacoOMMedGwyNumInMessages	Unsigned32	Counts only for last 15 min	Total number of messages received from the Gateway Controller (GWC) during this interval.	MG5K Virtual Media Gateway	VMG Statistics : History data	Total number of messages received on the link	nnMegacoOMMedGwyIntervalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	On the MG9K EM Performance Browser collect all 96 intervals of this particular OM under the following conditions: 1.) No traffic 2.) with traffic The counts for this OM will be higher during traffic. To ensure exact counts are collected a Packet Sniffer will have to be used to collect the actual number of messages. Also wait for a little longer than 15 min, collect the 96 OM entries, and ensure the counts have moved to the proper time interval.
nnMegacoOMMedGwyNumInOctets	Unsigned32	Counts only for last 15 min	Total number of octets received from the Gateway Controller (GWC) during this interval.	MG5K Virtual Media Gateway	VMG Statistics : History data	Total number of octets received on the link	nnMegacoOMMedGwyIntervalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMMedGwyAvgInMsgRate	Unsigned32	Counts only for last 15 min	Average message send rate (per minute) for messages sent to the GWC during this interval.	MG5K Virtual Media Gateway	VMG Statistics : History data	Average message rate for received messages	nnMegacoOMMedGwyIntervalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMMedGwyMaxInMsgRate	Unsigned32	Counts only for last 15 min	Maximum message send rate (per minute) for messages sent to the GWC during this interval.	MG5K Virtual Media Gateway	VMG Statistics : History data	Maximum received message rate per minute	nnMegacoOMMedGwyIntervalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMMedGwyNumOutMessages	Unsigned32	Counts only for last 15 min	Total number of messages sent to the Gateway Controller (GWC) during this interval.	MG5K Virtual Media Gateway	VMG Statistics : History data	Total number of messages sent on the link	nnMegacoOMMedGwyIntervalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMMedGwyNumOutOctets	Unsigned32	Counts only for last 15 min	Total number of octets sent to the Gateway Controller (GWC) during this interval.	MG5K Virtual Media Gateway	VMG Statistics : History data	Total number of octets sent on the link	nnMegacoOMMedGwyIntervalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMMedGwyAvgOutMsgRate	Unsigned32	Counts only for last 15 min	Average message send rate (per minute) for messages sent to the GWC during this interval.	MG5K Virtual Media Gateway	VMG Statistics : History data	Average message rate for sent messages	nnMegacoOMMedGwyIntervalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMMedGwyMaxOutMsgRate	Unsigned32	Counts only for last 15 min	Maximum message send rate (per minute) for messages sent to the GWC during this interval.	MG5K Virtual Media Gateway	VMG Statistics : History data	Maximum sent message rate per minute	nnMegacoOMMedGwyIntervalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMMedGwyCurrentDayTotalTable											
nnMegacoOMMedGwyNumInMessagesTotCurDay	Unsigned32	Rolling 24 hour total	Total number of messages received from the Gateway Controller (GWC) during this interval.	MG5K Virtual Media Gateway	VMG Day Total Statistics : Current data	Total number of messages received on the link	nnMegacoOMMedGwyCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	On the MG9K EM Performance Browser collect this particular OM under the following conditions: 1.) No traffic 2.) with traffic The counts for this OM will be higher during traffic. To ensure exact counts are collected a Packet Sniffer will have to be used to collect the actual number of messages. Also wait for a little longer than 15 min, collect the 96 OM entries, and ensure the counts have moved to the proper time interval.
nnMegacoOMMedGwyNumInOctetsTotCurDay	Unsigned32	Rolling 24 hour total	Total number of octets received from the Gateway Controller (GWC) during this interval.	MG5K Virtual Media Gateway	VMG Day Total Statistics : Current data	Total number of octets received on the link	nnMegacoOMMedGwyCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMMedGwyAvgInMsgRateTotCurDay	Unsigned32	Rolling 24 hour total	Average message send rate (per minute) for messages sent to the GWC during this interval.	MG5K Virtual Media Gateway	VMG Day Total Statistics : Current data	Average message rate for received messages	nnMegacoOMMedGwyCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMMedGwyMaxInMsgRateTotCurDay	Unsigned32	Rolling 24 hour total	Maximum message send rate (per minute) for messages sent to the GWC during this interval.	MG5K Virtual Media Gateway	VMG Day Total Statistics : Current data	Maximum received message rate per minute	nnMegacoOMMedGwyCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMMedGwyNumOutMessagesTotCurDay	Unsigned32	Rolling 24 hour total	Total number of messages sent to the Gateway Controller (GWC) during this interval.	MG5K Virtual Media Gateway	VMG Day Total Statistics : Current data	Total number of messages sent on the link	nnMegacoOMMedGwyCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMMedGwyNumOutOctetsTotCurDay	Unsigned32	Rolling 24 hour total	Total number of octets sent to the Gateway Controller (GWC) during this interval.	MG5K Virtual Media Gateway	VMG Day Total Statistics : Current data	Total number of octets sent on the link	nnMegacoOMMedGwyCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMMedGwyAvgOutMsgRateTotCurDay	Unsigned32	Rolling 24 hour total	Average message send rate (per minute) for messages sent to the GWC during this interval.	MG5K Virtual Media Gateway	VMG Day Total Statistics : Current data	Average message rate for sent messages	nnMegacoOMMedGwyCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMMedGwyMaxOutMsgRateTotCurDay	Unsigned32	Rolling 24 hour total	Maximum message send rate (per minute) for messages sent to the GWC during this interval.	MG5K Virtual Media Gateway	VMG Day Total Statistics : Current data	Maximum sent message rate per minute	nnMegacoOMMedGwyCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMCMRIntervalTable											
nnMegacoOMCMRmaxSimultCNDreq	Unsigned32	Counts only for last 15 min	The maximum simultaneous number of CND requests during this interval.	ITP Card	Class Modern Statistics : History data	Maximum simultaneous number of CND requests	nnMegacoOMCMRIntervalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Starting with no calls made display all 96 entries and ensure they are all zero. Then make a number of Caller ID calls (some at the same time) and then display this OM. The counts will show appropriate results matching the number of calls. Do this over a number of 15 min intervals, then display all 96 entries. Also ensure the counts have moved to the proper time interval after each 15 min interval.
nnMegacoOMCMRtotNumberCNDreq	Unsigned32	Counts only for last 15 min	The total number of CND requests during this interval.	ITP Card	Class Modern Statistics : History data	Total number of CND requests	nnMegacoOMCMRIntervalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMCMRnumCNDcompleted	Unsigned32	Counts only for last 15 min	The number of CND requests during this interval that completed.	ITP Card	Class Modern Statistics : History data	Number of CND requests that completed	nnMegacoOMCMRIntervalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMCMRmaxSimultADSIreq	Unsigned32	Counts only for last 15 min	The maximum simultaneous number of ADSI requests during this interval.	ITP Card	Class Modern Statistics : History data	Maximum simultaneous number of ADSI requests	nnMegacoOMCMRIntervalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Starting with no calls made display all 96 entries and ensure they are all zero. Then make a number of ADSI calls (some at the same time) and then display this OM. The counts will show appropriate results matching the number of calls. Do this over a number of 15 min intervals, then display all 96 entries.
nnMegacoOMCMRtotNumberADSIreq	Unsigned32	Counts only for last 15 min	The total number of ADSI requests during this interval.	ITP Card	Class Modern Statistics : History data	Total number of ADSI requests	nnMegacoOMCMRIntervalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMCMRnumADSIcompleted	Unsigned32	Counts only for last 15 min	The number of ADSI requests during this interval that completed.	ITP Card	Class Modern Statistics : History data	Number of ADSI requests that completed	nnMegacoOMCMRIntervalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMCMRmaxSimultBCLIDreq	Unsigned32	Counts only for last 15 min	The maximum simultaneous number of BCLID requests during this interval.	ITP Card	Class Modern Statistics : History data	Maximum simultaneous number of BCLID requests	nnMegacoOMCMRIntervalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Starting with no calls made display all 96 entries and ensure they are all zero. Then make a number of BCLID calls (some at the same time) and then display this OM. The counts will show appropriate results matching the number of calls. Do this over a number of 15 min intervals, then display all 96 entries. Also ensure the counts have moved to the proper time interval after each 15 min interval.
nnMegacoOMCMRtotNumberBCLIDreq	Unsigned32	Counts only for last 15 min	The total number of BCLID requests during this interval.	ITP Card	Class Modern Statistics : History data	Total number of BCLID requests	nnMegacoOMCMRIntervalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMCMRnumBCLIDcompleted	Unsigned32	Counts only for last 15 min	The number of BCLID requests during this interval that completed.	ITP Card	Class Modern Statistics : History data	Number of BCLID requests that completed	nnMegacoOMCMRIntervalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above

nnMegacoOMCMRmaxSimultSCWIDreq	Unsigned32	Counts only for last 15 min	The maximum simultaneous number of SCWID requests during this interval.	ITP Card	Class Modem Statistics : History data	Maximum simultaneous number of SCWID requests	nnMegacoOMCMRIntervalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Starting with no calls made display all 96 entries and ensure they are all zero. Then make a number of SCWID calls (some at the same time) and then display this OM. The counts will show appropriate results matching the number of calls. Do this over a number of 15 min intervals, then display all 96 entries. Also ensure the counts have moved to the proper time interval after each 15 interval.
nnMegacoOMCMRtoNumberSCWIDreq	Unsigned32	Counts only for last 15 min	The total number of SCWID requests during this interval.	ITP Card	Class Modem Statistics : History data	Total number of SCWID requests	nnMegacoOMCMRIntervalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Same as above
nnMegacoOMCMRnumSCWIDcompleted	Unsigned32	Counts only for last 15 min	The number of SCWID requests during this interval that completed.	ITP Card	Class Modem Statistics : History data	Number of SCWID requests that completed	nnMegacoOMCMRIntervalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Same as above
nnMegacoOMCMRCurrentDayTotalTable											
nnMegacoOMCMRmaxSimultCNDreqTotCurDay	Unsigned32	Rolling 24 hour total	The current day's highest maximum simultaneous number of CND requests.	ITP Card	Class Modem Day Total Statistics : Current data	Maximum simultaneous number of CND requests	nnMegacoOMCMRCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Starting with no calls made display the OM and ensure it is zero. Then make a number of Caller ID calls (some at the same time) and then display this OM. The count will show appropriate results matching the number of calls.
nnMegacoOMCMRtoNumberCNDreqTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total number of CND requests.	ITP Card	Class Modem Day Total Statistics : Current data	Total number of CND requests	nnMegacoOMCMRCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Same as above
nnMegacoOMCMRnumCNDcompletedTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total number of CND requests that completed.	ITP Card	Class Modem Day Total Statistics : Current data	Number of CND requests that completed	nnMegacoOMCMRCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Same as above
nnMegacoOMCMRmaxSimultADSIreqTotCurDay	Unsigned32	Rolling 24 hour total	The current day's highest maximum simultaneous number of ADSI requests.	ITP Card	Class Modem Day Total Statistics : Current data	Maximum simultaneous number of ADSI requests	nnMegacoOMCMRCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Starting with no calls made display the OM and ensure it is zero. Then make a number of ADSI calls (some at the same time) and then display this OM. The count will show appropriate results matching the number of calls.
nnMegacoOMCMRtoNumberADSIreqTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total number of ADSI requests.	ITP Card	Class Modem Day Total Statistics : Current data	Total number of ADSI requests	nnMegacoOMCMRCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Same as above
nnMegacoOMCMRnumADSIcompletedTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total number of ADSI requests that completed.	ITP Card	Class Modem Day Total Statistics : Current data	Number of ADSI requests that completed	nnMegacoOMCMRCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Same as above
nnMegacoOMCMRmaxSimultBCLIDreqTotCurDay	Unsigned32	Rolling 24 hour total	The current day's highest maximum simultaneous number of BCLID requests.	ITP Card	Class Modem Day Total Statistics : Current data	Maximum simultaneous number of BCLID requests	nnMegacoOMCMRCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Starting with no calls made display the OM and ensure it is zero. Then make a number of BCLID calls (some at the same time) and then display this OM. The count will show appropriate results matching the number of calls.
nnMegacoOMCMRtoNumberBCLIDreqTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total number of BCLID requests.	ITP Card	Class Modem Day Total Statistics : Current data	Total number of BCLID requests	nnMegacoOMCMRCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Same as above
nnMegacoOMCMRnumBCLIDcompletedTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total number of BCLID requests that completed.	ITP Card	Class Modem Day Total Statistics : Current data	Number of BCLID requests that completed	nnMegacoOMCMRCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Same as above
nnMegacoOMCMRmaxSimultSCWIDreqTotCurDay	Unsigned32	Rolling 24 hour total	The current day's highest maximum simultaneous number of SCWID requests.	ITP Card	Class Modem Day Total Statistics : Current data	Maximum simultaneous number of SCWID requests	nnMegacoOMCMRCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Starting with no calls made display the OM and ensure it is zero. Then make a number of SCWID calls (some at the same time) and then display this OM. The count will show appropriate results matching the number of calls.
nnMegacoOMCMRtoNumberSCWIDreqTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total number of SCWID requests.	ITP Card	Class Modem Day Total Statistics : Current data	Total number of SCWID requests	nnMegacoOMCMRCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Same as above
nnMegacoOMCMRnumSCWIDcompletedTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total number of SCWID requests that completed.	ITP Card	Class Modem Day Total Statistics : Current data	Number of SCWID requests that completed	nnMegacoOMCMRCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Same as above
nnMegacoOMDSPIntervalTable											
nnMegacoOMDSPmaxSimultToneRcvInUse	Unsigned32	Counts only for last 15 min	The maximum simultaneous number of tone receivers in use during this interval.	ITP Card	Digital Signal Statistics : History data	Maximum simultaneous number of tone receivers in use	nnMegacoOMDSPIntervalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	On the MG9K EM Performance Browser collect all 96 intervals of this particular OM under the following conditions. 1.) No traffic 2.) with traffic The counts for this OM will be higher during traffic. To ensure exact counts are collected keep track of the number of calls made. Also ensure the counts have moved to the proper time interval after each 15 interval.
nnMegacoOMDSPnumToneRcvReq	Unsigned32	Counts only for last 15 min	The number of tone receiver requests during this interval.	ITP Card	Digital Signal Statistics : History data	Number of tone receiver requests	nnMegacoOMDSPIntervalTable	NORTEL-UEMG-MEGACO-MB	Yes	SN04	Same as above
nnMegacoOMDSPnumToneRcvReqFail	Unsigned32	Counts only for last 15 min	The number of tone receiver requests that failed during this interval.	ITP Card	Digital Signal Statistics : History data	Number of tone receiver requests which failed	nnMegacoOMDSPIntervalTable	NORTEL-UEMG-MEGACO-MB	Yes	SN04	Same as above
nnMegacoOMDSPmaxSimultToneGenInUse	Unsigned32	Counts only for last 15 min	The maximum simultaneous number of tone generators in use during this interval.	ITP Card	Digital Signal Statistics : History data	Maximum simultaneous number of tone generators in use	nnMegacoOMDSPIntervalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Same as above
nnMegacoOMDSPnumToneGenReq	Unsigned32	Counts only for last 15 min	The number of tone generator requests during this interval.	ITP Card	Digital Signal Statistics : History data	Number of tone generator requests	nnMegacoOMDSPIntervalTable	NORTEL-UEMG-MEGACO-MB	Yes	SN04	Same as above
nnMegacoOMDSPnumToneGenReqFail	Unsigned32	Counts only for last 15 min	The number of tone generator requests that failed during this interval.	ITP Card	Digital Signal Statistics : History data	Number of tone generator requests which failed	nnMegacoOMDSPIntervalTable	NORTEL-UEMG-MEGACO-MB	Yes	SN04	Same as above
nnMegacoOMDSPmaxSimultCMRmodemInUse	Unsigned32	Counts only for last 15 min	The maximum simultaneous number of CMR modems in use during this interval.	ITP Card	Digital Signal Statistics : History data	Maximum simultaneous number of CMR modems in use	nnMegacoOMDSPIntervalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Starting with no calls made display all 96 entries and ensure they are all zero. Then make a number of Caller ID calls (some at the same time) and then display this OM. The counts will show appropriate results matching the number of calls. Do this over a number of 15 min intervals, then display all 96 entries. Also ensure the counts have moved to the proper time interval after each 15 interval.
nnMegacoOMDSPnumCMRmodemReq	Unsigned32	Counts only for last 15 min	The number of CMR modem requests during this interval.	ITP Card	Digital Signal Statistics : History data	Number of CMR modem requests	nnMegacoOMDSPIntervalTable	NORTEL-UEMG-MEGACO-MB	Yes	SN04	Same as above
nnMegacoOMDSPnumCMRmodemReqFail	Unsigned32	Counts only for last 15 min	The number of CMR modem requests that failed during this interval.	ITP Card	Digital Signal Statistics : History data	Number of CMR modem requests which failed	nnMegacoOMDSPIntervalTable	NORTEL-UEMG-MEGACO-MB	Yes	SN04	Same as above
nnMegacoOMDSPCurrentDayTotalTable											
nnMegacoOMDSPmaxSimultToneRcvInUseTotCurDay	Unsigned32	Rolling 24 hour total	The current day's highest maximum simultaneous number of tone receivers in use.	ITP Card	Digital Signal Day Total Statistics : Current data	Maximum simultaneous number of tone receivers in use	nnMegacoOMDSPCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	On the MG9K EM Performance Browser collect this particular OM under the following conditions. 1.) No traffic 2.) with traffic The count for this OM will be higher during traffic. To ensure exact count is collected keep track of the number of calls made.
nnMegacoOMDSPnumToneRcvReqTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total of the number of tone receiver requests.	ITP Card	Digital Signal Day Total Statistics : Current data	Number of tone receiver requests	nnMegacoOMDSPCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Same as above
nnMegacoOMDSPnumToneRcvReqFailTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total of the number tone receiver requests that failed.	ITP Card	Digital Signal Day Total Statistics : Current data	Number of tone receiver requests which failed	nnMegacoOMDSPCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Same as above
nnMegacoOMDSPmaxSimultToneGenInUseTotCurDay	Unsigned32	Rolling 24 hour total	The current day's highest maximum simultaneous number of tone generators in use.	ITP Card	Digital Signal Day Total Statistics : Current data	Maximum simultaneous number of tone generators in use	nnMegacoOMDSPCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Same as above
nnMegacoOMDSPnumToneGenReqTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total of the number of tone generator requests.	ITP Card	Digital Signal Day Total Statistics : Current data	Number of tone generator requests	nnMegacoOMDSPCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Same as above
nnMegacoOMDSPnumToneGenReqFailTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total of the number tone generator requests that failed.	ITP Card	Digital Signal Day Total Statistics : Current data	Number of tone generator requests which failed	nnMegacoOMDSPCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Same as above
nnMegacoOMDSPmaxSimultCMRmodemInUseTotCurDay	Unsigned32	Rolling 24 hour total	The current day's highest maximum simultaneous number of CMR modems in use.	ITP Card	Digital Signal Day Total Statistics : Current data	Maximum simultaneous number of CMR modems in use	nnMegacoOMDSPCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Starting with no calls made display the OM and ensure it is zero. Then make a number of Caller ID calls (some at the same time) and then display this OM. The counts will show appropriate results matching the number of calls.
nnMegacoOMDSPnumCMRmodemReqTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total of the number of CMR modem requests.	ITP Card	Digital Signal Day Total Statistics : Current data	Number of CMR modem requests	nnMegacoOMDSPCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Same as above
nnMegacoOMDSPnumCMRmodemReqFailTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total of the number CMR modem requests that failed.	ITP Card	Digital Signal Day Total Statistics : Current data	Number of CMR modem requests which failed	nnMegacoOMDSPCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	Same as above
nnMegacoOMCESIntervalTable											
nnMegacoOMCESmaxSimultIntraSwitch	Unsigned32	Counts only for last 15 min	The maximum simultaneous number of channels in use for intra-switched calls during this interval.	ITP, OC3, MA & ABI Card	Circuit Emulation Statistics : History data	Intra maximum simultaneous number of channels in use	nnMegacoOMCESIntervalTable	NORTEL-UEMG-MEGACO-MB	No	SN04	On the MG9K EM Performance Browser collect all 96 intervals of this particular OM under the following conditions. 1.) No traffic 2.) with traffic from/to lines within the same SMA or LGCL. The counts for this OM will be higher during traffic. To ensure exact counts are collected keep track of the number of calls made. Also ensure the counts have moved to the proper time interval after each 15 interval.

nnMegacoOMCESnumChnlAllocIntra	Unsigned32	Counts only for last 15 min	The total number of channel allocation requests for intra-switched calls during this interval.	ITP, OC3, IMA & ABI Card	Circuit Emulation Statistics : History data	Intra total number of channel allocation requests	nnMegacoOMCESIntervalTable	NORTEL-UEMG-MEGACO-MIB	Yes	SN04	Same as above
nnMegacoOMCESnumChnlAllocIntraFail	Unsigned32	Counts only for last 15 min	The total number of channel allocation requests for intra-switched calls that failed during this interval.	ITP, OC3, IMA & ABI Card	Circuit Emulation Statistics : History data	Intra total number of failed channel allocation requests	nnMegacoOMCESIntervalTable	NORTEL-UEMG-MEGACO-MIB	Yes	SN04	Same as above
nnMegacoOMCESmaxSimultInterSwitch	Unsigned32	Counts only for last 15 min	The maximum simultaneous number of channels in use for inter-switched calls during this interval.	ITP, OC3, IMA & ABI Card	Circuit Emulation Statistics : History data	Inter maximum simultaneous number of channels in use	nnMegacoOMCESIntervalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	On the MG9K EM Performance Browser collect all 96 intervals of this particular OM under the following conditions: 1.) No traffic 2.) with traffic from lines within a SMA or LGCI to lines not on that SAM or LGCI. The counts for this OM will be higher during traffic. To ensure exact counts are collected keep track of the number of calls made. Also ensure the counts have moved to the proper time interval after each 15 interval.
nnMegacoOMCESnumChnlAllocInter	Unsigned32	Counts only for last 15 min	The total number of channel allocation requests for inter-switched calls during this interval.	ITP, OC3, IMA & ABI Card	Circuit Emulation Statistics : History data	Inter total number of channel allocation requests	nnMegacoOMCESIntervalTable	NORTEL-UEMG-MEGACO-MIB	Yes	SN04	Same as above
nnMegacoOMCESnumChnlAllocInterFail	Unsigned32	Counts only for last 15 min	The total number of channel allocation requests for inter-switched calls that failed during this interval.	ITP, OC3, IMA & ABI Card	Circuit Emulation Statistics : History data	Inter total number of failed channel allocation requests	nnMegacoOMCESIntervalTable	NORTEL-UEMG-MEGACO-MIB	Yes	SN04	Same as above
nnMegacoOMCESCurrentDayTotalTable											
nnMegacoOMCESmaxSimultIntraSwitchTotCurDay	Unsigned32	Rolling 24 hour total	The current day's highest maximum simultaneous number of channels in use for intra-switched calls.	ITP, OC3, IMA & ABI Card	Circuit Emulation Day Total Statistics : Current data	Intra maximum simultaneous number of channels in use	nnMegacoOMCESCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	On the MG9K EM Performance Browser collect this particular OM under the following conditions: 1.) No traffic 2.) with traffic from lines within the same SMA or LGCI. The count for this OM will be higher during traffic. To ensure exact count is collected keep track of the number of calls made.
nnMegacoOMCESnumChnlAllocIntraTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total number of channel allocation requests for intra-switched calls.	ITP, OC3, IMA & ABI Card	Circuit Emulation Day Total Statistics : Current data	Intra total number of channel allocation requests	nnMegacoOMCESCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMCESnumChnlAllocIntraFailTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total number of channel allocation requests for intra-switched calls that failed.	ITP, OC3, IMA & ABI Card	Circuit Emulation Day Total Statistics : Current data	Intra total number of failed channel allocation requests	nnMegacoOMCESCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMCESmaxSimultInterSwitchTotCurDay	Unsigned32	Rolling 24 hour total	The current day's highest maximum simultaneous number of channels in use for inter-switched calls.	ITP, OC3, IMA & ABI Card	Circuit Emulation Day Total Statistics : Current data	Inter maximum simultaneous number of channels in use	nnMegacoOMCESCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	On the MG9K EM Performance Browser collect this particular OM under the following conditions: 1.) No traffic 2.) with traffic from lines within a SMA or LGCI to lines not on that SAM or LGCI. The count for this OM will be higher during traffic. To ensure exact count is collected keep track of the number of calls made.
nnMegacoOMCESnumChnlAllocInterTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total number of channel allocation requests for inter-switched calls.	ITP, OC3, IMA & ABI Card	Circuit Emulation Day Total Statistics : Current data	Inter total number of channel allocation requests	nnMegacoOMCESCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMCESnumChnlAllocInterFailTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total number of channel allocation requests for inter-switched calls that failed.	ITP, OC3, IMA & ABI Card	Circuit Emulation Day Total Statistics : Current data	Inter total number of failed channel allocation requests	nnMegacoOMCESCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMECANIntervalTable											
nnMegacoOMECANmaxSimultResrcInUse	Unsigned32	Counts only for last 15 min	The maximum simultaneous number of ECAN resources in use during this interval.	ITP Card	Echo Cancellation Statistics : History data	Maximum simultaneous number of ECAN resources in use	nnMegacoOMECANIntervalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	On the MG9K EM Performance Browser collect all 96 intervals of this particular OM under the following conditions: 1.) No traffic 2.) with traffic from lines within a SMA or LGCI to lines not on that SAM or LGCI. The count for this OM will be higher during traffic. To ensure exact counts are collected keep track of the exact number of calls made. There will be a count for each end of a call. Also ensure the counts have moved to the proper time interval after each 15 interval.
nnMegacoOMECANnumResrcReq	Unsigned32	Counts only for last 15 min	The total number of ECAN resource request attempts during this interval.	ITP Card	Echo Cancellation Statistics : History data	Total number of ECAN resource request attempts	nnMegacoOMECANIntervalTable	NORTEL-UEMG-MEGACO-MIB	Yes	SN04	Same as above
nnMegacoOMECANnumResrcReqFail	Unsigned32	Counts only for last 15 min	The total number of ECAN resource request attempts that failed during this interval.	ITP Card	Echo Cancellation Statistics : History data	Total number of ECAN resource request attempts that failed	nnMegacoOMECANIntervalTable	NORTEL-UEMG-MEGACO-MIB	Yes	SN04	Same as above
nnMegacoOMECANCurrentDayTotalTable											
nnMegacoOMECANmaxSimultResrcInUseCurDay	Unsigned32	Rolling 24 hour total	The current day's maximum simultaneous number of ECAN resources in use.	ITP Card	Echo Cancellation Day Total Statistics : Current data	Maximum simultaneous number of ECAN resources in use	nnMegacoOMECANCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	On the MG9K EM Performance Browser collect this particular OM under the following conditions: 1.) No traffic 2.) with traffic from lines within a SMA or LGCI to lines not on that SAM or LGCI. The count for this OM will be higher during traffic. To ensure exact count is collected keep track of the exact number of calls made. There will be a count for each end of a call.
nnMegacoOMECANnumResrcReqCurDay	Unsigned32	Rolling 24 hour total	The current day's total number of ECAN resource requests.	ITP Card	Echo Cancellation Day Total Statistics : Current data	Total number of ECAN resource request attempts	nnMegacoOMECANCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoOMECANnumResrcReqFailCurDay	Unsigned32	Rolling 24 hour total	The current day's total number of ECAN resource requests that failed.	ITP Card	Echo Cancellation Day Total Statistics : Current data	Total number of ECAN resource request attempts that failed	nnMegacoOMECANCurrentDayTotalTable	NORTEL-UEMG-MEGACO-MIB	No	SN04	Same as above
nnMegacoQoSIntervalTable											
nnMegacoQoSIntervalCalls	Unsigned32	Counts only for this 15 min	total number of calls (in this 15-min interval).*	VMG	VMG QoS Interval Statistics : Current Interval QoS data	Number of Calls	nnMegacoQoSIntervalTable	NORTEL-UEMG-MEGACO-MIB	Yes	SN06	
nnMegacoQoSIntervalBadCalls	Unsigned32	Counts only for this 15 min	total number of bad calls (in this 15-min interval).*	VMG	VMG QoS Interval Statistics : Current Interval QoS data	Number of bad calls	nnMegacoQoSIntervalTable	NORTEL-UEMG-MEGACO-MIB	Yes	SN06	
nnMegacoQoSIntervalPktsSent	Unsigned32	Counts only for this 15 min	number of packets sent (in this 15-min interval).*	VMG	VMG QoS Interval Statistics : Current Interval QoS data	Number of packets sent	nnMegacoQoSIntervalTable	NORTEL-UEMG-MEGACO-MIB	Yes	SN06	
nnMegacoQoSIntervalPktsLost	Unsigned32	Counts only for this 15 min	number of packets lost (in this 15-min interval).*	VMG	VMG QoS Interval Statistics : Current Interval QoS data	Number of packets lost	nnMegacoQoSIntervalTable	NORTEL-UEMG-MEGACO-MIB	Yes	SN06	
nnMegacoQoSIntervalPktLossPct	Integer	Counts only for this 15 min	% of packets lost (in this 15-min interval).*	VMG	VMG QoS Interval Statistics : Current Interval QoS data	Percentage of packets lost	nnMegacoQoSIntervalTable	NORTEL-UEMG-MEGACO-MIB	Yes	SN06	
nnMegacoQoSIntervalJitter	Unsigned32	Counts only for this 15 min	average jitter (in a 15-min interval).*	VMG	VMG QoS Interval Statistics : Current Interval QoS data	Average jitter	nnMegacoQoSIntervalTable	NORTEL-UEMG-MEGACO-MIB	Yes	SN06	
nnMegacoQoSIntervalLatency	Unsigned32	Counts only for this 15 min	average latency (in a 15-min interval).*	VMG	VMG QoS Interval Statistics : Current Interval QoS data	Average Latency	nnMegacoQoSIntervalTable	NORTEL-UEMG-MEGACO-MIB	Yes	SN06	
nnMegacoQoSCurrDayTable											
nnMegacoQoSCurrDayCalls	Unsigned32	Rolling 24 hour total	total number of calls (in current day).*	VMG	VMG Total Day QoS data : Current Day Total QoS data	Number of Calls	nnMegacoQoSCurrDayTable	NORTEL-UEMG-MEGACO-MIB	No	SN06	
nnMegacoQoSCurrDayBadCalls	Unsigned32	Rolling 24 hour total	total number of bad calls (in current day).*	VMG	VMG Total Day QoS data : Current Day Total QoS data	Number of bad calls	nnMegacoQoSCurrDayTable	NORTEL-UEMG-MEGACO-MIB	No	SN06	
nnMegacoQoSCurrDayPktsSent	Unsigned32	Rolling 24 hour total	number of packets sent (in current day).*	VMG	VMG Total Day QoS data : Current Day Total QoS data	Number of packets sent	nnMegacoQoSCurrDayTable	NORTEL-UEMG-MEGACO-MIB	No	SN06	
nnMegacoQoSCurrDayPktsLost	Unsigned32	Rolling 24 hour total	number of packets lost (in this 15-min interval).*	VMG	VMG Total Day QoS data : Current Day Total QoS data	Number of packets lost	nnMegacoQoSCurrDayTable	NORTEL-UEMG-MEGACO-MIB	No	SN06	
nnMegacoQoSCurrDayPktLossPct	Integer	Rolling 24 hour total	% of packets lost (in current day).*	VMG	VMG Total Day QoS data : Current Day Total QoS data	Percentage of packets lost	nnMegacoQoSCurrDayTable	NORTEL-UEMG-MEGACO-MIB	No	SN06	
nnMegacoQoSCurrDayJitter	Unsigned32	Rolling 24 hour total	average jitter (in current day).*	VMG	VMG Total Day QoS data : Current Day Total QoS data	Average jitter	nnMegacoQoSCurrDayTable	NORTEL-UEMG-MEGACO-MIB	No	SN06	
nnMegacoQoSCurrDayLatency	Unsigned32	Rolling 24 hour total	average latency (in current day).*	VMG	VMG Total Day QoS data : Current Day Total QoS data	Average Latency	nnMegacoQoSCurrDayTable	NORTEL-UEMG-MEGACO-MIB	No	SN06	

nnMegacoOMMedGwyIntervalTable											
nnMegacoOMMedGwyNumInMessages	Unsigned32	Counts only for this 15 min	Number of messages received from the Gateway Controller (GWC) during this interval.	VMG	VMG Statistics History data	Total number of messages received on the link	MegacoOMMedGwyIntervalTable	NORTEL-UEMG-MEGACO-MB	Yes	SN06	
nnMegacoOMMedGwyNumInOctets	Unsigned32	Counts only for this 15 min	Number of octets received from the Gateway Controller (GWC) during this interval.	VMG	VMG Statistics History data	Total number of octets received on the link	MegacoOMMedGwyIntervalTable	NORTEL-UEMG-MEGACO-MB	Yes	SN06	
nnMegacoOMMedGwyAvgInMsgRate	Unsigned32	Counts only for this 15 min	Average message rate (per minute) for messages received from the GWC during this interval.	VMG	VMG Statistics History data	Average message rate for received messages	MegacoOMMedGwyIntervalTable	NORTEL-UEMG-MEGACO-MB	Yes	SN06	
nnMegacoOMMedGwyMaxInMsgRate	Unsigned32	Counts only for this 15 min	Maximum message rate (per minute) for messages received from the GWC during this interval.	VMG	VMG Statistics History data	Maximum message rate for received messages	MegacoOMMedGwyIntervalTable	NORTEL-UEMG-MEGACO-MB	Yes	SN06	
nnMegacoOMMedGwyNumOutMessages	Unsigned32	Counts only for this 15 min	Number of messages sent to the Gateway Controller (GWC) during this interval.	VMG	VMG Statistics History data	Total number of messages sent on the link	MegacoOMMedGwyIntervalTable	NORTEL-UEMG-MEGACO-MB	Yes	SN06	
nnMegacoOMMedGwyNumOutOctets	Unsigned32	Counts only for this 15 min	Number of octets sent to the Gateway Controller (GWC) during this interval.	VMG	VMG Statistics History data	Total number of octets sent on the link	MegacoOMMedGwyIntervalTable	NORTEL-UEMG-MEGACO-MB	Yes	SN06	
nnMegacoOMMedGwyAvgOutMsgRate	Unsigned32	Counts only for this 15 min	Average message rate (per minute) for messages sent to the GWC during this interval.	VMG	VMG Statistics History data	Average message rate for sent messages	MegacoOMMedGwyIntervalTable	NORTEL-UEMG-MEGACO-MB	Yes	SN06	
nnMegacoOMMedGwyMaxOutMsgRate	Unsigned32	Counts only for this 15 min	Maximum message rate (per minute) for messages sent to the GWC during this interval.	VMG	VMG Statistics History data	Maximum message rate for sent messages	MegacoOMMedGwyIntervalTable	NORTEL-UEMG-MEGACO-MB	Yes	SN06	
nnMegacoOMMedGwyCurrentDayTotTable											
nnMegacoOMMedGwyNumInMessagesTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total Number of messages received from the Gateway Controller (GWC).	VMG	VMG Day Total Statistics : Current data	Total number of messages received on the link	nnMegacoOMMedGwyCurrentDayTotTable	NORTEL-UEMG-MEGACO-MB	No	SN06	
nnMegacoOMMedGwyNumInOctetsTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total Number of octets received from the Gateway Controller (GWC).	VMG	VMG Day Total Statistics : Current data	Total number of octets received on the link	nnMegacoOMMedGwyCurrentDayTotTable	NORTEL-UEMG-MEGACO-MB	No	SN06	
nnMegacoOMMedGwyAvgInMsgRateTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total Average message rate (per minute) for messages received from the GWC.	VMG	VMG Day Total Statistics : Current data	Average message rate for received messages	nnMegacoOMMedGwyCurrentDayTotTable	NORTEL-UEMG-MEGACO-MB	No	SN06	
nnMegacoOMMedGwyMaxInMsgRateTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total Maximum message rate (per minute) for messages received from the GWC.	VMG	VMG Day Total Statistics : Current data	Maximum message rate for received messages	nnMegacoOMMedGwyCurrentDayTotTable	NORTEL-UEMG-MEGACO-MB	No	SN06	
nnMegacoOMMedGwyNumOutMessagesTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total Number of messages sent to the Gateway Controller (GWC).	VMG	VMG Day Total Statistics : Current data	Total number of messages sent on the link	nnMegacoOMMedGwyCurrentDayTotTable	NORTEL-UEMG-MEGACO-MB	No	SN06	
nnMegacoOMMedGwyNumOutOctetsTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total Number of octets sent to the Gateway Controller (GWC).	VMG	VMG Day Total Statistics : Current data	Total number of octets sent on the link	nnMegacoOMMedGwyCurrentDayTotTable	NORTEL-UEMG-MEGACO-MB	No	SN06	
nnMegacoOMMedGwyAvgOutMsgRateTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total Average message rate (per minute) for messages sent to the GWC.	VMG	VMG Day Total Statistics : Current data	Average message rate for sent messages	nnMegacoOMMedGwyCurrentDayTotTable	NORTEL-UEMG-MEGACO-MB	No	SN06	
nnMegacoOMMedGwyMaxOutMsgRateTotCurDay	Unsigned32	Rolling 24 hour total	The current day's total Maximum message rate (per minute) for messages sent to the GWC.	VMG	VMG Day Total Statistics : Current data	Maximum message rate for sent messages	nnMegacoOMMedGwyCurrentDayTotTable	NORTEL-UEMG-MEGACO-MB	No	SN06	
NORTEL-UEMG-BANDWIDTH-MB											
nnBwShellCurrentSloaBandwidthResrvdTable											
nnBwShellCurrentSloaBandwidthResrvd	NnBwCells PerSec	count goes up and down, does not rollover	Current amount of reserved bandwidth currently allocated for the aggregate of all Switched Lines over ATM VCs on This UEMG shelf.	MG9K Shelf	Bandwidth Reserved Statistics : Current data	Current bandwidth reserved	nnBwShellCurrentSloaBandwidthResrvdTable	NORTEL-UEMG-BANDWIDTH-MB	No	SN04	On the MG9K EM Performance Browser collect this particular OM under the following conditions. 1.) No traffic 2.) with active calls (from a line on this shelf to a line not on this shelf). The count should be close to 0 for no traffic and higher with active calls. To ensure exact count is collected keep track of the exact number of calls made. There will be a set usage for each active call (171 cells/sec per active call).
nnBwShellCapacitySloaBandwidthResrvd	NnBwCells PerSec	count goes up and down, does not rollover	Current amount of reserved bandwidth Capacity for the aggregate of all Switched Lines over ATM VCs on This UEMG shelf.	MG9K Shelf	Bandwidth Reserved Statistics : Current data	Capacity bandwidth reserved	nnBwShellCurrentSloaBandwidthResrvdTable	NORTEL-UEMG-BANDWIDTH-MB	Yes	SN04	This is just the opposite of the OM above. It starts at max (or close to max) and decreases per call. So collect this OM and add the OM above and the two should equal the max value.
nnBwNettBwResIntervalTable											
nnBwNettBwResIntervalTotal	NnBwCells PerSec	count goes up and down, does not rollover	The 15min measure of the amount of reserved bandwidth currently allocated to VCs on the network interface.	MG9K Network Element	Interval Bandwidth Reserved Statistics : History data	Total bandwidth reserved	nnBwNettBwResIntervalTable	NORTEL-UEMG-BANDWIDTH-MB	No	SN04	On the MG9K EM Performance Browser collect this particular OM under the following conditions. 1.) No traffic 2.) with active calls (from a line on this MG9000 to a line not on this MG9000). The count should be close to 0 for no traffic and higher with active calls. To ensure exact count is collected keep track of the exact number of calls made. There will be a set usage for each active call (171 cells/sec per active call). Collect this for all 96 intervals.
nnBwNettBwResIntervalSloa	NnBwCells PerSec	count goes up and down, does not rollover	The 15min measure of the amount of reserved bandwidth currently allocated for the aggregate of all Switched Lines over ATM VCs on the network interface.	MG9K Network Element	Interval Bandwidth Reserved Statistics : History data	Sloa bandwidth reserved	nnBwNettBwResIntervalTable	NORTEL-UEMG-BANDWIDTH-MB	No	SN04	On the MG9K EM Performance Browser collect this particular OM under the following conditions. 1.) No traffic 2.) with active calls (from a line on this MG9000 to a line not on this MG9000). The count should be close to 0 for no traffic and higher with active calls. To ensure exact count is collected keep track of the exact number of calls made. There will be a set usage for each active call (171 cells/sec per active call).
nnBwShellIntervalSloaBandwidthResrvdTable	NnBwCells PerSec	count goes up and down, does not rollover	The 15-minute measure amount of reserved bandwidth allocated for the aggregate of all Switched Lines over ATM VCs on This UEMG shelf.	MG9K Shelf	Interval Bandwidth Reserved Statistics : History data	Amount of bandwidth reserved	nnBwShellIntervalSloaBandwidthResrvdTable	NORTEL-UEMG-BANDWIDTH-MB	Yes	SN04	On the MG9K EM Performance Browser collect this particular OM under the following conditions. 1.) No traffic 2.) with active calls (from a line on this shelf to a line not on this shelf). The counts should be close to 0 for no traffic and higher with active calls. To ensure exact counts are collected keep track of the exact number of calls made. There will be a set usage for each active call (171 cells/sec per active call). Collect this for all 96 intervals.
nnBwIntervalBandwidthUITTable											
nnBwBandwidthIntervalInCellRate	NnBwCells PerSec	count goes up and down, does not rollover	The 15min measure of the inbound bandwidth utilization.	MG9K Network Element	Interval Bandwidth Utilization Statistics : History data	Cell rate in	nnBwIntervalBandwidthUITable	NORTEL-UEMG-BANDWIDTH-MB	Yes	SN04	On the MG9K EM Performance Browser collect this particular OM under the following conditions. 1.) No traffic 2.) with active calls (from a line on this MG9000 to a line not on this MG9000). The count should be close to 0 for no traffic and higher with active calls. To ensure exact count is collected keep track of the exact number of calls made. There will be a set usage for each active call (171 cells/sec per active call).
nnBwBandwidthIntervalOutCellRate	NnBwCells PerSec	count goes up and down, does not rollover	The 15min measure of the outbound bandwidth utilization.	MG9K Network Element	Interval Bandwidth Utilization Statistics : History data	Cell rate out	nnBwIntervalBandwidthUITable	NORTEL-UEMG-BANDWIDTH-MB	Yes	SN04	Same as above
nnBwBandwidthIntervalInDslCellRate	NnBwCells PerSec	count goes up and down, does not rollover	The 15min measure of the inbound dsl bandwidth utilization.	MG9K Network Element	Interval Bandwidth Utilization Statistics : History data	Dsl cell rate in	nnBwIntervalBandwidthUITable	NORTEL-UEMG-BANDWIDTH-MB	Yes	SN04	On the MG9K EM Performance Browser collect this particular OM under the following conditions. 1.) No data traffic 2.) with active DSL data being sent (from a line on this MG9000 to a line not on this MG9000). The count should be close to 0 for no data and higher with data. To ensure exact count is collected keep track of the actual data rates (added together). Collect this for all 96 intervals. Also ensure the counts have moved to the proper time interval after each 15 interval.
nnBwBandwidthIntervalOutDslCellRate	NnBwCells PerSec	count goes up and down, does not rollover	The 15min measure of the outbound dsl bandwidth utilization.	MG9K Network Element	Interval Bandwidth Utilization Statistics : History data	Dsl cell rate out	nnBwIntervalBandwidthUITable	NORTEL-UEMG-BANDWIDTH-MB	Yes	SN04	Same as above
nnBwIntervalQueueFillTable											
nnBwQueueFillIntervalTotal	NnBwPercent	count goes up and down, does not rollover	The 15-minute value % fill of the entire input cell queue associated with the central switching fabric.	MG9K Network Element	Switch Fabric Congestion Statistics : History data	Fill percentage of the input cell queue	nnBwIntervalQueueFillTable	NORTEL-UEMG-BANDWIDTH-MB	Yes	SN04	On the MG9K EM Performance Browser collect this particular OM under the following conditions. 1.) No traffic 2.) with a large number of active calls (from a line on this MG9000 to a line not on this MG9000). The count should be 0 for no traffic and higher with active calls (warning: % may not change). To ensure exact count is collected keep track of the exact number of calls made. Collect this for all 96 intervals. Also ensure the counts have moved to the proper time interval after each 15 interval.
nnBwQueueFillIntervalCbr	NnBwPercent	count goes up and down, does not rollover	The 15-minute value % fill of the entire input queue associated with the aggregate of all CBR VCs.	MG9K Network Element	Switch Fabric Congestion Statistics : History data	Fill percentage of the CBR VCs input queue	nnBwIntervalQueueFillTable	NORTEL-UEMG-BANDWIDTH-MB	Yes	SN04	On the MG9K EM Performance Browser collect this particular OM under the following conditions. 1.) No PLoA traffic 2.) with very high number of active PLoA calls (from a line on this MG9000 to a line not on this MG9000). The counts should be 0 for no traffic and higher with active calls (warning: % may not change). To ensure exact counts are collected keep track of the exact number of calls made. Collect this for all 96 intervals.

nrBwQueueFillIntervalVbr	NrBwPerCent	count goes up and down, does not rollover	1h 15-minute value % fill of the entire input queue associated with the aggregate of all nr-VBR VCs.	MG9K Network Element	Switch Fabric Congestion Statistics : History data	Fill percentage of the nr-VBR VCs input queue	nrBwIntervalQueueFillTable	NORTEL-UEMG-BANDWIDTH-MB	Yes	SN04	On the MG9K EM Performance Browser collect this particular OM under the following conditions. 1.) No nr-VBR DSL Data 2.) with a very high rate of active nr-VBR DSL data from a line on this MG9000 to a line not on this MG9000. The count should be 0 for no data and higher with data (warning: % may not change. To ensure exact count is collected keep track of the exact number data rate. Collect this for all 96 intervals. Also ensure the counts have moved to the proper time interval after each 15 interval.
nrBwQueueFillIntervalNrtVbr	NrBwPerCent	count goes up and down, does not rollover	1h 15-minute value % fill of the entire input queue associated with the aggregate of all nrt-VBR VCs.	MG9K Network Element	Switch Fabric Congestion Statistics : History data	Fill percentage of the nrt-VBR VCs input queue	nrBwIntervalQueueFillTable	NORTEL-UEMG-BANDWIDTH-MB	Yes	SN04	Same as above but for nrt-VBR DSL data service
nrBwQueueFillIntervalUbr	NrBwPerCent	count goes up and down, does not rollover	1h 15-minute value % fill of the entire input queue associated with the aggregate of all UBR VCs.	MG9K Network Element	Switch Fabric Congestion Statistics : History data	Fill percentage of the UBR VCs input queue	nrBwIntervalQueueFillTable	NORTEL-UEMG-BANDWIDTH-MB	Yes	SN04	Same as above but for UBR DSL data service
nrBwQueueFillIntervalUbrPlus	NrBwPerCent	count goes up and down, does not rollover	1h 15-minute value % fill of the entire input queue associated with the aggregate of all UBR+ VCs.	MG9K Network Element	Switch Fabric Congestion Statistics : History data	Fill percentage of the UBR+ VCs input queue	nrBwIntervalQueueFillTable	NORTEL-UEMG-BANDWIDTH-MB	Yes	SN04	Same as above but for UBR+ DSL data service
nrBwQueueFillIntervalControl	NrBwPerCent	count goes up and down, does not rollover	1h 15-minute value % fill of the entire input queue associated with the aggregate of all Control VCs.	MG9K Network Element	Switch Fabric Congestion Statistics : History data	Fill percentage of all Control VCs input queue	nrBwIntervalQueueFillTable	NORTEL-UEMG-BANDWIDTH-MB	Yes	SN04	Collect this OM with no traffic and no OAMLP activity. The % should be low or 0. Run very high traffic and very high OAMLP traffic and the number may rise. Collect this for all 96 intervals. Also ensure the counts have moved to the proper time interval after each 15 interval.
nrBwAbiCurrentBandwResrvdTable											
nrBwAbiCurrentBandwReserved	NrBwCellsPerSec	count goes up and down, does not rollover	Current amount of reserved bandwidth currently allocated for the aggregate of all VCs on this UEMG ABI interface.	ABI Card	ABI card Bandwidth Reserved Statistics: Current data	Current bandwidth reserved	nrBwAbiCurrentBandwResrvdTable	NORTEL-UEMG-BANDWIDTH-MB	No	SN06	On the MG9K EM Performance Browser collect this particular OM under the following conditions. 1.) No traffic 2.) with active ABI calls (from a line on ABI to a line not on this MG9000). The count should be close to 0 for no traffic and higher with active calls. To ensure exact count is collected keep track of the exact number of calls made. There will be a set usage for each active call (171 cells/sec per active call).
nrBwAbiCapacityBandwReserved	NrBwCellsPerSec	count goes up and down, does not rollover	Current amount of reserved bandwidth Capacity Reserved for all VCs on this ABI interface.	ABI Card	ABI card Bandwidth Reserved Statistics: Current data	Capacity bandwidth reserved	nrBwAbiCurrentBandwResrvdTable	NORTEL-UEMG-BANDWIDTH-MB	Yes	SN06	This is just the opposite of the OM above. It starts at max (or close to max) and decreases per call. So collect this OM and add the OM above and the two should equal the max value.
nrBwAbiIntervalBandwResrvdEntry											
nrBwAbiIntervalBandwReserved	NrBwCellsPerSec	count goes up and down, does not rollover	1h 15-minute measure amount of reserved bandwidth allocated for the aggregate of all VCs on this ABI interface.	ABI Card	ABI card Interval Bandwidth Reserved Statistics: History data	Amount of bandwidth reserved	nrBwAbiIntervalBandwResrvdTable	NORTEL-UEMG-BANDWIDTH-MB	Yes	SN06	On the MG9K EM Performance Browser collect this particular OM under the following conditions. 1.) No traffic 2.) with active ABI calls (from a line on ABI to a line not on this MG9000). The count should be close to 0 for no traffic and higher with active calls. To ensure exact count is collected keep track of the exact number of calls made. There will be a set usage for each active call (171 cells/sec per active call). Collect for all 96 intervals.
SNMP-MPD-MIB SNMP Table											
snmpInvaldMags	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	The total number of packets received by the SNMP engine which were dropped because there were invalid or inconsistent components in the SNMP message.	Not supported			SNMP Table	SNMP-MPD-MIB	Yes	SN04	This is an error condition that cannot be tested under normal conditions. To test a special test tool or test box would be required to sent invalid SNMP messages.
SNMPv2-MIB											
snmpInBadCommunityNames	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	The total number of community-based SNMP messages (for example, SNMPv1) delivered to the SNMP entity which used an SNMP community name not known to said entity. Also, implementations which authenticate community-based SNMP messages using check(s) in addition to matching the community name (for example, by also checking whether the message originated from a transport address allowed to use a specified community name) MAY include in this value the number of messages which failed the additional check(s). It is to authenticate community-based SNMP messages specify the precise conditions that contribute to this value.	Not supported				SNMPv2-MIB	Yes	SN05	
snmpInPkts	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	The total number of messages delivered to the SNMP entity from the transport service.	Not supported				SNMPv2-MIB	Yes	SN05	
NORTEL-UEMG-CLKSYNC-MIB											
NrCkSyncRefTable											
nrCkSyncRefId	Integer	Fixed value	Reference Identification... Identifies the six possible clock synchronization references on the ITP card. This field along with endPhysicalIndex defines a unique row in the nrCkSyncRefTable. itx0 (1), -- reference coming from the left ITX (ITX 0) itx1 (2), -- reference coming from the right ITX (ITX 1) dcc0 (3), -- reference coming from the left DCC (DCC-0) dcc1 (4), -- reference coming from the right DCC (DCC-1) host0 (5), -- reference cabled into the ITP ATM25 phy0 host1 (6) -- reference cabled into the ITP ATM25 phy1 *	Not supported			NrCkSyncRefTable	NORTEL-UEMG-CLKSYNC-MB	Yes	SN04	See Below
nrCkSyncRefLossOfSignalCount	Unsigned32	Count From Last Init up to 255 then it rolls over to 0	Contains the count of the number of onsets of timing reference signal loss. Range is from 0 - 255	ITP Card	Clock Sync Left ITX Reference Statistics : Current data Clock Sync Right ITX Reference Statistics : Current data Clock Sync Left OC3 Reference Statistics : Current data Clock Sync Right OC3 Reference Statistics : Current data	Number of onsets of timing reference signal loss	NrCkSyncRefTable	NORTEL-UEMG-CLKSYNC-MB	Yes	SN05	Remove ITX cables to the ITP cards. This OM count will increase for each removal.
nrCkSyncRefLossOfFrameCount (SN05)	Unsigned32	Count From Last Init up to 255 then it rolls over to 0	Contains the count of the number of loss of frames. Range is from 0 - 255.	ITP Card	Clock Sync Left ITX Reference Statistics : Current data Clock Sync Right ITX Reference Statistics : Current data Clock Sync Left OC3 Reference Statistics : Current data Clock Sync Right OC3 Reference Statistics : Current data	Number of loss of frames	NrCkSyncRefTable	NORTEL-UEMG-CLKSYNC-MB	Yes	SN05	Remove all BITS and Network timing signals, individually (remove cables). This OM count will increase each time the signal is removed
NrCkSyncSignalTable											
			This table provides status information on each of the six timing signals coming into the UEMG host shelf. There is one entry for each network timing signal (total of two), and one entry for each BITS signal (total of 4)							SN05	

nnCkSyncSignalId	Integer	Fixed value	-- the BITS ITX connected pair. bitsB-0 (2), -- BITS B signal coming into the left ITX of -- the BITS ITX connected pair. bitsA-1 (3), -- BITS A signal coming into the right ITX of -- the BITS ITX connected pair. bitsB-1 (4), -- BITS B signal coming into the right ITX of -- the BITS ITX connected pair. dcc-0 (5), -- Network Traffic signal coming into DCC-0 dcc-1 (6) -- Network Traffic signal coming into DCC-1*	Not Supported			NnCkSyncSignalTable	NORTEL-UEMG-CLKSYN-MB	Yes		See Below
nnCkSyncSignalLossOfFrameCount	Unsigned32	Count From Last bit up to 255 then it rolls over to 0	Contains the count of the number of loss of frames.	Not supported			NnCkSyncSignalTable	NORTEL-UEMG-CLKSYN-MB	Yes	SN05	Remove all BITS and Network timing signals, individually (remove cables). This OM count will increase each time the signal is removed
nnCkSyncSignalLossOfSignalCount	Unsigned32	Count From Last bit up to 255 then it rolls over to 0	Contains the count of the number of onsets of timing source signal loss.	Not supported			NnCkSyncSignalTable	NORTEL-UEMG-CLKSYN-MB	Yes	SN05	Remove all BITS and Network timing signals, individually (remove cables). This OM count will increase each time the signal is removed
DS1-MIB											
dsx1CurrentTable											
dsx1CurrentESs	PerCurrentCount	Counts only for last 15 min	The number of Errored Seconds.	DS1 Port, IMA Port	Near-end Statistics : Current data	Number of errored seconds	dsx1CurrentTable	DS1-MIB	No	SN04	On a PLoA DS1 channel connect a test box that has the ability to inject errors (e.g. TBERD). Without injecting any errors collect the OM and it should be 0. Inject toward the near-end DS1 (DS0) the error and collect the OM and it should reflect the correct error count. Many of the NearEnd counts will be pegged just by pulling the DS1 cable.
dsx1CurrentSEs	PerCurrentCount	Counts only for last 15 min	The number of Severely Errored Seconds.	DS1 Port, IMA Port	Near-end Statistics : Current data	Number of severely errored seconds	dsx1CurrentTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentSEFs	PerCurrentCount	Counts only for last 15 min	The number of Severely Errored Framing Seconds.	DS1 Port, IMA Port	Near-end Statistics : Current data	Number of severely errored framing seconds	dsx1CurrentTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentUAs	PerCurrentCount	Counts only for last 15 min	The number of Unavailable Seconds.	DS1 Port, IMA Port	Near-end Statistics : Current data	Number of unavailable seconds	dsx1CurrentTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentCSs	PerCurrentCount	Counts only for last 15 min	The number of Controlled Slip Seconds.	DS1 Port, IMA Port	Near-end Statistics : Current data	Number of controlled slip seconds	dsx1CurrentTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentPCVs	PerCurrentCount	Counts only for last 15 min	The number of Path Coding Violations.	DS1 Port, IMA Port	Near-end Statistics : Current data	Number of path coding violations	dsx1CurrentTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentESs	PerCurrentCount	Counts only for last 15 min	The number of Line Errored Seconds.	DS1 Port, IMA Port	Near-end Statistics : Current data	Number of line errored seconds	dsx1CurrentTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentBEs	PerCurrentCount	Counts only for last 15 min	The number of Bursty Errored Seconds	DS1 Port, IMA Port	Near-end Statistics : Current data	Number of bursty errored seconds	dsx1CurrentTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentDMs	PerCurrentCount	Counts only for last 15 min	The number of Degraded Minutes	DS1 Port, IMA Port	Near-end Statistics : Current data	Number of degraded minutes	dsx1CurrentTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentLCVs	PerCurrentCount	Counts only for last 15 min	The number of Line Code Violations (LCVs).	DS1 Port, IMA Port	Near-end Statistics : Current data	Number of line code violations	dsx1CurrentTable	DS1-MIB	No	SN04	Same as above
dsx1IntervalTable											
dsx1CurrentESs	PerIntervalCount	Counts only for last 15 min	The number of Errored Seconds.	DS1 Port, IMA Port	Near-end Statistics : History data	Number of errored seconds	dsx1IntervalTable	DS1-MIB	No	SN04	On a PLoA DS1 channel connect a test box that has the ability to inject errors (e.g. TBERD). With out injecting any errors collect the OM and it should be 0. Inject toward the near-end DS1 (DS0) the error and collect the OM and it should reflect the correct error count. Many of the NearEnd counts will be pegged just by pulling the DS1 cable. Collect all 96 intervals, waiting 15+ minutes between tests, the counts will move to a higher interval each 15 minutes.
dsx1CurrentSEs	PerIntervalCount	Counts only for last 15 min	The number of Severely Errored Seconds.	DS1 Port, IMA Port	Near-end Statistics : History data	Number of severely errored seconds	dsx1IntervalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentSEFs	PerIntervalCount	Counts only for last 15 min	The number of Severely Errored Framing Seconds.	DS1 Port, IMA Port	Near-end Statistics : History data	Number of severely errored framing seconds	dsx1IntervalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentUAs	PerIntervalCount	Counts only for last 15 min	The number of Unavailable Seconds. This object may decrease if the occurrence of unavailable seconds occurs across an interval boundary.	DS1 Port, IMA Port	Near-end Statistics : History data	Number of unavailable seconds	dsx1IntervalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentCSs	PerIntervalCount	Counts only for last 15 min	The number of Controlled Slip Seconds.	DS1 Port, IMA Port	Near-end Statistics : History data	Number of controlled slip seconds	dsx1IntervalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentPCVs	PerIntervalCount	Counts only for last 15 min	The number of Path Coding Violations.	DS1 Port, IMA Port	Near-end Statistics : History data	Number of path coding violations	dsx1IntervalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentESs	PerIntervalCount	Counts only for last 15 min	The number of Line Errored Seconds.	DS1 Port, IMA Port	Near-end Statistics : History data	Number of line errored seconds	dsx1IntervalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentBEs	PerCurrentCount	Counts only for last 15 min	The number of Bursty Errored Seconds	DS1 Port, IMA Port	Near-end Statistics : History data	Number of bursty errored seconds	dsx1IntervalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentDMs	PerCurrentCount	Counts only for last 15 min	The number of Degraded Minutes	DS1 Port, IMA Port	Near-end Statistics : History data	Number of degraded minutes	dsx1IntervalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentLCVs	PerIntervalCount	Counts only for last 15 min	The number of Line Code Violations.	DS1 Port, IMA Port	Near-end Statistics : History data	Number of line code violations	dsx1IntervalTable	DS1-MIB	No	SN04	Same as above
dsx1TotalTable											
dsx1CurrentESs	PerTotalCount	Rolling 24 hour total	The sum of Errored Seconds encountered by a DS1 interface in the previous 24 hour interval. Invalid 15 minute intervals count as 0.	DS1 Port, IMA Port	Near-end Statistics : 24-hour current data	Number of errored seconds	dsx1TotalTable	DS1-MIB	No	SN04	On a PLoA DS1 channel connect a test box that has the ability to inject errors (e.g. TBERD). With out injecting any errors collect the OM and it should be 0. Inject toward the near-end DS1 (DS0) the error and collect the OM and it should reflect the correct error count across 24 hours. Many of the NearEnd counts will be pegged just by pulling the DS1 cable. This test can be done utilizing the current and interval tests.
dsx1CurrentSEs	PerTotalCount	Rolling 24 hour total	The number of Severely Errored Seconds encountered by a DS1 interface in the previous 24 hour interval. Invalid 15 minute intervals count as 0.	DS1 Port, IMA Port	Near-end Statistics : 24-hour current data	Number of severely errored seconds	dsx1TotalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentSEFs	PerTotalCount	Rolling 24 hour total	The number of Severely Errored Framing Seconds encountered by a DS1 interface in the previous 24 hour interval. Invalid 15 minute intervals count as 0.	DS1 Port, IMA Port	Near-end Statistics : 24-hour current data	Number of severely errored framing seconds	dsx1TotalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentUAs	PerTotalCount	Rolling 24 hour total	The number of Unavailable Seconds encountered by a DS1 interface in the previous 24 hour interval. Invalid 15 minute intervals count as 0.	DS1 Port, IMA Port	Near-end Statistics : 24-hour current data	Number of unavailable seconds	dsx1TotalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentCSs	PerTotalCount	Rolling 24 hour total	The number of Controlled Slip Seconds encountered by a DS1 interface in the previous 24 hour interval. Invalid 15 minute intervals count as 0.	DS1 Port, IMA Port	Near-end Statistics : 24-hour current data	Number of controlled slip seconds	dsx1TotalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentPCVs	PerTotalCount	Rolling 24 hour total	The number of Path Coding Violations encountered by a DS1 interface in the previous 24 hour interval. Invalid 15 minute intervals count as 0.	DS1 Port, IMA Port	Near-end Statistics : 24-hour current data	Number of path coding violations	dsx1TotalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentESs	PerTotalCount	Rolling 24 hour total	The number of Line Errored Seconds encountered by a DS1 interface in the previous 24 hour interval. Invalid 15 minute intervals count as 0.	DS1 Port, IMA Port	Near-end Statistics : 24-hour current data	Number of line errored seconds	dsx1TotalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentBEs	PerCurrentCount	Rolling 24 hour total	The number of Bursty Errored Seconds	DS1 Port, IMA Port	Near-end Statistics : 24-hour current data	Number of bursty errored seconds	dsx1TotalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentDMs	PerCurrentCount	Rolling 24 hour total	The number of Degraded Minutes	DS1 Port, IMA Port	Near-end Statistics : 24-hour current data	Number of degraded minutes	dsx1TotalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentLCVs	PerTotalCount	Rolling 24 hour total	The number of Line Code Violations (LCVs) encountered by a DS1 interface in the current 15 minute interval. Invalid 15 minute intervals count as 0.	DS1 Port, IMA Port	Near-end Statistics : 24-hour current data	Number of line code violations	dsx1TotalTable	DS1-MIB	No	SN04	Same as above
dsx1FarEndCurrentTable											
dsx1CurrentESs	PerCurrentCount	Counts only for last 15 min	The number of Far End Errored Seconds.	DS1 Port, IMA Port	Far-end Statistics : Current data	Number of errored seconds	dsx1FarEndCurrentTable	DS1-MIB	No	SN04	On a PLoA DS1 channel connect a test box that has the ability to inject errors (e.g. TBERD). With out injecting any errors collect the OM and it should be 0. Inject toward the Far-end DS1 (DS0) the error and collect the OM and it should reflect the correct error count
dsx1CurrentSEs	PerCurrentCount	Counts only for last 15 min	The number of Far End Severely Errored Seconds.	DS1 Port, IMA Port	Far-end Statistics : Current data	Number of severely errored seconds	dsx1FarEndCurrentTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentSEFs	PerCurrentCount	Counts only for last 15 min	The number of Far End Severely Errored Framing Seconds.	DS1 Port, IMA Port	Far-end Statistics : Current data	Number of severely errored framing seconds	dsx1FarEndCurrentTable	DS1-MIB	No	SN04	Same as above

dsx1CurrentUASs	Per/Current Count	Counts only for last 15 min	The number of Unavailable Seconds.	DS1 Port, IMA Port	Far-end Statistics : Current data	Number of unavailable seconds	dsx1FarEndCurrentTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentCSSs	Per/Current Count	Counts only for last 15 min	The number of Far End Controlled Slip Seconds.	DS1 Port, IMA Port	Far-end Statistics : Current data	Number of controlled slip seconds	dsx1FarEndCurrentTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentLESs	Per/Current Count	Counts only for last 15 min	The number of Far End Line Errored Seconds.	DS1 Port, IMA Port	Far-end Statistics : Current data	Number of path coding violations	dsx1FarEndCurrentTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentPCVs	Per/Current Count	Counts only for last 15 min	The number of Far End Path Coding Violations.	DS1 Port, IMA Port	Far-end Statistics : Current data	Number of line errored seconds	dsx1FarEndCurrentTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentBESs	Per/Current Count	Counts only for last 15 min	The number of Bursty Errored Seconds	DS1 Port, IMA Port	Far-end Statistics : Current data	Number of bursty errored seconds	dsx1FarEndCurrentTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentDMs	Per/Current Count	Counts only for last 15 min	The number of Degraded Minutes	DS1 Port, IMA Port	Far-end Statistics : Current data	Number of degraded minutes	dsx1FarEndCurrentTable	DS1-MIB	No	SN04	Same as above
dsx1FarEndIntervalTable											
dsx1CurrentESs	Per/Interval Count	Counts only for last 15 min	The number of Far End Errored Seconds.	DS1 Port, IMA Port	Far-end Statistics : History data	Number of errored seconds	dsx1FarEndIntervalTable	DS1-MIB	No	SN04	On a PLoA DS1 channel connect a test box that has the ability to inject errors (e.g. TBERD). With out injecting any errors collect the OM and it should be 0. Inject toward the Far-end DS1 (DS0) the error and collect the OM and it should reflect the correct error count. Collect all 96 intervals, waiting 15+ minutes between tests, the counts will move to a higher interval each 15 minutes.
dsx1CurrentSEsSs	Per/Interval Count	Counts only for last 15 min	The number of Far End Severely Errored Seconds.	DS1 Port, IMA Port	Far-end Statistics : History data	Number of severely errored seconds	dsx1FarEndIntervalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentSEFsSs	Per/Interval Count	Counts only for last 15 min	The number of Far End Severely Errored Framing Seconds.	DS1 Port, IMA Port	Far-end Statistics : History data	Number of severely errored framing seconds	dsx1FarEndIntervalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentUASs	Per/Interval Count	Counts only for last 15 min	The number of Unavailable Seconds.	DS1 Port, IMA Port	Far-end Statistics : History data	Number of unavailable seconds	dsx1FarEndIntervalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentCSSs	Per/Interval Count	Counts only for last 15 min	The number of Far End Controlled Slip Seconds.	DS1 Port, IMA Port	Far-end Statistics : History data	Number of controlled slip seconds	dsx1FarEndIntervalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentLESs	Per/Interval Count	Counts only for last 15 min	The number of Far End Line Errored Seconds.	DS1 Port, IMA Port	Far-end Statistics : History data	Number of path coding violations	dsx1FarEndIntervalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentPCVs	Per/Interval Count	Counts only for last 15 min	The number of Far End Path Coding Violations.	DS1 Port, IMA Port	Far-end Statistics : History data	Number of line errored seconds	dsx1FarEndIntervalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentBESs	Per/Current Count	Counts only for last 15 min	The number of Bursty Errored Seconds	DS1 Port, IMA Port	Far-end Statistics : History data	Number of bursty errored seconds	dsx1FarEndIntervalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentDMs	Per/Current Count	Counts only for last 15 min	The number of Degraded Minutes	DS1 Port, IMA Port	Far-end Statistics : History data	Number of degraded minutes	dsx1FarEndIntervalTable	DS1-MIB	No	SN04	Same as above
dsx1FarEndTotalTable											
dsx1CurrentESs	Per/TotalCo unit	Rolling 24 hour total	The number of Far End Errored Seconds encountered by a DS1 interface in the previous 24 hour interval. Invalid 15 minute intervals count as 0.	DS1 Port, IMA Port	Far-end Statistics : 24-hour current data	Number of errored seconds	dsx1FarEndTotalTable	DS1-MIB	No	SN04	On a PLoA DS1 channel connect a test box that has the ability to inject errors (e.g. TBERD). With out injecting any errors collect the OM and it should be 0. Inject toward the Far-end DS1 (DS0) the error and collect the OM and it should reflect the correct error count across 24 hours. This test can be done utilizing the current and interval tests.
dsx1CurrentSEsSs	Per/TotalCo unit	Rolling 24 hour total	The number of Far End Severely Errored Seconds encountered by a DS1 interface in the previous 24 hour interval. Invalid 15 minute intervals count as 0.	DS1 Port, IMA Port	Far-end Statistics : 24-hour current data	Number of severely errored seconds	dsx1FarEndTotalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentSEFsSs	Per/TotalCo unit	Rolling 24 hour total	The number of Far End Severely Errored Framing Seconds encountered by a DS1 interface in the previous 24 hour interval. Invalid 15 minute intervals count as 0.	DS1 Port, IMA Port	Far-end Statistics : 24-hour current data	Number of severely errored framing seconds	dsx1FarEndTotalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentUASs	Per/TotalCo unit	Rolling 24 hour total	The number of Unavailable Seconds encountered by a DS1 interface in the previous 24 hour interval. Invalid 15 minute intervals count as 0.	DS1 Port, IMA Port	Far-end Statistics : 24-hour current data	Number of unavailable seconds	dsx1FarEndTotalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentCSSs	Per/TotalCo unit	Rolling 24 hour total	The number of Far End Controlled Slip Seconds encountered by a DS1 interface in the previous 24 hour interval. Invalid 15 minute intervals count as 0.	DS1 Port, IMA Port	Far-end Statistics : 24-hour current data	Number of controlled slip seconds	dsx1FarEndTotalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentLESs	Per/TotalCo unit	Rolling 24 hour total	The number of Far End Line Errored Seconds encountered by a DS1 interface in the previous 24 hour interval. Invalid 15 minute intervals count as 0.	DS1 Port, IMA Port	Far-end Statistics : 24-hour current data	Number of path coding violations	dsx1FarEndTotalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentPCVs	Per/TotalCo unit	Rolling 24 hour total	The number of Far End Path Coding Violations reported via the far end block error count encountered by a DS1 interface in the previous 24 hour interval. Invalid 15 minute intervals count as 0.	DS1 Port, IMA Port	Far-end Statistics : 24-hour current data	Number of line errored seconds	dsx1FarEndTotalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentBESs	Per/Current Count	Rolling 24 hour total	The number of Bursty Errored Seconds	DS1 Port, IMA Port	Far-end Statistics : 24-hour current data	Number of bursty errored seconds	dsx1FarEndTotalTable	DS1-MIB	No	SN04	Same as above
dsx1CurrentDMs	Per/Current Count	Rolling 24 hour total	The number of Degraded Minutes	DS1 Port, IMA Port	Far-end Statistics : 24-hour current data	Number of degraded minutes	dsx1FarEndTotalTable	DS1-MIB	No	SN04	Same as above
SONET-MIB											
sonetSectionCurrentTable											
sonetSectionCurrentESs	Per/Current Count	Counts since last 15 min interval	The counter associated with the number of Errored Seconds encountered by a SONET/SDH Section in the current 15 minute interval.	OC3 Port, STS1	Sonet Section Statistics : Current data	Number of errored seconds	sonetSectionCurrentTable	SONET-MIB	No	SN04	On the OC3 connect a test box that has the ability to inject errors (e.g. ADTECH). With out injecting any errors collect the OM and it should be 0. Inject toward the near-end OC3 the error and collect the OM and it should reflect the correct error count. Many of the NearEnd counts will be pegged just by pulling the DS1 cable.
sonetSectionCurrentSEsSs	Per/Current Count	Counts since last 15 min interval	The counter associated with the number of Severely Errored Seconds encountered by a SONET/SDH Section in the current 15 minute interval.	OC3 Port, STS1	Sonet Section Statistics : Current data	Number of severely errored seconds	sonetSectionCurrentTable	SONET-MIB	No	SN04	Same as above
sonetSectionCurrentSEFsSs	Per/Current Count	Counts since last 15 min interval	The counter associated with the number of Severely Errored Framing Seconds encountered by a SONET/SDH Section in the current 15 minute interval.	OC3 Port, STS1	Sonet Section Statistics : Current data	Number of severely errored framing seconds	sonetSectionCurrentTable	SONET-MIB	No	SN04	Same as above
sonetSectionCurrentCVs	Per/Current Count	Counts since last 15 min interval	The counter associated with the number of Coding Violations encountered by a SONET/SDH Section in the current 15 minute interval.	OC3 Port, STS1	Sonet Section Statistics : Current data	Number of coding violations	sonetSectionCurrentTable	SONET-MIB	No	SN04	Same as above
sonetSectionIntervalTable											
sonetSectionIntervalESs	Per/Interval Count	Counts only for last 15 min	The counter associated with the number of Errored Seconds encountered by a SONET/SDH Section in a particular 15-minute interval in the past 24 hours.	OC3 Port, STS1	Sonet Section Statistics : History data	Number of errored seconds	sonetSectionIntervalTable	SONET-MIB	Yes	SN04	On the OC3 connect a test box that has the ability to inject errors (e.g. ADTECH). With out injecting any errors collect the OM and it should be 0. Inject toward the near-end OC3 the error and collect the OM and it should reflect the correct error count. Many of the NearEnd counts will be pegged just by pulling the DS1 cable. Collect all 96 intervals, waiting 15+ minutes between tests, the counts will move to a higher interval each 15 minutes.
sonetSectionIntervalSEsSs	Per/Interval Count	Counts only for last 15 min	The counter associated with the number of Severely Errored Seconds encountered by a SONET/SDH Section in a particular 15-minute interval in the past 24 hours.	OC3 Port, STS1	Sonet Section Statistics : History data	Number of severely errored seconds	sonetSectionIntervalTable	SONET-MIB	Yes	SN04	Same as above
sonetSectionIntervalSEFsSs	Per/Interval Count	Counts only for last 15 min	The counter associated with the number of Severely Errored Framing Seconds encountered by a SONET/SDH Section in a particular 15-minute interval in the past 24 hours.	OC3 Port, STS1	Sonet Section Statistics : History data	Number of severely errored framing seconds	sonetSectionIntervalTable	SONET-MIB	Yes	SN04	Same as above
sonetSectionIntervalCVs	Per/Interval Count	Counts only for last 15 min	The counter associated with the number of Coding Violations encountered by a SONET/SDH Section in a particular 15-minute interval in the past 24 hours.	OC3 Port, STS1	Sonet Section Statistics : History data	Number of coding violations	sonetSectionIntervalTable	SONET-MIB	Yes	SN04	Same as above
sonetLineCurrentTable											
sonetLineCurrentESs	Per/Current Count	Counts since last 15 min interval	The counter associated with the number of Errored Seconds encountered by a SONET/SDH Line in the current 15 minute interval.	OC3 Port, STS1	Sonet Line Statistics : Current data	Number of errored seconds	sonetLineCurrentTable	SONET-MIB	No	SN04	On the OC3 connect a test box that has the ability to inject errors (e.g. ADTECH). With out injecting any errors collect the OM and it should be 0. Inject toward the near-end OC3 the error and collect the OM and it should reflect the correct error count. Many of the NearEnd counts will be pegged just by pulling the DS1 cable.
sonetLineCurrentSEsSs	Per/Current Count	Counts since last 15 min interval	The counter associated with the number of Severely Errored Seconds encountered by a SONET/SDH Line in the current 15 minute interval.	OC3 Port, STS1	Sonet Line Statistics : Current data	Number of severely errored seconds	sonetLineCurrentTable	SONET-MIB	No	SN04	Same as above
sonetLineCurrentCVs	Per/Current Count	Counts since last 15 min interval	The counter associated with the number of Coding Violations encountered by a SONET/SDH Line in the current 15 minute interval.	OC3 Port, STS1	Sonet Line Statistics : Current data	Number of coding violations	sonetLineCurrentTable	SONET-MIB	No	SN04	Same as above

sonetLineCurrentUASs	Per/Current Count	Counts since last 15 min interval	The counter associated with the number of Unavailable Seconds encountered by a SONE/SDH Line in the current 15-minute inter. val.	OC3 Port, STS1	Sonet Line Statistics : Current data	Number of unavailable seconds	sonetLineCurrentTable	SONET-MIB	No	SN04	Same as above
sonetLineIntervalTable											
sonetLineIntervalESs	Per/Interval Count	Counts only for last 15 min	The counter associated with the number of Error/Seconds encountered by a SONE/SDH Line in a particular 15-minute interval in the past 24 hours.	OC3 Port, STS1	Sonet Line Statistics : History data	Number of errored seconds	sonetLineIntervalTable	SONET-MIB	Yes	SN04	On the OC3 connect a test box that has the ability to inject errors (e.g. ADTECH). With out injecting any errors collect the OM and it should be 0. Inject toward the near-end OC3 the error and collect the OM and it should reflect the correct error count. Many of the NearEnd counts will be pegged just by pulling the DS1 cable. Collect all 96 intervals, waiting 15+ minutes between tests, the counts will move to a higher interval each 15 minutes.
sonetLineIntervalSESs	Per/Interval Count	Counts only for last 15 min	The counter associated with the number of Severely Error/Seconds encountered by a SONE/SDH Line in a particular 15-minute interval in the past 24 hours.	OC3 Port, STS1	Sonet Line Statistics : History data	Number of severely errored seconds	sonetLineIntervalTable	SONET-MIB	Yes	SN04	Same as above
sonetLineIntervalCVs	Per/Interval Count	Counts only for last 15 min	The counter associated with the number of Coding Violations encountered by a SONE/SDH Line in a particular 15-minute interval in the past 24 hours.	OC3 Port, STS1	Sonet Line Statistics : History data	Number of coding violations	sonetLineIntervalTable	SONET-MIB	Yes	SN04	Same as above
sonetLineIntervalUASs	Per/Interval Count	Counts only for last 15 min	The counter associated with the number of Unavailable Seconds encountered by a SONE/SDH Line in a particular 15-minute interval in the past 24 hours.	OC3 Port, STS1	Sonet Line Statistics : History data	Number of unavailable seconds	sonetLineIntervalTable	SONET-MIB	Yes	SN04	Same as above
sonetFarEndLineCurrentTable											
sonetFarEndLineCurrentESs	Per/Current Count	Counts since last 15 min interval	The counter associated with the number of Far End Error/Seconds encountered by a SONE/SDH interface in the current 15 minute interval.	OC3 Port, STS1	Sonet Far End Line Statistics : Current data	Number of errored seconds	sonetFarEndLineCurrentTable	SONET-MIB	No	SN04	On the OC3 channel connect a test box that has the ability to inject errors (e.g. ADTECH). With out injecting any errors collect the OM and it should be 0. Inject toward the Far-end OC3 the error and collect the OM and it should reflect the correct error count
sonetFarEndLineCurrentSESs	Per/Current Count	Counts since last 15 min interval	The counter associated with the number of Far End Severely Error/Seconds encountered by a SONE/SDH Medium/Section/Line interface in the current 15 minute interval.	OC3 Port, STS1	Sonet Far End Line Statistics : Current data	Number of severely errored seconds	sonetFarEndLineCurrentTable	SONET-MIB	No	SN04	Same as above
sonetFarEndLineCurrentCVs	Per/Current Count	Counts since last 15 min interval	The counter associated with the number of Far End Coding Violations reported via the far end block error count encountered by a SONE/SDH Medium/Section/Line interface in the current 15 minute interval.	OC3 Port, STS1	Sonet Far End Line Statistics : Current data	Number of coding violations	sonetFarEndLineCurrentTable	SONET-MIB	No	SN04	Same as above
sonetFarEndLineCurrentUASs	Per/Current Count	Counts since last 15 min interval	The counter associated with the number of Far End Unavailable Seconds encountered by a SONE/SDH Medium/Section/Line interface in the current 15 minute interval.	OC3 Port, STS1	Sonet Far End Line Statistics : Current data	Number of unavailable seconds	sonetFarEndLineCurrentTable	SONET-MIB	No	SN04	Same as above
sonetFarEndLineIntervalTable											
sonetFarEndLineIntervalESs	Per/Interval Count	Counts only for last 15 min	The counter associated with the number of Far End Error/Seconds encountered by a SONE/SDH Line interface in a particular 15- minute interval in the past 24 hours.	OC3 Port, STS1	Sonet Far End Line Statistics : History data	Number of errored seconds	sonetFarEndLineIntervalTable	SONET-MIB	No	SN04	On the OC3 channel connect a test box that has the ability to inject errors (e.g. ADTECH). With out injecting any errors collect the OM and it should be 0. Inject toward the Far-end OC3 the error and collect the OM and it should reflect the correct error count. Collect all 96 intervals, waiting 15+ minutes between tests, the counts will move to a higher interval each 15 minutes.
sonetFarEndLineIntervalSESs	Per/Interval Count	Counts only for last 15 min	The counter associated with the number of Far End Severely Error/Seconds encountered by a SONE/SDH Line interface in a particular 15-minute interval in the past 24 hours.	OC3 Port, STS1	Sonet Far End Line Statistics : History data	Number of severely errored seconds	sonetFarEndLineIntervalTable	SONET-MIB	No	SN04	Same as above
sonetFarEndLineIntervalCVs	Per/Interval Count	Counts only for last 15 min	The counter associated with the number of Far End Coding Violations reported via the far end block error count encountered by a SONE/SDH Line interface in a particular 15-minute interval in the past 24 hours.	OC3 Port, STS1	Sonet Far End Line Statistics : History data	Number of coding violations	sonetFarEndLineIntervalTable	SONET-MIB	No	SN04	Same as above
sonetFarEndLineIntervalUASs	Per/Interval Count	Counts only for last 15 min	The counter associated with the number of Far End Unavailable Seconds encountered by a SONE/SDH Line interface in a particular 15-minute interval in the past 24 hours.	OC3 Port, STS1	Sonet Far End Line Statistics : History data	Number of unavailable seconds	sonetFarEndLineIntervalTable	SONET-MIB	No	SN04	Same as above
sonetPathCurrentTable											
sonetPathCurrentESs	Per/Current Count	Counts since last 15 min interval	The counter associated with the number of Error/Seconds encountered by a SONE/SDH Path in the current 15 minute interval.	OC3 Port, STS1	Sonet Path Statistics : Current data	Number of errored seconds	sonetPathCurrentTable	SONET-MIB	No	SN04	On the OC3 connect a test box that has the ability to inject errors (e.g. ADTECH). With out injecting any errors collect the OM and it should be 0. Inject toward the near-end OC3 the error and collect the OM and it should reflect the correct error count. Many of the NearEnd counts will be pegged just by pulling the DS1 cable
sonetPathCurrentSESs	Per/Current Count	Counts since last 15 min interval	The counter associated with the number of Severely Error/Seconds encountered by a SONE/SDH Path in the current 15 minute interval.	OC3 Port, STS1	Sonet Path Statistics : Current data	Number of severely errored seconds	sonetPathCurrentTable	SONET-MIB	No	SN04	Same as above
sonetPathCurrentCVs	Per/Current Count	Counts since last 15 min interval	The counter associated with the number of Coding Violations encountered by a SONE/SDH Path in the current 15 minute interval.	OC3 Port, STS1	Sonet Path Statistics : Current data	Number of coding violations	sonetPathCurrentTable	SONET-MIB	No	SN04	Same as above
sonetPathCurrentUASs	Per/Current Count	Counts since last 15 min interval	The counter associated with the number of Unavailable Seconds encountered by a Path in the current 15 minute interval.	OC3 Port, STS1	Sonet Path Statistics : Current data	Number of unavailable seconds	sonetPathCurrentTable	SONET-MIB	No	SN04	Same as above
sonetPathIntervalTable											
sonetPathIntervalESs	Per/Interval Count	Counts only for last 15 min	The counter associated with the number of Error/Seconds encountered by a SONE/SDH Path in a particular 15-minute interval in the past 24 hours.	OC3 Port, STS1	Sonet Path Statistics : History data	Number of errored seconds	sonetPathIntervalTable	SONET-MIB	Yes	SN04	On the OC3 connect a test box that has the ability to inject errors (e.g. ADTECH). With out injecting any errors collect the OM and it should be 0. Inject toward the near-end OC3 the error and collect the OM and it should reflect the correct error count. Many of the NearEnd counts will be pegged just by pulling the DS1 cable. Collect all 96 intervals, waiting 15+ minutes between tests, the counts will move to a higher interval each 15 minutes.
sonetPathIntervalSESs	Per/Interval Count	Counts only for last 15 min	The counter associated with the number of Severely Error/Seconds encountered by a SONE/SDH Path in a particular 15-minute interval in the past 24 hours.	OC3 Port, STS1	Sonet Path Statistics : History data	Number of severely errored seconds	sonetPathIntervalTable	SONET-MIB	Yes	SN04	Same as above
sonetPathIntervalCVs	Per/Interval Count	Counts only for last 15 min	The counter associated with the number of Coding Violations encountered by a SONE/SDH Path in a particular 15-minute interval in the past 24 hours.	OC3 Port, STS1	Sonet Path Statistics : History data	Number of coding violations	sonetPathIntervalTable	SONET-MIB	Yes	SN04	Same as above
sonetPathIntervalUASs	Per/Interval Count	Counts only for last 15 min	The counter associated with the number of Unavailable Seconds encountered by a Path in a particular 15-minute interval in the past 24 hours.	OC3 Port, STS1	Sonet Path Statistics : History data	Number of unavailable seconds	sonetPathIntervalTable	SONET-MIB	Yes	SN04	Same as above
sonetFarEndPathCurrentTable											
sonetFarEndPathCurrentESs	Per/Current Count	Counts since last 15 min interval	The counter associated with the number of Far End Error/Seconds encountered by a SONE/SDH interface in the current 15 minute interval.	OC3 Port, STS1	Sonet Far End Path Statistics : Current data	Number of errored seconds	sonetFarEndPathCurrentTable	SONET-MIB	No	SN04	On the OC3 connect a test box that has the ability to inject errors (e.g

sonetFarEndPathIntervalSESs	PerInterval Count	Counts only for last 15 min	The counter associated with the number of Far End Severely Errored Seconds encountered by a SONET/SDH Path interface in a particular 15-minute interval in the past 24 hours.	OC3 Port, STS1	Sonet Far End Path Statistics History data	Number of severely errored seconds	sonetFarEndPathIntervalTable	SONET-MIB	No	SN04	Same as above
sonetFarEndPathIntervalCVs	PerInterval Count	Counts only for last 15 min	The counter associated with the number of Far End Coding Violations reported via the far end block error count encountered by a SONET/SDH Path interface in a particular 15-minute interval in the past 24 hours.	OC3 Port, STS1	Sonet Far End Path Statistics History data	Number of coding violations	sonetFarEndPathIntervalTable	SONET-MIB	No	SN04	Same as above
sonetFarEndPathIntervalUAs	PerInterval Count	Counts only for last 15 min	The counter associated with the number of Far End Unavailable Seconds encountered by a SONET/SDH Path interface in a particular 15-minute interval in the past 24 hours.	OC3 Port, STS1	Sonet Far End Path Statistics History data	Number of unavailable seconds	sonetFarEndPathIntervalTable	SONET-MIB	No	SN04	Same as above
APS-MIB											
apsStatusTable											
apsStatusModeMismatches	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	A count of Mode Mismatch conditions. Modes other than 1+1 unidirectional monitor protection line K2 bit 5, which indicates the architecture and K2 bits 6-8, which indicate if the mode is unidirectional or bidirectional. A conflict between the current local mode and the received K2 mode information constitutes a mode mismatch	OC3 Protection Switch	APS Status Statistics : Current data	Number of Mode Mismatch conditions	apsStatusTable	APS-MIB	No	SN04	Connect the OC3 (fiber) to an ATM switch that does not support UNI Directional Non-revertive signaling (like the Bay switch).
apsChanStatusTable											
apsChanSignalDegrades	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	A count of Signal Degrade conditions. This condition occurs when the line Bit Error Rate exceeds the currently configured threshold.	OC3 Protection Switch	Active APS Channel Status Statistics : Current data Inactive APS Channel Status Statistics : Current data	Number of Signal Degrade conditions	apsChanStatusTable	APS-MIB	Yes	SN04	Inject bit error rates up to 10-5 on the active OC3 fiber using a test set (WNG ANT20).
apsChanSignalFailures	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	A count of Signal Failure conditions that have been detected on the incoming signal. This condition occurs when a loss of signal, loss of frame, AIS-L or a Line bit error rate exceeding 10 ⁻³ is detected on an incoming line.	OC3 Protection Switch	Active APS Channel Status Statistics : Current data Inactive APS Channel Status Statistics : Current data	Number of Signal Failure conditions	apsChanStatusTable	APS-MIB	Yes	SN04	Pull the active OC3 fiber or inject bit error rates up to 10 ⁻³ on the active OC3 fiber using a test set (WNG ANT20).
apsChanSwitchovers	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	The number of times this channel has switched to the protection line. When queried with index value apsChanNumber set to 0, which is the protection line, this object will return 0.	OC3 Protection Switch	Active APS Channel Status Statistics : Current data Inactive APS Channel Status Statistics : Current data	Number of times this channel was switched to the protection line	apsChanStatusTable	APS-MIB	Yes	SN04	Display this OM count. Cause a link (OC3) failure (remove cable) on the active fiber. Display this OM count again and it should be increased by one.
ATM-MIB											
atmInterfaceTCTable											
atmInterfaceOCDEvents	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	The number of times the Out of Cell Delineation (OCD) events occur. If seven consecutive ATM cells have a Header Error Control (HEC) violation, an OCD event occurs. A high number of OCD events may indicate a problem with the TC Sublayer.	ATM Interface	Interface Statistics : Current data	Cumulative OCD anomalies	atmInterfaceTCTable	ATM-MIB	No	SN04	Display this OM. Using a test set on the OC3 interface, create HEC violations. Display this OM again, it should have increased by the number of injected faults.
ATM2-MIB											
atmSigStatTable											
atmSigSSCOPConEvents	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	SSCOP Connection Events Counter.	ATM Interface	Signaling Statistics : Current data	SSCOP connection errors	atmSigStatTable	ATM2-MIB	No	SN04	SWACT the MG9000 DCC card. Increment will appear on newly active DCC as result of receiving BGIN pdu
atmSigSSCOPErrnPdus	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	SSCOP Errored PDUs Counter.	ATM Interface	Signaling statistics : Current data	SSCOP errored PDUs	atmSigStatTable	ATM2-MIB	No	SN04	Use Radcom protocol analyzer to inject invalid sscop PDU. Verify counter increments.
atmSigDetectSetupAttempts	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Call Setup Attempts Counter. This counter counts the number of call setup attempts (both successful and unsuccessful) detected on this interface.	ATM Interface	Signaling statistics : Current data	Incoming call/connection attempts	atmSigStatTable	ATM2-MIB	No	SN04	Display this OM, make an call to a line on this MG9000 from another MG9000, display count again. It will increase by the number of calls made
atmSigEmitSetupAttempts	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Call Setup Attempts Counter. This counter counts the number of call setup attempts (both successful and unsuccessful) transmitted on this interface.	ATM Interface	Signaling statistics : Current data	Outgoing call/connection attempts	atmSigStatTable	ATM2-MIB	No	SN04	Display this OM, make an call from this MG9000 to another MG9000, display count again. It will increase by the number of calls made
atmSigDetectUnavailRoutes	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Number of Route Unavailability detected on this interface.	ATM Interface	Signaling statistics : Current data	Unavailable outgoing routes	atmSigStatTable	ATM2-MIB	No	SN04	Display this OM. Setup a PLOA passive endpoint with an invalid destination AESA. Request a PLOA service to this endpoint. OM will increment.
atmSigEmitUnavailRoutes	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Number of Route Unavailability transmitted from this interface.	ATM Interface	Signaling Statistics : Current data	Unavailable incoming routes	atmSigStatTable	ATM2-MIB	No	SN04	Use Radcom protocol analyzer as a virtual endpoint to send SETUP msg to the MG9K with invalid AESA. Counter will increment.
atmSigDetectUnavailResrcs	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Number of Resource Unavailability detected on this interface.	ATM Interface	Signaling statistics : Current data	Resources unavailable messages received	atmSigStatTable	ATM2-MIB	No	SN04	Use Radcom protocol analyzer as a virtual endpoint to respond to MG9K SETUP msg with unavail resource cause code. Counter will increment.
atmSigEmitUnavailResrcs	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Number of Resource Unavailability transmitted from this interface.	ATM Interface	Signaling statistics : Current data	Resources unavailable messages transmitted	atmSigStatTable	ATM2-MIB	No	SN04	Use Radcom protocol analyzer as a virtual endpoint to send SETUP msg to MG9K with invalid IE bearer capability. Counter will increment.
atmSigDetectCldPyEvents	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Number of Called Party Responsible For Unsuccessful Call detected on this interface.	ATM Interface	Signaling Statistics : Current data	Called Party Events received	atmSigStatTable	ATM2-MIB	No	SN04	Use Radcom protocol analyzer as a virtual endpoint. Make call from MG9K to virtual endpoint already in use. Counter will increment.
atmSigEmitCldPyEvents	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Number of Called Party Responsible For Unsuccessful Call transmitted from this interface.	ATM Interface	Signaling statistics : Current data	Called Party Events transmitted	atmSigStatTable	ATM2-MIB	No	SN04	Use Radcom protocol analyzer as a virtual endpoint to send SETUP msg to MG9K to endpoint already in use. Counter will increment.
atmSigDetectMsgErrors	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Number of Incorrect Messages detected on this interface.	ATM Interface	Signaling Statistics : Current data	Incorrect messages received	atmSigStatTable	ATM2-MIB	No	SN04	Not possible to force condition without modifying software.
atmSigEmitMsgErrors	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Number of Incorrect Messages transmitted on this interface.	ATM Interface	Signaling statistics : Current data	Incorrect messages transmitted	atmSigStatTable	ATM2-MIB	No	SN04	Use Radcom protocol analyzer as a virtual endpoint to send SETUP msg to MG9K with missing IE. Counter will increment.
atmSigDetectCigPyEvents	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Number of Calling Party Events detected on this interface.	ATM Interface	Signaling statistics : Current data	Calling Party Events received	atmSigStatTable	ATM2-MIB	No	SN04	Not possible to force condition without modifying software.
atmSigEmitCigPyEvents	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Number of Calling Party Events transmitted from this interface.	ATM Interface	Signaling statistics : Current data	Calling Party Events transmitted	atmSigStatTable	ATM2-MIB	No	SN04	Use Radcom protocol analyzer as a virtual endpoint to send SETUP msg to MG9K with invalid IE bearer capability. Counter will increment.
atmSigDetectTimerExpires	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Number of Timer Expires detected on this interface.	ATM Interface	Signaling statistics : Current data	Timer Expiry events received	atmSigStatTable	ATM2-MIB	No	SN04	Not possible to force condition without modifying software.
atmSigEmitTimerExpires	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Number of Timer Expires transmitted from this interface.	ATM Interface	Signaling Statistics : Current data	Timer Expiry events transmitted	atmSigStatTable	ATM2-MIB	No	SN04	Not possible to force condition without modifying software.
atmSigDetectRestarts	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Number of Restart Activity errors detected on this interface.	ATM Interface	Signaling statistics : Current data	DSS2 Restarts received	atmSigStatTable	ATM2-MIB	No	SN04	Not possible to force condition without modifying software.
atmSigEmitRestarts	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Number of Restart Activity errors transmitted from this interface.	ATM Interface	Signaling statistics : Current data	DSS2 Restarts transmitted	atmSigStatTable	ATM2-MIB	No	SN04	Not possible to force condition without modifying software.
atmSigInEstabls	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Number of SVC VCCs established at this signaling entity for incoming connections.	ATM Interface	Signaling Statistics : Current data	InEstabls	atmSigStatTable	ATM2-MIB	No	SN04	Display this OM, make an call from a line on this MG9000 to another MG9000, display count again. It will increase by the number of calls made

atmSigOutEtabl	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Number of SVC VCCs established at this signaling entry for outgoing connections.	ATM Interface	Signaling Statistics : Current data	OutEtabl	atmSigStatTable	ATM2-MB	No	SN04	Display this OM, make an call to a line on this MG9000 from another MG9000, display count again. It will increase by the number of calls made
ATMF-CES-MIB											
atmCESStatsTable											
atmCESHdrErrors	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	The count of the number of AAL1 header errors detected, including those corrected. Header errors include correctable and uncorrectable CRC, plus bad parity.	AAL1	AAL1 Statistics : Current data	Number of header errors	atmCESStatsTable	ATMF-CES-MIB	No	SN04	On a PLoA (SVC) VPI & VCI, using a test set (e.g. Adtech), inject this error into AAL1 cell stream. The before and after counts should show a increase. For more accurate measurements keep track on the number (or duration) of the errors and check to see that they match.
atmCESPointerReframes	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	This records the count of the number of events in which the AAL1 reassembler found that an SDT pointer is not where it is expected, and the pointer must be readjusted. This count is only meaningful for structured CES modes, as unstructured CES modes do not use pointers. For unstructured CES modes, this count, if present, should indicate zero.	AAL1	AAL1 Statistics : Current data	Number of SDT pointer errors	atmCESStatsTable	ATMF-CES-MIB	No	SN04	Same as above
atmCESPointerParityErrors	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	This records the count of the number of events in which the AAL1 reassembler detects a parity check failure at the point where a structured data pointer is expected. This count is only meaningful for structured CES modes, as unstructured CES modes do not use pointers. For unstructured CES modes, this count, if present, should indicate zero.	AAL1	AAL1 Statistics : Current data	Number of parity check failures	atmCESStatsTable	ATMF-CES-MIB	No	SN04	Same as above
atmCESLostCells	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Number of lost cells, as detected by the AAL1 sequence number processing, for example. This records the count of the number of cells detected as lost in the network prior to the destination CES WFF AAL1 layer processing.	AAL1	AAL1 Statistics : Current data	Number of lost cells	atmCESStatsTable	ATMF-CES-MIB	No	SN04	Same as above
atmCESMisinsertedCells	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Number of AAL1 sequence violations which the AAL Convergence sublayer interprets as a misinserted cell, as defined by ITU-T 1.363.1.	AAL1	AAL1 Statistics : Current data	Number of misinserted cells	atmCESStatsTable	ATMF-CES-MIB	No	SN04	Same as above
atmCESBufUnderflows	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Number of buffer underflows. This records the count of the number of times the CES reassembly buffer underflows. In the case of a continuous underflow caused by a loss of ATM cell flow, a single buffer underflow should be counted. If the CES WFF is implemented with multiple buffers (such as a cell level buffer and a bit level buffer), then either buffer underflow will cause this count to be incremented.	AAL1	AAL1 Statistics : Current data	Number of reassembly buffer underflows	atmCESStatsTable	ATMF-CES-MIB	No	SN04	Same as above
atmCESBufOverflows	Counter32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Number of buffer overflows. This records the count of the number of times the CES reassembly buffer overflows, if the CES WFF is implemented with multiple buffers (such as a cell level buffer and a bit level buffer, then either buffer overflow will cause this count to be incremented.	AAL1	AAL1 Statistics : Current data	Number of reassembly buffer overflows	atmCESStatsTable	ATMF-CES-MIB	No	SN04	Same as above
NORTEL-UEMG-ATM-MIB											
nnAtmStatsIDataTable											
nnAtmStatsInOctets	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Total octets received on this interface	ATM Interface	Interface Statistics : Current data Interface Statistics : History data	incoming total cells X 53	nnAtmStatsIDataTable	NORTEL-UEMG-ATM-MIB	No	SN04	Display the current and all 96 intervals entries. This counter should always be increasing (over time). Using a PLoA or DSL Data line send data down that connection. Display these counters, with data traffic on the line the counts will increase a greater pace.
nnAtmStatsInErrors	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Total inbound errors	ATM Interface	Interface Statistics : Current data Interface Statistics : History data	uncorrectable HEC Errors	nnAtmStatsIDataTable	NORTEL-UEMG-ATM-MIB	No	SN04	On the OC3 interface, using a test set, inject this error. The before and after counts should show a increase. For more accurate measurements keep track on the number (or duration) of the errors and check to see that they match.
nnAtmStatsInProtoError	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Total incoming unknown/unsupported Protocol discards	ATM Interface	Interface Statistics : Current data Interface Statistics : History data	invalid cell headers	nnAtmStatsIDataTable	NORTEL-UEMG-ATM-MIB	No	SN04	Same as above
nnAtmStatsInOam	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Total incoming OAM cells.	ATM Interface	Interface Statistics : Current data Interface Statistics : History data	incoming OAM cells	nnAtmStatsIDataTable	NORTEL-UEMG-ATM-MIB	No	SN04	Activate Continuity Check on an active PLoA service. Display the current and all 96 intervals entries. This counter should always be increasing (over time)
nnAtmStatsOutOctets	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Total octets sent on this interface	ATM Interface	Interface Statistics : Current data Interface Statistics : History data	outgoing total cells X 53	nnAtmStatsIDataTable	NORTEL-UEMG-ATM-MIB	No	SN04	Display the current and all 96 intervals entries. This counter should always be increasing (over time). Using a PLoA or DSL Data line send data down that connection. Display these counters, with data traffic on the line the counts will increase a greater pace.
nnAtmStatsOutDiscards	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Total outbound errors	ATM Interface	Interface Statistics : Current data Interface Statistics : History data	outbound discarded	nnAtmStatsIDataTable	NORTEL-UEMG-ATM-MIB	No	SN04	Not possible to force condition without modifying software.
nnAtmStatsOutOam	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Total outgoing OAM cells.	ATM Interface	Interface Statistics : Current data Interface Statistics : History data	outgoing OAM cells	nnAtmStatsIDataTable	NORTEL-UEMG-ATM-MIB	No	SN04	Activate Continuity Check on an active PLoA service. Display the current and all 96 intervals entries. This counter should always be increasing (over time)
nnAtmStatsVcDataTable											
nnAtmStatsVclnTotal	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Total incoming cells (CLP = 01).	AAL1	ATM VCL Statistics : Current Data ATM VCL Statistics : History Data	incoming total cells	nnAtmStatsVcDataTable	NORTEL-UEMG-ATM-MIB	No	SN04	Display the current and all 96 intervals entries. This counter should always be increasing (over time). Using a PLoA or DSL Data line send data down that connection. Display these counters, with data traffic on the line the counts will increase a greater rate than without.
nnAtmStatsVchlTotalCip0	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Total incoming cells (CLP = 0)	AAL1	ATM VCL Statistics : Current Data ATM VCL Statistics : History Data	incoming cip0 cells	nnAtmStatsVcDataTable	NORTEL-UEMG-ATM-MIB	No	SN04	Same as above
nnAtmStatsVchlDiscarded	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Total incoming cells discarded (CLP = 01).	AAL1	ATM VCL Statistics : Current Data ATM VCL Statistics : History Data	incoming discard cells	nnAtmStatsVcDataTable	NORTEL-UEMG-ATM-MIB	No	SN04	Not possible to force condition without modifying software.
nnAtmStatsVchlDiscardedCip0	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Total incoming cells discarded (CLP = 0)	AAL1	ATM VCL Statistics : Current Data ATM VCL Statistics : History Data	incoming cip0 discards	nnAtmStatsVcDataTable	NORTEL-UEMG-ATM-MIB	No	SN04	Display the current and all 96 intervals entries. This counter should always be increasing (over time). Using a PLoA or DSL Data line send data down that connection. Display these counters, with data traffic on the line the counts will increase a greater rate than without.
nnAtmStatsVcOutTotal	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Total outgoing cells (CLP = 01).	AAL1	ATM VCL Statistics : Current Data ATM VCL Statistics : History Data	outgoing total cells	nnAtmStatsVcDataTable	NORTEL-UEMG-ATM-MIB	No	SN04	Same as above
nnAtmStatsVcOutTotalCip0	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Total outgoing cells (CLP = 0)	AAL1	ATM VCL Statistics : Current Data ATM VCL Statistics : History Data	outgoing cip0 cells	nnAtmStatsVcDataTable	NORTEL-UEMG-ATM-MIB	No	SN04	Same as above
nnAtmStatsVcOutTagged	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Total outgoing cells tagged (CLP = 0 -> CLP = 1).	AAL1	ATM VCL Statistics : Current Data ATM VCL Statistics : History Data	outgoing tagged cells	nnAtmStatsVcDataTable	NORTEL-UEMG-ATM-MIB	No	SN04	Not possible to force condition without modifying software.
nnAtmPmVcDataTable											
nnAtmPmVcFwImpBlk	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	forward impaired block.	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	FW impaired blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MIB	No	SN04	On a PLoA (SVC) activate Performance Monitoring. Using a test set (e.g. Adtech), inject this error. The before and after counts should show a increase. For more accurate measurements keep track on the number (or duration) of the errors and check to see that they match.

nnAtmPmVcFwSeCbkImp	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	forward lost/misinserted impaired block.	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	FW lost or misinserted impaired blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcFwSeCbkLat	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	forward severely errored cell block (lost).	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	FW lost severely errored cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcFwSeCbkMist	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	forward severely errored cell block (misinserted).	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	FW misinserted severely errored cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcFwSeCbkBvt	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	forward severely errored cell block - (BIP-16 violations).	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	FW BIP-16 violation severely errored cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcFwSeCbkComb	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	forward severely errored cell block combined.	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	FW combined severely errored cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcLWstClp01Cnt	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	forward lost CLP0+1 cell count.	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	FW lost CLP0 & 1 cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcFwLstClp0Cnt	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	forward lost CLP0 cell count.	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	FW lost CLP0 cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcFwMistClp01Cnt	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	forward misinserted CLP0+1 cell count.	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	FW misinserted CLP0 & 1 cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcFwErrCnt	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	forward errored cell count.	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	FW errored cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcFwTotalLstClp01Cnt	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	forward total lost CLP0+1 cell count.	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	FW total lost CLP0 & 1 cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcFwTotalLstClp0Cnt	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	forward total lost CLP0 cell count.	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	FW total lost CLP0 cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcBwImpBk	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	backward impaired block.	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	BW impaired blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcBwSeCbkImp	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	backward lost/misinserted impaired block.	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	BW lost or misinserted impaired blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcBwSeCbkLat	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	backward severely errored cell block (lost).	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	BW lost severely errored cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcBwSeCbkMist	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	backward severely errored cell block (misinserted).	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	BW misinserted severely errored cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcBwSeCbkBvt	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	backward severely errored cell block - (BIP-16 violations).	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	BW BIP-16 violation severely errored cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above

nnAtmPmVcBwSeCbkCombNsat	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	backward severely errored cell block combined(non-saturating).	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	BW non-saturating severely errored cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcBwLatCip01Cnt	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	backward lost CLP0+1 cell count.	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	BW lost CLP0 & 1 cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcBwLatCipCnt	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	backward lost CLP0 cell count.	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	BW lost CLP0 cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcBwMistCip01Cnt	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	backward misinserted CLP0+1 cell count.	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	BW misinserted CLP0 & 1 cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcBwErrCnt	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	backward errored cell count.	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	BW errored cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcBwTotalLatCip01Cnt	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	backward total lost CLP01 cell count.	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	BW total lost CLP0 & 1 cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcBwTotalLatCip0Cnt	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	backward total lost CLP0 cell count.	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	BW total lost CLP0 cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcTotalTransCip01Cnt	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	total transmitted CLP0+1 cell count.	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	Total transmitted CLP0 & 1 cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
nnAtmPmVcTotalTransCip0Cnt	Unsigned32	Count From Last Init up to 4,294,967,296 then it rolls over to 0	total transmitted CLP0 cell count.	AAL1	End-to-end PM: Current data End-to-end PM: History data Segment PM: Current data Segment PM: History data	Total transmitted CLP0 cell blocks	nnAtmPmVcDataTable	NORTEL-UEMG-ATM-MB	No	SN04	Same as above
ADSL-LINE-MIB											
adslAtucPerfDataTable											
adslAtucPerfCurr15MinLoss	PerCurrent Count	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Count of seconds in the current 15 minute interval when there was Loss of Framing.	XDSL Card	ATUC Performance: Current data	Number of seconds Lost of frame	adslAtucPerfDataTable	ADSL-LINE-MIB	No	SN04	Display this OM. Using a test set on the DSL Data interface, inject this error. Display this OM again, it should have increased by the number of injected faults.
adslAtucPerfCurr15MinLoss	PerCurrent Count	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Count of seconds in the current 15 minute interval when there was Loss of Signal.	XDSL Card	ATUC Performance: Current data	Number of seconds Lost of signal	adslAtucPerfDataTable	ADSL-LINE-MIB	No	SN04	Same as above
adslAtucPerfCurr15MinLoss	PerCurrent Count	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Count of seconds in the current 15 minute interval when there was Loss of Link.	XDSL Card	ATUC Performance: Current data	Number of seconds LOfs	adslAtucPerfDataTable	ADSL-LINE-MIB	No	SN04	Same as above
adslAtucPerfCurr15MinLprs	PerCurrent Count	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Count of seconds in the current 15 minute interval when there was Loss of Power.	XDSL Card	ATUC Performance: Current data	Number of seconds LPRs	adslAtucPerfDataTable	ADSL-LINE-MIB	No	SN04	Same as above
adslAtucPerfCurr15MinEss	PerCurrent Count	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Count of Errored Seconds in the current 15 minute interval. The errored second parameter is a count of one-second intervals containing one or more CRC anomalies or one or more los or sef defects.	XDSL Card	ATUC Performance: Current data	Number of seconds Ess	adslAtucPerfDataTable	ADSL-LINE-MIB	No	SN04	Same as above
adslAtucPerfCurr15MinInits	PerCurrent Count	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Count of the line initialization attempts in the current 15 minute interval. Includes both successful and failed attempts.	XDSL Card	ATUC Performance: Current data	Number of seconds Inits	adslAtucPerfDataTable	ADSL-LINE-MIB	No	SN04	Same as above
adslAturPerfDataTable											
adslAturPerfCurr15MinLoss	PerCurrent Count,	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Count of seconds in the current 15 minute interval when there was Loss of Framing.	XDSL Card	ATUR Performance: Current data	Number of seconds Lost of frame	adslAturPerfDataTable	ADSL-LINE-MIB	No	SN04	Display this OM. Using a test set on the DSL Data interface, inject this error. Display this OM again, it should have increased by the number of injected faults.
adslAturPerfCurr15MinLoss	PerCurrent Count,	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Count of seconds in the current 15 minute interval when there was Loss of Signal.	XDSL Card	ATUR Performance: Current data	Number of seconds Lost of signal	adslAturPerfDataTable	ADSL-LINE-MIB	No	SN04	Same as above
adslAturPerfCurr15MinLprs	PerCurrent Count,	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Count of seconds in the current 15 minute interval when there was Loss of Power.	XDSL Card	ATUR Performance: Current data	Number of seconds LPRs	adslAturPerfDataTable	ADSL-LINE-MIB	No	SN04	Same as above
adslAturPerfCurr15MinEss	PerCurrent Count,	Count From Last Init up to 4,294,967,296 then it rolls over to 0	Count of Errored Seconds in the current 15 minute interval. The errored second parameter is a count of one-second intervals containing one or more CRC anomalies, or one or more los or sef defects.	XDSL Card	ATUR Performance: Current data	Number of seconds Ess	adslAturPerfDataTable	ADSL-LINE-MIB	No	SN04	Same as above
adslAtucIntervalTable											
adslAtucPerfLoss	PerInterval Count	Counts only for last 15 min	Count of seconds in the interval when there was Loss of Framing.	XDSL Card	ATUC Interval: History data	Number of seconds Lost of frame	adslAtucIntervalTable	ADSL-LINE-MIB	No	SN04	Display all 96 OM entries. Using a test set on the DSL Data interface, inject this error over each interval. Display this OM again, it should have increased by the number of injected faults. Also ensure the counts have moved to the proper time interval after each 15 interval.
adslAtucPerfLoss	PerInterval Count	Counts only for last 15 min	Count of seconds in the interval when there was Loss of Signal.	XDSL Card	ATUC Interval: History data	Number of seconds Lost of signal	adslAtucIntervalTable	ADSL-LINE-MIB	No	SN04	Same as above
adslAtucPerfLoss	PerInterval Count	Counts only for last 15 min	Count of seconds in the interval when there was Loss of Link.	XDSL Card	ATUC Interval: History data	Number of seconds LOfs	adslAtucIntervalTable	ADSL-LINE-MIB	No	SN04	Same as above
adslAtucPerfLoss	PerInterval Count	Counts only for last 15 min	Count of seconds in the interval when there was Loss of Power.	XDSL Card	ATUC Interval: History data	Number of seconds LPRs	adslAtucIntervalTable	ADSL-LINE-MIB	No	SN04	Same as above

Appendix B, SN07 OSS Advance Feature Guide (IP) PLN-07IP-OSS Standard 01.04 December 2004

nnUemgDsAtucPerfNcd	Integer32	Counts only for last 15 min	Number of No Cell Delineation anomalies which on the ATUC channel during this interval.	XDSL Card	nnATUR Interval: History data	Number of No Cell Delineation	nnUemgDsAtucPerfTable	NORTEL-UEMG-ADSL-MIB	No	SN04	Same as above
nnUemgDsAtucPerfOcd	Integer32	Counts only for last 15 min	Number of Out of Cell Delineation anomalies which on the ATUC channel during this interval.	XDSL Card	nnATUR Interval: History data	Number of Out of Cell Delineation	nnUemgDsAtucPerfTable	NORTEL-UEMG-ADSL-MIB	No	SN04	Same as above
nnUemgDsAtucPerfHec	Integer32	Counts only for last 15 min	Number of Header Error Check anomalies which on the ATUC channel during this interval.	XDSL Card	nnATUR Interval: History data	Number of Header Error Check	nnUemgDsAtucPerfTable	NORTEL-UEMG-ADSL-MIB	No	SN04	Same as above
nnUemgDsAtucPerfLcd	Integer32	Counts only for last 15 min	Number of Loss of Cell Delineation anomalies on the ATUC channel during this interval.	XDSL Card	nnATUR Interval: History data	Number of Loss of Cell Delineation	nnUemgDsAtucPerfTable	NORTEL-UEMG-ADSL-MIB	No	SN04	Same as above
IMA-MIB (new in SN05)											
imaGroupCurrentTable											
imaGroupCurrentUnavailSecs	Gauge32	Counts since last 15 min interval	Count of one second intervals where the IMA Group Traffic State Machine is Down in current 15 minute interval	DS1IMAGroup	DS1 IMA Group Statistics: Current data	Group Unavailable Seconds	imaGroupCurrentTable	IMA-MIB	No	SN05	Display this OM, on the IMA card pull and replace the DS1 cable, display this count again. The count will be higher.
imaGroupCurrentNeNumFailures	Gauge32	Counts since last 15 min interval	The number of times a near-end group failure (Config-Aborted, Insufficient-Links) has been reported in current 15 minute interval	DS1IMAGroup	DS1 IMA Group Statistics: Current data	Group Near End Number of Failures	imaGroupCurrentTable	IMA-MIB	No	SN05	This OM cannot be externally invoked by a manual action. It will only occur if there is some HW or SW errors. The easiest way to generate is using the "fakelgprnm" command in the /hal/ima MG9K Dshell directory.
imaGroupCurrentFeNumFailures	Gauge32	Counts since last 15 min interval	The number of times a far-end group failure (Config-Aborted-FE, Insufficient-Links-FE, Blocked-FE) has been reported in current 15 minute interval. This is an optional attribute.	DS1IMAGroup	DS1 IMA Group Statistics: Current data	Group Far End Number of Failures	imaGroupCurrentTable	IMA-MIB	No	SN05	This OM cannot be externally invoked by a manual action. It will only occur if there is some HW or SW errors. The easiest way to generate is using the "fakelgprnm" command in the /hal/ima MG9K Dshell directory.
imaGroupIntervalTable											
imaGroupIntervalUnavailSecs	Gauge32	Counts since last 15 min interval	Count of one second intervals where the IMA Group Traffic State Machine is Down in one of the previous 96, individual 15 minute, intervals	DS1IMAGroup	DS1 IMA Group Statistics: History data	Group Unavailable Seconds	imaGroupIntervalTable	IMA-MIB	Yes	SN05	Display all 96 OM entries, on the IMA card pull and replace the DS1 cable, display these count again. The count will be higher for each interval the cable was pulled. Also ensure the counts have moved to the proper time interval after each 15 interval.
imaGroupIntervalNeNumFailures	Gauge32	Counts since last 15 min interval	The number of times a near-end group failure (Config-Aborted, Insufficient-Links) has been reported in one of the previous 96, individual 15 minute, intervals	DS1IMAGroup	DS1 IMA Group Statistics: History data	Group Near End Number of Failures	imaGroupIntervalTable	IMA-MIB	Yes	SN05	Same as above
imaGroupIntervalFeNumFailures	Gauge32	Counts since last 15 min interval	The number of times a far-end group failure (Config-Aborted-FE, Insufficient-Links-FE, Blocked-FE) has been reported in one of the previous 96, individual 15 minute, intervals. This is an optional attribute	DS1IMAGroup	DS1 IMA Group Statistics: History data	Group Far End Number of Failures	imaGroupIntervalTable	IMA-MIB	No	SN05	This OM cannot be externally invoked by a manual action. It will only occur if there is some HW or SW errors. The easiest way to generate is using the "fakelgprnm" command in the /hal/ima MG9K Dshell directory. Display all 96 OM entries
imaGroupTotalTable											
imaGroupTotalUnavailSecs	Gauge32	Rolling 24 hour total	Count of one second intervals where the IMA Group Traffic State Machine is Down in the previous 24 hour interval. Invalid 15 minute intervals count as 0.	DS1IMAGroup	DS1 IMA Group Statistics: 24-hour current data	Group Unavailable Seconds	imaGroupTotalTable	IMA-MIB	No	SN05	Display this OM, on the IMA card pull and replace the DS1 cable, display this count again. The count will be higher.
imaGroupTotalNeNumFailures	Gauge32	Rolling 24 hour total	The number of times a near-end group failure (Config-Aborted, Insufficient-Links) has been reported in the previous 24 hour interval. Invalid 15 minute intervals count as 0.	DS1IMAGroup	DS1 IMA Group Statistics: 24-hour current data	Group Near End Number of Failures	imaGroupTotalTable	IMA-MIB	No	SN05	This OM cannot be externally invoked by a manual action. It will only occur if there is some HW or SW errors. The easiest way to generate is using the "fakelgprnm" command in the /hal/ima MG9K Dshell directory.
imaGroupTotalFeNumFailures	Gauge32	Rolling 24 hour total	The number of times a far-end group failure (Config-Aborted-FE, Insufficient-Links-FE, Blocked-FE) has been reported in the previous 24 hour interval. Invalid 15 minute intervals count as 0. This is an optional attribute	DS1IMAGroup	DS1 IMA Group Statistics: 24-hour current data	Group Far End Number of Failures	imaGroupTotalTable	IMA-MIB	No	SN05	This OM cannot be externally invoked by a manual action. It will only occur if there is some HW or SW errors. The easiest way to generate is using the "fakelgprnm" command in the /hal/ima MG9K Dshell directory.
imaLinkCurrentTable											
imaLinkCurrentIaViolations	Gauge32	Counts since last 15 min interval	ICP violations: count of errored, invalid or missing ICP cells, except during SES-IMA or UAS-IMA conditions, in the current 15 minute interval	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Ima Violations	imaLinkCurrentTable	IMA-MIB	No	SN05	Display this OM, on the IMA card pull and replace the DS1 cable, display this count again. The count will be higher.
imaLinkCurrentOfAnomalies	Gauge32	Counts since last 15 min interval	The number of OIF anomalies, except during SES-IMA or UAS-IMA conditions, at the near-end in the current 15 minute interval. This is an optional attribute	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Of Anomalies	imaLinkCurrentTable	IMA-MIB	No	SN05	Same as above
imaLinkCurrentNeSevErroredSecs	Gauge32	Counts since last 15 min interval	Count of one second intervals containing >= 30% of the ICP cells counted as W-IMA, or one or more link defects (e.g., LOS, LOF, LOF, AIS, or LCD), LIF defects, or LODS defects, except during UAS-IMA condition, in the current 15 minute interval	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Ne Sev Errored Secs	imaLinkCurrentTable	IMA-MIB	No	SN05	This OM cannot be externally invoked by a manual action. It will only occur if there is some HW or SW errors. The easiest way to generate is using the "fakelgprnm" command in the /hal/ima MG9K Dshell directory.
imaLinkCurrentFeSevErroredSecs	Gauge32	Counts since last 15 min interval	Count of one second intervals containing one or more RDI-IMA defects, except during UAS-IMA-FE condition, in the current 15 minute interval	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Fe Sev Errored Secs	imaLinkCurrentTable	IMA-MIB	No	SN05	Display this OM, on the IMA card pull and replace the DS1 cable, display this count again. The count will be higher.
imaLinkCurrentNeUnavailSecs	Gauge32	Counts since last 15 min interval	Count of unavailable seconds at near-end in the current 15 minute interval: unavailability begins at the onset of 10 contiguous SES-IMA and ends at the onset of 10 contiguous seconds with no SES-IMA	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Ne Unavail Secs	imaLinkCurrentTable	IMA-MIB	No	SN05	Same as above
imaLinkCurrentFeUnavailSecs	Gauge32	Counts since last 15 min interval	Count of unavailable seconds at far-end in the current 15 minute interval: unavailability begins at the onset of 10 contiguous SES-IMA-FE and ends at the onset of 10 contiguous seconds with no SES-IMA-FE	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Fe Unavail Secs	imaLinkCurrentTable	IMA-MIB	No	SN05	This OM cannot be externally invoked by a manual action. It will only occur if there is some HW or SW errors. The easiest way to generate is using the "fakelgprnm" command in the /hal/ima MG9K Dshell directory.
imaLinkCurrentNeTxUnusableSecs	Gauge32	Counts since last 15 min interval	Tx Unusable seconds: count of Unusable seconds at the near-end Tx LSM in the current 15 minute interval	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Ne Tx Unusable Secs	imaLinkCurrentTable	IMA-MIB	No	SN05	Display this OM, on the IMA card pull and replace the DS1 cable, display this count again. The count will be higher.
imaLinkCurrentNeRxUnusableSecs	Gauge32	Counts since last 15 min interval	Rx Unusable seconds: count of Unusable seconds at the near-end Rx LSM in the current 15 minute interval	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Ne Rx Unusable Secs	imaLinkCurrentTable	IMA-MIB	No	SN05	Same as above
imaLinkCurrentFeTxUnusableSecs	Gauge32	Counts since last 15 min interval	Tx Unusable seconds at far-end: count of seconds with Tx Unusable indications from the far-end Tx LSM in the current 15 minute interval	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Fe Tx Unusable Secs	imaLinkCurrentTable	IMA-MIB	No	SN05	Same as above
imaLinkCurrentFeRxUnusableSecs	Gauge32	Counts since last 15 min interval	Rx Unusable seconds at far-end: count of seconds with Rx Unusable indications from the far-end Rx LSM in the current 15 minute interval	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Fe Rx Unusable Secs	imaLinkCurrentTable	IMA-MIB	No	SN05	Same as above
imaLinkCurrentNeTxNumFailures	Gauge32	Counts since last 15 min interval	The number of times a near-end transmit failure alarm condition has been entered on this link (i.e., some form of implementation specific transmit fault) in the current 15 minute interval	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Ne Tx Num Failures	imaLinkCurrentTable	IMA-MIB	No	SN05	Same as above
imaLinkCurrentNeRxNumFailures	Gauge32	Counts since last 15 min interval	The number of times a near-end receive failure alarm condition has been entered on this link (i.e., LIF, LODS, RFI-IMA, Mis-Connected, or some form of implementation specific receive fault) in the current 15 minute interval	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Ne Rx Num Failures	imaLinkCurrentTable	IMA-MIB	No	SN05	Same as above
imaLinkCurrentFeTxNumFailures	Gauge32	Counts since last 15 min interval	The number of times a far-end transmit failure alarm condition has been entered on this link (i.e., Tx-Unusable-FE) in the current 15 minute interval. This is an optional attribute	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Fe Tx Num Failures	imaLinkCurrentTable	IMA-MIB	No	SN05	Same as above
imaLinkCurrentFeRxNumFailures	Gauge32	Counts since last 15 min interval	The number of times a far-end receive failure alarm condition has been entered on this link (i.e., Rx-Unusable-FE) in the current 15 minute interval. This is an optional attribute	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Fe Rx Num Failures	imaLinkCurrentTable	IMA-MIB	No	SN05	Same as above
imaLinkCurrentTxStuffs	Gauge32	Counts since last 15 min interval	Count of stuff events inserted in the transmit direction in the current 15 minute interval. This is an optional attribute	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Tx Stuffs	imaLinkCurrentTable	IMA-MIB	No	SN05	Display this OM, it should be non-zero, wait a short time, display count again. This count will be higher. This will not increase if the link is offline and disabled.
imaLinkCurrentRxStuffs	Gauge32	Counts since last 15 min interval	Count of stuff events detected in the receive direction in the current 15 minute interval. This is an optional attribute	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Rx Stuffs	imaLinkCurrentTable	IMA-MIB	No	SN05	Same as above
imaLinkIntervalTable											
imaLinkIntervalIaViolations	Gauge32	Counts only for last 15 min	ICP violations: count of errored, invalid or missing ICP cells, except during SES-IMA or UAS-IMA conditions, in one of the previous 96, individual 15 minute, intervals	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Ima Violations	imaLinkIntervalTable	IMA-MIB	Yes	SN05	Display all 96 OM entries, on the IMA card pull and replace the DS1 cable, display these count again. The count will be higher for each interval the cable was pulled. Also ensure the counts have moved to the proper time interval after each 15 interval.
imaLinkIntervalOfAnomalies	Gauge32	Counts only for last 15 min	The number of OIF anomalies, except during SES-IMA or UAS-IMA conditions, at the near-end in one of the previous 96, individual 15 minute, intervals. This is an optional attribute	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link OIF Anomalies	imaLinkIntervalTable	IMA-MIB	Yes	SN05	Same as above

imaLinkIntervalNeSevErroredSecs	Gauge32	Counts only for last 15 min	Count of one second intervals containing >= 30% of the ICP cells counted as IV-IMAs, or one or more link defects (e.g., LOS, OOF/LOF, AIS, or LOD), LIF defects, or LODS defects, except during UAS-IMA condition, in one of the previous 96, individual 15 minute, intervals	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Ne Sev Errored Secs	imaLinkIntervalTable	IMA-MIB	Yes	SN05	This OM cannot be externally invoked by a manual action. It will only occur if there is some HW or SW errors. The easiest way to generate is using the "fakelgppm" command in the /hal/ima MG9K Dshall directory. Display all 96 OM entries
imaLinkIntervalFeSevErroredSecs	Gauge32	Counts only for last 15 min	Count of one second intervals containing one or more RDI-IMA defects, except during UAS-IMA-FE condition, in one of the previous 96, individual 15 minute, intervals	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Fe Sev Errored Secs	imaLinkIntervalTable	IMA-MIB	No	SN05	Display all 96 OM entries, on the IMA card pull and replace the DS1 cable, display these count again. The count will be higher for each interval the cable was pulled. Also ensure the counts have moved to the proper time interval after each 15 interval.
imaLinkIntervalNeUnavailSecs	Gauge32	Counts only for last 15 min	Count of unavailable seconds at near-end in one of the previous 96, individual 15 minute, intervals: unavailability begins at the onset of 10 contiguous SES-IMA and ends at the onset of 10 contiguous seconds with no SES-IMA	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Ne Unavail Secs	imaLinkIntervalTable	IMA-MIB	Yes	SN05	Same as above
imaLinkIntervalFeUnavailSecs	Gauge32	Counts only for last 15 min	Count of unavailable seconds at far-end in one of the previous 96, individual 15 minute, intervals: unavailability begins at the onset of 10 contiguous SES-IMA-FE and ends at the onset of 10 contiguous seconds with no SES-IMA-FE	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Fe Unavail Secs	imaLinkIntervalTable	IMA-MIB	No	SN05	This OM cannot be externally invoked by a manual action. It will only occur if there is some HW or SW errors. The easiest way to generate is using the "fakelgppm" command in the /hal/ima MG9K Dshall directory. Display all 96 OM entries
imaLinkIntervalNeTxUnusableSecs	Gauge32	Counts only for last 15 min	Tx Unusable seconds: count of Unusable seconds at the near-end Tx LSM in one of the previous 96, individual 15 minute, intervals	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Ne Tx Unusable Secs	imaLinkIntervalTable	IMA-MIB	Yes	SN05	Display all 96 OM entries, on the IMA card pull and replace the DS1 cable, display these count again. The count will be higher for each interval the cable was pulled. Also ensure the counts have moved to the proper time interval after each 15 interval.
imaLinkIntervalNeRxUnusableSecs	Gauge32	Counts only for last 15 min	Rx Unusable seconds: count of Unusable seconds at the near-end Rx LSM in one of the previous 96, individual 15 minute, intervals	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Ne Rx Unusable Secs	imaLinkIntervalTable	IMA-MIB	Yes	SN05	Same as above
imaLinkIntervalFeTxUnusableSecs	Gauge32	Counts only for last 15 min	Tx Unusable seconds at far-end: count of seconds with Tx Unusable indications from the far-end Tx LSM in one of the previous 96, individual 15 minute, intervals	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Fe Tx Unusable Secs	imaLinkIntervalTable	IMA-MIB	No	SN05	Same as above
imaLinkIntervalFeRxUnusableSecs	Gauge32	Counts only for last 15 min	Rx Unusable seconds at far-end: count of seconds with Rx Unusable indications from the far-end Rx LSM in one of the previous 96, individual 15 minute, intervals	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Fe Rx Unusable Secs	imaLinkIntervalTable	IMA-MIB	No	SN05	Same as above
imaLinkIntervalNeTxNumFailures	Gauge32	Counts only for last 15 min	The number of times a near-end transmit failure alarm condition has been entered on this link (i.e., some form of implementation specific transmit fault) in one of the previous 96, individual 15 minute, intervals	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Ne Tx Num Failures	imaLinkIntervalTable	IMA-MIB	Yes	SN05	Same as above
imaLinkIntervalNeRxNumFailures	Gauge32	Counts only for last 15 min	The number of times a near-end receive failure alarm condition has been entered on this link (i.e., LIF, LODS, RFI-IMA, Mis-Connected, or some form of implementation specific receive fault) in one of the previous 96, individual 15 minute, intervals	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Ne Rx Num Failures	imaLinkIntervalTable	IMA-MIB	Yes	SN05	Same as above
imaLinkIntervalFeTxNumFailures	Gauge32	Counts only for last 15 min	The number of times a far-end transmit failure alarm condition has been entered on this link (i.e., Tx-Unusable-FE) in one of the previous 96, individual 15 minute, intervals. This is an optional attribute	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Fe Tx Num Failures	imaLinkIntervalTable	IMA-MIB	No	SN05	Same as above
imaLinkIntervalFeRxNumFailures	Gauge32	Counts only for last 15 min	The number of times a far-end receive failure alarm condition has been entered on this link (i.e., Rx-Unusable-FE) in one of the previous 96, individual 15 minute, intervals. This is an optional attribute	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Fe Rx Num Failures	imaLinkIntervalTable	IMA-MIB	No	SN05	Same as above
imaLinkIntervalTxStuffs	Gauge32	Counts only for last 15 min	Count of stuff events inserted in the transmit direction in one of the previous 96, individual 15 minute, intervals. This is an optional attribute	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Tx Stuffs	imaLinkIntervalTable	IMA-MIB	Yes	SN05	Display all 96 OM entries, it should be non-zero, wait 20 min, display counts again. These count will move up to next interval and current will replace first entry. This will not increase if the link is offline and disabled.
imaLinkIntervalRxStuffs	Gauge32	Counts only for last 15 min	Count of stuff events detected in the receive direction in one of the previous 96, individual 15 minute, intervals. This is an optional attribute	DS1IAMLink	DS1 IMA Link Statistics: Current Data	Link Rx Stuffs	imaLinkIntervalTable	IMA-MIB	Yes	SN05	Same as above
imaLinkTotalTable											
imaLinkTotalmaViolations	Gauge32	Rolling 24 hour total	ICP violations: count of errored, invalid or missing ICP cells, except during SES-IMA or UAS-IMA conditions, in the previous 24 hour interval	DS1IAMLink	DS1 IMA Link Statistics: 24-hour Current Data	Link Ima Violations	imaLinkTotalTable	IMA-MIB	No	SN05	Display this OM, on the IMA card pull and replace the DS1 cable, display this count again. The count will be higher.
imaLinkTotalOifAnomalies	Gauge32	Rolling 24 hour total	The number of OIF anomalies, except during SES-IMA or UAS-IMA conditions, at the near-end in the previous 24 hour interval. This is an optional attribute	DS1IAMLink	DS1 IMA Link Statistics: 24-hour Current Data	Link OIF Anomalies	imaLinkTotalTable	IMA-MIB	No	SN05	Same as above
imaLinkTotalNeSevErroredSecs	Gauge32	Rolling 24 hour total	Count of one second intervals containing >= 30% of the ICP cells counted as IV-IMAs, or one or more link defects (e.g., LOS, OOF/LOF, AIS, or LOD), LIF defects, or LODS defects, except during UAS-IMA condition, in the previous 24 hour interval	DS1IAMLink	DS1 IMA Link Statistics: 24-hour Current Data	Link Ne Sev Errored Secs	imaLinkTotalTable	IMA-MIB	No	SN05	This OM cannot be externally invoked by a manual action. It will only occur if there is some HW or SW errors. The easiest way to generate is using the "fakelgppm" command in the /hal/ima MG9K Dshall directory.
imaLinkTotalFeSevErroredSecs	Gauge32	Rolling 24 hour total	Count of one second intervals containing one or more RDI-IMA defects, except during UAS-IMA-FE condition, in the previous 24 hour interval	DS1IAMLink	DS1 IMA Link Statistics: 24-hour Current Data	Link Fe Sev Errored Secs	imaLinkTotalTable	IMA-MIB	No	SN05	Display this OM, on the IMA card pull and replace the DS1 cable, display this count again. The count will be higher.
imaLinkTotalNeUnavailSecs	Gauge32	Rolling 24 hour total	Count of unavailable seconds at near-end in the previous 24 hour interval: unavailability begins at the onset of 10 contiguous SES-IMA and ends at the onset of 10 contiguous seconds with no SES-IMA	DS1IAMLink	DS1 IMA Link Statistics: 24-hour Current Data	Link Ne Unavail Secs	imaLinkTotalTable	IMA-MIB	No	SN05	Same as above
imaLinkTotalFeUnavailSecs	Gauge32	Rolling 24 hour total	Count of unavailable seconds at far-end in the previous 24 hour interval: unavailability begins at the onset of 10 contiguous SES-IMA-FE and ends at the onset of 10 contiguous seconds with no SES-IMA-FE	DS1IAMLink	DS1 IMA Link Statistics: 24-hour Current Data	Link Fe Unavail Secs	imaLinkTotalTable	IMA-MIB	No	SN05	This OM cannot be externally invoked by a manual action. It will only occur if there is some HW or SW errors. The easiest way to generate is using the "fakelgppm" command in the /hal/ima MG9K Dshall directory.
imaLinkTotalNeTxUnusableSecs	Gauge32	Rolling 24 hour total	Tx Unusable seconds: count of Unusable seconds at the near-end Tx LSM in the previous 24 hour interval	DS1IAMLink	DS1 IMA Link Statistics: 24-hour Current Data	Link Ne Tx Unusable Secs	imaLinkTotalTable	IMA-MIB	No	SN05	Display this OM, on the IMA card pull and replace the DS1 cable, display this count again. The count will be higher.
imaLinkTotalNeRxUnusableSecs	Gauge32	Rolling 24 hour total	Rx Unusable seconds: count of Unusable seconds at the near-end Rx LSM in the previous 24 hour interval	DS1IAMLink	DS1 IMA Link Statistics: 24-hour Current Data	Link Ne Rx Unusable Secs	imaLinkTotalTable	IMA-MIB	No	SN05	Same as above
imaLinkTotalFeTxUnusableSecs	Gauge32	Rolling 24 hour total	Tx Unusable seconds at far-end: count of seconds with Tx Unusable indications from the far-end Tx LSM in the previous 24 hour interval	DS1IAMLink	DS1 IMA Link Statistics: 24-hour Current Data	Link Fe Tx Unusable Secs	imaLinkTotalTable	IMA-MIB	No	SN05	Same as above
imaLinkTotalFeRxUnusableSecs	Gauge32	Rolling 24 hour total	Rx Unusable seconds at far-end: count of seconds with Rx Unusable indications from the far-end Rx LSM in the previous 24 hour interval	DS1IAMLink	DS1 IMA Link Statistics: 24-hour Current Data	Link Fe Rx Unusable Secs	imaLinkTotalTable	IMA-MIB	No	SN05	Same as above
imaLinkTotalNeTxNumFailures	Gauge32	Rolling 24 hour total	The number of times a near-end transmit failure alarm condition has been entered on this link (i.e., some form of implementation specific transmit fault) in the previous 24 hour interval	DS1IAMLink	DS1 IMA Link Statistics: 24-hour Current Data	Link Ne Tx Num Failures	imaLinkTotalTable	IMA-MIB	No	SN05	Same as above
imaLinkTotalNeRxNumFailures	Gauge32	Rolling 24 hour total	The number of times a near-end receive failure alarm condition has been entered on this link (i.e., LIF, LODS, RFI-IMA, Mis-Connected, or some form of implementation specific receive fault) in the previous 24 hour interval	DS1IAMLink	DS1 IMA Link Statistics: 24-hour Current Data	Link Ne Rx Num Failures	imaLinkTotalTable	IMA-MIB	No	SN05	Same as above
imaLinkTotalFeTxNumFailures	Gauge32	Rolling 24 hour total	The number of times a far-end transmit failure alarm condition has been entered on this link (i.e., Tx-Unusable-FE) in the previous 24 hour interval. This is an optional attribute	DS1IAMLink	DS1 IMA Link Statistics: 24-hour Current Data	Link Fe Tx Num Failures	imaLinkTotalTable	IMA-MIB	No	SN05	Same as above
imaLinkTotalFeRxNumFailures	Gauge32	Rolling 24 hour total	The number of times a far-end receive failure alarm condition has been entered on this link (i.e., Rx-Unusable-FE) in the previous 24 hour interval. This is an optional attribute	DS1IAMLink	DS1 IMA Link Statistics: 24-hour Current Data	Link Fe Rx Num Failures	imaLinkTotalTable	IMA-MIB	No	SN05	Same as above
imaLinkTotalTxStuffs	Gauge32	Rolling 24 hour total	Count of stuff events inserted in the transmit direction in the previous 24 hour interval. This is an optional attribute	DS1IAMLink	DS1 IMA Link Statistics: 24-hour Current Data	Link Tx Stuffs	imaLinkTotalTable	IMA-MIB	No	SN05	Display this OM, it should be non-zero, wait a short time, display count again. This count will be higher. This will not increase if the link is offline and disabled.
imaLinkTotalRxStuffs	Gauge32	Rolling 24 hour total	Count of stuff events detected in the receive direction in the previous 24 hour interval. This is an optional attribute	DS1IAMLink	DS1 IMA Link Statistics: 24-hour Current Data	Link Rx Stuffs	imaLinkTotalTable	IMA-MIB	No	SN05	Same as above
UEMO-PERFMON-MIB											

nnPmUtilOmRecentTable			This table contains measurements of CPU, Ram, Flash and Channel Usage. Measurements in this table are rolling (peak and average values) on the most recent 15 minutes.								
nnPmUtilRecentCpuPeak	Integer	Counts only for current 15 min	Peak CPU Occupancy (as a percentage of usage)	ITP, OC3, IMA, ITX, DS1, and ABI Card	Performance Utilization Statistics: Current data	Peak CPU Occupancy	nnPmUtilOmRecentTable	UEMG-PERFMON-MIB	No	SN06	Since these are usage measurements they will always change over time. Collect a measurement when the system is quite. Generate different levels of CallP traffic. Collect measurements on each card (every 15 min) and insure the values increase as usage increases.
nnPmUtilRecentCpuAvg	Integer	Counts only for current 15 min	Average CPU Occupancy (as a percentage of usage)	ITP, OC3, IMA, ITX, DS1, and ABI Card	Performance Utilization Statistics: Current data	Average CPU Occupancy	nnPmUtilOmRecentTable	UEMG-PERFMON-MIB	No	SN06	Same as above
nnPmUtilRecentRamPeak	Integer	Counts only for current 15 min	Peak RAM Usage (as a percentage of usage)	ITP, OC3, IMA, ITX, DS1, and ABI Card	Performance Utilization Statistics: Current data	Peak RAM Usage	nnPmUtilOmRecentTable	UEMG-PERFMON-MIB	No	SN06	Same as above
nnPmUtilRecentRamAvg	Integer	Counts only for current 15 min	Average RAM Usage (as a percentage of usage)	ITP, OC3, IMA, ITX, DS1, and ABI Card	Performance Utilization Statistics: Current data	Average RAM Usage	nnPmUtilOmRecentTable	UEMG-PERFMON-MIB	No	SN06	Same as above
nnPmUtilRecentFlashPeak	Integer	Counts only for current 15 min	Peak Flash Memory Usage (as a percentage of usage)	ITP, OC3, IMA, ITX, DS1, and ABI Card	Performance Utilization Statistics: Current data	Peak Flash Usage	nnPmUtilOmRecentTable	UEMG-PERFMON-MIB	No	SN06	Same as above
nnPmUtilRecentFlashAvg	Integer	Counts only for current 15 min	Average Flash Memory Usage (as a percentage of usage)	ITP, OC3, IMA, ITX, DS1, and ABI Card	Performance Utilization Statistics: Current data	Average Flash Usage	nnPmUtilOmRecentTable	UEMG-PERFMON-MIB	No	SN06	Same as above
nnPmUtilRecentChanPeak	Integer	Counts only for current 15 min	Peak Channel Usage (as a percentage of usage)	ITP, OC3, IMA, ITX, DS1, and ABI Card	Performance Utilization Statistics: Current data	Peak Channel Usage	nnPmUtilOmRecentTable	UEMG-PERFMON-MIB	No	SN06	Same as above
nnPmUtilRecentChanAvg	Integer	Counts only for current 15 min	Average Channel Usage (as a percentage of usage)	ITP, OC3, IMA, ITX, DS1, and ABI Card	Performance Utilization Statistics: Current data	Average Channel Usage	nnPmUtilOmRecentTable	UEMG-PERFMON-MIB	No	SN06	Same as above
nnPmUtilOmIntervTable			This table contains history measurements of CPU, Ram, Flash and Channel Usage. Measurements in this table are rolling (peak and average values) of each 15 minute interval up to 24 hours old.								
nnPmUtilIntervCpuPeak	Integer	Counts only for last 15 min	Peak CPU Occupancy (as a percentage of usage)	ITP, OC3, IMA, ITX, DS1, and ABI Card	Performance Utilization Statistics: History data	Peak CPU Occupancy	nnPmUtilOmIntervTable	UEMG-PERFMON-MIB	Yes	SN06	Since these are usage measurements they will always change over time. Collect a measurement when the system is quite. Generate different levels of CallP traffic. Collect measurements on each card (every 15 min) and insure the values increase as usage increases. Also insure that the counts move to the next interval every 15 min.
nnPmUtilIntervCpuAvg	Integer	Counts only for last 15 min	Average CPU Occupancy (as a percentage of usage)	ITP, OC3, IMA, ITX, DS1, and ABI Card	Performance Utilization Statistics: History data	Average CPU Occupancy	nnPmUtilOmIntervTable	UEMG-PERFMON-MIB	Yes	SN06	Same as above
nnPmUtilIntervRamPeak	Integer	Counts only for last 15 min	Peak RAM Usage (as a percentage of usage)	ITP, OC3, IMA, ITX, DS1, and ABI Card	Performance Utilization Statistics: History data	Peak RAM Usage	nnPmUtilOmIntervTable	UEMG-PERFMON-MIB	Yes	SN06	Same as above
nnPmUtilIntervRamAvg	Integer	Counts only for last 15 min	Average RAM Usage (as a percentage of usage)	ITP, OC3, IMA, ITX, DS1, and ABI Card	Performance Utilization Statistics: History data	Average RAM Usage	nnPmUtilOmIntervTable	UEMG-PERFMON-MIB	Yes	SN06	Same as above
nnPmUtilRecentFlashPeak	Integer	Counts only for last 15 min	Peak Flash Memory Usage (as a percentage of usage)	ITP, OC3, IMA, ITX, DS1, and ABI Card	Performance Utilization Statistics: History data	Peak Flash Usage	nnPmUtilOmIntervTable	UEMG-PERFMON-MIB	Yes	SN06	Same as above
nnPmUtilRecentFlashAvg	Integer	Counts only for last 15 min	Average Flash Memory Usage (as a percentage of usage)	ITP, OC3, IMA, ITX, DS1, and ABI Card	Performance Utilization Statistics: History data	Average Flash Usage	nnPmUtilOmIntervTable	UEMG-PERFMON-MIB	Yes	SN06	Same as above
nnPmUtilRecentChanPeak	Integer	Counts only for last 15 min	Peak Channel Usage (as a percentage of usage)	ITP, OC3, IMA, ITX, DS1, and ABI Card	Performance Utilization Statistics: History data	Peak Channel Usage	nnPmUtilOmIntervTable	UEMG-PERFMON-MIB	Yes	SN06	Same as above
nnPmUtilRecentChanAvg	Integer	Counts only for last 15 min	Average Channel Usage (as a percentage of usage)	ITP, OC3, IMA, ITX, DS1, and ABI Card	Performance Utilization Statistics: History data	Average Channel Usage	nnPmUtilOmIntervTable	UEMG-PERFMON-MIB	Yes	SN06	Same as above
nnPmSmpRecentRequestsPeak	Integer32	Counts only for current 15 min	The Peak number of SNMP Requests/PDUs in the most recent 15 minutes. These are accumulated on 1-minute cycles.	OC3 and IMA Card	SNMP Messaging Current Data	Peak number of SNMP Requests	N/A	UEMG-PERFMON-MIB	No	SN06	Since these are usage measurements they will always change over time. Collect a measurement when the system is quite. Generate different levels of OAM&P traffic. Collect measurements (every 15 min) and insure the values increase as usage increases.
nnPmSmpRecentRequestsAvg	Integer32	Counts only for current 15 min	The average number of SNMP Requests/PDUs in the most recent 15 minutes. These are accumulated on 1-minute cycles. Thus, the avg is the average of the last 15 x 1-minute cycles.	OC3 and IMA Card	SNMP Messaging Current Data	Average number of SNMP Requests	N/A	UEMG-PERFMON-MIB	No	SN06	Same as above
nnPmSmpRecentNotifsPeak	Integer32	Counts only for current 15 min	The Peak number of SNMP Notifications sent in the most recent 15 minutes. These are accumulated on 1-minute cycles.	OC3 and IMA Card	SNMP Messaging Current Data	Peak number of SNMP Notifications	N/A	UEMG-PERFMON-MIB	No	SN06	Same as above
nnPmSmpRecentNotifsAvg	Integer32	Counts only for current 15 min	The average number of SNMP Notifications sent in the most recent 15 minutes. These are accumulated on 1-minute cycles. Thus, the average is the average of the last 15 x 1-minute cycles.	OC3 and IMA Card	SNMP Messaging Current Data	Average number of SNMP Notifications	N/A	UEMG-PERFMON-MIB	No	SN06	Same as above
nnPmSmpOmIntervTable			This table contains measurements of SNMP requests and events. Measurements in this table are rolling (peak and average values) of each 15 minute interval up to 24 hours old.								
nnPmSmpIntervReqPeak	Integer32	Counts only for last 15 min	The Peak number of SNMP Requests/PDUs in the most Recent 15 mins. These are accumulated on 1-minute cycles.	OC3 and IMA Card	SNMP Messaging History Data	Peak number of SNMP Requests	nnPmSmpOmIntervTable	UEMG-PERFMON-MIB	Yes	SN06	Since these are usage measurements they will always change over time. Collect a measurement when the system is quite. Generate different levels of OAM&P traffic. Collect measurements (every 15 min) and insure the values increase as usage increases. Also insure that the counts move to the next interval every 15 min.
nnPmSmpIntervReqAvg	Integer32	Counts only for last 15 min	The Avg number of SNMP Requests/PDUs in the most Recent 15 mins. These are accumulated on 1-minute cycles. Thus, the avg is the avg of the last 15x 1-minute cycles. Precision is tenths, thus 816 is 81.6	OC3 and IMA Card	SNMP Messaging History Data	Average number of SNMP Requests	nnPmSmpOmIntervTable	UEMG-PERFMON-MIB	Yes	SN06	Same as above
nnPmSmpIntervNotifPeak	Integer32	Counts only for last 15 min	The Peak number of SNMP Notifications in the most Recent 15 mins. These are accumulated on 1-minute cycles.	OC3 and IMA Card	SNMP Messaging History Data	Peak number of SNMP Notifications	nnPmSmpOmIntervTable	UEMG-PERFMON-MIB	Yes	SN06	Same as above
nnPmSmpIntervNotifAvg	Integer32	Counts only for last 15 min	The Avg number of SNMP Notifications sent in the most Recent 15 mins. These are accumulated on 1-minute cycles. Thus, the avg is the avg of the last 15x 1-minute cycle. Precision is tenths, thus 816 is 81.6	OC3 and IMA Card	SNMP Messaging History Data	Average number of SNMP Notifications	nnPmSmpOmIntervTable	UEMG-PERFMON-MIB	Yes	SN06	Same as above
nnPmOvldRscDccIntervTable								UEMG-PERFMON-MIB			
nnPmOvldRscDccIntervPduRatePeak	Integer32	Counts only for last 15 min	Peak # received AAL5 PDUs per sec for this 15 minute interval	OC3 and IMA Card	DCC Overload Interval Statistics: History Data	Peak number of received AAL5 PDUs per second	nnPmOvldRscDccIntervTable	UEMG-PERFMON-MIB	Yes	SN06.2	
nnPmOvldRscDccIntervPduRateAvg	Integer32	Counts only for last 15 min	Avg num recvd AAL5 PDUs per sec for this 15 minute interval	OC3 and IMA Card	DCC Overload Interval Statistics: History Data	Average number of recd AAL5 PDUs per second	nnPmOvldRscDccIntervTable	UEMG-PERFMON-MIB	Yes	SN06.2	
nnPmOvldRscDccIntervCbwMgRPeak	NnPerfMon Hundredths	Counts only for last 15 min	Peak recvd conn request msgs per sec for this 15 minute interval	OC3 and IMA Card	DCC Overload Interval Statistics: History Data	Peak received conn request msgs per second	nnPmOvldRscDccIntervTable	UEMG-PERFMON-MIB	Yes	SN06.2	
nnPmOvldRscDccIntervCbwMgRAvg	NnPerfMon Hundredths	Counts only for last 15 min	Avg conn request msgs per sec for this 15 minute interval	OC3 and IMA Card	DCC Overload Interval Statistics: History Data	Average connection request messages per second	nnPmOvldRscDccIntervTable	UEMG-PERFMON-MIB	Yes	SN06.2	
nnPmOvldRscDccIntervConnQDelPeak	NnPerfMon Hundredths	Counts only for last 15 min	Milliseconds...peak time a connRequest is pending in its queue for this 15 minute interval	OC3 and IMA Card	DCC Overload Interval Statistics: History Data	Peak time in milliseconds a connRequest is pending in its queue	nnPmOvldRscDccIntervTable	UEMG-PERFMON-MIB	Yes	SN06.2	
nnPmOvldRscDccIntervConnQDelAvg	NnPerfMon Hundredths	Counts only for last 15 min	Milliseconds...Avg time a connRequest is pending in its queue for this 15 minute interval	OC3 and IMA Card	DCC Overload Interval Statistics: History Data	Ave time in milliseconds a connRequest is pending in its queue	nnPmOvldRscDccIntervTable	UEMG-PERFMON-MIB	Yes	SN06.2	

nnPmOvldRscDccIntervCpuUtilPeak	NrPerfMon Percent	Counts only for last 15 min	Peak cpu occupancy for this 15 minute interval	OC3 and IMA Card	DCC Overload Interval Statistics: History Data	Peak CPU Occupancy	nnPmOvldRscDccIntervTable	UEMG-PERFMON-MIB	Yes	SN06.2	
nnPmOvldRscDccIntervCpuUtilAvg	NrPerfMon Percent	Counts only for last 15 min	Avg cpu occupancy this 15 minute interval	OC3 and IMA Card	DCC Overload Interval Statistics: History Data	Average CPU Occupancy	nnPmOvldRscDccIntervTable	UEMG-PERFMON-MIB	Yes	SN06.2	
nnPmOvldConnDenyIntervTable											
nnPmOvldConnDenyIntervCoun	Integer32	Counts only for last 15 min	Count of the number of Connection requests Denied for this 15 minute interval	OC3 and IMA Card	DCC Overload Conn Deny Statistics: History Data	Number of Connection requests Denied	nnPmOvldConnDenyIntervTable	UEMG-PERFMON-MIB	Yes	SN06.2	
DS3-MIB											
dsx3CurrentTable											
dsx3CurrentPESs	PerfCurrent Count	Counts since last 15 min interval	The counter associated with the number of P - bit Errored Seconds encountered by a SONET (STS1 with DS3 payload selected) Section in the current 15 minute interval.	STS1	DS3 Path Statistics: Current Data	P-bit Number of errored seconds	dsx3CurrentTable	DS3 - MIB	No	SN07	On the OC3 connect a test box that has the ability to inject errors (e.g. ADTECH). With out injecting any errors collect the OM and it should be 0. Inject toward the near-end OC3 the error and collect the OM and it should reflect the correct error count.
dsx3CurrentPSEs	PerfCurrent Count	Counts since last 15 min interval	The counter associated with the number of P - bit Severely Errored Seconds encountered by a SONET (STS1 with DS3 payload selected) Section in the current 15 minute interval.	STS1	DS3 Path Statistics: Current Data	P-bit Number of severely errored seconds	dsx3CurrentTable	DS3 - MIB	No	SN07	Same as above
dsx3CurrentSEFs	PerfCurrent Count	Counts since last 15 min interval	The counter associated with the number of Severely Errored Framing Seconds encountered by a SONET (STS1 with DS3 payload selected) Section in the current 15 minute interval.	STS1	DS3 Path Statistics: Current Data	Number of severely errored seconds	dsx3CurrentTable	DS3 - MIB	No	SN07	Same as above
dsx3CurrentUASs	PerfCurrent Count	Counts since last 15 min interval	The counter associated with the number of Unavailable Seconds encountered by a SONET (STS1 with DS3 payload selected) Section in the current 15 minute interval.	STS1	DS3 Path Statistics: Current Data	Number of unavailable seconds	dsx3CurrentTable	DS3 - MIB	No	SN07	Same as above
dsx3CurrentPCVs	PerfCurrent Count	Counts since last 15 min interval	The counter associated with the number of P - bit Coding Violations encountered by a SONET (STS1 with DS3 payload selected) Section in the current 15 minute interval.	STS1	DS3 Path Statistics: Current Data	P-bit Number of coding violations	dsx3CurrentTable	DS3 - MIB	No	SN07	Same as above
dsx3CurrentCCVs	PerfCurrent Count	Counts since last 15 min interval	The counter associated with the number of C - bit Coding Violations encountered by a SONET (STS1 with DS3 payload selected) Section in the current 15 minute interval.	STS1	DS3 Path Statistics: Current Data	C-bit Number of coding violations	dsx3CurrentTable	DS3 - MIB	No	SN07	Same as above
dsx3CurrentCESs	PerfCurrent Count	Counts since last 15 min interval	The counter associated with the number of C - bit Errored Seconds encountered by a SONET (STS1 with DS3 payload selected) Section in the current 15 minute interval.	STS1	DS3 Path Statistics: Current Data	C-bit Number of errored seconds	dsx3CurrentTable	DS3 - MIB	No	SN07	Same as above
dsx3CurrentCSEs	PerfCurrent Count	Counts since last 15 min interval	The counter associated with the number of C - bit Severely Errored Seconds encountered by a SONET (STS1 with DS3 payload selected) Section in the current 15 minute interval.	STS1	DS3 Path Statistics: Current Data	C-bit Number of severely errored seconds	dsx3CurrentTable	DS3 - MIB	No	SN07	Same as above
dsx3IntervalTable											
dsx3IntervalPESs	PerfInterval Count	Counts only for last 15 min	The counter associated with the number of P - bit Errored Seconds encountered by a SONET (STS1 with DS3 payload selected) Section in the current 15 minute interval.	STS1	DS3 Path Statistics: History Data	P-bit Number of errored seconds	dsx3IntervalTable	DS3 - MIB	No	SN07	On the OC3 connect a test box that has the ability to inject errors (e.g. ADTECH). With out injecting any errors collect the OM and it should be 0. Inject toward the near-end OC3 the error and collect the OM and it should reflect the correct error count. Collect all 96 intervals, waiting 15-minutes between tests, the counts will move to a higher interval each 15 minutes.
dsx3IntervalPSEs	PerfInterval Count	Counts only for last 15 min	The counter associated with the number of P - bit Severely Errored Seconds encountered by a SONET (STS1 with DS3 payload selected) Section in the current 15 minute interval in the past 24 hours.	STS1	DS3 Path Statistics: History Data	P-bit Number of severely errored seconds	dsx3IntervalTable	DS3 - MIB	No	SN07	Same as above
dsx3IntervalSEFs	PerfInterval Count	Counts only for last 15 min	The counter associated with the number of Severely Errored Framing Seconds encountered by a SONET (STS1 with DS3 payload selected) Section in the current 15 minute interval in the past 24 hours.	STS1	DS3 Path Statistics: History Data	Number of severely errored seconds	dsx3IntervalTable	DS3 - MIB	No	SN07	Same as above
dsx3IntervalUASs	PerfInterval Count	Counts only for last 15 min	The counter associated with the number of Unavailable Seconds encountered by a SONET (STS1 with DS3 payload selected) Section in the current 15 minute interval in the past 24 hours.	STS1	DS3 Path Statistics: History Data	Number of unavailable seconds	dsx3IntervalTable	DS3 - MIB	No	SN07	Same as above
dsx3IntervalPCVs	PerfInterval Count	Counts only for last 15 min	The counter associated with the number of P - bit Coding Violations encountered by a SONET (STS1 with DS3 payload selected) Section in the current 15 minute interval in the past 24 hours.	STS1	DS3 Path Statistics: History Data	P-bit Number of coding violations	dsx3IntervalTable	DS3 - MIB	No	SN07	Same as above
dsx3IntervalCCVs	PerfInterval Count	Counts only for last 15 min	The counter associated with the number of C - bit Coding Violations encountered by a SONET (STS1 with DS3 payload selected) Section in the current 15 minute interval in the past 24 hours.	STS1	DS3 Path Statistics: History Data	C-bit Number of coding violations	dsx3IntervalTable	DS3 - MIB	No	SN07	Same as above
dsx3IntervalCESs	PerfInterval Count	Counts only for last 15 min	The counter associated with the number of C - bit Errored Seconds encountered by a SONET (STS1 with DS3 payload selected) Section in the current 15 minute interval.	STS1	DS3 Path Statistics: History Data	C-bit Number of errored seconds	dsx3IntervalTable	DS3 - MIB	No	SN07	Same as above
dsx3IntervalCSEs	PerfInterval Count	Counts only for last 15 min	The counter associated with the number of C - bit Severely Errored Seconds encountered by a SONET (STS1 with DS3 payload selected) Section in the current 15 minute interval in the past 24 hours.	STS1	DS3 Path Statistics: History Data	C-bit Number of severely errored seconds	dsx3IntervalTable	DS3 - MIB	No	SN07	Same as above
dsx3FarEndCurrentTable											
dsx3FarEndCurrentCESs	PerfCurrent Count	Counts since last 15 min interval	The counter associated with the number of FarEnd Errored Seconds encountered by a SONET (STS1 with DS3 payload selected) interface in the current 15 minute interval.	STS1	DS3 FarEndPath Statistics: Current Data	Number of errored seconds	dsx3FarEndCurrentTable	DS3 - MIB	No	SN07	On the OC3 connect a test box that has the ability to inject errors (e.g. ADTECH). With out injecting any errors collect the OM and it should be 0. Inject toward the far-end OC3 the error and collect the OM and it should reflect the correct error count.
dsx3FarEndCurrentCSEs	PerfCurrent Count	Counts since last 15 min interval	The counter associated with the number of Far End Severely Errored Seconds encountered by a SONET (STS1 with DS3 payload selected) Path interface in the current 15 minute interval.	STS1	DS3 FarEndPath Statistics: Current Data	Number of severely errored seconds	dsx3FarEndCurrentTable	DS3 - MIB	No	SN07	Same as above
dsx3FarEndCurrentCCVs	PerfCurrent Count	Counts since last 15 min interval	The counter associated with the number of Far End Coding Violations reported via the far end block error count encountered by a SONET (STS1 with DS3 payload selected) Path interface in the current 15 minute interval.	STS1	DS3 FarEndPath Statistics: Current Data	Number of coding violations	dsx3FarEndCurrentTable	DS3 - MIB	No	SN07	Same as above
dsx3FarEndCurrentUASs	PerfCurrent Count	Counts since last 15 min interval	The counter associated with the number of Far End Unavailable Seconds encountered by a SONET (STS1 with DS3 payload selected) Path interface in the current 15 minute interval.	STS1	DS3 FarEndPath Statistics: Current Data	Number of unavailable seconds	dsx3FarEndCurrentTable	DS3 - MIB	No	SN07	Same as above
dsx3FarEndIntervalTable											
dsx3FarEndIntervalCESs	PerfInterval Count	Counts only for last 15 min	The counter associated with the number of Far End Errored Seconds encountered by a SONET (STS1 with DS3 payload selected) Path interface in a particular 15-minute interval in the past 24 hours.	STS1	Sonet Far End Path Statistics: History data	Number of errored seconds	dsx3FarEndIntervalTable	DS3 - MIB	No	SN07	On the OC3 channel connect a test box that has the ability to inject errors (e.g. ADTECH). With out injecting any errors collect the OM and it should be 0. Inject toward the Far-end OC3 the error and collect the OM and it should reflect the correct error count. Collect all 96 intervals, waiting 15-minutes between tests, the counts will move to a higher interval each 15 minutes.
dsx3FarEndIntervalCSEs	PerfInterval Count	Counts only for last 15 min	The counter associated with the number of Far End Severely Errored Seconds encountered by a SONET (STS1 with DS3 payload selected) Path interface in a particular 15-minute interval in the past 24 hours.	STS1	Sonet Far End Path Statistics: History data	Number of severely errored seconds	dsx3FarEndIntervalTable	DS3 - MIB	No	SN07	Same as above
dsx3FarEndIntervalCCVs	PerfInterval Count	Counts only for last 15 min	The counter associated with the number of Far End Coding Violations reported via the far end block error count encountered by a SONET (STS1 with DS3 payload selected) Path interface in a particular 15-minute interval in the past 24 hours.	STS1	Sonet Far End Path Statistics: History data	Number of coding violations	dsx3FarEndIntervalTable	DS3 - MIB	No	SN07	Same as above
dsx3FarEndIntervalUASs	PerfInterval Count	Counts only for last 15 min	The counter associated with the number of Far End Unavailable Seconds encountered by a SONET (STS1 with DS3 payload selected) Path interface in a particular 15-minute interval in the past 24 hours.	STS1	Sonet Far End Path Statistics: History data	Number of unavailable seconds	dsx3FarEndIntervalTable	DS3 - MIB	No	SN07	Same as above
NORTEL-UEMG-RELMSGING-MIB											
nnRelMsgSctpAssocOmCurrTable											
nnRelMsgSctpAssocOmCurrClosed	Unsigned32	Counts only for last 15 min	number of times that this association closed (both aborts and shutdowns)				nnRelMsgSctpAssocOmCurrTable	NORTEL-UEMG-RELMSGING-MIB	No	SN07	

nnRelMsgSctpAscCurrAbort	Unsigned32	Counts only for last 15 min	number of times that this association aborted.				nnRelMsgSctpAssocOmCurr Table	NORTEL-UEMG-RELMMSGING-MIB	No	SN07	
nnRelMsgSctpAscCurrOutPacks	Unsigned32	Counts only for last 15 min	number of packets transmitted				nnRelMsgSctpAssocOmCurr Table	NORTEL-UEMG-RELMMSGING-MIB	No	SN07	
nnRelMsgSctpAscCurrInPacks	Unsigned32	Counts only for last 15 min	number of packets received, this association				nnRelMsgSctpAssocOmCurr Table	NORTEL-UEMG-RELMMSGING-MIB	No	SN07	
nnRelMsgSctpAscCurrDiscPacks	Unsigned32	Counts only for last 15 min	number of packets discarded by this association.				nnRelMsgSctpAssocOmCurr Table	NORTEL-UEMG-RELMMSGING-MIBNo	No	SN07	
nnRelMsgSctpAscCurrRetranPacks	Unsigned32	Counts only for last 15 min	number of packets retransmitted by this association, this interval				nnRelMsgSctpAssocOmCurr Table	NORTEL-UEMG-RELMMSGING-MIB	No	SN07	
nnRelMsgSctpAscCurrT1expires	Unsigned32	Counts only for last 15 min	number of T1 Expires				nnRelMsgSctpAssocOmCurr Table	NORTEL-UEMG-RELMMSGING-MIB	No	SN07	
nnRelMsgSctpAscCurrT2expires	Unsigned32	Counts only for last 15 min	number of T2 expires.				nnRelMsgSctpAssocOmCurr Table	NORTEL-UEMG-RELMMSGING-MIB	No	SN07	
nnRelMsgSctpAscCurrT3expires	Unsigned32	Counts only for last 15 min	number of T3 expires				nnRelMsgSctpAssocOmCurr Table	NORTEL-UEMG-RELMMSGING-MIB	No	SN07	
nnRelMsgSctpAscCurrCongCount	Unsigned32	Counts only for last 15 min	number of times this assoc entered congestion.				nnRelMsgSctpAssocOmCurr Table	NORTEL-UEMG-RELMMSGING-MIB	No	SN07	
nnRelMsgSctpAscCurrCongCleared	Unsigned32	Counts only for last 15 min	number of times congestion cleared by audit.				nnRelMsgSctpAssocOmCurr Table	NORTEL-UEMG-RELMMSGING-MIB	No	SN07	
nnRelMsgSctpAssocOminervTable											
nnRelMsgSctpAscIntervClosed	Unsigned32	Counts only for last 15 min	number of times that this association closed (both aborts and shutdowns)				nnRelMsgSctpAssocOminerv Table	NORTEL-UEMG-RELMMSGING-MIB	Yes	SN07	
nnRelMsgSctpAscIntervAbort	Unsigned32	Counts only for last 15 min	number of times that this association aborted.				nnRelMsgSctpAssocOminerv Table	NORTEL-UEMG-RELMMSGING-MIB	Yes	SN07	
nnRelMsgSctpAscIntervOutPacks	Unsigned32	Counts only for last 15 min	number of packets transmitted				nnRelMsgSctpAssocOminerv Table	NORTEL-UEMG-RELMMSGING-MIB	Yes	SN07	
nnRelMsgSctpAscIntervInPacks	Unsigned32	Counts only for last 15 min	number of packets received, this association				nnRelMsgSctpAssocOminerv Table	NORTEL-UEMG-RELMMSGING-MIB	Yes	SN07	
nnRelMsgSctpAscIntervDiscPacks	Unsigned32	Counts only for last 15 min	number of packets discarded by this association.				nnRelMsgSctpAssocOminerv Table	NORTEL-UEMG-RELMMSGING-MIB	Yes	SN07	
nnRelMsgSctpAscIntervRetranPacks	Unsigned32	Counts only for last 15 min	number of packets retransmitted by this association, this interval				nnRelMsgSctpAssocOminerv Table	NORTEL-UEMG-RELMMSGING-MIB	Yes	SN07	
nnRelMsgSctpAscIntervT1expires	Unsigned32	Counts only for last 15 min	number of T1 Expires				nnRelMsgSctpAssocOminerv Table	NORTEL-UEMG-RELMMSGING-MIB	Yes	SN07	
nnRelMsgSctpAscIntervT2expires	Unsigned32	Counts only for last 15 min	number of T2 expires.				nnRelMsgSctpAssocOminerv Table	NORTEL-UEMG-RELMMSGING-MIB	Yes	SN07	
nnRelMsgSctpAscIntervT3expires	Unsigned32	Counts only for last 15 min	number of T3 expires				nnRelMsgSctpAssocOminerv Table	NORTEL-UEMG-RELMMSGING-MIB	Yes	SN07	
nnRelMsgSctpAscIntervCongCount	Unsigned32	Counts only for last 15 min	number of times this assoc entered congestion.				nnRelMsgSctpAssocOminerv Table	NORTEL-UEMG-RELMMSGING-MIB	Yes	SN07	
nnRelMsgSctpAscIntervCongCleared	Unsigned32	Counts only for last 15 min	number of times congestion cleared by audit.				nnRelMsgSctpAssocOminerv Table	NORTEL-UEMG-RELMMSGING-MIB	Yes	SN07	

Appendix C: Succession VOA/IP Passport 15000 and Preside MDM Alarm Log Summary

Introduction

This document provides a list of Passport 15000 (PP15000), Passport Voice Gateway (PVG) and Preside Multiservice Data Manager (MDM) alarm logs applicable to up to Succession SN06.2 for Voice over ATM (VOA) and Voice over IP (VOIP) solutions. This document supercedes the PP15000/MDM portions of [1], which contains alarm logs applicable to pre-SN04 Succession releases.

The purpose of this document includes:

- It provides a Succession VOA/VOIP customer (and more specifically an OSS Fault application writer) a summarized subset of the possible alarms that can appear when PP15000 and MDM are configured for the Succession VOA/VOIP application. The descriptions of the alarms are found in [3] and [4].
- When configured to receive PP15000/MDM Alarm logs in SCC2 format from the Supernode Data Manager (SDM), it also provides the mapping information needed to interpret the SCC2 format.
- It is also input to solution-level OSS Guide information which is in progress of being delivered to provide this information in the FCAPS-based solution documentation.

SCC2 Log Format

The SCC2 log report for Passport and MDM alarms comprises a one line header, followed by seven lines of body text, as per the following example:

```
37 PPEM300 8169 TBL
time: 2002 01 11 15 37 06
event: clear
compld: EM P15KF LP 7 SONET 3
severity: cleared
faultCode: 70115201
alarmType: communications
commentData: Loss of frame condition has been cleared.
```

The header is of format:

```
aabbccdddeeeffgghhijjj
```

Each field, as applicable for Passport and MDM alarms, is described in Table 1.

Table 1 Passport 15000 and MDM SCC2 Header Field Description

Field	Description	Applicable Log Values
aa	Alarm severity Passport/MDM alarm log severity	"*C" = critical alarm "***" = major alarm "* " = minor and warning and indeterminate alarm " " = clear alarm Two characters, left justified, padded with blanks.

Field	Description	Applicable Log Values
bb	Minute indicator Two numeric character indicator representing the minutes after the hour. Generated by SDM at time SDM receives the alarm log from MDM.	Ranges from 00 to 59, right justified, padded with zeros.
c	single space	" "
dddd	Log Name Assigned by SDM. Based upon the first four digits ("Index Group") of the eight-digit Passport or MDM alarm identifier.	Four characters, left justified, padded with blanks. "CA " for index group 0000. "PPEM" for index groups beginning with 70xx and some fault codes in group 0999. "MDM " for index groups beginning with 30xx and some fault codes in group 0999.
eee	Log Number Three numeric characters representing the Passport or MDM Alarm Type. Note that the Alarm Type "debug" is not translated as a fault, but rather as information log.	"300" = communications "301" = quality of service "302" = processing "303" = equipment "304" = environmental "305" = security "306" = operator "307" = unknown
f	A single space for all Passport and MDM alarm logs.	" "
gg	Global Sequence Number Generated by SDM. Two numeric characters, incremented by SDM upon receipt of every alarm log.	Ranges from 00 to 99, right justified, padded with zeros.
hh	Device Sequence Number Generated by SDM. Two numeric characters, incremented by SDM upon receipt of every device specific alarm log from MDM (originated by Passport or MDM).	Ranges from 00 to 99, right justified, padded with zeros.
i	single space	" "
jjjj	Event Type Assigned by SDM. String assigned for all Passport and MDM alarm logs.	"TBL " Four characters, left justified, padded with blanks.
Lines 2, 3, 4, 5, 6, 7, 8	Body Text Seven textual lines, each of form <AlarmFieldName>: <AlarmFieldValue>	"time: " "event: " "compld: " "severity: " "faultCode: " "alarmType: " "commentData: " Comment data is truncated so that entire log does not exceed 900 bytes.

Passport 15000 Alarm Logs

Table 2 presents the list of Passport set/clear alarm logs that are applicable for Succession VOA/VOIP.

Table 2 does not explicitly state all Passport clear alarm logs that correspond to each set. The SCC2 header for the clear differs from its corresponding set by only the first two characters. The characters “aa” are replaced by “ ” (two spaces). This format is presented in Table 1.

The Passport alarm identifier consists of an eight-digit number identifying the alarm. The first four digits comprise the **Index Group**, which represents logical groupings of alarms. The last four digits are the **SubIndex**, which is an identifier within each index group.

Component Name indicates the managed object against which the alarm Log is generated. This table contains the CLI format of a component name. The “compld” field in SCC2 format contains this information (with the module’s <nodename> pre-pended). Also, “compld” follows the MDM API-style format (with component type and instance separated by a space instead of a slash, and ‘\$’ appearing in place of a null instance value). Variables (usually instance value ranges) are denoted by <> and the reader should reference the Alarms NTP’s [3] and [4] for further information.

Table 2 Passport 15000 Set/Clear Alarms Supported for Succession

Passport Index Group	Component Name	PP/PVG configuration (N/A)	Passport SubIndex	Importance Category (N/A)	SCC2 Header
0000	OSI administrative state changes, general engineering and memory alarms, internal software error detected, etc.				
	This alarm can apply to many Passport components.		0000		bb CA eee gghh TBL where: eee = 302, 303, 306
	This alarm can apply to many Passport components.		1000		aabb CA eee gghh TBL where: aa = “*C”, “**”, “*” eee = 300, 306
	This alarm can apply to many Passport components.		1001		aabb CA 303 gghh TBL where: aa = “*C”, “**”, “*”
	This alarm can apply to many Passport components.		3000		aabb CA eee gghh TBL where: aa = “*C”, “**”, “*” eee = 300, 302
	This alarm can apply to many Passport components.		3001 3002		aabb CA 302 gghh TBL where: aa = “*C”, “**”, “*”
7000	Provisioning alarms. These alarms apply to failures resulting from provisioning attempts. e.g., loading a provisioning file has failed.				
	Prov		0007		aabb PPEM306 gghh TBL where: aa = “*C”, “**”, “*”

Passport Index Group	Component Name	PP/PVG configuration (N/A)	Passport Subindex	Importance Category (N/A)	SCC2 Header
	This alarm can apply to many Passport components.		0010		* bb PPEM302 gghh TBL
	Prov Migration		0033		aabb PPEM306 gghh TBL where: aa = “*C”, “*”
	Prov		0036		aabb PPEM301 gghh TBL where: aa = “*”, “*”
	Prov		0037		*Cbb PPEM301 gghh TBL
	Prov		0038		* bb PPEM301 gghh TBL
	Prov		0040		**bb PPEM302 gghh TBL
	Provisioning Patch		0041		* bb PPEM306 gghh TBL
7002	Backplane control system alarms; e.g., communication failure between a card and the backplane. Note: FabricCard instance range (<i>): X, Y Card instance range (<n>): 0-15				
	Shelf FabricCard/<i>		0002		**bb PPEM303 gghh TBL
	Shelf FabricCard/<i>		0003		* bb PPEM303 gghh TBL
	Shelf FabricCard/<i>		0005		**bb PPEM302 gghh TBL
	Shelf FabricCard/<i>		0006		**bb PPEM302 gghh TBL
	Shelf FabricCard/<i>		0007		**bb PPEM302 gghh TBL
	Shelf Card/<n>		0008		* bb PPEM303 gghh TBL
	Shelf FabricCard/<i>		0009		* bb PPEM303 gghh TBL
7003	Data collection system alarms; e.g., an alarm or log queue size has exceeded a threshold. Collector instance range (<t>): accounting, alarm, log, debug, scn, trap, stats, rtstats, appl Agent instance range (<n>): 0-15 LP instance range (<n>): 0-15				
	Collector/<t> Agent/<n>		0001		**bb PPEM301 gghh TBL
	Collector/<t> Spooler		0002		**bb PPEM302 gghh TBL
	Collector/<t> Spooler		0003		* bb PPEM301 gghh TBL
	LP/<n> Eng AAList		0007		**bb PPEM301 gghh TBL
	Collector/<t> Spooler		0008		* bb PPEM306 gghh TBL

Passport Index Group	Component Name	PP/PVG configuration (N/A)	Passport Subindex	Importance Category (N/A)	SCC2 Header
7008	File system alarms. Disk instance range (<n>): 0-1 Card instance range (<x>): 0-1				
	FileSystem		1001		**bb PPEM302 gghh TBL
	FileSystem		1002		*Cbb PPEM302 gghh TBL
	FileSystem		1004		*Cbb PPEM303 gghh TBL
	FileSystem		1005		* bb PPEM303 gghh TBL
	FileSystem		1006		**bb PPEM302 gghh TBL
	FileSystem Disk/<n>		1008		**bb PPEM303 gghh TBL
			1009		
			1010		
			1011		
	FileSystem		1019		* bb PPEM303 gghh TBL
7011	Port management system and Automatic Protection Switching alarms. LP instance range (<n>): 0-15 Port types (<type>): Sonet, EDS1, DS3, BridgedSonet(Bso), Ethernet, Sdh Sonet instance range (<n2>): 0-15 (16-port); 0-3 (4-port) EDS1 instance range (<n2>): 0-1 IMA instance range (<n3>): 0-13 LK instance range (<n4>): 0-31 DS3 instance range (<n2>): 0-3 (4-port); 0-11 (12-port) DS1 instance range (<n3>): 1-28 Ethernet instance range (<n2>): 0-3 LAPS instance range (<n>): 0-15999 Chan instance range (<n4>): 0-23 Bso instance range (<n2>): 0-15 Pbg instance range (<n>): 0-15999 Sdh instance range (<n2>): 0-3 Sts instance range (<n2>): 0-2 Lag instance range (<y>): 0-7 Lag link instance range (<z>): 0-31				
	LP/<n> DS3/<n2> IMA <n3>		1100		*Cbb PPEM300 gghh TBL
	LP/<n> DS3/<n2> IMA/<n3>... ...LK/<n4>		1200		*Cbb PPEM300 gghh TBL
			1210		
			1211		
			1212		
			1213		
			1214		
			1215		
			1216		
	LP/<n> Lag/<y>		1500		*Cbb PPEM300 gghh TBL

Passport Index Group	Component Name	PP/PVG configuration (N/A)	Passport Subindex	Importance Category (N/A)	SCC2 Header
	LP/<n> Lag/<y> Link/<z>		1501		*Cbb PPEM300 gghh TBL
	LP/<n> <type>/<n2>		2000		*Cbb PPEM303 gghh TBL
	LP/0 EDS1/<n2> LP/<n> DS3/<n2> DS1/<n3> Lp/<n> Sdh/<n2> Vc4/0 Vc12/{1-3,1-7,1-3} E1 Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} DS1		5000		*Cbb PPEM300 gghh TBL
	LP/0 EDS1/<n2> LP/<n> DS3/<n2> DS1/<n3> Lp/<n> Sdh/<n2> Vc4/0 Vc12/{1-3,1-7,1-3} E1 Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} DS1		5001		* bb PPEM300 gghh TBL
	LP/0 EDS1/<n2> Lp/<n> Sdh/<n2> Vc4/0 Vc12/{1-3,1-7,1-3} E1 Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} DS1		5002		*Cbb PPEM300 gghh TBL
	LP/<n> DS3/<n2> DS1/<n3> Lp/<n> Sdh/<n2> Vc4/0 Vc12/{1-3,1-7,1-3} E1 Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} DS1		5003		*Cbb PPEM300 gghh TBL
	LP/<n> DS3/<n2> DS1/<n3> Lp/<n> Sdh/<n2> Vc4/0 Vc12/{1-3,1-7,1-3} E1 Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} DS1		5004		*Cbb PPEM300 gghh TBL
	LP/<n> DS3/<n2> DS1/<n3> Lp/<n> Sdh/<n2> Vc4/0 Vc12/{1-3,1-7,1-3} E1 Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} DS1		5005		*Cbb PPEM300 gghh TBL
	LP/<n> DS3/<n2> DS1/<n3> Lp/<n> Sdh/<n2> Vc4/0 Vc12/{1-3,1-7,1-3} E1 Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} DS1		5006		**bb PPEM300 gghh TBL
	LP/<n> DS3/<n2> DS1/<n3> Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} DS1 Lp/<n> Sdh/<n2> Vc4/0 Vc12/{1-3,1-7,1-3} E1		5010		* bb PPEM300 gghh TBL
	LP/<n> DS3/<n2> DS1/<n3>		5011		* bb PPEM300 gghh TBL

Passport Index Group	Component Name	PP/PVG configuration (N/A)	Passport Subindex	Importance Category (N/A)	SCC2 Header
	LP/0 EDS1/<n2>		5050		aabb PPEM303 gghh TBL where: aa = “*C”, “* “
	LP/<n> DS3/<n2> Lp/<n> Sdh/<n2> Vc4/0 Vc12/{1-3,1-7,1-3} E1 Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} DS1		5100		*Cbb PPEM300 gghh TBL
	LP/<n> DS3/<n2>		5101		*Cbb PPEM300 gghh TBL
			5102		
			5103		
			5104		
	LP/<n> DS3/<n2>		5105		* bb PPEM300 gghh TBL
	LP/<n> DS3/<n2>		5110		*Cbb PPEM300 gghh TBL
	LP/<n> DS3/<n2>		5111		* bb PPEM300 gghh TBL
			5120		
			5121		
			5122		
	LP/<n> Sonet/<n2> LP/<n> Sdh/<n2>		5200		*Cbb PPEM300 gghh TBL
			5201		
			5202		
	LP/<n> Sonet/<n2> LP/<n> Sdh/<n2>		5203		* bb PPEM300 gghh TBL
			5204		
			5210		
			5211		
	LP/<n> Sonet/<n2> Sts/<n2> Lp/<n> Sdh/<n2> Vc4/0 LAPS/<n> Sts/<n2> LAPS/<n> Vc4/0 Pbg/<n> Sts/0		5250		*Cbb PPEM300 gghh TBL
			5251		
	LP/<n> Sonet/<n2> Sts/<n2> Lp/<n> sdh/<n2> Vc4/0 LAPS/<n> Sts/<n2> LAPS/<n> Vc4/0 Pbg/<n> Sts/0		5252		* bb PPEM300 gghh TBL
	LP/<n> Sonet/<n2> Sts/<n2> Lp/<n> Sdh/<n2> Vc4/0 LAPS/<n> Sts/<n2> LAPS/<n> Vc4/0 Pbg/<n> Sts/0		5253		*Cbb PPEM300 gghh TBL

Passport Index Group	Component Name	PP/PVG configuration (N/A)	Passport Subindex	Importance Category (N/A)	SCC2 Header
	LP/<n> Sonet/<n2> Sts/<n2> Lp/<n> Sdh/<n2> Vc4/0 LAPS/<n> Sts/<n2> LAPS/<n> Vc4/0 Pbg/<n> Sts/0		5254		*Cbb PPEM300 gghh TBL
	LP/<n> Sonet/<n2> Sts/<n2> Lp/<n> Sdh/<n2> Vc4/0 LAPS/<n> Sts/<n2> LAPS/<n> Vc4/0 Pbg/<n> Sts/0		5255		*Cbb PPEM300 gghh TBL
	Lp/<n> Sonet/<n2> Sts/<n2> Lp/<n> Sdh/<n2> Vc4/0 Lp/<num1> Sdh/<n2> Vc4/0 Vc12/{1-3, 1-7, 1-3} Laps/<n> Sts/<num3> Laps/<n> Sdh/<num2> Vc4/0 Laps/<n> Sdh/<n2> Vc4/0 Vc12/{1-3, 1-7, 1-3} Pbg/<n> Sts/{0-11}		5256		*Cbb PPEM300 gghh TBL
	LP/<n> Sonet/<n2> Sts/<n2> LP/<n> Sdh/<n2> Vc4/0 LAPS/<n> Sts/<n2> LAPS/<n> Vc4/0 Pbg/<n> Sts/0		5260		* bb PPEM300 gghh TBL
			5261		
	LAPS/<n>		5270		**bb PPEM300 gghh TBL
	LAPS/<n>		5271		* bb PPEM300 gghh TBL
	LAPS/<n>		5272		* bb PPEM300 gghh TBL
	LAPS/<n>		5273		* bb PPEM300 gghh TBL
	LAPS/n		5274		* bb PPEM300 gghh TBL
	LAPS/<n>		5275		*Cbb PPEM300 gghh TBL
	LP/<n> Sdh/<n2> Vc4/0 Vc12/{1-3,1-7,1-3} Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} LAPS/<n> Vc4/0 Vc12/{1-3,1-7,1-3} LAPS/<n> Sts/<n2> Vt1dot5/{1-7,1-4}		5290		* bb PPEM303 gghh TBL
			5291		
			5292		
			5293		
			5294		

Passport Index Group	Component Name	PP/PVG configuration (N/A)	Passport Subindex	Importance Category (N/A)	SCC2 Header
	LP/<n> Sdh/<n2> Vc4/0 Vc12/{1-3,1-7,1-3} Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} LAPS/<n> Vc4/0 Vc12/{1-3,1-7,1-3} LAPS/<n> Sts/<n2> Vt1dot5/{1-7,1-4}		5295 5296		*Cbb PPEM303 gghh TBL
	LP/<n> Sdh/<n2> Vc4/0 Vc12/{1-3,1-7,1-3} Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} LAPS/<n> Vc4/0 Vc12/{1-3,1-7,1-3} LAPS/<n> Sts/<n2> Vt1dot5/{1-7,1-4}		5297		*Cbb PPEM303/6 gghh TBL
	LP/<n> Ethernet/<n2> LP/<n> Ethernet/<n2> LP/<n> Ethernet/<n2> LP/<n> Ethernet/<n2> LP/<n> Ethernet/<n2> OpticalModule		5400		*Cbb PPEM300 gghh TBL
			5401		*Cbb PPEM300 gghh TBL
			5402		*Cbb PPEM300 gghh TBL
			5403		*Cbb PPEM300 gghh TBL
			5480		**bb PPEM300 gghh TBL
	LP/<n> Sonet/<n2> LP/<n> Sonet/<n2> Sts/0 LAPS/<n> Sts/0 LP/<n> DS3/<n2> LP/<n> DS3/<n2> DS1/<n3> LP/<n> DS3/<n2> DS1/<n3> Chan/<n4> Pbg/<n> Sts/0		5501		**bb PPEM300 gghh TBL
	LP/<n> DS3/<n2>		5601 5602		* bb PPEM300 gghh TBL
	LP/<n> DS3/<n2>		5603 5604		**bb PPEM300 gghh TBL
7012	Processor control system alarms. LP instance range (<n>): 0-15 Card instance range (<n>): 0-15 FabricCard instance range (<i>): X, Y				
	Shelf		0050		**bb PPEM303 gghh TBL
	Shelf		0051		aabb PPEM303 gghh TBL where: aa = " ", " "
	Shelf Shelf FabricCard/<i>		0052		**bb PPEM303 gghh TBL

Passport Index Group	Component Name	PP/PVG configuration (N/A)	Passport Subindex	Importance Category (N/A)	SCC2 Header
	Shelf		0053		**bb PPEM303 gghh TBL
	Shelf		0055		aabb PPEM303 gghh TBL where: aa = “**” , “*”
	Shelf		0056		* bb PPEM303 gghh TBL
	Shelf		0057		**bb PPEM303 gghh TBL
	Shelf		0058		TBL
	Shelf		0059		*Cbb PPEM304 gghh TBL
	Shelf Card/<n>		0100		aabb PPEM303 gghh TBL where: aa = “*C” , “*”
	Shelf Card/<n>		0103		**bb PPEM303 gghh TBL
	Shelf Card/<n>		0104		TBL
	Shelf Card/<n>		0105		* bb PPEM306 gghh TBL
	LP/<n>		0200		*Cbb PPEM302 gghh TBL
	LP/<n>		0202		* bb PPEM306 gghh TBL
	Shelf Card/<n> SpServ		0301		* bb PPEM302 gghh TBL
7013	Message block usage alarms. LP instance range (<n>): 0-15				
	LP/<n>		0000		* bb PPEM301 gghh TBL
	LP/<n>		0001		**bb PPEM301 gghh TBL
	LP/<n>		0002		* bb PPEM301 gghh TBL
			0003		
			0004		
			0005		
	LP/<n>		0011		**bb PPEM301 gghh TBL
			0021		
	LP/<n>		0022		* bb PPEM301 gghh TBL
7014	Memory management alarms				
	LP/<n>		0000		* bb PPEM301 gghh TBL
	LP/<n>		0001		**bb PPEM301 gghh TBL
7015	Network time-of-day (TOD) synchronization alarms. Server instance range (<n>): 1-10				
	Time		0000		**bb PPEM304 gghh

Passport Index Group	Component Name	PP/PVG configuration (N/A)	Passport Subindex	Importance Category (N/A)	SCC2 Header
			0002		TBL
	Time Server/<n>		0010		* bb PPEM300 gghh
			0011		TBL
	Time Server/<n>		0012		* bb PPEM300 gghh TBL
7017	Network clock synchronization alarms				
	NS		1000		* bb PPEM300 gghh TBL
7021	Internet protocol alarms. For Succession VOA, the IP stack is used only for network management connectivity purposes. For VOIP VR is used to connect to IP network. More than 1 VR may be provisioned in this configuration. VR instance range (<i>): any string, but often specified simply as a digit (e.g., "0") Cache instance range (<n>): 0-15 Name of the vrf (<y>) LP number (<lpnum>): 0-15 IP address (<ipaddress>): address of the local IpLogicalInterface				
	Vr/<i> Ip Cache/<n>		0006		**bb PPEM302 gghh TBL
	Vr/<i> Ip Cpp IsolatedDa/<ipaddress>, <lpnum> Rtr/<i> Cpp IsolatedDa/<ipaddress>, <lpnum> Rtr/<i> Vrf/<y> Cpp IsolatedDa/<ipaddress>, <lpnum>		0013		* bb PPEM305 gghh TBL
			0014		**bb PPEM305 gghh TBL
7026	LAN port management system alarms. For Succession VOA, the LAN port management system is used only for network management connectivity purposes Same alarms are used for VOIP.				
	LP/0 OamEnet/0		3000		*Cbb PPEMeee gghh TBL where: eee = 300, 303
	LP/0 OamEnet/0		3005		* bb PPEMeee gghh TBL where: eee = 300, 303
7039	ATM Core alarms. AtmIf instance range (<n>): 1-4095 Vcc instance range (<n2.n3>): n2 is VPI; n3 is VCI				
	Atmif/<n>		1000		* bb PPEM300 gghh TBL
	Atmif/<n> Vcc/<n2.n3>		2000		* bb PPEM302 gghh
			2003		TBL
	Atmif/<n> Vpt/<n2>		3000		* bb PPEM300 gghh TBL
	Atmif/<n>		4001		**bb PPEM300 gghh TBL

Passport Index Group	Component Name	PP/PVG configuration (N/A)	Passport Subindex	Importance Category (N/A)	SCC2 Header
	Atmif/<n>		5000		*Cbb PPEM300 gghh TBL
7041	ATM Networking alarms. AtmIf instance range (<n>): 1-4095 Vpt instance range (<n2>): 0-4095 CfgNode instance range (<n>): 0-104				
	Atmif/<n> Uni Ilmi		0050		**bb PPEMeee gghh TBL where: eee = 300, 303
	Atmif/<n> Uni Sig Atmif/<n> Pnni Sig		0150		**bb PPEM300 gghh TBL
	Atmif/<n> Uni Sig Atmif/<n> Pnni Sig Atmif/<n> Uni Ilmi Atmif/<n> Pnni Rcc		0200		**bb PPEM300 gghh TBL
	Atmif/<n> Pnni Rcc		0250		**bb PPEM300 gghh TBL
	Atmif/<n> Pnni Rcc		0253		**bb PPEM300 gghh TBL
	Artg Pnni		0301		**bb PPEM300 gghh TBL
	Artg Pnni CfgNode<n> Rcc		0302		**bb PPEM300 gghh TBL
	Atmif/<n> Uni Atmif/<n> Pnni		0400		* bb PPEM300 gghh TBL
	Atmif/<n>		0401		**bb PPEM30? gghh TBL
	Atmif/<n> Uni Atmif/<n> Pnni		0500		* bb PPEM300 gghh TBL
	Atmif/<n> Uni Atmif/<n> Pnni		0600 0601		* bb PPEM302 gghh TBL
	Artg Pnni CfgNode /<n>		0700		**bb PPEM300 gghh TBL
	Atmif/<n> Pnni Rcc		0701		**bb PPEM300 gghh TBL
	Artg Pnni CfgNode /<n>		0703		* bb PPEM300 gghh TBL
7042	Circuit Emulation Service (CES) alarms. Aal1Ces instance range (<n>) : 1-16383				
	Aal1Ces/<n>		0001		**bb PPEM301 gghh TBL
	Aal1Ces/<n>		0002		**bb PPEM302 gghh TBL
	Aal1Ces/<n>		0003		**bb PPEM300 gghh TBL
7054	Sparing panel subsystem alarms. Card instance range (<n>): 0-15				
	Shelf Card/<n>		0100 0101		**bb PPEM303 gghh TBL

Passport Index Group	Component Name	PP/PVG configuration (N/A)	Passport Subindex	Importance Category (N/A)	SCC2 Header
			0102		
			0103		
			0104		
			0105		
7056	Voice Services Processor (VSP) / Narrowband Service Trunk over ATM (Nsta) This group is specific to PVG application (e.g. severe failure of the VSP card) Lp instance range (<x>): 0-15 PModule instance range (<y>): 1-24 PBlock instance range (<z>): 1-2 NSTA instance range (<i>): 0-15999 GigE instance range (<m>): 0-1 Control instance range (<n>): mg or sg Conn instance range (<l>): 0-128 Brag instance range (<d>): 0-159999 Q921 instance range (<r>): 1-31 LapV5 instance value (<w>): 15, 16, 31 Tag instance range (<u>): 0-16777215 AtmTConn instance range (<h>): 1-2700 (max 4094) dBrag instance range (<t>): 0-127 BragS instance range (<k>): 0-15 CasDefn instance range (<z>): 0-24				
	Lp/<x> Vsp PModule/<y>		0002		** bb PPEM306 gghh TBL
	Lp/<x> Vsp PModule/<y> PBlock/<z>		0003		*Cbb PPEM303 gghh TBL
	Lp/<x> Vsp GigE/<m>		0500		** bb PPEM300 gghh TBL
			0501		
			0502		
	Nsta/<i> Conn/<l> Nsta/<i> Vgs AtmTConn/<h>		1000		**bb PEM300 gghh TBL
	Nsta/<l> Vgs		1200		* bb PPEM300 gghh TBL
	Nsta/<i> Vgs IpMConn		1201		** bb PPEM300 gghh TBL
	Nsta/<i> Vgs Control/<n> Mediagateway		1202		** bb PPEM300 gghh TBL
	Nsta/<i> Vgs Control/<n> Signalingateway				

Passport Index Group	Component Name	PP/PVG configuration (N/A)	Passport Subindex	Importance Category (N/A)	SCC2 Header
	Nsta/<i> Vgs Control/<n> MediaGateway Aap Nsta/<i> Vgs Control/<n> Signalinggateway Aap Nsta/<i>Vgs Control/<n> SpvcAp Nsta/<i> Vgs IpMConn Aap Nsta/<i> Vgs IpMConn SpvcAp Nsta/<i> Vgs AtmTConn/<h> Aap Nsta/<l> Vgs AtmTConn/<h> Aap		1203		** bb PPEM300 gghh TBL
	Nsta/<i> Vgs		1204		* bb PPEM302 gghh TBL
	Nsta/<i> Vgs CasDefn/<z>		1208		* bb PPEM302 gghh TBL
	Lp/<x> Vsp PModule/y>		1209		* bb PPEM303 gghh TBL
	Nsta/<x> Vgs Brag/<d> Q921/<r> Nsta/<i> Vgs BragS/<k> dBrag/<t> Q921		1210		** bb PPEM300 gghh TBL
	Nsta/<x> Vgs lua		1211		** bb PPEM300 gghh TBL
	Nsta/<x> Vgs Brag/<d> V5Link LapV5/<w>		1213		** bb PPEM300 gghh TBL
	Nsta/<x> Vgs Tag/<u>		1217		*Cbb PPEM302 gghh TBL
7060	ATM and Frame Resource Control alarms. LP instance range (<n>): 0-15 Aqm instance range (<n2>): 0-3				
	LP/<n> Eng Fcrc		1000		**bb PPEM300 gghh TBL
	LP/<n> Eng Arc Aqm/<n2>		1100		* bb PPEM300 gghh TBL

The following table specifies the alarms where field “event” has the value “message”. There won’t be a “clear” for these, but some action may still be required (e.g., security issue).

Table 3 Passport 15000 Message Alarms Supported for Succession VOA/VOIP

Passport Index Group	Component Name	Solution Notes	Passport Subindex	Importance Category	SCC2 Header
0000	OSI administrative state changes, general engineering and memory alarms, etc.				
	These alarms can apply to many Passport components. Often, it is: EM/<nodename>		9000		* bb CA eee gghh TBL where:
			9001		
			9002		

Passport Index Group	Component Name	Solution Notes	Passport Subindex	Importance Category	SCC2 Header
			9003		eee = 300, 302
7000	Provisioning alarms. These alarms apply to failures resulting from provisioning attempts. e.g., loading a provisioning file has failed.				
	Prov		0001		*Cbb PPEM302 gghh TBL
	Prov		0002		* bb PPEM302 gghh TBL
	Prov		0003		*Cbb PPEM302 gghh TBL
	Prov		0004		*Cbb PPEM302 gghh TBL
	Prov		0005		* bb PPEM302 gghh TBL
	Prov		0006		*Cbb PPEM302 gghh TBL
	Prov		0008		**bb PPEM302 gghh TBL
	Prov		0009		**bb PPEM302 gghh TBL
	Prov		0012		* bb PPEM306 gghh TBL
	Prov		0013		* bb PPEM302 gghh TBL
	Prov		0015		* bb PPEM302 gghh TBL
	Prov		0016		* bb PPEM30? gghh TBL
	Prov		0029		* bb PPEM30? gghh TBL
	Prov		0030		* bb PPEM30? gghh TBL
	Prov		0031		* bb PPEM302 gghh TBL
	Prov		0032		* bb PPEM30? gghh TBL
	This alarm can apply to many Passport components.		0035		* bb PPEM307 gghh TBL
	Prov		0039		* bb PPEM306 gghh TBL
7002	Backplane control system alarms; e.g., communication failure between a card and the backplane. Note: Card instance range (<n>): 0-15 FabricCard instance range (<i>): X,Y				
	Shelf FabricCard/<i>		0010		* bb PPEM303 gghh TBL
	Shelf FabricCard/<i>		0012		* bb PPEM303 gghh TBL
	Shelf FabricCard/<i>		0013		* bb PPEM303 gghh TBL
	Shelf FabricCard/<i>		0014		* bb PPEM303 gghh TBL

Passport Index Group	Component Name	Solution Notes	Passport Subindex	Importance Category	SCC2 Header
	Shelf Card/<n>		1000		*Cbb PPEM303 gghh TBL
7003	Data collection system alarms; e.g., an alarm or log queue size has exceeded a threshold. Collector instance range (<t>): accounting, alarm, log, debug, scn, trap, stats, rtstats, appl Agent instance range (<n>): 0-15				
	Collector/<t> Agent/<n>		0004		* bb PPEM301 gghh TBL
	Collector/<t> Spooler		0008		* bb PPEM306 gghh TBL
7006	Network Management Interface system alarms. Management Interface type (<type>): Fmip, Ftp, Local, Telnet Session instance range (<n>): 1-35 (Fmip); 1-16 (Ftp); 1-2 (Local); 1-16 (Telnet)				
	Nmis <type>		0001		**bb PPEM305 gghh TBL
	Nmis <type> Session/<n>		0002		* bb PPEM305 gghh TBL
	Nmis <type> Session/<n>		0003		**bb PPEM300 gghh TBL
	Nmis Ftp		0005		**bb PPEM302 gghh TBL
	Nmis Fmip		0006		**bb PPEM305 gghh TBL
	Nmis <type> Session/<n>		0007		**bb PPEM300 gghh TBL
	Nmis Fmip		0008		**bb PPEM300 gghh TBL
7008	File system alarms. Disk instance range (<n>): 0-1				
	FileSystem		1003		**bb PPEM302 gghh TBL
	FileSystem Disk/<n>		1012		* bb PPEM303 gghh TBL
	FileSystem Disk/<n>		1013		**bb PPEM303 gghh TBL
	FileSystem Disk/<n>		1014		**bb PPEM307 gghh TBL
	FileSystem Disk/<n>		1015		* bb PPEM307 gghh TBL
	FileSystem Disk/<n>		1016		* bb PPEM307 gghh TBL
	FileSystem Disk/<n>		1018		* bb PPEM303 gghh TBL
	FileSystem		1020		* bb PPEM303 gghh TBL
	Shelf Card/<x>		1021		**bb PPEM303 gghh TBL
7011	Port management system and Automatic Protection Switching alarms. LP instance range (<n>): 0-15 Port types (<type>): Sonet, DS3 Sonet instance range (<n2>): 0-15 (16-port); 0-3 (4-port) DS3 instance range (<n2>): 0-11 (12-port); 0-3 (4-port)				

Passport Index Group	Component Name	Solution Notes	Passport Subindex	Importance Category	SCC2 Header
	LP/<n> <type>/<n2>		2002		**bb PPEM303 gghh TBL
	LP/<n> DS3/<n2>		5112		* bb PPEM300 gghh TBL
	LP/<n> <type>/<n2>		8000		* bb PPEM300 gghh TBL
7012	Processor control system alarms. LP instance range (<n>): 0-15 Card instance range (<n>): 0-15				
	Shelf		0054		**bb PPEM303 gghh TBL
	Shelf Card/<n>		0101		* bb PPEM303 gghh TBL
	Shelf Card/<n>		0102		* bb PPEM301 gghh TBL
	Shelf Card/<n>		0151		**bb PPEM302 gghh TBL
			0152		
			0153		
	Shelf Card/<n>		0154		**bb PPEM303 gghh TBL
			0155		
			0156		
	LP/<n>		0201		* bb PPEM306 gghh TBL
	LP/0		0203		* bb PPEM303 gghh TBL
	LP/<n>		0204		* bb PPEM306 gghh TBL
	Shelf Card/<n> SpServ		0300		aabb PPEMeee gghh TBL where: aa = “*C”, “* “ eee=any
7015	Network time-of-day (TOD) synchronization alarms.				
	Time		0001		* bb PPEMeee gghh TBL eee=304, 306, 307
7017	Network clock synchronization alarms.				
	Ns		1001		* bb PPEM301 gghh TBL
7021	Internet protocol alarms. For Succession VOA, the IP stack is used only for network management connectivity purposes. For VOIP VR is used to connect to IP network. OSPF and IP static Routes can be used. More than 1 VR can be provisioned. VR instance range (<i>): any string, but often specified simply as a digit (e.g., “0”)				
	VR/<i> Ip		0000		* bb PPEM300 gghh TBL
	VR/<i> Ip OSPF		1000		
	VR/<i> Ip OSPF		1001		
	VR/<i> Ip OSPF		1002		
	VR/<i> Ip OSPF		1003		

Passport Index Group	Component Name	Solution Notes	Passport Subindex	Importance Category	SCC2 Header
	VR/<i> Ip OSPF VR/<i> Ip OSPF VR/<l> Ip OSPF VR/<l> Ip OSPF VR/<i> Ip				
			1011		
			1016		
			1017		
			1100		
			4000		
	Vr/<i>		1021		**bb PPEM302 gghh TBL
	Vr/<i> Ip Ospf		1101		* bb PPEM302 gghh TBL
7026	LAN port management system alarms. For Succession VOA, the LAN port management system is used only for network management connectivity purposes. For VOIP same alarms are used.				
	LP/0 OamEnet/0		3002		* bb PPEM30? gghh TBL
	LP/0 OamEnet/0		3003		* bb PPEM303 gghh TBL
	LP/0 OamEnet/0		3006		* bb PPEM302 gghh TBL
7039	ATM Core alarms. AtmIf instance range (<n>): 1-4095 Vcc instance range (<n2.n3>): n2 is VPI; n3 is VCI				
	Atmif/<n> Vcc/<n2.n3>		2001		* bb PPEM302 gghh TBL
	Atmif/<n>		4000		* bb PPEM300 gghh TBL
7041	ATM Networking alarms. AtmIf instance range (<n>): 1-4095 CfgNode instance range (<n>): 0-104 Top instance range (<n>): 0-104 Node instance range (<id>): 44-hex digit id Vpt instance range (<n2>): 0-4095				
	Atmif/<n> Uni		0000		* bb PPEM306 gghh TBL
	Atmif/<n> Uni		0001		* bb PPEM303 gghh TBL
	Atmif/<n> Uni Ilmi		0051		**bb PPEM300 gghh TBL
	Atmif/<n> Uni Atmif/<n> Pnni Atmif/<n> Vpt/<n2> Uni Atmif/<n> Vpt/<n2> Pnni		0151		*Cbb PPEM300 gghh TBL
	Atmif/<n> Pnni Rcc		0251		**bb PPEM300 gghh TBL
	Atmif/<n> Pnni Rcc		0252		**bb PPEM300 gghh TBL
	Artg Pnni Top/<n> Node/<id>		0602		**bb PPEM301 gghh TBL

Passport Index Group	Component Name	Solution Notes	Passport Subindex	Importance Category	SCC2 Header
	Artg		0603		**bb PPEM303 gghh TBL
7056	Voice Services Processor (VSP) / Narrowband Service Trunk over ATM (Nsta) This group is specific to PVG application (e.g. severe failure of the VSP card) Lp instance range (<x>): 0-15 PModule instance range (<y>): 1-24 PBlock instance range (<z>): 1-2 NSTA instance range (<i>): 0-15999 Conn instance range (<l>): 0-128 Brag instance range (<d>): 0-159999 BragS instance range (<p>): 0-15				
	Lp/<x> Vsp PModule/<y>		0006		* bb PPEM303 gghh TBL
	Nsta/<i> Conn/<l> Brag/<d> Ccst		1101		* bb PPEM300 gghh TBL
	Nsta/<i> Vgs lua		1212		* bb PPEM300 gghh TBL
	Lp/<x> Vsp PModule/<y>		1214		**bb PPEM302 gghh TBL
	Nsta/<i> Vgs BragS/<p>		1215		** bb PPEM302 gghh TBL
7060	ATM and Frame Resource Control alarms. LP instance range (<n>): 0-15				
	LP/<n> Eng Arc Ov		1200		* bb PPEM301 gghh TBL
	LP/<n> Eng		1300		
	LP/<n> Eng		1400		
	LP/<n> Eng		1500		
	LP/<n> Eng		1600		
7071	LAN ApplicationLAN application instance (<n>): 0-255				
	LA/<n>		1000		*Cbb PPEM302 gghh TBL
7080	Software file system. <name> = name of the software application				
	Sw Av/<name>		0100		**bb PPEM302 gghh TBL

Reference [3] provides detailed descriptions of Passport alarm logs, of which only a portion are applicable for Succession VOA/VOIP.

MDM Alarm Logs

Table 4 presents the list of MDM and MDM proxy set/clear alarm logs that are applicable for Succession VOA/VOIP.

Applicable MDM set/clear alarms logs include those due to MDM software failure, and alarms related to the monitoring of the platform on which MDM is operating. MDM proxy alarm logs are alarms that MDM initiates on behalf of Passport (for a number of reasons) and injects into the Passport alarm log stream.

The table does not explicitly state all MDM clear alarm logs that correspond to each set. The clear differs from its corresponding set by only the first two characters. The characters “aa” are replaced by “ ” (two spaces). This format is presented in Table 1.

The MDM alarm identifier consists of an eight-digit number identifying the alarm. The first four digits comprise the **Index Group**, which represents logical groupings of alarms. The last four digits are the **SubIndex**, which is an identifier within each index group.

Component Name indicates the managed object against which the alarm Log is generated. This table contains the CLI format of a component name. The “compld” field in SCC2 format contains this information (with the module’s <nodename> pre-pended). Also, “compld” follows the MDM API-style format (with component type and instance separated by a space instead of a slash, and ‘\$’ appearing in place of a null instance value). Variables (usually instance value ranges) are denoted by <> and the reader should reference the Alarms NTP’s [3] and [4] for further information.

Table 4 MDM Set/Clear Alarms Supported for Succession VOA/VOIP

MDM Index Group	Component Name	N/A	MDM SubIndex	Importance category (N/A)	SCC2 Header
0999	Loss of access to a Passport shelf from MDM. MDM tries to reconnect and when it succeeds in doing so, will do a “state walk” of major components on the shelf and issue alarms for those components that are out-of-service. EM instance range (<nodename>): a string, typically the CLLI identifier for the PP15000				
	EM/<nodename>		0001		*Cbb MDM 303 gghh TBL
0999	MDM Proxy-alarm. MDM-originated alarm sent on behalf of the Passport, either due to a state walk or a state-change notification.				
	This alarm can apply to many Passport components.		0012		**bb PPEMeee gghh TBL where: eee = 300, 301, 302, 303, 304, 305, 306, 307
3010	Indicates faults on MDM server processes, which are needed by the MDM tools/applications. The MDM Log Display GUI or corresponding Unix Utility (nmslog) may also be used to find the information for the cause of the problem. NMS instance range (<x>): a string, typically the hostname of the MDM server platform APP instance range (<a>): a string, denoting the name of an MDM software application GROUP instance range (<g>): a string, which is the HGDS group name for a set of Passports PP instance range (<nodename>): a string, typically the CLLI identifier for the PP15000				
	NMS/<x> APP/<a>		0000		**bb MDM 302 gghh TBL
	NMS/<x> GROUP/<g>		0700		* bb MDM 305 gghh TBL

MDM Index Group	Component Name	N/A	MDM SubIndex	Importance category (N/A)	SCC2 Header
	NMS/<x> PP/<nodename>		0701		* bb MDM 300 gghh TBL
	NMS/<x> PP/<nodename>		0702		* bb MDM 300 gghh TBL
	NMS/<x> APPL/TODCHANGEVER		0703		* bb MDM 304 gghh TBL
3011	MDM Platform monitoring; e.g. Solaris and Sun monitoring, including: CPU, disk space, memory, local ports and connectivity to adjacent neighbors. The severity of resource problems are determined via thresholds. Connectivity problems are determined using ping command. NMS instance range (<x>): a string, typically the hostname of the MDM server platform APP instance range (<a>): a string, denoting the name of an MDM software application DISK instance range (<v>): a string, denoting disk volume name CPU instance range (<c>): a string, denoting the CPU id PORT and CONNECTION instance range (<ip>): an IP address or host name SDS instance range (<d>): logical disk name				
	NMS/<x> APP/<a>		0001		*Cbb MDM 303 gghh TBL
	NMS/<x> DISK/<v>		0100		aabb MDM 303 gghh TBL where: aa = “*C”, “**”, “*”
	NMS/<x> CPU/<c>		0200		aabb MDM 303 gghh TBL where: aa = “*C”, “**”, “*”
	NMS/<x> MEMORY		0300		aabb MDM 303 gghh TBL where: aa = “*C”, “**”, “*”
	NMS/<x> PORT/<ip>		0401		**bb MDM 303 gghh TBL
	NMS/<x> CONNECTION/<ip>		0501		*Cbb MDM 303 gghh TBL
	NMS/<x> SDS/<d>		0600		*Cbb MDM 303 gghh TBL
	NMS/<x>		0700		aabb MDM 303 gghh TBL where: aa = “*C”, “**”
600x	MDP application alarms. NMS instance range (<x>): a string, typically the hostname of the MDM server platform MDP instance range (<a>): a string, denoting the name of an MDP software application				
	NMS/<x> MDP/<a>		00001-40000		aabb MDM 307 gghh TBL where: aa = “*C”, “**”, “*”

Reference [4] provides detailed descriptions of MDM and MDM proxy alarm logs, of which only a portion are applicable for Succession VOA/VOIP.

SN06(VOA)-to-SN06.2(VOA/VOIP) Delta Summary

The following table captures the SN06.2 (VOA/VOIP) alarm log delta that includes PVG application as compared with SN06 (VOA) documentation that did not include any PVG application specifics

Table 5 SN06 (non PVG content) -to-SN06.2 (including PVG content) Change Summary Description

Fault Code	Description of Change
SET ALARMS	
70115400	New
70115401	New
70115402	New
70115403	New
70115480	New
7026 3000	New
7056 0002	New
7056 0003	New
7056 0500	New
7056 0501	New
7056 0502	New
7056 1000	New
7056 1200	New
7056 1201	New
7056 1202	New
7056 1203	New
7056 1204	New
7056 1209	New
7056 1210	New
7056 1211	New
7056 1213	New
MESSAGE Alarms	
7000 0039	New
7021 1000	New
7021 1002	New
7021 1003	New
7021 1004	New
7021 1005	New
7021 1006	New
7021 100B	New
7021 1100	New
7056 1101	New
7056 1212	New
70561214	New
7056 1215	New
7060 1300	New

7060 1400	New
7060 1500	New
7060 1600	New
7071 1200	New

SN06.2-to-SN07(VOA/VOIP) Delta Summary

The following table captures the SN07 (VOA/VOIP) alarm log delta as compared with SN06.2 (VOA/VOIP) documentation.

Table 6 SN06.2-to-SN07 Change Summary Description

Fault Code	Description of Change
SET ALARMS	
7000 0041	New
7003 0008	New
7011 1500	New
7011 1501	New
7011 5254	New
7011 5255	New
7011 5256	New
7012 0059	New
7021 0013	New
7021 0014	New
7041 0700	New
7041 0701	New
7041 0703	New
7056 1208	New
7056 1217	New
MESSAGE Alarms	
7008 1021	New
7021 1021	New
7021 1101	New
7041 0151	New
7056 0006	New
7080 0100	New

References

1. Passports and MDM Logs, draft 1.2, March 2001 (PassportMDMLog_v1.2.doc), by the SDM team.
2. Passport 15000 for Universal Access – AAL1 (SN06) Integrated Solution Specification, Issue 3.04, Oct 22, 2002
3. NTP 241-5701-500 Passport 6400, 7400, 15000, 20000 Alarms, 5.2S1, Nov/2003.
4. NTP 241-6001-501 MDM Proxy Alarms Reference Guide, 14.3RSUP, 2003.
5. NTP 241-6001-309 Preside MDM Management Data Provider User Guide, 14.3RSUP, 2003.
6. Supernode Data Manager - Log Applications Enhancement Design Summary (DSUM), 2002.
7. NTP NN10600-500 Multiservice Switch 7400/15000/20000 Alarms Reference, 6.1M2, July 2004

Appendix D: USP OMs

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	ATM Driver Messaging, Plane 1 CRC Error Count	This OM measures the number of Plane 1 CRC errors.
Accumulation OM	ASP Path Management, Application Server became Active	This OM measures the total number of times per measurement period that an Application Server became active either by a controlled or a forced change of activity.
Accumulation OM	ASP Path Management, Application Server became Inactive	This OM measures the total number of times per measurement period that an Application Server became inactive either by a controlled or a forced change of activity.
Accumulation OM	ASP Path Management, Path Active Time	This OM measures the total time that a Path was inactive and in the Restoring state.
Accumulation OM	ASP Path Management, Path entered Active state	This OM measures the total number of times per measurement period that a Path entered the Active state.
Accumulation OM	ASP Path Management, Path entered Down state	This OM measures the total number of times per measurement period that a Path entered the Down state.
Accumulation OM	ASP Path Management, Path entered Restoring state	This OM measures the total number of times per measurement period that a Path entered the Restoring state.
Accumulation OM	ASP Path Management, Path Inactive Time	This OM measures the total time that a Path was inactive and in the Restoring state.
Accumulation OM	ASP Path Traffic, Discarded MSUs Count	This OM measures the total number of received MSUs on an ASP Path which were discarded because the Network Appearance (or System Identity) associated with the incoming message was not found on the USP.
Accumulation OM	ASP Path Traffic, Originated MSUs Count	This OM measures the number of originated MSUs (MSUs that contain the PC or capability code for the USP in the OPC field) that are successfully passed to the ASP Path for transmission (for example, network management messages).
Accumulation OM	ASP Path Traffic, Received MSUs Count	This OM measures the total number of received MSUs on an ASP Path.
Accumulation OM	ASP Path Traffic, Terminated MSUs Count	This OM measures the number of terminated MSUs (acknowledged, incoming MSUs that contain the PC or capability code of the USP in the DPC field) received.
Accumulation OM	ASP Path Traffic, Through-Switched MSUs Count	This OM measures the number of through-switched MSUs (MSUs that do not contain the PC or capability code for the USP in either the OPC or DPC) that are acknowledged, translated, and successfully passed to the ASP Path for transmission.
Accumulation OM	ASP Path Utilization, DAUD Received Count	This OM measures the number of destination audit (DAUD) messages transmitted.
Accumulation OM	ASP Path Utilization, DAVA Transmitted Count	This OM measures the number of destination available (DAVA) messages transmitted.
Accumulation OM	ASP Path Utilization, DUNA Transmitted Count	This OM measures the number of destination unavailable messages transmitted.
Accumulation OM	ASP Path Utilization, SCON Transmitted Count	This OM measures the number of Signaling Congestion (SCON) messages transmitted.
Accumulation OM	ATM Driver Messaging, Duplicate Messages Count	This OM measures the number of duplicate messages.
Accumulation OM	ATM Driver Messaging, IP Message Count	This OM measures the number of incoming IP messages.
Accumulation OM	ATM Driver Messaging, Plane 1 Messages Count	This OM measures the number of incoming Plane 1 messages.
Accumulation OM	ATM Driver Messaging, Plane 2 CRC Error Count	This OM measures the number of Plane 2 CRC errors.
Accumulation OM	ATM Driver Messaging, Plane 2 Messages Count	This OM measures the number of incoming Plane 2 messages.
Accumulation OM	ATM Driver Messaging, Raw Cell Count	This OM measures the number of raw cells. Raw cells are typically bad cells or OAM cells.

Accumulation OM	ATM Driver Messaging, Raw Message Count	This OM measures the number of ATM raw messages. Raw messages are messages not assigned to a protocol.
Accumulation OM	ATM Driver Messaging, Sequence Number Reset Count	This OM measures the number of times the sequence numbers are reset due to the receipt of five consecutive duplicate cells.
Accumulation OM	ATM Driver Messaging, SSCOP Message Count	This OM measures the number of incoming SSCOP messages.
Accumulation OM	ATM Link Traffic, Discarded cells with HEC Viol.	This OM measures the number of ATM cells discarded due to Header Error Control (HEC) violations.
Accumulation OM	ATM Link Traffic, Discarded cells with Prot. Errs	This OM measures the number of cells discarded due to Protocol (ATM-Layer Header) Errors.
Accumulation OM	ATM Link Traffic, In NDC-valid cells on HSL VCL	This OM measures the number of incoming Network Data Collection (NDC) valid cells on the High Speed Links (HSL) VCL.
Accumulation OM	ATM Link Traffic, Incoming ATM UI cells	This OM measures the number of incoming ATM User Information (UI) cells.
Accumulation OM	ATM Link Traffic, OCD Anomalies	This OM measures the number of Out of Cell Delineation (OCD) anomalies.
Accumulation OM	ATM Link Traffic, Out NDC-valid cells on HSL VCL	This OM measures the number of outgoing Network Data Collection (NDC) valid cells on the High Speed Links (HSL) VCL.
Accumulation OM	ATM Link Traffic, Outgoing ATM UI cells	This OM measures the number of outgoing ATM User Information (UI) cells.
Accumulation OM	BICC Received Message Counts, BICC Call P Received Count	This OM measures the number of BICC call processing messages received from the SS7 Network.
Accumulation OM	BICC Received Message Counts, BICC Error No OPC Route	This OM measures the number of BICC messages discarded as a result of not being able to find the associated OPC route for the received BICC message.
Accumulation OM	BICC Received Message Counts, BICC Error No Path	This OM measures the number of BICC messages discarded as a result of not being able to find an inservice path to a given AS.
Accumulation OM	BICC Received Message Counts, BICC Error No Route	This OM measures the number of BICC messages discarded as a result of not being able to find a route to a given AS.
Accumulation OM	BICC Received Message Counts, BICC Maint Received Count	This OM measures the number of BICC maintenance messages received from the SS7 Network.
Accumulation OM	BICC Received Message Counts, Wrong NE Received Count	This OM measures the number of BICC messages discarded as a result of not receiving the message for a SG Network Element.
Accumulation OM	Carrier, Far End Line - Errored Seconds	This OM measures the Far End Performance data: Far End Errored Seconds - Line.
Accumulation OM	Carrier, Far End P - Sev Err Frm/AIS Sec	This OM measures the Far End Performance data: Far End Severely Errored Frame/AIS Seconds - Path.
Accumulation OM	Carrier, Far End P - Severely Err Secs	This OM measures the Far End Performance data: Far End Severely Errored Seconds - Path.
Accumulation OM	Carrier, Far End P - Unavailable Seconds	This OM measures the Far End Performance data: Far End Unavailable Seconds - Path.
Accumulation OM	Carrier, Far End Path - Code Violations	This OM measures the Far End Performance data: Far End Code Violations - Path.
Accumulation OM	Carrier, Far End Path - Controlled Slips	This OM measures the Far End Performance data: Far End Controlled Slips - Path.
Accumulation OM	Carrier, Far End Path - Errored Seconds	This OM measures the Far End Performance data: Far End Errored Seconds - Path.
Accumulation OM	Carrier, Far End Path - Failure Count	This OM measures the Far End Performance data: Far End Failure Count - Path.
Accumulation OM	Carrier, Line - Code Violations	This OM measures the Near End Performance data: Code Violations - Line.
Accumulation OM	Carrier, Line - Errored Seconds	This OM measures the Near End Performance data: Errored Seconds -Line.

Accumulation OM	Carrier, Line - Loss of Signal Seconds	This OM measures the Near End Performance data: Loss of Signal Seconds - Line. All performance parameters including this parameter are defined in ANSI T1.231-1997 'Digital Hierarchy - Layer 1 in-Service Digital Transmission Performance Monitoring'.
Accumulation OM	Carrier, Line - Severely Errored Seconds	This OM measures the Near End Performance data: Severely Errored Seconds - Line.
Accumulation OM	Carrier, P - Severely Err Frame/AIS Secs	This OM measures the Near End Performance data: Severely Errored Frame/AIS Seconds - Path.
Accumulation OM	Carrier, Path - AIS Seconds	This OM measures the Near End Performance data: AIS Seconds - Path.
Accumulation OM	Carrier, Path - Code Violations	This OM measures the Near End Performance data: Code Violations - Path.
Accumulation OM	Carrier, Path - Errored Seconds	This OM measures the Near End Performance data: Errored Seconds - Path.
Accumulation OM	Carrier, Path - Failure Count	This OM measures the Near End Performance data: Failure Count - Path.
Accumulation OM	Carrier, Path - Severely Errored Seconds	This OM measures the Near End Performance data: Severely Errored Seconds - Path.
Accumulation OM	Carrier, Path - Unavailable Seconds	This OM measures the Near End Performance data: Unavailable Seconds - Path.
Accumulation OM	Gateway Screening Results, Disallowed Cld Party Addr Count	This OM measures the number of MSUs rejected on a particular link, because of disallowed SCCP Called Party Addresses.
Accumulation OM	Gateway Screening Results, Disallowed ISUP Count	This OM measures the number of MSUs rejected on a particular link, because of a disallowed ISDN User Part message type.
Accumulation OM	Gateway Screening Results, Disallowed Trans Type Count	This OM measures the number of MSUs rejected on a particular link, because of a disallowed SCCP GTT type.
Accumulation OM	Gateway Screening Results, Invalid Affct Destination Count	This OM measures the number of MSUs rejected on a particular link, because the destination fields in signaling-routeset-test, TFX/TCx, or TFC messages from the MSUs did not pass GWS checking based on the provisioned criteria.
Accumulation OM	Gateway Screening Results, Invalid Affct PC-SSN Count	This OM measures the number of MSUs rejected on a particular link, because the affected PCs in SCCP subsystem-prohibited (SSP) and subsystem-allowed (SSA) messages and an invalid PC or SSN in SCCP subsystem-status-test (SST) messages from the MSUs did not pass GWS checking based on the provisioned criteria.
Accumulation OM	Gateway Screening Results, Invalid Cng Party Addr Count	This OM measures the number of MSUs rejected on a particular link, because the Calling Party Addresses (PC or SSN) from the MSUs did not pass GWS checking based on the provisioned criteria.
Accumulation OM	Gateway Screening Results, Invalid DPC Count	This OM measures the number of MSUs rejected on a particular link, because the DPCs from the MSUs did not pass GWS checking based on the provisioned criteria.
Accumulation OM	Gateway Screening Results, Invalid OPC Count	This OM measures the number of MSUs rejected on a particular link, because the OPCs from the MSUs did not pass GWS checking based on the provisioned criteria.
Accumulation OM	Gateway Screening Results, Invalid SIO Count	This OM measures the number of MSUs rejected on a particular link, because the SIOs from the MSUs did not pass GWS checking based on the provisioned criteria.
Accumulation OM	GTT Type, GTTs Not Performed Count	This OM measures the total number of GTTs that could not be performed for a particular translation type (all reasons).
Accumulation OM	GTT Type, GTTs Performed Count	This OM measures the total number of MSUs that successfully completed GTT (that is, a match was found for the global title) for a particular translation type.

Accumulation OM	GTT Type, No Translation for Addr Count	This OM measures the number of times the Address Not Found error was encountered for a particular translation type (that is, there was no match found for the global title in the GTT table).
Accumulation OM	ISUP Received Message Counts, ACM Received Count	This OM measures the number of ISUP Address Complete Messages (ACM) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, ALT Received Count	This OM measures the number of ISUP Altering Messages (ALT) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, ANM Received Count	This OM measures the number of ISUP Answer Messages (ANM) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, BLA Received Count	This OM measures the number of ISUP Blocking Acknowledgement (BLA) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, BLO Received Count	This OM measures the number of ISUP Blocking Messages (BLO) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, CCR Received Count	This OM measures the number of ISUP Continuity Check Request Messages (CCR) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, CFN Received Count	This OM measures the number of ISUP Confusion Messages (CFN) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, CGB Received Count	This OM measures the number of ISUP Circuit Group Blocking Messages (CGB) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, CGBA Received Count	This OM measures the number of ISUP Circuit Group Blocking Acknowledgement Messages (CGBA) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, CGU Received Count	This OM measures the number of ISUP Circuit Group Unblocking Messages (CGU) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, CGUA Received Count	This OM measures the number of ISUP Circuit Group Unblocking Acknowledgement Messages (CGUA) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, CMC Received Count	This OM measures the number of ISUP Call Modification Completed Messages (CMC) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, CMR Received Count	This OM measures the number of ISUP Call Modification Request Messages (CMR) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, CMRJ Received Count	This OM measures the number of ISUP Call Modification Rejected Messages (CMRJ) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, CON Received Count	This OM measures the number of ISUP Connect Messages (CON) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, COT Received Count	This OM measures the number of ISUP Continuity Test Messages (COT) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, CPG Received Count	This OM measures the number of ISUP Call Progress Messages (CPG) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, CQM Received Count	This OM measures the number of ISUP Circuit Query Messages (CQM) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, CQR Received Count	This OM measures the number of ISUP Circuit Query Response Messages (CQR) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, CRA Received Count	This OM measures the number of ISUP Circuit Reservation Acknowledgement Messages (CRA) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, CRG Received Count	This OM measures the number of ISUP Charge Information Messages (CRG) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, CRM Received Count	This OM measures the number of ISUP Circuit Reservation Messages (CRM) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, CSV Received Count	This OM measures the number of ISUP Closed User Group Selection and Validation Request Messages (CSV) received from the SS7 Network.

Accumulation OM	ISUP Received Message Counts, CSVS Received Count	This OM measures the number of ISUP Closed User Group Selection and Validation Response Messages (CSVs) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, CVR Received Count	This OM measures the number of ISUP Circuit Validation Response Messages (CVR) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, CVT Received Count	This OM measures the number of ISUP Circuit Validation Test Messages (CVT) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, DRS Received Count	This OM measures the number of ISUP Delayed Release Messages (DRS) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, EXM Received Count	This OM measures the number of ISUP Exit Messages (EXM) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, FAA Received Count	This OM measures the number of ISUP Facility Accepted Messages (FAA) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, FAC Received Count	This OM measures the number of ISUP Facility Messages (FAC) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, FAD Received Count	This OM measures the number of ISUP Facility Deactivated Messages (FAD) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, FAI Received Count	This OM measures the number of ISUP Facility Information Messages (FAM) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, FAR Received Count	This OM measures the number of ISUP Facility Request Messages (FAR) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, FOT Received Count	This OM measures the number of ISUP Forward Transfer Messages (FOT) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, FRJ Received Count	This OM measures the number of ISUP Facility Rejected Messages (FRJ) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, GRA Received Count	This OM measures the number of ISUP Circuit Group Reset Acknowledgement Messages (GRA) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, GRS Received Count	This OM measures the number of ISUP Circuit Group Reset Messages (GRS) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, IAM Received Count	This OM measures the number of ISUP Initial Address Message Messages (IAM) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, IAMN1 Received Count	This OM measures the number of ISUP Initial Address Message Not Priority One Messages (IAMN1) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, IDR Received Count	This OM measures the number of ISUP Identification Request Messages (IDR) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, INF Received Count	This OM measures the number of ISUP Information Messages (INF) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, INR Received Count	This OM measures the number of ISUP Information Request Messages (INR) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, IRS Received Count	This OM measures the number of ISUP Identification Response Messages (IRS) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, ISUP Error No AS for OPC/CIC	This OM measures the number of ISUP messages discarded as a result of not being able to find a valid AS for a given OPC/CIC.
Accumulation OM	ISUP Received Message Counts, ISUP Error No OPC/CIC Data	This OM measures the number of ISUP messages discarded as a result of missing database entry for a given OPC/CIC.
Accumulation OM	ISUP Received Message Counts, ISUP Error No Path	This OM measures the number of ISUP messages discarded as a result of not being able to find a path to a given AS.
Accumulation OM	ISUP Received Message Counts, ISUP Error No Route	This OM measures the number of ISUP messages discarded as a result of not being able to find a route to a given AS.
Accumulation OM	ISUP Received Message Counts, ISUP Error Unknown Message	This OM measures the number of unrecognized ISUP Messages received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, LOP Received Count	This OM measures the number of ISUP Loop Prevention Messages (LOP) received from the SS7 Network.

Accumulation OM	ISUP Received Message Counts, LPA Received Count	This OM measures the number of ISUP Loop Back Acknowledgement Messages (LPA) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, NRM Received Count	This OM measures the number of ISUP Network Resource Management Messages (NRM) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, PAM Received Count	This OM measures the number of ISUP Pass Along Message Messages (PAM) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, PRG Received Count	This OM measures the number of ISUP Progress Messages (PRG) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, REL Received Count	This OM measures the number of ISUP Release Messages (RLC) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, RES Received Count	This OM measures the number of ISUP Resume Messages (RES) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, RLC Received Count	This OM measures the number of ISUP Release Complete Messages (RLC) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, RPM Received Count	This OM measures the number of ISUP Reconfiguration Progress Message Messages (ACM) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, RSC Received Count	This OM measures the number of ISUP Reset Circuit Messages (RSC) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, SAM Received Count	This OM measures the number of ISUP Subsequent Address Message Messages (SAM) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, SGM Received Count	This OM measures the number of ISUP Segmentation Messages (SGM) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, SUS Received Count	This OM measures the number of ISUP Suspend Messages (SUS) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, UBA Received Count	This OM measures the number of ISUP Unblocking Acknowledgement Messages (UBA) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, UBL Received Count	This OM measures the number of ISUP Unblocking Messages (UBL) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, UCIC Received Count	This OM measures the number of ISUP Unequipped Circuit Identification Code Messages (UCIC) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, UPA Received Count	This OM measures the number of ISUP User Part Available Messages (UPA) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, UPT Received Count	This OM measures the number of ISUP User Part Test Messages (UPT) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, USR Received Count	This OM measures the number of ISUP User-to-User Information Messages (USR) received from the SS7 Network.
Accumulation OM	ISUP Received Message Counts, Wrong NE Received Count	This OM measures the number of ISUP messages discarded as a result of not receiving the message from at a SG Network Element
Accumulation OM	Link Faults and Performance, Number of negative ack received	1.9 of Q.752 This OM measures number of negative acknowledgements received on the link indicating that the far end did not receive the message correctly.
Accumulation OM	Link Faults and Performance, Number of SUs received in error	1.8 of Q.752 This OM measures signaling units on a link, received in error.
Accumulation OM	Link Faults and Performance, Octets Retransmitted	3.2 of Q.752 This OM counts number of bytes that are retransmitted. This count includes SIO, SIF, opening flags and check bits.
Accumulation OM	Link Faults and Performance, SL alignment or proving failure	1.7 of Q.752 This OM measures link synchronization failures during alignment or proving and indicates a signaling data link fault which prevents the SdL moving into service.

Accumulation OM	Link Faults and Performance, SL failure-Abnormal FIBR/BSNR	1.3 of Q.752 This OM measures link synchronization failures and indicates complex failures in transmission or an intermittent hardware fault or even designer error.
Accumulation OM	Link Faults and Performance, SL failure-All reasons	1.2 of Q.752 This OM measures in_service link failures due to any reason. It does not count link activation failures.
Accumulation OM	Link Faults and Performance, SL failure-Exc. delay of ack	1.4 of Q.752 This OM measures link synchronization failures and indicates serious disturbances or an interruption of signaling data link.
Accumulation OM	Link Faults and Performance, SL failure-Exc. duration of cong.	1.6 of Q.752 This OM measures link synchronization failures caused by prolonged congestion on the link.
Accumulation OM	Link Faults and Performance, SL failure-Excessive error rate	1.5 of Q.752 This OM measures link synchronization failures and indicates noisy link.
Accumulation OM	Link Faults and Performance, SL failure-Other reasons	This OM measures link synchronization failures due to reasons other than Abnormal FIBR/BSNR, Excessive delay of ack, Excessive error rate or Excessive duration of congestion .
Accumulation OM	Link Management, Changeover Procedure Count	This OM measures the number of times the changeover procedure is used to move traffic from a link taken out of service to one or more alternate in-service links.
Accumulation OM	Link Management, Far End Mgmt Inhibit Count	This OM measures the number of times a link was successfully inhibited from the far end.
Accumulation OM	Link Management, Level 1 Congestion Count	This OM measures the number of times a link entered Level 1 congestion from no congestion.
Accumulation OM	Link Management, Level 1 Congestion Duration	This OM measures the total time, in seconds, a link was in Level 1 congestion.
Accumulation OM	Link Management, Level 2 Congestion Count	This OM measures the number of times a link entered Level 2 congestion from Level 1 or no congestion.
Accumulation OM	Link Management, Level 2 Congestion Duration	This OM measures the total time, in seconds, a link was in Level 2 congestion.
Accumulation OM	Link Management, Level 3 Congestion Count	This OM measures the number of times a link entered Level 3 congestion from Level 1, Level 2, or no congestion.
Accumulation OM	Link Management, Level 3 Congestion Duration	This OM measures the total time, in seconds, a link was in Level 3 congestion.
Accumulation OM	Link Management, Link Available Duration	This OM measures the total time, in seconds, a link was available to MTP Level 3.
Accumulation OM	Link Management, Link Deactivated Duration	This OM measures the total time, in seconds, a link was manually made unavailable to MTP Level 3 by deactivation.
Accumulation OM	Link Management, Link Local Inhibit Duration	This OM measures the total time, in seconds, a link was manually made unavailable to MTP Level 3 by local inhibition.
Accumulation OM	Link Management, Link Remote Inhibit Duration	This OM measures the total time, in seconds, a link was manually made unavailable to MTP Level 3 by remote inhibition.
Accumulation OM	Link Management, Near End Forced Unavailable Count	This OM measures the number of times a link was manually made unavailable to MTP Level 3.
Accumulation OM	Link Management, RPO Count	This OM measures the number of times a link became unavailable to MTP Level 3 after the system received SIPO from the far end. This OM is not applicable for SAAL-based High Speed Links.
Accumulation OM	Link Management, RPO Cumulative Duration	This OM measures the total time, in seconds, that a link was unavailable to MTP Level 3 after the system received SIPO from the far end. This OM is not applicable for SAAL-based High Speed Links.
Accumulation OM	Link Management, Unavailable Duration	This OM measures the total time, in seconds, a link was unavailable (automatically or manually made unavailable) to MTP Level 3.

Accumulation OM	Link Traffic, MSUs Received Count	This OM measures the number of MSUs received on a link, including those MSUs for which retransmission was requested in the SS7 network. For the SAAL-based High Speed Links, the above description applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, MSUs Requiring GTT Count	This OM measures the number of incoming MSUs that require GTT, regardless of the outcome of any GWS operation. For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, MSUs Transmitted Count	This OM measures the number of MSUs transmitted to the far end, including those MSUs that were retransmitted in the SS7 network. For the SAAL-based High Speed Links, the above description applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, Network Indicator Discard Count	This OM measures the number of received MSUs which were discarded due to a mismatch between the MSU's network indicator (NI) and the NI provisioned in this system. The NI may be provisioned on a network appearance basis. For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, Octets Received Count	This OM measures the total number of octets actually received for all MSUs counted in the MSUs Received Count OM, before the octets are removed in MTP Level 2 processing for the SS7 network. For the MTP2-based links, this count accounts for MTP User Data + MTP L3 Data + MTP L2 Data octets. For the SAAL-based High Speed Links, this count applies to Message octets (MTP User Data + MTP L3 Data octets).
Accumulation OM	Link Traffic, Octets Requiring GTT Count	This OM measures the total number of MSU octets received for MSUs requiring GTT, including octets removed in MTP Level 2 processing. For the MTP2-based links, this count applies to MSU octets (MTP User Data + MTP L3 Data + MTP L2 Data octets). For the SAAL-based High Speed Links, this count applies to Message octets (MTP User Data + MTP L3 Data octets).
Accumulation OM	Link Traffic, Octets Transmitted Count	This OM measures the total number of octets actually transmitted for all MSUs counted in the MSUs Transmitted Count OM, including octets added in MTP Level 2 processing for the SS7 network. For the MTP2-based links, this count accounts for MTP User Data + MTP L3 Data + MTP L2 Data octets. For the SAAL-based High Speed Links, this count applies to Message octets (MTP User Data + MTP L3 Data octets).
Accumulation OM	Link Traffic, Originated MSU Octets Count	This OM measures the total number of originated MSU octets (MSU that contains the PC or capability code of this system in the OPC field) transmitted, including those octets that were added in MTP Level 2 processing for the SS7 network. For the MTP2-based links, this count accounts for MTP User Data + MTP L3 Data + MTP L2 Data octets. For the SAAL-based High Speed Links, this count applies to Message octets (MTP User Data + MTP L3 Data octets).

Accumulation OM	Link Traffic, Originated MSUs Count	This OM measures the number of originated MSUs (MSUs that contain the PC or capability code of this system in the OPC field) that are successfully passed to Level 2 for transmission (for example, network management messages and MSUs completing GTT) in the SS7 network. For the MTP2-based links, this count applies to MSU octets (MTP User Data + MTP L3 Data + MTP L2 Data octets). For the SAAL-based High Speed Links, this count applies to Message octets (MTP User Data + MTP L3 Data octets).
Accumulation OM	Link Traffic, Pri 0 MSU Inbd Discard Count	This OM measures the number of priority 0 MSUs discarded by the inbound link due to congestion at levels 1, 2, or 3 in the transmit buffers for the outbound link in the SS7 network. For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, Pri 0 MSU Outbd Discard Count	This OM measures the number of priority 0 MSUs discarded due to congestion at levels 1, 2, or 3 in the SS7 network. For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, Pri 1 MSU Inbd Discard Count	This OM measures the number of priority 1 MSUs discarded by the inbound link due to congestion at levels 2 or 3 in the transmit buffers in the outbound link in the SS7 network. For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, Pri 1 MSU Outbd Discard Count	This OM measures the number of priority 1 MSUs discarded due to congestion at levels 2 or 3 in the SS7 network. For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, Pri 2 MSU Inbd Discard Count	This OM measures the number of priority 2 MSUs discarded by the inbound link due to congestion at level 3 in the transmit buffers for the outbound link in the SS7 network. For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, Pri 2 MSU Outbd Discard Count	This OM measures the number of priority 2 MSUs discarded due to level 3 congestion in the SS7 network. For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, Pri 3 MSU Inbd Discard Count	This OM measures the number of priority 3 MSUs discarded by the inbound link due to full transmit buffers for the outbound link in the SS7 network. For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, Pri 3 MSU Outbd Discard Count	This OM measures the number of priority 3 MSUs discarded due to a full transmit buffer in the SS7 network. For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).

Accumulation OM	Link Traffic, Terminated MSU Octets Count	This OM measures the total number of terminated MSU octets (acknowledged, incoming MSU that contains the PC or capability code of this system in the DPC field) received, including octets removed in MTP Level 2 processing for the SS7 network. For the MTP2-based links, this count accounts for MTP User Data + MTP L3 Data + MTP L2 Data octets. For the SAAL-based High Speed Links, this count applies to Message octets (MTP User Data + MTP L3 Data octets).
Accumulation OM	Link Traffic, Terminated MSUs Count	This OM measures the number of terminated MSUs (acknowledged, incoming MSUs that contain the PC or capability code of this system in the DPC field) received from the SS7 network. For the MTP2-based links, this count applies to MSUs (MTP User Data + MTP L3 Data + MTP L2 Data). For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data).
Accumulation OM	Link Traffic, Through-Switched MSUs Count	This OM measures the number of through-switched MSUs (MSUs that do not contain the PC or capability code of this system in either the OPC or DPC) that are acknowledged, translated, and successfully passed to MTP Level 2 for transmission in the SS7 network. For the MTP2-based links, this count applies to MSUs (MTP User Data + MTP L3 Data + MTP L2 Data). For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data).
Accumulation OM	Link Traffic, Thru-Switched MSU Octets Count	This OM measures the total number of through-switched MSU octets (MSU that does not contain the PC or capability code of this system in either the OPC or DPC) received, including those octets that were added in MTP Level 2 processing for the SS7 network. For the MTP2-based links, this count accounts for MTP User Data + MTP L3 Data + MTP L2 Data octets. For the SAAL-based High Speed Links, this count applies to Message octets (MTP User Data + MTP L3 Data octets).
Accumulation OM	Linkset Utilization, Linkset Inactivity Duration	This OM measures the total time, in seconds, that all links in the linkset were unavailable (automatically or manually made unavailable) to MTP Level 3.
Accumulation OM	Linkset Utilization, RST Received Count	This OM measures the number of restart (RST) messages received.
Accumulation OM	Linkset Utilization, RST Transmitted Count	This OM measures the number of restart (RST) messages transmitted.
Accumulation OM	Linkset Utilization, TFA and TCA Received Count	This OM measures the number of transfer-allowed (TFA) and transfer-cluster-allowed (TCA) messages received.
Accumulation OM	Linkset Utilization, TFA and TCA Transmitted Count	This OM measures the number of transfer-allowed (TFA) and transfer-cluster-allowed (TCA) messages transmitted.
Accumulation OM	Linkset Utilization, TFC Received Count	This OM measures the number of transfer-controlled (TFC) messages received by the gateway, listed by the originating network.
Accumulation OM	Linkset Utilization, TFC Transmitted Count	This OM measures the number of transfer-controlled (TFC) messages transmitted by the gateway, listed by the destination network.
Accumulation OM	Linkset Utilization, TFP and TCP Received Count	This OM measures the number of transfer-prohibited (TFP) and transfer-cluster-prohibited (TCP) messages received.
Accumulation OM	Linkset Utilization, TFP and TCP Transmitted Count	This OM measures the number of transfer-prohibited (TFP) and transfer-cluster-prohibited (TCP) messages transmitted.
Accumulation OM	Linkset Utilization, TFR and TCR Received Count	This OM measures the number of transfer-restricted (TFR) and transfer-cluster-restricted (TCR) messages received.
Accumulation OM	Linkset Utilization, TFR and TCR Transmitted Count	This OM measures the number of transfer-restricted (TFR) and transfer-cluster-restricted (TCR) messages transmitted.

Accumulation OM	Log Server, Critical Alarms Ack Count	This OM measures the number of critical alarms acknowledged by the Log server.
Accumulation OM	Log Server, Critical Alarms Cleared Count	This OM measures the number of critical alarms cleared by the Log server.
Accumulation OM	Log Server, Critical Alarms Received Count	This OM measures the number of critical alarms received by the Log server.
Accumulation OM	Log Server, Major Alarms Ack Count	This OM measures the number of major alarms acknowledged by the Log server.
Accumulation OM	Log Server, Major Alarms Cleared Count	This OM measures the number of major alarms cleared by the Log server.
Accumulation OM	Log Server, Major Alarms Received Count	This OM measures the number of major alarms received by the Log server.
Accumulation OM	Log Server, Minor Alarms Ack Count	This OM measures the number of minor alarms acknowledged by the Log server.
Accumulation OM	Log Server, Minor Alarms Cleared Count	This OM measures the number of minor alarms cleared by the Log server.
Accumulation OM	Log Server, Minor Alarms Received Count	This OM measures the number of minor alarms received by the Log server.
Accumulation OM	NP Database Totals, Add/Change Updates	This OM measures the total number of add/change updates received from the LSMS.
Accumulation OM	NP Database Totals, Delete Updates	This OM measures the total number of delete updates received from the LSMS.
Accumulation OM	NP Database Totals, Emergency Updates	This OM measures the total number of application database updates received from the USP debug facility and can only be displayed from the debug facility Note: Debug is only accessible by Nortel Networks Support Personnel.
Accumulation OM	NP Database Totals, Operational Time	This OM measures the total time within the OM interval that the NPDB was operational.
Accumulation OM	NP Database Totals, Retransmitted Updates	This OM measures the total number of updates retransmitted within the BroadBand STP.
Accumulation OM	NP INAP Totals, INAP CdPN Normalize Failures	This OM measures the number of called party number normalization failures.
Accumulation OM	NP INAP Totals, INAP Indeterminate Queries	This OM measures the number of INAP indeterminate queries.
Accumulation OM	NP INAP Totals, INAP Invalid Context	This OM measures the number of INAP queries with invalid application context.
Accumulation OM	NP INAP Totals, INAP Queries Non-Ported	This OM measures the number of INAP non ported number queries received.
Accumulation OM	NP INAP Totals, INAP Queries Ported	This OM measures the number of INAP ported number queries received.
Accumulation OM	NP INAP Totals, INAP Queries Ported Across	This OM measures the number of INAP ported across number queries received.
Accumulation OM	NP INAP Totals, INAP Queries Ported In	This OM measures the number of INAP ported in number queries received.
Accumulation OM	NP INAP Totals, INAP Queries Ported Out	This OM measures the number of INAP ported out number queries received.
Accumulation OM	NP INAP Totals, INAP Queries Unknown	This OM measures the number of INAP queries received for numbers with unknown ported status.
Accumulation OM	NP INAP Totals, INAP Query Failures	This OM measures the number of INAP query failures.
Accumulation OM	NP INAP Totals, INAP Query Time Outs	This OM measures the total number of INAP query time outs.
Accumulation OM	NP INAP Totals, INAP Total Queries	This OM measures the total number of INAP queries received.
Accumulation OM	NP LSSI Totals, MR Query Received	This OM measures the total number of MR queries received by an NPC or NPS system node.
Accumulation OM	NP LSSI Totals, NP Query Received	This OM measures the total number of NP queries received by an NPC or an NPS system node.
Accumulation OM	NP NETID Totals, MR Failures	This OM measures the total number of MR query failures identified. The MR Failures value is based upon the Network ID of a received SCCP message.

Accumulation OM	NP NETID Totals, MR GTT Overrides	This OM measures the total number of MR queries receiving GTT override. The MR GTT Overrides value is based upon the Network ID of a received SCCP message.
Accumulation OM	NP NETID Totals, MR Loop Detection	This OM measures the total number of potential looping detections. The MR Loop Detection value is based upon the Network ID of a received SCCP message.
Accumulation OM	NP NETID Totals, MR Non-Ported	This OM measures the total number of MR queries received for non-porting numbers. The MR Non-Ported value is based upon the Network ID of a received SCCP message.
Accumulation OM	NP NETID Totals, MR Ported	This OM measures the total number of MR queries received for porting numbers. The MR Ported value is based upon the Network ID of a received SCCP message.
Accumulation OM	NP NETID Totals, MR Total	This OM measures the total number of MR queries received. The MR Total value is based upon the Network ID of a received SCCP message.
Accumulation OM	NP NETID Totals, NP Failures	This OM measures the total number of NP query failures. The NP Failures value is based upon the Network ID of a received TCAP message.
Accumulation OM	NP NETID Totals, NP Non-Ported	This OM measures the total number of NP queries received for non-porting numbers. The NP Non-Ported value is based upon the Network ID in the TCAP message.
Accumulation OM	NP NETID Totals, NP Ported	This OM measures the total number of NP queries received for porting numbers. The NP Ported value is based upon the Network ID contained in the NETID of a received TCAP message.
Accumulation OM	NP NETID Totals, NP Total	This OM measures the total number of NP queries received. The NP Total value is based upon the Network ID of a received TCAP message.
Accumulation OM	NP Service Rule Totals, Service Rule Match	This OM measures the total number of matches for the Service Rule.
Accumulation OM	NP Service Rule Totals, Service Rule Mismatch	This OM measures the total number of mismatches for all the Service Rules.
Accumulation OM	NP Service Totals, Database Mismatches	This OM measures the total number of Database mismatches. This OM is collected by Service ID.
Accumulation OM	NP Service Totals, GTA Normalization Failures	This OM measures the total number of GTA number normalization failures. This OM is collected by Service ID.
Accumulation OM	NP Service Totals, GTA Replacement	This OM measures the total number of service queries receiving GTA replacement. This OM is collected by Service ID.
Accumulation OM	NP Service Totals, GTT Overrides	This OM measures the total number of service queries receiving GTT override. This OM is collected by Service ID.
Accumulation OM	NP Service Totals, RN Check Failures	This OM measures the total number of RN check failures on incoming messages using the NoA/RN table. This OM is collected by Service ID.
Accumulation OM	NP Service Totals, Service Failures	This OM measures the total number of Service query failures identified. Service query failures occur when the query logic is unable to process the Service query. This OM is collected by Service ID.
Accumulation OM	NP Service Totals, Service Non-Ported	This OM measures the total number of Service queries received for non-porting numbers. This OM is collected by Service ID.
Accumulation OM	NP Service Totals, Service Ported	This OM measures the total number of Service queries received for porting numbers. The Service Ported value is the total of OMR_SERVICE_PORTED_IN, OMR_SERVICE_PORTED_OUT, and OMR_SERVICE_PORTED_ACROSS This OM is collected by Service ID.
Accumulation OM	NP Service Totals, Service Total	This OM measures the total number of Service queries received. This OM is collected by Service ID.

Accumulation OM	NP Service Totals, TT Replacement	This OM measures the total number of service queries receiving TT replacement. This OM is collected by Service ID.
Accumulation OM	NP SMI Totals, High Congestion	This OM measures the total number of times that the high level congestion state was entered.
Accumulation OM	NP SMI Totals, Login Failures	This OM measures the total number of failed LSMS login attempts.
Accumulation OM	NP SMI Totals, Low Congestion	This OM measures the total number of times that the low level congestion state was entered.
Accumulation OM	NP SMI Totals, Medium Congestion	This OM measures the total number of times that the medium level congestion state was entered.
Accumulation OM	NP SMI Totals, Messages Invalid	This OM measures the total number of invalid messages received from the LSMS.
Accumulation OM	NP SMI Totals, Messages Received	This OM measures the total number of messages received from the LSMS.
Accumulation OM	NP SMI Totals, Messages Rejected	This OM measures the total number of received messages from the LSMS that were rejected.
Accumulation OM	NP SRF Totals, SRF Ind. Routing with Ref. Sub.	This OM measures the number of SRF messages relayed to the subscription network via indirect routing with reference to the subscription network.
Accumulation OM	NP SRF Totals, SRF No NP DB Record Found	This OM measures the number of SRF queries received when no record is found in the NP DB.
Accumulation OM	NP SRF Totals, SRF Queries Non-Ported	This OM measures the number of SRF non ported number queries received.
Accumulation OM	NP SRF Totals, SRF Queries Ported Across	This OM measures the number of SRF ported across number queries received.
Accumulation OM	NP SRF Totals, SRF Queries Ported In	This OM measures the number of SRF ported in number queries received.
Accumulation OM	NP SRF Totals, SRF Queries Ported Out	This OM measures the number of SRF ported out number queries received.
Accumulation OM	NP SRF Totals, SRF Queries Unknown	This OM measures the number of SRF queries received for numbers with unknown ported status.
Accumulation OM	NP SRF Totals, SRF Query Failures	This OM measures the number of SRF query failures.
Accumulation OM	NP SRF Totals, SRF Relayed to HLR	This OM measures the number of SRF messages relayed to the HLR.
Accumulation OM	NP SRF Totals, SRF Successful Messages to MSC	This OM measures the number of SRF successful messages sent back to the MSC.
Accumulation OM	NP SRF Totals, SRF Total Queries	This OM measures the total number of SRF queries received.
Accumulation OM	NP SRF Totals, SRF Total Queries Ported	This OM measures the total number of SRF ported number queries received.
Accumulation OM	NP SRF Totals, SRF Transaction Errors Sent Out	This OM measures the number of SRF transaction error messages sent out.
Accumulation OM	NP TnT Totals, TNT Acks Sent	This OM measures the number of Tariff non Transparency acknowledgement messages transmitted.
Accumulation OM	NP TnT Totals, TNT Decode Errors	This OM measures the number of Tariff non Transparency MAP decode failures due to incorrect parameters that could not be decoded.
Accumulation OM	NP TnT Totals, TNT Decode Invalid Params	This OM measures the number of Tariff non Transparency MAP decode failures due to invalid parameters. (i.e. IMSI instead of MSISDN included)
Accumulation OM	NP TnT Totals, TNT No NP DB Rec Found	This OM measures the number of Tariff non Transparency queries received for numbers not found in the NP DB.
Accumulation OM	NP TnT Totals, TNT Queries Non-Ported	This OM measures the number of Tariff non Transparency non ported number queries received.
Accumulation OM	NP TnT Totals, TNT Queries Ported Across	This OM measures the number of Tariff non Transparency ported across number queries received.
Accumulation OM	NP TnT Totals, TNT Queries Ported In	This OM measures the number of Tariff non Transparency ported in number queries received.

Accumulation OM	NP TnT Totals, TNT Queries Ported Out	This OM measures the number of Tariff non Transparency ported out number queries received.
Accumulation OM	NP TnT Totals, TNT Queries Unknown	This OM measures the number of Tariff non Transparency queries received for numbers with unknown ported status.
Accumulation OM	NP TnT Totals, TNT Query Failures	This OM measures the number of Tariff non Transparency query failures during processing.
Accumulation OM	NP TnT Totals, TNT Total Messages Received	This OM measures the total number of Tariff non Transparency queries received.
Accumulation OM	NP TnT Totals, TNT Total Queries Ported	This OM measures the total number of Tariff non Transparency ported number queries received.
Accumulation OM	NP TnT Totals, TNT Transmission Failures	This OM measures the number of Tariff non Transparency failures during transmission of Ack.
Accumulation OM	Route Set Management, RouteSet Congested Count	This OM measures the number of times, a routeset went into network congestion.
Accumulation OM	Route Set Management, Routeset Man-busied Count	This OM measures the number of times a routeset was manually made unavailable.
Accumulation OM	Route Set Management, Routeset Unavailability Count	This OM measures the number of times a routeset was unavailable.
Accumulation OM	Route Set Management, Routeset Unavailability Dur.	This OM measures the total time, in seconds, a routeset was unavailable.
Accumulation OM	RTC Sanity, RTC12 Passive Audit Count	This OM hooks into the node maintenance audit, and is pegged on the control shelf CCs, when it does not receive audit request from RTC12 even once. Thus this is a passive audit of RTC
Accumulation OM	RTC Sanity, RTC15 Passive Audit Count	This OM hooks into the node maintenance audit, and is pegged on both the control shelf CCs, when it does not receive audit request from RTC15 even once. Thus this is a passive audit of RTC.
Accumulation OM	SAAL Link Management, Cum. Dur. of FE Processor Out.	This OM measures the cumulative duration in seconds during which the use of the link was precluded due to a remote (far-end) processor outage condition, summed across all far-end processor outage events.
Accumulation OM	SAAL Link Management, Cum. Dur. of Lack-of-Credit	This OM measures the cumulative duration of time in seconds during which SSCOP had PDUs to send to its peer but could not do so because it was not given credit by the far end, summed over all the Lack-of-Credit events occurring during the measurement interval.
Accumulation OM	SAAL Link Management, Duration of Link in Service	This OM measures the number of seconds the link is regarded in service.
Accumulation OM	SAAL Link Management, Invalid SSCOP PDUs Rx	This OM measures the number of Invalid SSCOP PDUs Received.
Accumulation OM	SAAL Link Management, Lack of Credit Events	This OM measures the number of Lack-of-Credit Events.
Accumulation OM	SAAL Link Management, PDUs Tx Requiring RTx	This OM measures the number of SSCOP PDUs transmitted that required retransmission because they were not acknowledged by the far-end's SSCOP peer.
Accumulation OM	SAAL Link Management, Signaling Link Alig. Failures	This OM measures the number of Signaling Link Alignment Failures.
Accumulation OM	SAAL Link Management, SSCOP Connection Disconnects	This OM measures the number of SSCOP Connection Disconnects which are characterized by the expiry of Timer_NO_RESPONSE.
Accumulation OM	SAAL Link Management, SSCOP Connection Init. Fails	This OM measures the number of SSCOP Initiation Failures, i.e. the inability to establish an SSCOP Connection.
Accumulation OM	SAAL Link Management, SSCOP Connection Re-est/Resync	This OM measures the number of SSCOP Re-establishments/Resynchronizations.
Accumulation OM	SAAL Link Management, SSCOP Connection Sum-of-Errors	This OM measures the total number of SSCOP Connection Disconnects, Connection Initiation Failures and Connection Re-establishment/Resynchronization.

Accumulation OM	SAAL Link Management, SSCOP PDUs Sum-of-Errors	This OM measures the total number of Unexpected SSCOP PDUs, Invalid SSCOP PDUs and SSCOP PDUs with Other/List Element Errors.
Accumulation OM	SAAL Link Management, SSCOP PDUs with List Elem. Errs	This OM measures the number of SSCOP PDUs Received with List Element Errors.
Accumulation OM	SAAL Link Management, Unexpected SSCOP PDUs Rx	This OM measures the number of Unexpected SSCOP PDUs Received.
Accumulation OM	SAAL Link Traffic, PDU Octets RTx	This OM measures the number of octets associated with retransmitted SSCOP Sequenced Data PDUs.
Accumulation OM	SAAL Link Traffic, PDU Octets Rx	This OM measures the number of octets associated with SSCOP Sequenced Data PDUs received.
Accumulation OM	SAAL Link Traffic, PDU Octets Tx	This OM measures the number of octets associated with SSCOP Sequenced Data PDUs transmitted, including retransmissions.
Accumulation OM	SAAL Link Traffic, PDUs RTx	This OM measures the number of SSCOP Sequenced Data PDUs retransmitted.
Accumulation OM	SAAL Link Traffic, PDUs Rx	This OM measures the number of SSCOP Sequenced Data PDUs received.
Accumulation OM	SAAL Link Traffic, PDUs Tx	This OM measures the number of SSCOP Sequenced Data PDUs transmitted including retransmissions.
Accumulation OM	SAAL Link Traffic, Total PDU Octets Rx	This OM measures the number of octets associated with received SSCOP PDUs of all types.
Accumulation OM	SAAL Link Traffic, Total PDU Octets Tx	This OM measures the number of octets associated with transmitted SSCOP PDUs of all types which may include Sequenced Data PDU retransmissions.
Accumulation OM	SAAL Link Traffic, Total PDUs Rx	This OM measures the number of SSCOP PDUs of all types received.
Accumulation OM	SAAL Link Traffic, Total PDUs Tx	This OM measures the number of transmitted SSCOP PDUs of all types including Sequenced Data PDU retransmissions.
Accumulation OM	SCCP GTT, Alt Routing on Cong Count	This OM measures the number of times a message is routed to the backup system because the routeset to the primary system is congested.
Accumulation OM	SCCP GTT, GTT Performed Count	This OM measures the total number of MSUs that successfully completed GTT (that is, a match was found for the global title). The count is kept across all translation types.
Accumulation OM	SCCP GTT, Hop Counter Violation Count	This OM measures the number of times that a SCCP hop counter violation has occurred.
Accumulation OM	SCCP GTT, No Translation for Addr Count	This OM measures the number of times a match could not be found for the GTA in the translation table. The count is kept across all translation types.
Accumulation OM	SCCP GTT, Trans Type Not Found Count	This OM measures the number of times the translation type specified in the MSU was not supported by the USP.
Accumulation OM	SCCP Local Subsystem, # Msgs for Local SS discarded	This OM measures the number of messages destined to local subsystems that were discarded.
Accumulation OM	SCCP Local Subsystem, # Msgs for Local SS UDTSed	This OM measures the number of messages destined to local subsystems that receive an error response (UDTS).
Accumulation OM	SCCP Local Subsystem, Subsystem Activated	This OM measures the number of times a subsystem has been manually activated.
Accumulation OM	SCCP Local Subsystem, Subsystem Allowed	This OM measures the number of times a subsystem has gone in service (allowed).
Accumulation OM	SCCP Local Subsystem, Subsystem Allowed Duration	This OM measures the total duration that the subsystem was in service (allowed).
Accumulation OM	SCCP Local Subsystem, Subsystem Deactivated	This OM measures the number of times a subsystem has been manually deactivated.
Accumulation OM	SCCP Local Subsystem, Subsystem Prohibited	This OM measures the number of times a subsystem has gone out of service (prohibited). Unit of measure is a 10 second period.

Accumulation OM	SCCP Local Subsystem, Subsystem Prohibited Duration	This OM measures the total duration that a subsystem was out of service (prohibited). Unit of measure is a 10 second period.
Accumulation OM	SCCP LSS Instance, SSI Activated	This OM measures the number of times a subsystem instance has been manually activated.
Accumulation OM	SCCP LSS Instance, SSI Allowed	This OM measures the number of times a subsystem instance has gone in service (allowed).
Accumulation OM	SCCP LSS Instance, SSI Allowed Duration	This OM measures the duration that the subsystem instance was in service (allowed). Unit of measure is a 10 second period.
Accumulation OM	SCCP LSS Instance, SSI Application Failure	This OM measures the number of times a subsystem instance has gone out of service (application failure).
Accumulation OM	SCCP LSS Instance, SSI Congested	This OM measures the number of times a subsystem instance has gone into congestion.
Accumulation OM	SCCP LSS Instance, SSI Deactivated	This OM measures the number of times a subsystem instance has gone out of service (manually deactivated).
Accumulation OM	SCCP LSS Instance, SSI Platform Failure	This OM measures the number of times a subsystem instance has gone out of service (platform failure).
Accumulation OM	SCCP LSS Instance, SSI Prohibited Duration	This OM measures the duration a local subsystem instance has been out of service (prohibited). Unit of measure is a 10 second period.
Accumulation OM	SCCP System Totals, Conn-Orient IP Dist Viol Count	This OM measures the number of IP originated connection-oriented messages that were discarded because they requested SCCP distribution
Accumulation OM	SCCP System Totals, Conn-Orient Msg Handled Count	This OM measures the number of connection- oriented messages that were successfully routed
Accumulation OM	SCCP System Totals, Conn-Orient Msg Rtg Fail Count	This OM measures the number of connection- oriented messages that the USP was unable to route
Accumulation OM	SCCP System Totals, LUDT Msg Rcvd Count	This OM measures the number of LUDT messages that the SCCP level received.
Accumulation OM	SCCP System Totals, LUDT Msg Sent Count	This OM measures the number of LUDT messages that the SCCP level sent.
Accumulation OM	SCCP System Totals, LUDTS Msg Rcvd Count	This OM measures the number of LUDTS messages that the SCCP level received.
Accumulation OM	SCCP System Totals, LUDTS Msg Sent Count	This OM measures the number of LUDTS messages that the SCCP level sent.
Accumulation OM	SCCP System Totals, Msg Incompatibility	This OM measures the number of LUDTS messages that the SCCP level sent.
Accumulation OM	SCCP System Totals, Msg too large for segmentation	This OM measures the number of times segmentation fails due to an over-long message.
Accumulation OM	SCCP System Totals, MSUs Disc-Unrec SCCP Msg Count	This OM measures the number of MSUs discarded because of an unrecognized SCCP message type.
Accumulation OM	SCCP System Totals, Out of sequence SCCP msg count	This OM measures the number of times Segments are received out of sequence
Accumulation OM	SCCP System Totals, Reassembly buffer unavailable	This OM measures the number of times Reassembly resources unavailable occurred
Accumulation OM	SCCP System Totals, Reassembly failed	This OM measures the number of times Reassembly fails for any non-specified reason.
Accumulation OM	SCCP System Totals, Reassembly Timer Expired	This OM measures the number of times Reassembly Timer expired
Accumulation OM	SCCP System Totals, Routing Failure - Unequip.User	This OM measures the number of times SCCP Routing control fails to find a subsystem to route the message.
Accumulation OM	SCCP System Totals, SCCP Routing Failure Count	This OM measures the number of messages that SCCP was unable to route.
Accumulation OM	SCCP System Totals, Segmentation failed	This OM measures the number of times segmentation fails for any non-specified reason.
Accumulation OM	SCCP System Totals, SSA Received Count	This OM measures the number of subsystem-allowed (SSA) messages received.
Accumulation OM	SCCP System Totals, SSA Transmitted Count	This OM measures the number of subsystem-allowed (SSA) messages transmitted.

Accumulation OM	SCCP System Totals, SSP Received Count	This OM measures the number of subsystem-prohibited (SSP) messages received.
Accumulation OM	SCCP System Totals, SSP Transmitted Count	This OM measures the number of subsystem-prohibited (SSP) messages transmitted.
Accumulation OM	SCCP System Totals, SST Received Count	This OM measures the number of subsystem-status-test (SST) messages received.
Accumulation OM	SCCP System Totals, SST Transmitted Count	This OM measures the number of subsystem-status-test (SST) messages transmitted.
Accumulation OM	SCCP System Totals, Total messages handled	This OM measures all messages processed by SCCP routing control in both incoming and outgoing directions, whether or not the message is processed or delivered successfully. It includes Class 2 and Class 3 connection oriented messages. It does not include Subsystem Status messages such as SSP, SSA, or SST.
Accumulation OM	SCCP System Totals, UDT Msg Rcvd Count	This OM measures the number of UDT messages that the SCCP level received.
Accumulation OM	SCCP System Totals, UDT Msg Sent Count	This OM measures the number of UDT messages sent from the SCCP level.
Accumulation OM	SCCP System Totals, UDTs Msg Rcvd Count	This OM measures the number of UDTs messages that the SCCP level received.
Accumulation OM	SCCP System Totals, UDTs Msg Sent Count	This OM measures the number of UDTs messages sent from the SCCP level.
Accumulation OM	SCCP System Totals, XUDT Msg Rcvd Count	This OM measures the number of XUDT messages that the SCCP level received.
Accumulation OM	SCCP System Totals, XUDT Msg Sent Count	This OM measures the number of XUDT messages sent from the SCCP level.
Accumulation OM	SCCP System Totals, XUDTS Msg Rcvd Count	This OM measures the number of XUDTS messages that the SCCP level received.
Accumulation OM	SCCP System Totals, XUDTS Msg Sent Count	This OM measures the number of XUDTS messages sent from the SCCP level.
Accumulation OM	SCTP Management/Traffic Counts, Association Aborted Count	This OM measures the number of associations that are aborted by the application, the peer connection or a failure in the network.
Accumulation OM	SCTP Management/Traffic Counts, Association Establish Attempts	This OM measures the number of associations which the user or peer SCTP tried to established.
Accumulation OM	SCTP Management/Traffic Counts, Association Terminated Count	This OM measures the number of associations that are terminated by the application or the peer connection.
Accumulation OM	SCTP Management/Traffic Counts, Chunk Retransmitted Count	This OM measures the number of SCTP chunks retransmitted due to SCTP Packets or SCTP Sacks lost in the network. Note: A SCTP packet may contain more than one chunk.
Accumulation OM	SCTP Management/Traffic Counts, Chunks Received Count	This OM measures the number of SCTP chunks received. Note: A SCTP packet may contain more than one chunk.
Accumulation OM	SCTP Management/Traffic Counts, Chunks Transmitted Count	This OM measures the number of SCTP chunks transmitted. Note: A SCTP packet may contain more than one chunk.
Accumulation OM	SCTP Management/Traffic Counts, Established Association Count	This OM measures the number of associations which are in a established state.
Accumulation OM	SCTP Management/Traffic Counts, Out of Blue SCTP Packet	This OM measures the number of SCTP packets that are received but are not able to identify the association to which they belong.
Accumulation OM	SLR Database Totals, Add/Change Updates	This OM measures the total number of add/change updates received from the HLR provisioning system.
Accumulation OM	SLR Database Totals, Delete Updates	This OM measures the total number of delete updates received from the HLR provisioning system.
Accumulation OM	SLR Database Totals, Emergency Updates	This OM measures the total number of application database updates received from the USP debug facility and can only be displayed from the debug facility Note: Debug is only accessible by Nortel Networks Support Personnel.

Accumulation OM	SLR Database Totals, Operational Time	This OM measures the total time within the OM interval that the SLRDB was operational.
Accumulation OM	SLR Database Totals, Retransmitted Updates	This OM measures the total number of updates retransmitted within the BroadBand STP.
Accumulation OM	SLR LSSI Totals, Total Failed Queries	This OM measures the total number of SLR queries received by an NPC or NPS system node that failed for any reason across all services and message types.
Accumulation OM	SLR LSSI Totals, Total Queries Received	This OM measures the total number of SLR queries received by an NPC or an NPS system node across all services and message types.
Accumulation OM	SLR Message Type Totals, IMSI Failed Queries	This OM measures the total number of IMSI queries received by an NPC or an NPS system node that failed for any reason.
Accumulation OM	SLR Message Type Totals, IMSI Failed SLRDB Lookup	This OM measures the total number of IMSI queries received by an NPC or an NPS system node that failed in their SLRDB lookup.
Accumulation OM	SLR Message Type Totals, IMSI Query Received	This OM measures the total number of IMSI queries received by an NPC or an NPS system node.
Accumulation OM	SLR Message Type Totals, IMSI Successful SLRDB Lookup	This OM measures the total number of IMSI queries received by an NPC or an NPS system node that succeeded in their SLRDB lookup.
Accumulation OM	SLR Message Type Totals, MSISDN Failed Queries	This OM measures the total number of MSISDN queries received by an NPC or an NPS system node that failed for any reason.
Accumulation OM	SLR Message Type Totals, MSISDN Failed SLRDB Lookup	This OM measures the total number of MSISDN queries received by an NPC or an NPS system node that failed in their SLRDB lookup.
Accumulation OM	SLR Message Type Totals, MSISDN Query Received	This OM measures the total number of MSISDN queries received by an NPC or an NPS system node.
Accumulation OM	SLR Message Type Totals, MSISDN Successful SLRDB Lookup	This OM measures the total number of MSISDN queries received by an NPC or an NPS system node that succeeded in their SLRDB lookup.
Accumulation OM	SLR SMI Totals, High Congestion	This OM measures the total number of times that the high level congestion state was entered.
Accumulation OM	SLR SMI Totals, Login Failures	This OM measures the total number of failed HLR provisioning system login attempts.
Accumulation OM	SLR SMI Totals, Low Congestion	This OM measures the total number of times that the low level congestion state was entered.
Accumulation OM	SLR SMI Totals, Medium Congestion	This OM measures the total number of times that the medium level congestion state was entered.
Accumulation OM	SLR SMI Totals, Messages Failed Authentication	This OM measures the total number of received messages from the HLR provisioning system that failed authentication of the retrieved RN against an associated GTT entry with an RN matching the retrieved value.
Accumulation OM	SLR SMI Totals, Messages Invalid	This OM measures the total number of invalid messages received from the HLR provisioning system.
Accumulation OM	SLR SMI Totals, Messages Passed Authentication	This OM measures the total number of received messages from the HLR provisioning system that successfully authenticated the retrieved RN against an associated GTT entry with an RN matching the retrieved value.
Accumulation OM	SLR SMI Totals, Messages Received	This OM measures the total number of messages received from the HLR provisioning system.
Accumulation OM	SLR SMI Totals, Messages Rejected	This OM measures the total number of received messages from the HLR provisioning system that were rejected.
Accumulation OM	Special Study Totals, MSUs Received Count	This OM measures the number of incoming MSUs acknowledged on the specified linkset with the specified OPC/DPC/SIO combination.
Accumulation OM	Special Study Totals, MSUs Transmitted Count	This OM measures the number of outgoing MSUs successfully transmitted to the far end on the specified linkset with the specified OPC/DPC/SIO combination.

Accumulation OM	Special Study Totals, Octets Received Count	This OM measures the total number of MSU octets received on a specified linkset with the specified OPC/DPC/SIO combination, including the octets removed in MTP Level 2 processing.
Accumulation OM	Special Study Totals, Octets Transmitted Count	This OM measures the total number of MSU octets transmitted on the specified linkset with the specified OPC/DPC/SIO combination, including those octets that were added in MTP Level 2 processing.
Accumulation OM	System Node State, Disabled, Locked Duration	This OM measures the number of seconds that a specific RTC, CC, or application system node is disabled and locked.
Accumulation OM	System Node State, Disabled, Unlocked Duration	This OM measures the number of seconds that a specific RTC, CC, or application system node is disabled and unlocked.
Accumulation OM	System Node State, Enabled, Locked Duration	This OM measures the number of seconds that a specific RTC, CC, or application system node is enabled and locked.
Accumulation OM	System Node State, Enabled, Unlocked Duration	This OM measures the number of seconds that a specific RTC, CC, or application system node is enabled and unlocked.
Accumulation OM	System Node State, Locked, Off-line Duration	This OM measures the number of seconds that a specific RTC, CC, or application system node is locked and off-line.
Accumulation OM	System Totals, No Route MSU Discard Count	This OM measures the number of MSUs discarded due to routing failure of various causes (for example, an inaccessible DPC).
Accumulation OM	Task Management, Idle Task Duration	This OM measures the number of milliseconds spent in idle time.
Accumulation OM	TUP Received Message Counts, B/TUP Error No AS for OPC/CIC	This OM measures the number of TUP messages discarded as a result of not being able to find a valid AS for a given OPC/CIC.
Accumulation OM	TUP Received Message Counts, B/TUP Error No OPC/CIC Data	This OM measures the number of TUP and BTUP messages discarded as a result of missing database entry for a given OPC or OPC/CIC.
Accumulation OM	TUP Received Message Counts, B/TUP Error No Path	This OM measures the number of TUP and BTUP messages discarded as a result of not being able to find an inservice path to a given AS.
Accumulation OM	TUP Received Message Counts, B/TUP Error No Route	This OM measures the number of TUP messages discarded as a result of not being able to find a route to a given AS.
Accumulation OM	TUP Received Message Counts, BTUP Call P Received Count	This OM measures the number of BTUP call processing messages received from the SS7 Network.
Accumulation OM	TUP Received Message Counts, BTUP Maint Received Count	This OM measures the number of BTUP maintenance messages received from the SS7 Network.
Accumulation OM	TUP Received Message Counts, TUP Call P Received Count	This OM measures the number of TUP call processing messages received from the SS7 Network.
Accumulation OM	TUP Received Message Counts, TUP Maint Received Count	This OM measures the number of TUP maintenance messages received from the SS7 Network.
Accumulation OM	TUP Received Message Counts, Wrong NE Received Count	This OM measures the number of TUP messages discarded as a result of not receiving the message for a SG Network Element
Accumulation OM	UDP, Full Socket Count	This OM measures the number of counts that the udpstat full_socket variable has changed in the om period.
Maximum OM	Link Traffic, Link utilization	This OM provides percentage of link utilization. For LSL it is calculated in erlangs while for HSL it is calculated as percentage of processor utilization.
Maximum OM	NP Database Totals, Max Average Update Rate	This OM measures the highest update rate (in updates per second) averaged over a 60 second period. i.e. total updates over the 60 second window divided by 60. If the number of updates received in the 60 second window is less than 60 , the OM will be 0.

Maximum OM	NP Transaction Mgmt Totals, TxMgr Percent Used	This OM measures the maximum percentage of used transactions in the Transaction Management application.
Maximum OM	SLR Database Totals, Max. Update Rate	This OM measures the highest update rate (in updates per second) during any 60 second period
No Action	System Node State, Percentage Enabled	This OM measures the percentage of time that a specific RTC, CC, or application system node is enabled, or busy (for the Processor Utilization OM, GR-82-CORE section 6.4.5, item 10). The value for this OM ranges from 0 to 100 percent.
No Action	Task Management, Collection Period Duration	This OM measures the total number of milliseconds for an OM collection period. This OM can be used to calculate the percentage of use for all the other Task Management OMs.
No action	Task Management, Level 0 Priority Task Duration	This OM measures the number of milliseconds spent in Level 0 priority task(s).
No Action	Task Management, Level 1 Priority Task Duration	This OM measures the number of milliseconds spent in Level 1 priority task(s).
No Action	Task Management, Level 2 Priority Task Duration	This OM measures the number of milliseconds spent in Level 2 priority task(s).
No Action	Task Management, Level 3 Priority Task Duration	This OM measures the number of milliseconds spent in Level 3 priority task(s).
No Action	Task Management, Level 4 Priority Task Duration	This OM measures the number of milliseconds spent in Level 4 priority task(s).
No Action	Task Management, Level 5 Priority Task Duration	This OM measures the number of milliseconds spent in Level 5 priority task(s).
No Action	Task Management, Level 6 Priority Task Duration	This OM measures the number of milliseconds spent in Level 6 priority task(s).
No Action	Task Management, Level 7 Priority Task Duration	This OM measures the number of milliseconds spent in Level 7 priority task(s).
No Action	Task Management, Level 8 Priority Task Duration	This OM measures the number of milliseconds spent in Level 8 priority task(s).
No Action	Task Management, Level 9 Priority Task Duration	This OM measures the number of milliseconds spent in Level 9 priority task(s).
No Action	Task Management, OS System Tasks Duration	This OM measures the number of milliseconds spent in VxWorks OS tasks.

Appendix E: MG9000 Reported Alarms, Event Logs, Audit Logs

Appendix E: SN07 OSS Advance Feature Guide (IP) PLN-07IP-OSS Standard 01.04 December 2003

	CLK306	lossClockOutput	Major	Phase PLD reference clock oscillator not triggering (OUTPUT OF PHASE PLD HAS BEEN LOST)	Y	yes	This alarm cannot be generated by a test set or manual action. These are HW or SW faults. The easiest way to produce them is to use the MG9000 FTS Default commands. To set it -> 1. <code>./halwrite 0x1230a08a 0x1324./halwrite 0x1230a092 0x0010</code> 2. <code>./halwrite 0x1230a08a 0x1324./halwrite 0x1230a090 0x0010</code> To clear it -> 1. <code>./halwrite 0x1230a08a 0x1324./halwrite 0x1230a092 0x0000</code> 2. <code>./halwrite 0x1230a08a 0x1324./halwrite 0x1230a090 0x0010</code>	SN05	
	CLK306	singleReferenceFailure	Minor	Single monitored reference source has been lost	Y	yes	With the MG9000 using BTS but with network clocking available, pull the BTS cable	SN05	
	CLK307	allReferenceFailure	Major	Absolute and Delta reference source signals have been lost	Y	yes	Remove the receiver side of the active DCC cards fiber	SN04	
	CLK308	singleSyncUnitFailure	Major	Station 3 sync unit failed	Y	yes	This alarm cannot be generated by a test set or manual action. These are HW or SW faults. The easiest way to produce them is to use the MG9000 Default FTS commands > of InteroResources > /selectfault	SN04	
	CLK312	signalsOf	Minor	Single HW source reference occurred due to loss of	Y	yes	Remove both Clock sources (BTS and Network interfaces)	SN05	
	CLK313	signalsOf	Minor	Single HW source reference occurred due to loss of	Y	yes	Remove both Clock sources (BTS and Network interfaces)	SN05	
NE301	FlashRnc	FlashRnc	Major	Flash Memory	Y	yes	OW software may not detect all alarm conditions listed. However, OW provides capability to generate these alarms using the debug commands in DBHELL in DBHELL, enter the following commands: > of InteroResources > /selectfault When this command is entered, values for additional parameters are listed.	Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.	SN05
	ProcessorRnc	ProcessorRnc	Major	Processor	Y	yes	OW software may not detect all alarm conditions listed. However, OW provides capability to generate these alarms using the debug commands in DBHELL in DBHELL, enter the following commands: > of InteroResources > /selectfault When this command is entered, values for additional parameters are listed.	Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.	SN05
	IdromRnc	IdromRnc	Major	Idrom	Y	yes	Same as Processor fault	same as above	SN05
	AmisDspRnc	AmisDspRnc	Minor	ATM600 Port (0-15): Not at 200 speed, or not initialized	N	yes	Same as Processor fault	same as above	SN05.2
	HarmonRnc	HarmonRnc	Major	Harmon	Y	yes	Same as Processor fault	same as above	SN05
	CardTypeMismatchRnc	CardTypeMismatchRnc	Critical	Incorrect Card in Slot	N	yes	Same as Processor fault	same as above	SN05.2
	RedundancyLossRnc	RedundancyLossRnc	Critical	Single Master: No Redundancy	N	yes	Same as Processor fault	same as above	SN05.2
	CardFiberDCCRnc	CardFiberDCCRnc	Warning	Active/Master: Card Out Of Service	N	yes	Same as Processor fault	same as above	SN05.2
	CardRnc	CardRnc	Major	DS1 Card	Y	yes	Same as Processor fault	Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.	SN04
	DS1AertRnc	DS1AertRnc	Major	AA1 SAR - DS1 Card TDM to ATM converter	Y	yes	Same as Processor fault	Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.	SN04
	DS1LineRnc	DS1LineRnc	Minor	DS1 Line (0 to 15)	Y	yes	Same as Processor fault	same as above	SN05
	DS1FrameRnc	DS1FrameRnc	Major	DS1 Frame for DS1 Line (0, 7, 8, 15)	Y	yes	Same as Processor fault	same as above	SN04
	DS1LineRnc	DS1LineRnc	Major	DS1 Line IP Line for DS1 Line (0, 7, 8, 15)	Y	yes	Same as Processor fault	same as above	SN04
	CardRnc	CardRnc	Major	ITP card	Y	yes	Same as Processor fault	Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.	SN04
	ITPInewbitRnc	ITPInewbitRnc	Major	Timeswitch - call processing ending	Y	yes	Same as Processor fault	Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.	SN04
	ITPDSVCServiceCircuitRnc	ITPDSVCServiceCircuitRnc	Major	DSB (0-3)	Y	yes	Same as Processor fault	Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.	SN04
	ITPDSVCServiceCircuitRnc	ITPDSVCServiceCircuitRnc	Minor	ECAN	Y	yes	Same as Processor fault	same as above	SN04
	ITPFaultRnc	ITPFaultRnc	Major	AA1 SAR - Call Traffic TDM to ATM converter	Y	yes	Same as Processor fault	same as above	SN04
	ITPArbitratorControllerRnc	ITPArbitratorControllerRnc	Major	Serial Link Control - controls communication with ITX cards	Y	yes	Same as Processor fault	If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, treat them as a card fault.	SN04
	ITPDSVCServiceCircuitRnc	ITPDSVCServiceCircuitRnc	Minor	DCC Idrom - DSP Daughter Card Idrom	N	yes	Same as Processor fault	Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.	SN05.2
	ITPDSVCServiceCircuitRnc	ITPDSVCServiceCircuitRnc	Major	DCC Callout - DSP Daughter Card Callout	N	yes	Same as Processor fault	same as above	SN05.2
	ITPDSVCServiceCircuitRnc	ITPDSVCServiceCircuitRnc	Critical	Voice Path	N	yes	Same as Processor fault	same as above	SN05.2
	CardRnc	CardRnc	Major	ITX Card	Y	yes	Same as Processor fault	Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.	SN04
	CardRnc	CardRnc	Major	SOCSIO card	Y	yes	Same as Processor fault	Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.	SN05
	SCTerminalRnc	SCTerminalRnc	Warning	RS-232 Port	N	yes	Same as Processor fault	same as above	SN05
	SCBoardFlashMemoryRnc	SCBoardFlashMemoryRnc	Warning	Flash Memory containing software load	Y	yes	Same as Processor fault	same as above	SN05
	SCLocalBufferRnc	SCLocalBufferRnc	Major	Local Memory	Y	yes	Same as Processor fault	same as above	SN05
	SCChannelRnc	SCChannelRnc	Warning	External Link	N	yes	Same as Processor fault	same as above	SN05
	SCDWDRnc	SCDWDRnc	Minor	ATM Switch - MAC Chipset	Y	yes	Same as Processor fault	Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.	SN05
	SCNetworkRnc	SCNetworkRnc	Major	Network Interface (SCIO 0-7) (SCIO)	Y	yes	Same as Processor fault	same as above	SN05
	SCNetworkRnc	SCNetworkRnc	Critical	ATM Card Firmware	N	yes	Same as Processor fault	same as above	SN05.2
	CardRnc	CardRnc	Major	ABI card	Y	yes	Same as Processor fault	Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.	SN05
	MTTimeswitchRnc	MTTimeswitchRnc	Major	Timeswitch - call p engine (network side)	Y	yes	Same as Processor fault	Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.	SN05
	MTTimeswitchRnc	MTTimeswitchRnc	Major	Timeswitch - call p engine (line side)	Y	yes	Same as Processor fault	same as above	SN05
	MTTimeswitchRnc	MTTimeswitchRnc	Major	Timeswitch - call p engine (line side)	Y	yes	Same as Processor fault	same as above	SN05
	ABISvcCircuitRnc	ABISvcCircuitRnc	Minor	ECAN - unit 0	Y	yes	Same as Processor fault	same as above	SN05
	ABISvcCircuitRnc	ABISvcCircuitRnc	Minor	ECAN - unit 0	Y	yes	Same as Processor fault	same as above	SN05
	ABISvcCircuitRnc	ABISvcCircuitRnc	Major	AA1 SAR - Call Traffic TDM to ATM converter	Y	yes	Same as Processor fault	same as above	SN05
	ABISvcCircuitRnc	ABISvcCircuitRnc	Major	Asit Network side - unit 0	Y	yes	Same as Processor fault	same as above	SN05
	ABISvcCircuitRnc	ABISvcCircuitRnc	Major	Asit Network side - unit 1	Y	yes	Same as Processor fault	same as above	SN05
	ABISvcCircuitRnc	ABISvcCircuitRnc	Major	Asit Line side - unit 0	Y	yes	Same as Processor fault	same as above	SN05
	ABISvcCircuitRnc	ABISvcCircuitRnc	Major	Asit Line side - unit 1	Y	yes	Same as Processor fault	same as above	SN05
	ABISvcCircuitRnc	ABISvcCircuitRnc	Major	Serial Link Control - controls communication with ITX cards	Y	yes	Same as Processor fault	If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, treat them as a card fault.	SN05
	MTLocalRnc	MTLocalRnc	Critical	Voice Path	N	yes	Same as Processor fault	same as above	SN05.2
	CardRnc	CardRnc	Major	8XV ADSL Card	Y	yes	Same as Processor fault	Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.	SN04
NE302	AtmDataSyncRnc	AtmDataSyncRnc	Critical	ATM Data Sync	Y	yes	Same as Processor fault	Lock/Unlock the card and the card will restart, most likely causing the alarm to go away. Wait to make sure that the card goes enabled after the restart and no faults re-appear.	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
	AtmDataSyncRnc	AtmDataSyncRnc	Critical	Atm Data Sync	Y	yes	Same as Processor fault	same as above	SN05
NE303	SCNetworkLinkRnc	SCNetworkLinkRnc	Minor	Link to DCC Card in slot 10 or 11 - Isolation in progress	Y	yes	Same as Processor fault	This alarm means two cards cannot communicate with each other. The diagnostics will determine (locally) where the fault is and this alarm will change into an NE303 within 3 minutes.	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
NE304	SCNetworkLinkRnc	SCNetworkLinkRnc	Minor	Link to DCC Card in slot 10 or 11 - Isolation in progress	Y	yes	Same as Processor fault	This alarm means two cards cannot communicate with each other. The diagnostics will determine (locally) where the fault is and this alarm will change into an NE303 within 3 minutes.	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
NE305	SCNetworkLinkRnc	SCNetworkLinkRnc	Minor	Link to DCC Card in slot 10 or 11 - Isolation in progress	Y	yes	Same as Processor fault	This alarm means two cards cannot communicate with each other. The diagnostics will determine (locally) where the fault is and this alarm will change into an NE303 within 3 minutes.	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2
	ITPLinkToExternalRnc	ITPLinkToExternalRnc	Minor	Link to ITX, port [0 to 1] - Isolation in progress	Y	yes	Same as Processor fault	same as above	SN05.2

noNodeFault (NORTEL) UEMG NODE-MTE	ITXExternalRnc	Minor	EXTERNAL: DCC Slot 10 serial device EXTERNAL: DCC Slot 11 serial device EXTERNAL: ITP attached to port [0-7]	N	yes	Same as Processor fault	Check the ITP to see if it has alarms. If so, handle them first. If no alarms on ITP or only EXTERNAL alarms on the ITP, replace the cable between ITP and ITP. If the alarm is to a DCC card, fix any DCC alarms first. Repeat ITP card, see if problem clears. Repeat DCC card, see if problem clears.	SN06.2	
	ITXPorRnc	Minor	Serial Device 0 - to DCC card in slot 10 Serial Device 1 - to DCC card in slot 11 Serial Device 4 - to ITP card Serial Device 5 - to ITP card Serial Device 6 - to ITP card Serial Device 7 - to ITP card Serial Device 8 - to ITP card Serial Device 9 - to ITP card Serial Device 10 - to ITP card Serial Device 11 - to ITP card Serial Device 12 - to ITP card Serial Device 13 - to ITP card Serial Device 14 - to ITP card Serial Device 15 - to ITP card Serial Device 16 - to ITP card Serial Device 17 - to ITP card Serial Device 18 - to ITP card Serial Device 19 - to ITP card	Y	yes	Same as Processor fault	same as above	SN04	30 NE 318 10113 TBL M90K-Frame000.Slot2.Slot12 Location: 1-RMK-Frame000.Slot2.Slot12 Notification: IE 850 State: not acknowledged Category: Equipment Alarm Cause: Equipment Malfunction Time: Apr 24 14:59:40 2003 Component ID: CardNameAndSlot2.Slot12.ITP Specific Problem: Node Fault - Proxy fault Description: Card communication failure - Proxy mode activated Site: P3 RP05 Bay Jd FFFF FF FFF FFFF FFF
	ITXLinkInRnc	Major	Link 0 to 7 to ITP pair	Y	yes	Same as Processor fault	same as above	SN04	
	ITXNetForwarderRnc	Major	Net side cell forwarder	Y	yes	Same as Processor fault	If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, treat them as a card fault.	SN04	
	ITXLinkForwarderRnc	Major	Link side cell forwarder	Y	yes	Same as Processor fault	If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, treat them as a card fault.	SN04	
	SCLineExternalRnc	Minor	EXTERNAL: Master Shelf ITP slot 13 EXTERNAL: Master Shelf ITP slot 12 EXTERNAL: Main DCC EXTERNAL: Card in slot [2-9, 14-21]	N	yes	Same as Processor fault	Check the far end slot to see if it has alarms. If so, handle them first. If no alarms on far end card, or only EXTERNAL alarms on the far end slot, there is a backplane issue between the far end card and DCC. Repeat other card in question, see if problem clears. Repeat DCC card, see if problem clears.	SN06.2	
	SCLinePortRnc	Minor	Serial Device 0 - to Master Shelf ITP Slot 13 Serial Device 1 - to Master Shelf ITP Slot 12 Serial Device 3 - Link to Main DCC card Serial Device 4 - to card in slot 2 Serial Device 5 - to card in slot 6 Serial Device 6 - to card in slot 14 Serial Device 7 - to card in slot 18 Serial Device 8 - to card in slot 3 Serial Device 9 - to card in slot 7 Serial Device 10 - to card in slot 15 Serial Device 11 - to card in slot 4 Serial Device 13 - to card in slot 8 Serial Device 14 - to card in slot 16 Serial Device 15 - to card in slot 20 Serial Device 16 - to card in slot 5 Serial Device 17 - to card in slot 9 Serial Device 18 - to card in slot 17 Serial Device 19 - to card in slot 21	Y	yes	Same as Processor fault	If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, treat them as a card fault.	SN05	
	SCQuadrantControlRnc	Major	Group of Serial Ports	Y	yes	Same as Processor fault	same as above	SN05	
	ABNetworkExternalRnc	Minor	EXTERNAL: DCC slot 10 or 11	N	yes	Same as Processor fault	Check the DCC to see if it has alarms. If so, handle them first. If no alarms on DCC, or only EXTERNAL alarms on the DCC, there is a backplane issue between the AB and DCC. Repeat AB card, see if problem clears. Repeat DCC card, see if problem clears.	SN06.2	
	ABNetworkPortRnc	Minor	Serial Device 0 - to DCC Card in slot 10 Serial Device 1 - to DCC Card in slot 11	Y	yes	Same as Processor fault	If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, treat them as a card fault.	SN05	
NE305	ABNetworkRnc	Critical	Both lines to DCC Card	Y	yes	Same as Processor fault	same as above	SN05	
	GLANRnc	Minor	GLAN Link to hub on Active ITP card	Y	yes	Same as Processor fault	The GLAN hub is located on the active ITP in the shelf where the fault appears. First by swatching ITPs and re-run diag on the affected card. If that fixes the problem, replace the newly inactive ITP, otherwise treat the fault as a card fault.	SN05	
	ITPGLANHubRnc	Critical	GLAN Hub, communicates with other cards on shelf	Y	yes	Same as Processor fault	The GLAN hub is located on the active ITP in the shelf where the fault appears. First by swatching ITPs and re-run diag on the affected card. If that fixes the problem, replace the newly inactive ITP, otherwise treat the fault as a card fault.	SN04	
	ABLinkSideRnc	Major	DS12 port	Y	yes	Same as Processor fault	Verify UEMG is in service Verify the AB card is unlocked Verify this AB card is not disabled, if so, solve other issues causing this card to be disabled. Check DS12 fibers, (tight check, clean fibers, verify fibers are present)	SN05	
	ABLinkLocalRnc	Minor	XPM link or DS12 connection	Y	yes	Same as Processor fault	same as above	SN05	
	ABLinkACRnc	Major	All DS12 channels closed	Y	yes	Put cable to XPM	Verify UEMG is in service Verify the AB card is unlocked Verify that AB card is not disabled, if so, solve other issues causing this card to be disabled. Check DS12 fibers, (tight check, clean fibers, verify fibers are present)	SN05	
	SCWanBISOMP-Rnc	Major	Inband Messaging OMP Link [0,1]	Y	yes	Same as Processor fault	Check for alarms on shelf controller Use LCJ to verify that AESA provisioning information is correct. If the problem persists, call your next level of support.	SN05	
	SCWanBISCC-Rnc	Major	Inband Messaging CC Link [0,1]	Y	yes	Same as Processor fault	same as above	SN05	
	SCWanBIS-Rnc	Major	Shardlet to Shared Manager	Y	yes	Same as Processor fault	same as above	SN05.2	
	SCWanBISDS12-Rnc	Major	Inband Messaging DS12 Link [0,1]	Y	yes	Same as Processor fault	same as above	SN05	
NE306	ITPclockSyncRnc	Critical	Clock Sync	Y	yes	Same as Processor fault	- If fault is on both ITPs 1) Verify Clock source is connected. 2) Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3) If fault persists, lock/unlock to restart the card. 4) If fault persists, call next level of support. - If fault is on one ITP 1) Verify Clock source is connected. 2) Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3) If fault persists, lock/unlock to restart the card. 4) Replace the faulty card.	SN04	
	ITPClockPhaseLockRnc	Major	Clock Sync: Loss of Phase Lock	Y	yes	Same as Processor fault	same as Clock Sync above	SN05	
	ITPClockTempPhaseLockRnc	Major	Clock Sync: Loss of Temp Phase Lock	Y	yes	Same as Processor fault	same as Clock Sync above	SN05	
	ITPClockMvClockRnc	Major	Clock Sync: Loss of Mv Clock	Y	yes	Same as Processor fault	same as Clock Sync above	SN05	
	ITPClockLocalClockRnc	Major	Clock Sync: Loss of Local Clock	Y	yes	Same as Processor fault	same as Clock Sync above	SN05	
	ITPClockOutputRnc	Major	Clock Sync: Loss of Clock Output	Y	yes	Same as Processor fault	same as Clock Sync above	SN05	
	ITPSyncRefRnc	Minor	Clock Sync: Single Reference Failure	Y	yes	Same as Processor fault	same as Clock Sync above	SN05	
	ITPSyncRefRnc	Major	Clock Sync: All Reference Failure	Y	yes	Same as Processor fault	same as Clock Sync above	SN05	
	ITPSyncRefRnc	Minor	Clock Sync: Single Sync Unit Failure	Y	yes	Same as Processor fault	same as Clock Sync above	SN05	
	ITPSyncRefRnc	Minor	Clock Sync: Loss of Sync	Y	yes	Same as Processor fault	same as Clock Sync above	SN05	
NE307	ITPsyncRefRnc	Minor	Clock Sync: Out of Frame	Y	yes	Same as Processor fault	same as Clock Sync above	SN05	
	ITPsyncRefRnc	Minor	Clock Sync: Clock	Y	yes	Same as Processor fault	same as Clock Sync above	SN05	
	ITPsyncRefRnc	variable	Clock Sync: Clock	Y	yes	Same as Processor fault	same as Clock Sync above	SN05	
	ITPsyncRefRnc	Minor	Clock Sync: Sync	Y	yes	Same as Processor fault	same as Clock Sync above	SN05	
	ITPsyncRefRnc	Minor	Clock Sync: Holdover Mode	Y	yes	Same as Processor fault	same as Clock Sync above	SN05	
	ICIdentRefRnc	Major	BTIS Forwarder	N	yes	Same as Processor fault	same as Clock Sync above	SN05.2	
	ICIdentRefRnc	Minor	BTIS clock reference (A or B)	N	yes	Same as Processor fault	same as Clock Sync above	SN05.2	
	ITXFrameRnc	Major	Frame - timing synchronization device	Y	yes	Same as Processor fault	- If fault is on both ITPs 1) Verify Clock source is connected. 2) Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3) If fault persists, lock/unlock to restart the card. 4) If fault persists, call next level of support. - If fault is on one ITP 1) Verify Clock source is connected. 2) Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3) If fault persists, lock/unlock to restart the card. 4) Replace the faulty card.	SN04	
	ITXBWRefRnc	Minor	BTIS clock reference A	Y	yes				
	ITXBWRefRnc	Minor	BTIS clock reference B	Y	yes				
NE310	ITXNetworkRnc	Minor	Port 2 on serial device, port only used for diagnostics	Y	yes				
	SCQuadrantControlRnc	Minor	Serial Port 0 - UNABLE to ITP slot 12	Y	yes	Same as Processor fault		SN05	
	SCQuadrantControlRnc	Minor	Serial Port 0 - UNABLE to ITP slot 13	Y	yes	Same as Processor fault		SN05	
	SCQuadrantControlRnc	Warning	Unused data stream in I	N	yes	Same as Processor fault	No action required	SN05	
	SCQuadrantControlRnc	Warning	Unused data stream in I or B-13	N	yes	Same as Processor fault	No action required	SN05	
	SCQuadrantControlRnc	Warning	Unused data stream in I or B-13	N	yes	Same as Processor fault	No action required	SN05	
	SCQuadrantControlRnc	Warning	Unused data stream in I or B-13	N	yes	Same as Processor fault	No action required	SN05	
	SCQuadrantControlRnc	Warning	Unused data stream in I or B-13	N	yes	Same as Processor fault	No action required	SN05	
	SCQuadrantControlRnc	Warning	Unused data stream in I or B-13	N	yes	Same as Processor fault	No action required	SN05	
	SCQuadrantControlRnc	Warning	Unused data stream in I or B-13	N	yes	Same as Processor fault	No action required	SN05	
NE311	SCTimeOfDayRnc	Minor	Time of Day: Access to time server [6] failed	Y	yes	Same as Processor fault	Attempts to access the provisioned time server have failed. Verify the provisioned IP address of time server is correct Verify time server is operational and online. Use the LCJ to re-submit the Time of day parameters, this forces immediate time server access.	SN05	
	ITPCableRnc	Minor	Cable configuration conflict	Y	yes	Same as Processor fault	One of the cables to the ITPs has been connected in an unexpected way. Check to see if the cable on the two ITPs match, and that the ITP ends of the cable are in the right ports.	SN05	
	ITXCableRnc	Minor	Cable configuration conflict, port [0 to 7]	Y	yes	Same as Processor fault	One of the cables to the ITPs has been connected in an unexpected way. Check to see if the cable on the two ITPs matches the mate ITP, and that the ITP ends of the cable are in the right ports.	SN05	
	ABActivityCableRnc	Minor	Activity control cable between AB cards	Y	yes	Put activity cable between AB card pair	The activity control cable is a small cable on the front of the AB cards that is used for activity determination. Replace cable. If the fault persists, replace the inactive card. If the problem still persists, swap, replace newly inactive card.	SN05	
	SCRnc	Minor	Backplane Cross Connect	Y	yes	Same as Processor fault	The carriers between the two DCC cards cannot communicate. Verify and fix any CARRIER alarms 1) Restart the inactive DCC 2) If problem persists, replace inactive DCC 3) If problem persists, call next level of support If seen on inactive DCC 1) Restart the inactive DCC 2) If problem persists, swap DCC cards. This will cause carriers to go down momentarily. Be sure to call next level to verify it is permissible to swap. 3) Restart the newly inactive DCC card. 4) If problem persists, replace the newly inactive card. 5) If problem persists, call next level of support. If both DCCs have this fault, there is a backplane problem in the shelf. Replace the entire shelf backplane.	SN05	
	SCLinkRnc	Major	Resource Bandwidth	Y	yes	Same as Processor fault	Some of the carriers are not providing bandwidth. Verify and fix any CARRIER alarms. If problem persists, restart the card.	SN05	
	downstreamFFO	Major	ADSL: Downstream FFO	Y	yes		Throttle back the downstream data from the SCO	SN06	
	downstreamREC	Major	ADSL: Downstream REC error	Y	yes		1	SN06	
	atm60Fault	Critical	ADSL: ATM60 fault	Y	yes		Restart linecard	SN06	
	upstream buffer overflow	Critical	ADSL: Upstream buffer overflow	Y	yes		Throttle back the upstream data rate on the linecard	SN06	
NE316	downstream buffer overflow	Critical	ADSL: Downstream buffer overflow	Y	yes		Throttle back the downstream data to the linecard	SN06	
	atm device timeout	Critical	ADSL: ATM Device timeout	Y	yes		Restart linecard	SN06	
	clock recovery	Critical	ADSL: Loss of clock recovery	Y	yes		Restart linecard	SN06	
	upstream buffer overflow	Critical	ADSL: Upstream buffer overflow	Y	yes		Throttle back the upstream data rate on the linecard	SN06	
	downstream buffer overflow	Critical	ADSL: Downstream buffer overflow	Y	yes		Throttle back the downstream data to the linecard	SN06	
	atm device timeout	Critical	ADSL: ATM Device timeout	Y	yes		Restart linecard	SN06	
	clock recovery	Critical	ADSL: Loss of clock recovery	Y	yes		Restart linecard	SN06	
	upstream buffer overflow	Critical	ADSL: Upstream buffer overflow	Y	yes		Throttle back the upstream data rate on the linecard	SN06	
	downstream buffer overflow	Critical	ADSL: Downstream buffer overflow	Y	yes		Throttle back the downstream data to the linecard	SN06	
	atm device timeout	Critical	ADSL: ATM Device timeout	Y	yes		Restart linecard	SN06	
NE317	clock recovery	Critical	ADSL: Loss of clock recovery	Y	yes		Restart linecard	SN06	
	upstream buffer overflow	Critical	ADSL: Upstream buffer overflow	Y	yes		Throttle back the upstream data rate on the linecard	SN06	
	downstream buffer overflow	Critical	ADSL: Downstream buffer overflow	Y	yes		Throttle back the downstream data to the linecard	SN06	
	atm device timeout	Critical	ADSL: ATM Device timeout	Y	yes		Restart linecard	SN06	
	clock recovery	Critical	ADSL: Loss of clock recovery	Y	yes		Restart linecard	SN06	
	upstream buffer overflow	Critical	ADSL: Upstream buffer overflow	Y	yes		Throttle back the upstream data rate on the linecard	SN06	
	downstream buffer overflow	Critical	ADSL: Downstream buffer overflow	Y	yes		Throttle back the downstream data to the linecard	SN06	
	atm device timeout	Critical	ADSL: ATM Device timeout	Y	yes		Restart linecard	SN06	
	clock recovery	Critical	ADSL: Loss of clock recovery	Y	yes		Restart linecard	SN06	
	upstream buffer overflow	Critical	ADSL: Upstream buffer overflow	Y	yes		Throttle back the upstream data rate on the linecard	SN06	
NE318	downstream buffer overflow	Critical	ADSL: Downstream buffer overflow	Y	yes		Throttle back the downstream data to the linecard	SN06	
	atm device timeout	Critical	ADSL: ATM Device timeout	Y	yes		Restart linecard	SN06	
	clock recovery	Critical	ADSL: Loss of clock recovery	Y	yes		Restart linecard	SN06	
	upstream buffer overflow	Critical	ADSL: Upstream buffer overflow	Y	yes		Throttle back the upstream data rate on the linecard	SN06	
	downstream buffer overflow	Critical	ADSL: Downstream buffer overflow	Y	yes		Throttle back the downstream data to the linecard	SN06	
	atm device timeout	Critical	ADSL: ATM Device timeout	Y	yes		Restart linecard	SN06	
	clock recovery	Critical	ADSL: Loss of clock recovery	Y	yes		Restart linecard	SN06	
	upstream buffer overflow	Critical	ADSL: Upstream buffer overflow	Y	yes		Throttle back the upstream data rate on the linecard	SN06	
	downstream buffer overflow	Critical	ADSL: Downstream buffer overflow	Y	yes		Throttle back the downstream data to the linecard	SN06	
	atm device timeout	Critical	ADSL: ATM Device timeout	Y	yes		Restart linecard	SN06	

	NE317	dis.bkup	Critical	ADSL DRP Lockup	Y	yes		Reload DSPs	SN05		
		CallMacMinor	Minor	Shelf EIC Card Alarm	Y				SN05		
		CallMacMinor	Minor	Shelf FIC Card Alarm	Y				SN05		
		CallMacMinor	Minor	Shelf FIC Card Alarm	Y				SN05		
		CallMacMinor	Minor	Shelf FIC Card Alarm	Y				SN05		
	NE318	Major	Major	Shelf EIC Card Alarm	Y				SN05		
		Major	Major	Shelf FIC Card Alarm	Y				SN05		
		Major	Major	Shelf FIC Card Alarm	Y				SN05		
		Major	Major	Shelf FIC Card Alarm	Y				SN05		
		Major	Major	Shelf FIC Card Alarm	Y				SN05		
MG9000 Manager Reported Faults	MGEM000	EMDiskUnavailable	Major	Generated when MG9000 EM is not able to make connection to the Element Manager Database	Y	Yes	1. Make sure that persistence is turned on. 2. Make the database unavailable. 3. Perform some action (administrative change) on a VMG or termination. 4. Check the alarm browser for the alarm being SET.	1. Re-establish the database connection. 2. Perform some action (administrative change) on a VMG or termination. 3. Check the alarm browser for the alarm being CLEARED.	SN04		
	MGEM001	CommsLostToNE	Critical	Generated when the MG9000 EM loses SNMP communication with MG9000	Y	Yes	Break connection between the GW and the MSGK EM server. This can be done by taking the GWs OCS OOS at the PP15000, or disabling the Ethernet connect to the MSGK EM Server (disconnect the cable).	EM will periodically retry to establish communication to the Gateway. Check the following: 1. PING the IP address of the Shelf Controller to validate IP connectivity. 2. PING the IP address of the OCS CPOA port to validate IP connectivity. 3. Check connectivity between EM and MG. 4. Check for status of the OCS card and Node Maintenance task.	SN04	C57 MGEM001 9232 TBL MSGK CommsLostToNE Location: 2-HSRK Notification ID: 817 State: not acknowledged Category: Communication Alarm Cause: Communications Subsystem Failure Time: Apr 24 10:57:05 2003 Component ID: MSGK EM Core Network Specific Problem: Core Channel Down - Communication Lost to the	MEH12_100BE *** MGEM001 APR24 10:57:05 9232 TBL MSGK CommsLostToNE Location: 2-HSRK Notification ID: 817 State: not acknowledged Category: Communication Alarm Cause: Communications Subsystem Failure Time: Apr 24 10:57:05 2003 Component ID: MSGK EM Core Network Specific Problem: Core Channel Down - Communication Lost to the
	MGEM002	InvalidEMPAAddress	Major	Generated when the MG9000 Manager has added an re MG9000 and tries to discover the NE. It will check the MG9000 EM IP address provisioned at the MG9000 and if it is incorrect will raise this alarm	Y	Yes	At the MG9000 LCI test the IP address of the MG9000 Manager to an incorrect value. At the MG9000 Manager do a manual discovery of that MG9000	At the MG9000 LCI check the IP address of the MG9000 Manager and correct if necessary.	SN05		
	MGEM003	AlarmBeingThrottled	Minor	Generated when the MG9000 sends too many alarms within a 5 second window. When this happens the MG9000 Manager will request this particular MG9000 stop sending alarms and display this particular alarm. This condition will clear when the number of alarm within 5 sec falls below a set number.	Y	yes	At the MG9000 using DSHELL use the alarm generation utility an generate at least 10 alarm a second for at least 10 seconds	At the MG9000 LCI check the IP address of the MG9000 Manager and correct if necessary.	SN06		Description: Loss of Heartbeat to NE Site: PP PPHs Bay_ID: FFFF FF FFF FFFF FFF
	MGEM004	MSGK AlarmAuditFailed	Critical	Alarm Audit Failed - The alarm audit on the GW failed		yes			SN05.2		
(MEDIA_GATEWAY_MIB)	MGCS300	mgc300InvalidControllerAddress		Indicates that a message was received from a controller that did not match any valid controller IP address	n/a	no	N/A	N/A	SN04		
	MGCS301	mgc300InvalidTerminationID		Indicates a mismatch of Termination ID	n/a	no	N/A	N/A	SN04		
	MGCS302	mgc300InvalidPackageElement		Indicates that a message was received from a controller that contained an event, signal, or description that was not recognized for the package	n/a	no	N/A	N/A	SN04		
	MGCS303	mgc300InvalidPackageElement		Indicates that a message was received from a controller that contained an event, signal, or description that was not recognized for the package	n/a	no	N/A	N/A	SN04		
nMtaFault (NORTEL_MG_MTA-MIB)	TEST300	mta300InvalidPackageElement		Indicates that a message was received from a controller that contained an event, signal, or description that was not recognized for the package	n/a	no	N/A	N/A	SN05		
	TEST301	mta300InvalidPackageElement		Indicates that a message was received from a controller that contained an event, signal, or description that was not recognized for the package	n/a	no	N/A	N/A	SN05		
	TEST302	mta300InvalidPackageElement		Indicates that a message was received from a controller that contained an event, signal, or description that was not recognized for the package	n/a	no	N/A	N/A	SN05		
	TEST303	mta300InvalidPackageElement		Indicates that a message was received from a controller that contained an event, signal, or description that was not recognized for the package	n/a	no	N/A	N/A	SN05		
nMEsAFault (MEGACO-MIB)	ESA900	Entered ESA	Critical	Communication between GWC and GW is lost. Entered ESA mode	Y	yes	Break connection between the GW and the GWC when ESA is enabled. This can be done by taking the GWs OCS OOS at the PP15000, or disabling the Ethernet connect to the GWC (disconnect the cable).	Using the Traceroute or Ping MG9000 Manager tool test the network communications path between the EM the the MSGK, and the EM and the GWC. Check OCS connection at the MG900, PP15000, and the SAFET Shelf Controller. Check the Ethernet connection at the GWC, PP15000, and SAFET Shelf Controller. Check the state of the DCC cards at the MG9000. Correct any problems found	SN05		
	ESA901	nWESAActiveFailed	Critical	Shutdown load of ESA data from the CSKR Core has failed		yes			SN06.2		
	ESA902	nWESAActiveFailed	Critical	Failed to set up FIP connection to the CSKR Core has failed		yes			SN07		
	ESA903	nWESAActiveFailed	Critical	Failed to set up FIP connection to the CSKR Core has failed		yes			SN07		
nMMsgcooFault (NORTEL-UEMG-MEGACO-MIB)	VMG000	VMG OOS	Critical	Generated when Root Termination goes out of service (Communication between Gateway and GWC is lost and ESA is not enabled)	Y	yes	Break connection between the GW and the GWC when ESA is disabled. This can be done by taking the GWs OCS OOS at the PP15000, or disabling the Ethernet connect to the GWC (disconnect the cable).	Using the Traceroute or Ping MG9000 Manager tool test the network communications path between the EM the the MSGK, and the EM and the GWC. Check OCS connection at the MG900, PP15000, and the SAFET Shelf Controller. Check the Ethernet connection at the GWC, PP15000, and SAFET Shelf Controller. Check the state of the DCC cards at the MG9000. Correct any problems found	SN05	C1 VMG 300 1723 TBL MSGK VMMsgcooFault Location: 1-RMSK.Frame000.Shelf2 Slot12 Notification ID: 885 State: not acknowledged Category: Equipment Alarm Cause: Equipment Malfunction Time: Apr 24 15:11:34 2003 Component ID: ShelfFrame2.Shelf2.Slot12.ITP Specific Problem: VMMsgcooFault - Root Termination status change Description: Call Processing Out of Service. Site: PP PPHs Bay_ID: FFFF FF FFF FFFF FFF	nMMsgcooFault Location: 1-RMSK.Frame000.Shelf2 Slot12 Notification ID: 885 State: not acknowledged Category: Equipment Alarm Cause: Equipment Malfunction Time: Apr 24 15:11:34 2003 Component ID: ShelfFrame2.Shelf2.Slot12.ITP Specific Problem: VMMsgcooFault - Root Termination status change Description: Call Processing Out of Service. Site: PP PPHs Bay_ID: FFFF FF FFF FFFF FFF
	VMG001	BadCalls	Minor	QoS Alarm that is generated when the number of bad call reaches a certain threshold	N	SLIP only	In the MG9000 EM set the QoS threshold to a low level. Using a "Packet Storm" or "Shunna" test set, inject errors on the OCS/STMT network interface on a particular active calls SVC	Check GWC QoS collector for any QoS error patterns. Narrow down probable areas where errors could occur. Run test calls to narrow down further. If error is only on that one line there may be a card fault. If problem is in the network isolate problem area and correct.	SN06		
	VMG002	PacketLoss	Minor	QoS Alarm that is generated when the number of packet loss reaches a certain threshold	N	SLIP only	Same as above	Same as above	SN06		
	VMG003	Jitter	Minor	QoS Alarm that is generated when IP message jitter reaches a certain threshold	N	SLIP only	Same as above	Same as above	SN06		
nMMsgcooFault (NORTEL-UEMG-MEGACO-MIB)	VMG004	Latency	Minor	QoS Alarm that is generated when IP message latency reaches a certain threshold	N	SLIP only	Same as above	Same as above	SN06		
	VMG005	mgc300InvalidPackageElement	Critical	Indicates that a message was received from a controller that contained an event, signal, or description that was not recognized for the package	Y	Yes			SN07		
	VMG006	mgc300InvalidPackageElement	Critical	Indicates that a message was received from a controller that contained an event, signal, or description that was not recognized for the package	Y	Yes			SN07		
	VMG007	mgc300InvalidPackageElement	Critical	Indicates that a message was received from a controller that contained an event, signal, or description that was not recognized for the package	Y	Yes			SN07		
	VMG008	mgc300InvalidPackageElement	Critical	Indicates that a message was received from a controller that contained an event, signal, or description that was not recognized for the package	Y	Yes			SN07		
	VMG009	mgc300InvalidPackageElement	Critical	Indicates that a message was received from a controller that contained an event, signal, or description that was not recognized for the package	Y	Yes			SN07		
	VMG010	mgc300InvalidPackageElement	Critical	Indicates that a message was received from a controller that contained an event, signal, or description that was not recognized for the package	Y	Yes			SN07		
	VMG011	mgc300InvalidPackageElement	Critical	Indicates that a message was received from a controller that contained an event, signal, or description that was not recognized for the package	Y	Yes			SN07		
	VMG012	mgc300InvalidPackageElement	Critical	Indicates that a message was received from a controller that contained an event, signal, or description that was not recognized for the package	Y	Yes			SN07		
	VMG013	mgc300InvalidPackageElement	Critical	Indicates that a message was received from a controller that contained an event, signal, or description that was not recognized for the package	Y	Yes			SN07		
	VMG014	mgc300InvalidPackageElement	Critical	Indicates that a message was received from a controller that contained an event, signal, or description that was not recognized for the package	Y	Yes			SN07		
	VMG015	mgc300InvalidPackageElement	Critical	Indicates that a message was received from a controller that contained an event, signal, or description that was not recognized for the package	Y	Yes			SN07		
	VMG016	mgc300InvalidPackageElement	Critical	Indicates that a message was received from a controller that contained an event, signal, or description that was not recognized for the package	Y	Yes			SN07		
	VMG017	mgc300InvalidPackageElement	Critical	Indicates that a message was received from a controller that contained an event, signal, or description that was not recognized for the package	Y	Yes			SN07		
Performance (NORTEL-UEMG-PERFMON-MIB)	OVL004	Performance Degraded	Minor/Major	Overload Detection Alarm that is generated whenever the MG9000 actually enters an overload condition.		Yes			SN05.2		
	OVL005	nMMsgLinkSat	Critical	An external messaging link has closed and cannot be re-established.		yes			SN07		
	OVL006	nMMsgLinkSatDegraded	Major	Message loss is high enough such that the message link is in a degraded service state. For ASE, this must mean that some calls are failing and perhaps maintenance action are being (e.g. static data).		yes			SN07		
	OVL007	nMMsgLinkSat	Minor	Message loss is high enough such that the message link is in a degraded service state. For ASE, this must mean that some calls are failing and perhaps maintenance action are being (e.g. static data).		yes			SN07		

Supported in EM but not enabled at MG9000								
New or changed in SN07								
MG9000 Reported Event LOGs								
LOG Subsystem (MIB)	LOG Id	LOG Type	Description	SN06 VoA Telcordia Coverage?	Supported/ Enabled	Procedure To Generate LOG	EM Supported	LOG Output Example
ATM Event (NORTEL-UEMG-ATM-MIB)	VC800	atmPvcFailuresTrap	Indicates that one or more PVCs or PVLCs on this interface has failed since the last atmPvcFailuresTrap was sent.	n/a	no	N/A	SN04	
	VC800	rmAtmThreshold	Generated when an ATM interface stat exceeds the specified threshold.	n/a	no	N/A	SN04	
	VC801	noAtmStatVcThreshTrap	Generated when the VC stat exceeds specified threshold.	n/a	no	N/A	SN04	
Data Audit Event	MGAU800	AuditLogNotification	Generated my the MG9000 Manager when an Audit is started, stopped, a data mismatch was found between them MG9000 and the MG9000 Manager, or a communications failure occurred while the Audit was running	N	yes	Clear the data from an ITP card, start the Audit, letting it run to completion.	SN05	
Bandwidth Event (NORTEL-UEMG-BANDWIDTH-MIB)	BW800	nrBwSwitchFabricCongestion	A nrBwSwitchFabricCongestion Notification is generated when one of the input cellQueues Cross the configured threshold percentage.	N	yes	This fault is very difficult to produce during normal operations with a test set or manual action. The best way to generate this fault is using the following Dshell command. To do this "cd" to SNMP and use the "bwevent" command with the "testfabric" option.	SN04	NTL STD: RTPS BW800 JAN28 22:10:40 0462 THR MG8K BW Switch Fabric Congestion NE Number: 19 NE Name: CO_19 PhysLoc: Ne.ne19 Bandwidth Switch Fabric Congestion Type: CBR Switch Fabric Congestion Bandwidth Bandwidth Notification Value: 70.0 % Bandwidth Current Total Queue Fill: 90.0 %
	BW801	nrBwBandwUtilizationCongestion	A nrBwBandwUtilization Notification is generated when the total or dls'd cell rates Cross the configured threshold percentage.	N	yes	Set the DSL threshold (at BW Manager GUI an EM) to a low level, generate data traffic on a number of DSL lines until the LOG appears.	SN04	SCC2: 10 BW 800 8936 THR MG8K BW Switch Fabric Congestion NE Number: 19 NE Name: CO_19 PhysLoc: Ne.ne19 Bandwidth Switch Fabric Congestion Type: CBR Switch Fabric Congestion Bandwidth Bandwidth Notification Value: 70.0 % Bandwidth Current Total Queue Fill: 90.0 %
DS1 Carrier Event (NORTEL-UEMG-CARRIER-MIB)	MGCA800	dsx1LineStatus-Change	Trap is sent when the value of an instance dsx1Line Status changes.	N	yes	Remove the DS1 cable and replace	SN04	
	MGCA800	apsTrapSwitchover	Sent when the value of an instance of apsCircSwitchover increments.	n/a	no	N/A	SN04	
	MGCA801	apsTrapModeMis-match	Sent when the value of an instance of apsStatusModeMismatch increments	n/a	no	N/A	SN04	
	MGCA802	apsProtSwitchRejectEvent		n/a	no	N/A	SN04	
BIP Input/Output State Change (NORTEL-UEMG-SHF-MIB)	SHLF501	rmShiftInputOutputOperStatus	TRAP sent when any BIP Input/Output state change event occurs for an Input/Output with an alarm severity of Indeterminate.	N	yes	Change any BIP Input/Output Alarm Severity setting to indeterminate and then follow test procedure for that alarm.	SN04	
Test Event	TEST600	testComplete	Signifies that a test has completed for a particular entity.	N	yes	Run a Line test or Run a Line card Diag	SN04	
Link Event	LINK500	linkDown	Signifies that the SNMPv2 entity has detected that the IOperStatus object is about to enter the down state.	N	yes	Take the ITP card pair Lock and Offline	SN04	
	LINK501	linkUp	Signifies that the SNMP entity has detected that the IOperStatus object left the down state.	N	yes	Take the ITP card pair online and Unlocked	SN04	
Clock Sync Event (NORTEL-UEMG-CLOCKSYNC-MIB)	CLK500	ClockSyncChange	A change has occurred for Clock Sync: timingModeChange (1), clockModeChange (2).	N	yes	Remove the Colock source cable to the ITX card	SN04	
SLoA Event	SWL600	rmMaTrapConnectionStatus	Sent when SNM indicates status of the connection	N	yes	Put line under test	SN04	
MEGACO Event	MGC500	medGwyLinkStatus-Change	Indicates that status of media gateway control link has changed.	n/a	no	N/A	SN04	
	MGC501	medGwyTerminationStatusChange	Sent when a termination changes Status.	n/a	no	N/A	SN04	
SNMP Event	SNMP600	snmpEnableAuthen-Traps	Indicates permission to generate authenticationFailure traps	n/a	no	N/A	SN04	
	SNMP601	coldStart	Signifies that the SNMP entity is reinitializing itself and its configuration may have been altered	N	yes	Initiate Coldstart from the MG9K LCI	SN04	
	SNMP602	warmStart	Signifies that the SNMP entity is reinitializing itself such that its configuration is unaltered.	n/a	no	N/A	SN04	
Network Element Event (NORTEL-UEMG-NODE-MIB)	NE500	noNodeSwact	Generated when the Node does a switch of activity.	N	yes	SWAC the OC3 card pair	SN04	
	NE501	noNodeStateChange	Generated when the Node changes state.	N	yes	Take ITP OOS, put back inservice	SN04	
	NE502	DS1SpareOperationEvent	Generated when a DS1 card is spared	N	yes	Manually spare a ds1 card	SN04	
	NE503		ASL Switch Membership		yes		SN06.2	
	NE504		ASL State Change		yes		SN06.2	
	NE600	entConfigChange	Generated when the value of entLastChangeTime changes.	N	yes	Plug in new line card	SN04	
	NE601	noNodeRestartBegin	Generated when the Node is restarting.	N	yes	Restart ITP card	SN04	
	NE602	noNodeRestart-Complete	Generated when the Node completes its Restart	N	yes	Same as above	SN04	
	NE603	noNodeSWLoad-Complete	Generated when the Node completes its Software Load	N	yes	Load an ITP with new SW load	SN04	
	NE604	noNodeSWUpgrade-Complete	Generated when a SW Upgrade has completed	N	yes	Same as above	SN04	
	NE605		Generated when a Network Element is deleted	N	yes	Delete a MG9K from the EM	SN04	
	NE602		Generated when a Reinitialize Gateway event occurs	N	yes	Envoke the Reinitialize option on the OC3 card	SN05	
Alarm Reliability Event	ALM998	AlarmSequenceError	Generated when the MG9000 Manager detects it has missed Alarms from the MG9000	N	yes	Break connection (OC3) to MG9K, generate a number of alarms at MG9K, resetup MG9K connection.	SN04	
	ALM999	AlarmSequenceRestored	Generated when the MG9000 Manager recovered the missing Alarms from the MG9000	N	yes	Same as above	SN04	
DSL Event (NORTEL-UEMG-DSL-MIB)	XDSL600	adslAturRateChangeTrap	The ATUrs transmit rate has changed (RADSL mode only)	n/a	no	N/A	SN04	
	XDSL601	adslAturHFailureTrap	ATUC initialization failed	n/a	no	N/A	SN04	
	XDSL602	adslAturRateChangeTrap	The ATUrs transmit rate has changed (RADSL mode only)	N	yes	Using an ADSL Modem test set inject large numbers of this type of error.	SN04	
	XDSL800	adslAturPerfLossThreshTrap	Loss of Framing 15-minute interval threshold reached	N	yes	Using an ADSL Modem test set inject large numbers of this type of error.	SN04	
	XDSL801	adslAturPerfLossThreshTrap	Loss of Signal 15-minute interval threshold reached	N	yes	Using an ADSL Modem test set inject large numbers of this type of error.	SN04	
	XDSL802	adslAturPerfLprsThreshTrap	Loss of Power 15-minute interval threshold reached	N	yes	Using an ADSL Modem test set inject large numbers of this type of error.	SN04	
	XDSL803	adslAturPerfEsThreshTrap	Errored Second 15-minute interval threshold reached	N	yes	Using an ADSL Modem test set inject large numbers of this type of error.	SN04	
	XDSL804	adslAturPerfLofsThreshTrap	Loss of Link 15-minute interval threshold reached	N	yes	Using an ADSL Modem test set inject large numbers of this type of error.	SN04	
	XDSL805	adslAturPerfLofsThreshTrap	Loss of Framing 15-minute interval threshold reached	N	yes	Using an ADSL Modem test set inject large numbers of this type of error.	SN04	
	XDSL806	adslAturPerfLossThreshTrap	Loss of Signal 15-minute interval threshold reached	N	yes	Using an ADSL Modem test set inject large numbers of this type of error.	SN04	
	XDSL807	adslAturPerfLprsThreshTrap	LPRS 15-minute interval threshold reached	N	yes	Using an ADSL Modem test set inject large numbers of this type of error.	SN04	
	XDSL808	adslAturPerfEsThreshTrap	Errored Second 15-minute interval threshold reached	N	yes	Using an ADSL Modem test set inject large numbers of this type of error.	SN04	
Manager Upgrade Event	UPGD600		indicating an upgrade is needed.	N	yes	Requires the customer to perform the upgrade or downgrade procedure. Follow MG9K EM upgrade procedures	SN06	
	UPGD601		indicating an export has started	N	yes	Requires no immediate action	SN06	
	UPGD602		indicating an export has completed	N	yes	Same as above	SN06	
	UPGD603		indicating an import has started	N	yes	Same as above	SN06	
	UPGD604		indicating an import has completed	N	yes	Same as above	SN06	
	MGE700		MG9000 Manager Server application Startup	N	yes	Telnet into the MG9000 Manager server and execute the shutdown procedure then execute following command "topnortelmgksrv_06/bin/mgkmpkl start"	SN06	
	MGE701		MG9000 Manager Server application Shutdown	N	yes	Telnet into the MG9000 Manager server and execute the following command "topnortelmgksrv_06/bin/mgkmpkl stop"	SN06	

Manager Event	MGEM702		MG9000 Manager Mid-Tier Server application Startup	N	yes	Telnet into the MG9000 Manager Mid-Tier server and execute the shutdown procedure then execute the following command "opt/nortel/mg9kmsr_06/bin/mg9kmsdtmp1 start"	SN06
	MGEM703		MG9000 Manager Mid-Tier Server application Shutdown	N	yes	Telnet into the MG9000 Manager Mid-Tier server and execute the following command "opt/nortel/mg9kmsr_06/bin/mg9kmsdtmp1 stop"	SN06
	OMC700		MG9000 Manager Mid-Tier Server OM Collector application Startup	N	yes	Telnet into the MG9000 Manager Mid-Tier server and execute the shutdown procedure then execute the following command "opt/nortel/omctr_06/bin/OMtmp1 start"	SN06
	OMC701		MG9000 Manager Mid-Tier Server OM Collector application Shutdown	N	yes	Telnet into the MG9000 Manager Mid-Tier server and execute the following command "opt/nortel/omctr_06/bin/OMtmp1 stop"	SN06
Performance (NORTEL-UEMG-PERFMON-MIB)	OVLDB00	ovldRacMonPduRateFault	Pdu Rate Threshold crossed		yes		SN06.2
	OVLDB01	ovldRacMonCvMsgBFault	CvMsg Message Rate Overloaded Alarm		yes		SN06.2
	OVLDB02	ovldRacMonConnQueueFault	Connection Queue Overloaded Alarm		yes		SN06.2
	OVLDB03	ovldRacMonCpuUtilFault	PDU Rate Overloaded Alarm		yes		SN06.2
	OVLDB04	perfMonCPUFault	CPU Utilization Overloaded Alarm		yes		SN06.2
	OVLDB05	perfMonRamFault	RAM Utilization Overloaded Alarm		yes		SN06.2
	OVLDB06	perfMonFlashFault	Flash Utilization Overloaded Alarm		yes		SN06.2
	OVLDB07	perfMonChanFault	Chan Utilization Overloaded Alarm		yes		SN06.2

MG9000 Manager User Action Audit LOGs

LOG Subsystem	LOG Id	LOG Type	Description	SN06 VoA Telcordia Coverage?	Procedure To Generate LOG
MG9000 Manager	MGEM600	MG9000 HW	SWACT of ABI, ITP, ITX, OC3, or IMA card	n/a	See procedures in MG9000 FCAPS Document Fault Management section
	MGEM601	MG9000 HW	Lock of ABI, ITP, ITX, OC3, IMA, DS1, MTA, WLC, SAA, XDSL, SIC card	n/a	See procedures in MG9000 FCAPS Document Fault Management section
	MGEM602	MG9000 HW	Unlock of ABI, ITP, ITX, OC3, IMA, DS1, MTA, WLC, SAA, XDSL, SIC card	n/a	See procedures in MG9000 FCAPS Document Fault Management section
	MGEM603	MG9000 HW	Force Lock of ABI, ITP, ITX, OC3, IMA, DS1, MTA, WLC, SAA, XDSL, SIC card	n/a	See procedures in MG9000 FCAPS Document Fault Management section
	MGEM604	MG9000 HW	Force Unlock of ABI, ITP, ITX, OC3, IMA, DS1, MTA, WLC, SAA, XDSL, SIC card	n/a	See procedures in MG9000 FCAPS Document Fault Management section
	MGEM605	MG9000 HW	Diag of ABI, ITP, ITX, OC3, IMA, DS1, MTA, WLC, SAA, XDSL, SIC card	n/a	See procedures in MG9000 FCAPS Document Fault Management section
	MGEM606	SLoA Services	Create a VMG	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM607	SLoA Services	Delete a VMG	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM608	SLoA Services	ESA data configuration	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM609	SLoA Services	Gateway data configuration	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM610	SLoA Services	Create Termination	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM611	SLoA Services	Bulk Termination creation	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM612	SLoA Services	Create ESA Service Code	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM613	SLoA Services	Delete ESA Service Code	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM614	SLoA Services	Delete Termination	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM615	SLoA Services	Bulk Termination deletion	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM616	SLoA Services	Delete all termination on a card	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM617	SLoA Services	Change Termination data	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM618	PLoA Services	Create a PLoA Passive Endpoint	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM619	PLoA Services	Create a PLoA Active Endpoint	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM620	PLoA Services	Create a PLoA Hairpin connection	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM621	PLoA Services	PLoA Connection Admin State change	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM622	PLoA Services	PLoA Service Restart	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM623	PLoA Services	PLoA Connection SVC test initiated	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM624	PLoA Services	PLoA Connection SVC test abort	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM625	PLoA Services	PLoA Connection Unlock test	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM626	PLoA Services	Delete a PLoA Endpoint	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM627	ADSL Services	Modify ADSL data circuit provisioning attributes	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM628	ADSL Services	De-provision ADSL data circuit service	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM629	ADSL Services	Add new ADSL data circuit	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM630	ADSL Services	Change ADSL data circuit	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM631	ADSL Services	Delete ADSL data circuit	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM632	DS1 IMA	Set links in DS1 IMA group	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM633	DS1 IMA	Start DS1 IMA group pattern test	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM634	DS1 IMA	Stop DS1 IMA group pattern test	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM635	DS1 IMA	Add DS1 IMA link to group	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM636	DS1 IMA	Remove DS1 IMA link from group	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM637	DS1 IMA	Set administration state on DS1 IMA link	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM638	DS1 IMA	Set configuration state on DS1 IMA link	n/a	See procedures in MG9000 FCAPS Document Configuration Management

MGEM639	Carrier	OC3, DS1 IMA, DS1, DS0, carrier lock	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM640	Carrier	OC3, DS1 IMA, DS1, DS0, multiple carrier lock	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM641	Carrier	OC3, DS1 IMA, DS1, DS0, carrier unlock	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM642	Carrier	OC3, DS1 IMA, DS1, DS0, multiple carrier unlock	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM643	Carrier	OC3, DS1 IMA, DS1, DS0, forced carrier lock	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM644	Carrier	OC3, DS1 IMA, DS1, DS0, forced multiple carrier lock	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM645	Carrier	OC3, DS1 IMA, DS1, DS0, forced carrier unlock	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM646	Carrier	OC3, DS1 IMA, DS1, DS0, forced multiple carrier unlock	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM647	Carrier	OC3, DS1 IMA, DS1, DS0, carrier online	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM648	Carrier	OC3, DS1 IMA, DS1, DS0, multiple carrier online	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM649	Carrier	OC3, DS1 IMA, DS1, DS0, carrier offline	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM650	Carrier	OC3, DS1 IMA, DS1, DS0, multiple carrier offline	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM651	Line Circuit	WLC, ADSL Data/Line, SAA Line circuit lock	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM652	Line Circuit	WLC, ADSL Data/Line, SAA Line circuit multiple lock	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM653	Line Circuit	WLC, ADSL Data/Line, SAA Line circuit unlock	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM654	Line Circuit	WLC, ADSL Data/Line, SAA Line circuit multiple unlock	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM655	Line Circuit	WLC, ADSL Data/Line, SAA Line circuit diagnostic check	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM656	Line Circuit	WLC, ADSL Data/Line circuit abort diagnostic check	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM657	Line Circuit	WLC, ADSL Data/Line, SAA Line circuit set end to end test port	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM658	Line Circuit	WLC, ADSL Data/Line, SAA Line circuit set PAV test port	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM659	Line Circuit	WLC, ADSL Data/Line, SAA Line circuit clear test	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM660	LCI	Create new LCI user	n/a	
MGEM661	LCI	Delete existing LCI user	n/a	
MGEM662	LCI	Modify existing LCI user data	n/a	
MGEM663	DS1	Channelize DS1 carrier	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM664	DS1	Unchannelize DS1 carrier	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM665	DS1	Modify DS1 carrier provisioning attributes	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM666	DS1	Synchronize pre-provisioned bundles	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM667	DS1	Assign DS1 card spare	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM668	DS1	Release DS1 card spare	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM669	DS1	Revert DS1 card sparing activity	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM670	DS1	Initiate DS1 card sparing activity	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM671	DS1	Add DS1 card to protection group	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM672	DS1	Remove DS1 card from protection group	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM673	DS1 DS0	Provision DS0 bundle on DS1 carrier	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM674	DS1 DS0	Modify DS0 bundle	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM675	DS1 DS0	Set DS0 bundle circuit identifier	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM676	DS1 DS0	Lock DS0 bundle	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM677	DS1 DS0	Unlock DS0 bundle	n/a	See procedures in MG9000 FCAPS Document Configuration Management
MGEM678	DS1 DS0	Delete DS0 bundle	n/a	See procedures in MG9000 FCAPS Document Configuration Management
	MGEM679	ABI	ABI Card Switch Mastership requested	
	MGEM679		getCardType(+ restart requested	
	MGEM679		Frame location update requested	
	MGEM680		getCardType(+ configuration state (Online/Offline/Deprovision/Re-Initialize change requested	
	MGEM681		Unused	

	MGEM682		Unused		
	MGEM683		Unused		
	MGEM684		Unused		
	MGEM685		Unused		
	MGEM686		Unused		
	MGEM687		Unused		
	MGEM688		Unused		
	MGEM689		Unused		
	MGEM690		Unused		
	MGEM691		Unused		
	MGEM692		Unused		
	MGEM693		Unused		
	MGEM694		Unused		
	MGEM695		Unused		
	MGEM696		Unused		
	MGEM697		Unused		
	MGEM698		Unused		
	MGEM699		Unused		
	MGEM700		Audit request for one NE		
	MGEM701		Software Download Requested-single card type		
	MGEM704		Delete NE request		
	MGEM705		getCardType(+ deprovision requested		
	MGEM706		Provision/Create a DFAD Tap		
	MGEM707		Deprovision/Delete a DFAD Tap		
	MGEM708		Unused		
	MGEM709		Provision/Create an MTAP request		
	MGEM710		Deprovision/Delete an MTAP request		
	MGEM711		Upgrade VMG requested		
	MGEM712		Submit a request for audit		
	MGEM713		Discovery request		

Appendix F: CICM Logs and Alarms for SN07

The following table is the list of events that can be generated by the SAM21 blade-based CICM product in SN07. Some notes on the table's contents at the time of writing:

- The CICM353 log events are unique to the SAM16-based CICM product and are not contained in the table below.
- The CICM303 log (CorruptVLCM alarm) has no identified clear in the table below. A software issue discovered late in the release found that the alarm was being delivered improperly (as an SNMP trap instead of routed to the /var/log logging system on CS2000 Management Tools). When the CR tracking this issue is resolved, the event will have no severity and through the /var/log logging system.
- The CICM328 log (WindowsRestart alarm) has no identified clear in the table below. The WindowsRestart alarm occurs when CICM restarts. When the CICM application comes up, there is a cold start trap generated which is not documented in the table below. It may be possible to use this event as a "clear" for WindowsRestart.

CICM Logs and Alarms in SN07

Log	CICM Output	Alarm	Severity	Category	Description	Specific Problem
CICM300	/var/log/customerlog	LegacyError	None	environmental	Legacy Error Log.	Log details: XXX
CICM300	/var/log/customerlog	LegacyWarning	None	environmental	Legacy Warning Log.	Log details: XXX
CICM301	ALARM_TRAP_to_IEMS	softwareMismatch	Minor	environmental	Software Version Mismatch.	Version Mismatch. Local Version XXX. Mate Version XXX.
CICM301	ALARM_TRAP_to_IEMS	softwareMismatchClear	None	environmental	Software Version Mismatch.	Version Mismatch. Local Version XXX. Mate Version XXX.
CICM302	/var/log/customerlog	RouteOrElementStateMismatch	None	communications	Route/element state mismatch	Resetting adapter, state= XXX mate=XXX
CICM303	ALARM_TRAP_to_IEMS	CorruptVLCM	Warning	equipment	Corrupt VLCM.	VLCM name XXX is corrupt - in memory gateway already has id of XXX.
CICM304	/var/log/customerlog	UnableBindIP	None	communications	Unable to bind IP.	Unable to bind IP address XXX to interface XXX.
CICM305	/var/log/customerlog	NoAdapterMib	None	processingError	Unable To Bind Adapter.	Unable to obtain dynamic adapter config from Mib - cannot bind adapter.
CICM306	/var/log/customerlog	NoAdminIPNodeA	None	processingError	No admin Ip for node A.	No admin address datafilled for node A
CICM306	/var/log/customerlog	NoAdminIPNodeB	None	processingError	No admin Ip for node B.	No admin address datafilled for node B
CICM306	/var/log/customerlog	NoAdminNetMask	None	processingError	No admin net mask.	No admin net mask datafilled
CICM306	/var/log/customerlog	InvalidAdminAddr	None	processingError	Invalid admin address.	Invalid admin ip address specified XXX
CICM306	/var/log/customerlog	InvalidAdminMask	None	processingError	Invalid admin mask.	Invalid admin mask specified XXX
CICM307	/var/log/customerlog	SkippingDisabledAdapter	None	communications	Skipping disabled adapter	Skipping disabled XXX adapter.
CICM308	/var/log/customerlog	UFTPSessionTimeout1	None	communications	UFTPSessionTimeout.	Timed out after XXX secs - No request details received from client
CICM308	/var/log/customerlog	UFTPSessionTimeout2	None	communications	UFTPSessionTimeout.	Timed out after XXX secs - No response from client
CICM308	/var/log/customerlog	UFTPSessionTimeout3	None	communications	UFTPSessionTimeout.	Timed out after XXX secs - Terminated after error occurred
CICM309	/var/log/customerlog	NoStreamsAvailable	None	communications	NoStreamsAvailable.	No streams available for CreateConnection, XXX streams already allocated
CICM310	/var/log/customerlog	H248SendPortNotFoundInMIB	None	communications	H248 Send Port Not Found in MIB.	XXX : H248 send port not found in MIB.Defaulting to XXX
CICM310	/var/log/customerlog	H248ListenPortNotFoundInMIB	None	communications	H248 Listen Port Not Found in MIB.	XXX : H248 listen port not found in MIB.Defaulting to XXX

CICM311	/var/log/customerlog	CouldNotOpenRegKey	None	processingError	Could not open registry key.	Could not open XXX in registry. New hierarchy needs to be created. This event can be generated during initial configuration of the gateway.
CICM311	/var/log/customerlog	MibFailedOpenKey	None	processingError	Mib failed to open key.	Mib node error: failed to open key XXX.
CICM312	/var/log/customerlog	MIBCompatFailure	None	processingError	MIB compatibility failure.	MIB compatability failure. Could not find the MIB entries for release XXX
CICM312	/var/log/customerlog	MIBCompatRemFailure	None	processingError	MIB compatibility remote failure.	MIB compatability failure. Could not find the MIB entries for release XXX on remote node
CICM313	ALARM_TRAP_to_IEMS	GWCCConnectionLoss	Critical	communications	GWC Connection Loss	CICM has lost connection with the GWC
CICM313	ALARM_TRAP_to_IEMS	GWCCConnectionLossClear	None	communications	GWC Connection Loss	CICM has regained connection with GWC
CICM314	/var/log/customerlog	MibReadFailure	None	processingError	Mib Registry Read Failure.	Mib registry error: failed to read attribute XXX in key XXX. Probable cause is out of date config data.
CICM316	/var/log/customerlog	UnableCreateSocket	None	communications	Unable to create a socket.	Unable to create a socket. Error = XXX
CICM316	/var/log/customerlog	UnableBindSocketAddr	None	communications	Unable to Bind Socket to IP.	Unable to Bind Socket to IP address.
CICM316	/var/log/customerlog	AddrNotAvailable	None	communications	Addr not available.	Specified address is not available on the local host.
CICM316	/var/log/customerlog	AddrInUse	None	communications	Addr already in use.	Specified address is already in use.
CICM316	/var/log/customerlog	NoAsyncReadMode	None	communications	No async read mode	Unable to select asynchronous read mode. Error = XXX
CICM316	/var/log/customerlog	ErrorSetSocketTMO	None	communications	Error setting socket tmo	Error setting socket timeout. Error = XXX
CICM322	ALARM_TRAP_to_IEMS	SystemShutdown	Critical	processingError	System Shutdown	System is shutting down due to user command.
CICM322	ALARM_TRAP_to_IEMS	SystemStartUp	None	processingError	System Shutdown	System is starting up.
CICM323	/var/log/customerlog	SlaveAdapterReceivedNoPackets	None	communications	Slave adapter received no packets	Slave adapter XXX received no packets
CICM324	/var/log/customerlog	FatalStateError	None	equipment	Fatal Error in state	Fatal error in state XXX.
CICM325	/var/log/customerlog	ElementNotConfigured	None	processingError	Element Not Configured.	Element XXX is not configured.
CICM325	/var/log/customerlog	ElementNotConfigured2	None	processingError	Config data missing.	Configuration data missing, service cannot start.
CICM326	/var/log/customerlog	UnableToGetPhysicalLinkStatusForDevice	None	communications	Unable to get physical link status	Unable to get physical link status for device XXX
CICM327	/var/log/customerlog	FailedStartNetObj	None	equipment	Failed to start network status	Failed to start network status object, hr=0x XXX

CICM328	ALARM_TRAP_to_IEMS	WindowsRestart	Critical	equipment	Windows restart	Auto reboot on failure is set. Initiating windows restart.
CICM329	/var/log/customerlog	AuditMateDown	None	equipment	Audit Mate Node Down	Node initialisation: mate node is down
CICM329	/var/log/customerlog	AuditMateActive	None	equipment	Audit Mate Node Down	Node initialisation: mate node is active in state XXX
CICM330	/var/log/customerlog	CantDoPhysicalCheckOnLink	None	communications	Can't do physical check on link	Can't do physical check on link XXX
CICM331	/var/log/customerlog	CompFailureShutdown	None	equipment	Component failure : shutdown	Component XXX has failed. Initiating shutdown. XXX
CICM332	/var/log/customerlog	BadTransition	None	equipment	Bad transition on mate node	Bad transition on mate node from XXX to XXX
CICM333	/var/log/customerlog	NoAccessRemoteName	None	communications	No access to remote name	No access to the remote name in the MIB.
CICM334	ALARM_TRAP_to_IEMS	MateFailure	Warning	equipment	Audit: Mate Node Failed	Mate node failed - Broadcast failure and ask components to promote to Master.
CICM334	ALARM_TRAP_to_IEMS	MateRecovered	None	equipment	Audit: Mate Node Failed	Mate node recovered.
CICM335	/var/log/customerlog	RouteElementInvalid	None	communications	Route Element Invalid	Local route element XXX or remote route element XXX is invalid
CICM336	/var/log/customerlog	NetworkRecovery	None	communications	Network loss and recovery	Network has been lost and then recovered, mate (slave) must reboot.
CICM337	ALARM_TRAP_to_IEMS	NoMessageToA	Major	equipment	Message To Node A Failed	Failed to send message to Node A.
CICM337	ALARM_TRAP_to_IEMS	NoMessageToAClear	None	equipment	Message To Node A Failed	Clear Failed to send message to Node A.
CICM338	/var/log/customerlog	NetworkElementHasFailed	None	communications	Network Element Failed	Network Element XXX Failed
CICM339	ALARM_TRAP_to_IEMS	NoMessageFromB	Major	equipment	No Message Received From B	Have not received a message from Node B for 1.5*ALARM_POLL_PERIOD Seconds. XXX
CICM339	ALARM_TRAP_to_IEMS	NoMessageFromB Clear	None	equipment	No Message Received From B	Clear: Have not received a message from Node B for 1.5*ALARM_POLL_PERIOD Seconds. XXX
CICM340	/var/log/customerlog	CantSetLocalAdapter	None	communications	Can't set local adapter	Can't set local adapter, invalid adapter specified
CICM341	ALARM_TRAP_to_IEMS	BackupFail	Minor	processingError	Backup Fail.	Scheduled/on-demand backup failed during last iteration.
CICM341	ALARM_TRAP_to_IEMS	BackupFailClear	None	processingError	Backup Fail.	Scheduled/on-demand backup failed during last iteration.
CICM342	/var/log/customerlog	UnableToBindAdminIPAddressToInterface	None	communications	Unable to bind admin IP address to interface	Unable to bind admin IP address to interface XXX - will continue to attempt to bind
CICM344	/var/log/customerlog	CantSetSlaveAdapter	None	communications	Can't set slave adapter	Can't set slave adapter, invalid adapter specified xxx

CICM345	/var/log/customer log	EMMateDown	None	communications	EM Mate Down	Mate node down. Name: XXX. XXX
CICM346	/var/log/customer log	EMMibWriteFail	None	communications	EM Mate Down	Couldn't write EM remote node status to Mib
CICM348	/var/log/customer log	ChangingSlaveAda pter	None	communications	Changing slave adapter	Changing slave adapter from XXX to XXX
CICM350	/var/log/customer log	GetInterfaceDevice Mapping	None	communications	Get Interface Device Mapping Failed	Get Interface Device Mapping Failed
CICM352	/var/log/customer log	CantMapAdapter	None	communications	Can't map adapter	Can't map XXX to an NT device, link state won't be checked
CICM354	/var/log/customer log	maxRudpSessions NotPresent	None	communications	maxRudpSessionsNot Present.	Maximum sessions configuration not present
CICM354	/var/log/customer log	UnableToSetMaxR UDPSessions	None	communications	UnableToSetMaxRUD PSessions.	unable to set max RUDP sessions [may already be started]
CICM355	/var/log/customer log	VmgIplAddressBind Failed	None	communications	Bind UDP socket for vmg failed.	Failed to start UDP socket. hr XXX
CICM355	/var/log/customer log	VmgTerminationInv alid	None	communications	VMG termination invalid.	VMG XXX termination XXX invalid
CICM356	/var/log/customer log	AdapterDown	None	communications	Adapter down	Adapter XXX is down - aborting start until all adapters are up
CICM357	/var/log/customer log	EchoServerPortNot Present	None	communications	EchoServerPortNotPre sent.	Echo server port configuration not present
CICM358	/var/log/customer log	UnableToMapNET olInterfaceNumber	None	communications	Unable to map ne to an interface number	Unable to map ne XXX to an interface number
CICM360	/var/log/customer log	AutoBindAdapter	None	communications	Auto-bind adapter problem	Auto-bind adapter XXX XXX
CICM361	/var/log/customer log	HostPortNotPresen t	None	communications	HostPortNotPresent.	Host port configuration not present
CICM362	/var/log/customer log	SwactRequestReje cted	None	communications	Swact request rejected	Swact request rejected XXX
CICM363	/var/log/customer log	CreateConnectionA ckFailed	None	communications	Create ConnectionAck Failed.	CreateConnectionAck::can't determine destination for message
CICM363	/var/log/customer log	ModifyConnectionA ckFailed	None	communications	Modify ConnectionAck Failed.	ModifyConnectionAck::can't determine destination for message
CICM363	/var/log/customer log	SetConnectionAck Failed	None	communications	Set ConnectionAck Failed.	SetConnNetModeAck::can't determine destination for message
CICM363	/var/log/customer log	noPtimeCanBeNeg otiated	None	communications	no ptime can be negotiated.	Ensure a common ptime exists between the GWC and the CICM terminal audio profile
CICM363	/var/log/customer log	noCodecCanBeNe gotiated	None	communications	no codec can be negotiated.	Ensure a common codec exists between the GWC and the CICM terminal audio profile
CICM364	/var/log/customer log	RegisterGatewayFa iled	None	communications	Register Gateway Failed	Register Gateway XXX Failed

CICM364	/var/log/customerlog	UnRegisterGatewayFailed	None	communications	UnRegister Gateway Failed	UnRegister Gateway XXX Failed
CICM365	/var/log/customerlog	MibSyncMateFail	None	equipment	Mib Sync Mate Failure	Mate node failed during MIB synchronisation. This node will start partially Synchronised.
CICM366	/var/log/customerlog	MibSyncSCMPollfail	None	equipment	Mib Sync SCM Poll Failure	Opening Service Control Manager FAILURE.
CICM367	/var/log/customerlog	ErrorDatafillTones	None	equipment	Error Datafilling Tones	Error encountered datafilling tones!.
CICM368	/var/log/customerlog	NoMaxSessions	None	equipment	Max Sessions Not Present	Invalid config. Max Sessions not present.
CICM368	/var/log/customerlog	MaxSessionsNotPresent	None	communications	MaxSessionsNotPresent.	Maximum sessions configuration not specified
CICM369	/var/log/customerlog	NoDomainLicense	None	equipment	No Domain License	No network domain license for terminal at XXX
CICM370	ALARM_TRAP_to_IEMS	MateFailure	Major	communications	Mate Failure.	Admin reports mate node failure.
CICM370	ALARM_TRAP_to_IEMS	MateStarting	None	communications	Mate Failure.	Admin reports Mate Node start.
CICM371	/var/log/customerlog	TerminalError	None	equipment	An Error Occured on the Terminal	Terminal Error XXX
CICM372	/var/log/customerlog	UnableToMapAdapter	None	communications	Unable to map adapter	Unable to map XXX adapter XXX to an ip address.
CICM373	/var/log/customerlog	UFTPFWirmwareFileOpenFailed	None	communications	UFTPFWirmwareFileOpenFailed.	Failed to open file XXX.
CICM373	/var/log/customerlog	UFTPFWirmwareFileOpenFailedFatal	None	communications	UFTPFWirmwareFileOpenFailed.	Invalid directory or file XXX not found
CICM373	/var/log/customerlog	UFTPFWirmwareFileReadError	None	communications	UFTPFWirmwareFileReadError.	Firmware file XXX read error
CICM373	/var/log/customerlog	UFTPCommandFileReadError	None	communications	UFTPCommandFileReadError.	UFTPCommandFileReadError
CICM373	/var/log/customerlog	UFTPCommandFileCreationError	None	communications	UFTPCommandFileCreationError.	Command = XXX
CICM373	/var/log/customerlog	UFTPBaseDirectoryMissing	None	communications	UFTPBaseDirectoryMissing.	UFTP base directory missing from registry
CICM374	/var/log/customerlog	ReadPollPeriodFail	None	communications	Poll Period Read Fail	Couldn't read gwPollPeriod from mib. Defaulting to 30 seconds.
CICM375	ALARM_TRAP_to_IEMS	SAM21VersionMismatch	Minor	processingError	SAM21 Version Mismatch.	SAM21 Version Mismatch. Version XXX
CICM375	ALARM_TRAP_to_IEMS	SAM21VersionMismatchClear	None	processingError	SAM21 Version Mismatch.	SAM21 Version Mismatch. Version XXX
CICM376	/var/log/customerlog	ShuttingDownTerminals	None	communications	ShuttingDownTerminals.	Shutdown counter set to zero minutes, shutting down terminals immediately
CICM376	/var/log/customerlog	TerminalShutDownAborted	None	communications	TerminalShutDownAborted.	Terminal shutdown aborted
CICM377	ALARM_TRAP_to_IEMS	SyslogFailure	Major	communications	Syslog Failure.	Syslog failure. Last stream in failure XXX.
CICM377	ALARM_TRAP_to_IEMS	SyslogFailureClear	None	communications	Syslog Failure.	Syslog failure clear.

CICM378	/var/log/customer log	ExcessNodes	None	communications	Excessive Nodes on EM	More than 100 nodes present, unrecommended configuration
CICM379	/var/log/customer log	RegisterSessionFai led	None	communications	Register Session Failed	Register Session Failed on Gateway XXX
CICM379	/var/log/customer log	RegisterSessionFai ledRange	None	communications	Register Gateway Failed	Register Gateway XXX Failed termination XXX is out of range
CICM379	/var/log/customer log	RegisterSessionFai ledInvalid	None	communications	Register Gateway Failed	Register Gateway XXX Failed termination XXX is invalid
CICM379	/var/log/customer log	CouldntStartAuditTi mer	None	communications	Couldn't start audit timer	Couldn't start audit timer
CICM380	ALARM_TRAP_t o_IEMS	FailedPollIMG	Warning	communications	Fail Poll MG	Failed to Poll Media Gateway XXX.
CICM380	ALARM_TRAP_t o_IEMS	FailedPollIMGClear	None	communications	Fail Poll MG	Failed to Poll Media Gateway XXX.
CICM381	ALARM_TRAP_t o_IEMS	NetworkLoss	Critical	communications	Network Loss.	Critical network connection loss on adapter XXX
CICM381	ALARM_TRAP_t o_IEMS	ClearNetworkLoss	None	communications	Network Loss.	Critical network connection loss cleared on adapter XXX
CICM381	ALARM_TRAP_t o_IEMS	NetworkLossMajor	Major	communications	Network Loss.	Major network connection loss on adapter XXX
CICM381	ALARM_TRAP_t o_IEMS	ClearNetworkLoss Major	None	communications	Network Loss.	Major network connection loss cleared on adapter XXX
CICM382	ALARM_TRAP_t o_IEMS	RemoteHostFail	Minor	communications	Remote Host Fail.	Disabling client XXX with interface XXX.
CICM382	ALARM_TRAP_t o_IEMS	RemoteHostFailCle ar	None	communications	Remote Host Fail.	Enabling client XXX with interface XXX.
CICM383	ALARM_TRAP_t o_IEMS	FirmwareUpgradeF ail	Warning	communications	Firmware upgrade failure.	Firmware upgrade failure.
CICM383	ALARM_TRAP_t o_IEMS	FirmwareUpgradeF ailClear	None	communications	Firmware upgrade failure.	Firmware upgrade failure.
CICM383	/var/log/customer log	FirmwareUpgradeN otSupportedUFTP OverUnistim	None	communications	FirmwareUpgradeNotS upportedUFTPOverUni stim.	Firmware upgrade is not supported via UFTP over Unistim. File XXX
CICM384	/var/log/customer log	NodeIsolatedForcin gTransitionFromMa sterToSlave	None	communications	Node Isolated - Forcing transition from master to slave	Node Isolated - Forcing transition from master to slave
CICM385	/var/log/customer log	SlaveNodeIsolated	None	communications	Slave Node isolated	Slave Node isolated
CICM386	/var/log/customer log	UFTPmaxSessions MIBDataFatal	None	communications	UFTPmaxSessions value in the mib is incorrect	UFTPmaxSessions must be at least one. Value XXX is invalid
CICM386	/var/log/customer log	UFTPmaxSessions MIBDataNonFatal	None	communications	UFTPmaxSessions value is missing from the mib	UFTPmaxSessions missing using default value XXX
CICM387	ALARM_TRAP_t o_IEMS	CommsFailedCicm	Major	communications	CICM Poll Failed	Failed to Poll CICM Node XXX.
CICM387	ALARM_TRAP_t o_IEMS	CommsFailedCicm Clear	None	communications	CICM Poll Failed	Failed to Poll CICM Node XXX.
CICM388	/var/log/customer log	UFTPtimerTimeout MIBDataNonFatal	None	communications	UFTPtimerTimeout value is missing from the mib	UFTPtimerTimeout missing using default value XXX

CICM389	/var/log/customerlog	UFTPInvalidClient Message	None	communications	UFTP_INVALID_CLIENT_MESSAGE	UFTP_INVALID_CLIENT_MESSAGE XXX value XXX is invalid
CICM390	ALARM_TRAP_to_IEMS	FailedPAMConn	Major	communications	Failed To Connect PAM server	PAM server XXX is not responding to authentication requests
CICM390	ALARM_TRAP_to_IEMS	FailedPAMConnClear	None	communications	Failed To Connect PAM server	PAM server XXX is now responding to authentication requests
CICM391	/var/log/customerlog	ProcessNetworkStateTransitionStateError	None	communications	Invalid transition	ProcessNetworkStateTransition() called with invalid transition XXX
CICM392	/var/log/customerlog	PAMServerTMO	None	communications	PAM Server TMO	Timeout occurred whilst awaiting response from PAM server XXX
CICM393	/var/log/customerlog	TakeoverManualAbortedIsNotImplemented	None	communications	Takeover manual aborted, is not implemented	Takeover manual aborted, is not implemented
CICM394	/var/log/customerlog	FailedToUnbindAdapter	None	communications	Fatal error: Unable to unbind adapter	Fatal error: Unable to unbind adapter.
CICM395	/var/log/customerlog	MateNodeFailedTemporarily	None	communications	Mate node failed temporarily	Mate node failed temporarily for XXX iterations
CICM396	/var/log/customerlog	TakeoverAbortIsNotImplemented	None	communications	Takeover abort, is not implemented	Takeover abort, is not implemented
CICM397	/var/log/customerlog	MateNodeLostForcingTransitionFromSlaveToMaster	None	communications	Mate node lost - Forcing transition from slave to master	Mate node lost - Forcing transition from slave to master
CICM398	/var/log/customerlog	MateNodeLost	None	communications	Mate node lost	Mate node lost
CICM399	/var/log/customerlog	RouteMapError	None	communications	Route map error	Resetting adapter, state= XXX mate=XXX
CICM500	/var/log/customerlog	StateChange	None	processingError	State Change.	Admin reports a state change to XXX for component XXX.
CICM503	/var/log/customerlog	NetAccessStateChange	None	communications	Network Access State Change	Netork access state change to XXX
CICM504	/var/log/customerlog	EMNetworkChange	None	communications	EM Network State Change	Network connectivity XXX. hr=XXX
CICM505	/var/log/customerlog	StopMonitoring	None	communications	Stop Monitoring	Stopped monitoring node XXX
CICM506	/var/log/auditlog	MonitorStart	None	communications	Start Monitoring	Started to monitor node XXX.
CICM507	/var/log/auditlog	ConnectToPAMServer	None	environmental	Connect to PAM.	Connect to PAM.
CICM508	/var/log/customerlog	SlaveInstructedToChangeToInvalidAdapter	None	communications	Slave instructed to change to invalid adapter, selecting default	Slave instructed to change to invalid adapter, selecting default
CICM509	ALARM_TRAP_to_IEMS	ProcessStateChange	Critical	processingError	Critical Process State Change.	Critical Process XXX is not running.
CICM509	ALARM_TRAP_to_IEMS	ProcessStateChangeClear	None	processingError	Critical Process State Change.	Critical Process XXX is running.

CICM509	ALARM_TRAP_to_IEMS	ServiceStateChange	Major	processingError	Service State Change.	Service XXX is not running.
CICM509	ALARM_TRAP_to_IEMS	ServiceStateChangeClear	None	processingError	Service State Change.	Service XXX is running.
CICM510	/var/log/auditlog	EMMateUp	None	environmental	EM Mate Up.	EM Mate Up. Name: XXX.
CICM512	/var/log/customerlog	StartSWACT	None	processingError	Start SWACT.	Admin reports a request to start SWACT.
CICM512	/var/log/customerlog	PromoteToMaster	None	processingError	Promote to Master.	Admin reports a request to promote to Master.
CICM512	/var/log/customerlog	DemoteToSlave	None	processingError	Demote to Slave.	Admin reports a request to demote to slave.
CICM513	/var/log/auditlog	ChangingLocalAdapter	None	communications	Changing local adapter	Changing local adapter from XXX to XXX
CICM603	/var/log/customerlog	InvalidEventReport	None	processingError	Invalid Event Report.	Invalid report received from Admin.
CICM604	/var/log/customerlog	MateSyncErrState	None	processingError	Mate sync error state.	request for mate synchronisation received in state XXX.
CICM605	/var/log/customerlog	GWRegBadState	None	equipment	GW Reg in Bad State.	Gateway registration received in state XXX.
CICM606	/var/log/customerlog	PremSlaveGWReg	None	equipment	Premature reg slave gw.	Premature registration of the slave gateway.
CICM607	/var/log/customerlog	SwactReqRemoteMGM	None	equipment	Swact Request from Remote MGM.	Swact request received from the remote MGM.
CICM608	/var/log/customerlog	RetransRUDPMessagesThrottled	None	communications	Retransmitted RUDP messages.	Retransmitted XXX RUDP messages, XXX retransmissions were throttled.
CICM609	/var/log/customerlog	RetransRUDPMessages	None	communications	Retransmitted RUDP messages.	Retransmitted XXX RUDP messages.
CICM610	/var/log/customerlog	LossOfLogs	None	communications	Loss of logs.	XXX logs have been lost due to buffering.
CICM610	/var/log/customerlog	LossOfTraps	None	communications	Loss of traps.	XXX traps have been lost due to buffering.
CICM611	ALARM_TRAP_to_IEMS	ThresholdReached	Major	qualityOfService	Resource Threshold Crossed	Resource XXX is near or above its threshold of XXX
CICM611	ALARM_TRAP_to_IEMS	ThresholdReached Clear	None	qualityOfService	Threshold Crossed	Resource XXX is near or above its threshold value of XXX
CICM612	/var/log/customerlog	AuditStart	None	environmental	Start Audit.	Starting the daily audit.
CICM612	/var/log/customerlog	AuditEnd	None	environmental	Audit Complete	Daily audit completed.
CICM614	/var/log/customerlog	MsgFromInvalidComponent	None	equipment	Message from invalid component	Message received from invalid component type = 0x XXX
CICM615	/var/log/customerlog	NodeForcedMaster	None	equipment	Node forced to master	Node is being forced to become master.
CICM615	/var/log/customerlog	NodeForcedSlave	None	equipment	Node forced to slave	Node is being forced to become slave.
CICM617	/var/log/customerlog	MibSyncPollFail	None	equipment	Mib Sync Poll Failure	Network status remote state query returned hr=0x XXX.

CICM618	/var/log/customer log	NoLineID	None	equipment	No Line ID	User XXX has no LineID attribute in the mib.
CICM619	/var/log/customer log	NoToneset	None	equipment	No Toneset Found	Toneset XXX not found A standard tone will be used in place of all toneIDs
CICM620	/var/log/customer log	InvalidToneIndex	None	equipment	Invalid Tone Component Index	Invalid tone component index toneset XXX toneid XXX
CICM621	/var/log/customer log	NoVolume	None	equipment	Invalid Volume Datafilled	No volume datafilled for toneset XXX toneid XXX
CICM622	/var/log/customer log	Invalidtone	None	equipment	Invalid Tone Frequency	Invalid tone frequency count toneset XXX toneid XXX
CICM623	/var/log/customer log	NoFrequency	None	equipment	Invalid Frequency Datafilled	No frequency datafilled for toneset XXX toneid XXX
CICM624	/var/log/customer log	InvalidCadenceCount	None	equipment	Invalid Cadence Count	Invalid tone cadence count toneset XXX toneid XXX
CICM625	/var/log/customer log	NoCadenceOff	None	equipment	No Cadence Off	No Cadence off datafilled for toneset XXX toneid XXX
CICM625	/var/log/customer log	NoCadenceOn	None	equipment	No Cadence On	No Cadence on datafilled for toneset XXX toneid XXX
CICM627	/var/log/customer log	InvalidConnMap	None	equipment	Connection mapped to invalid line	Connection XXX is mapped to line XXX which isn't valid.
CICM628	/var/log/customer log	ConnNonE1	None	equipment	Connection mapped not in E1_CONN state	Connection XXX is mapped to line XXX which isn't in E1_CONNECTION state.
CICM629	/var/log/customer log	ResetNoConn	None	equipment	Reset Connection isn't in NO_CONNECTION state	Resetting connection for line XXX which isn't in NO_CONNECTION state.
CICM630	/var/log/customer log	CreateConFail	None	equipment	Create Connection Fail	Create connection failed. Call type = XXX, result = XXX
CICM631	/var/log/customer log	DelConFail	None	equipment	Delete Connection Fail	Delete connection failed.
CICM632	/var/log/customer log	NoLineObject	None	equipment	No line object	Create Connection: Could not find line object for conflicting connection XXX with lineid = XXX
CICM633	/var/log/customer log	CorruptConnMap	None	equipment	Corrupt Connection Map	Connection map is corrupt, or media control is reusing handles, connection id XXX is already in use my lineid XXX.
CICM634	/var/log/customer log	NoConIDMap	None	equipment	No Connection Id map	Connection map is corrupt, or media control is reusing handles, connection id XXX could not be found in the map.
CICM635	/var/log/customer log	UnableChangeLoss	None	equipment	Unable Change Rx Loss	Unable to change rx loss for connection XXX
CICM636	/var/log/customer log	TooManyFeatures	None	equipment	Too Many Features	Terminal type has too many features on the main set (max is XXX).
CICM637	/var/log/customer log	TooManyFeaturesExt	None	equipment	Too Many Features	Terminal type has too many features on the extension set (max is XXX).

CICM638	/var/log/securitylog	AuthUserProblem	None	equipment	Auth User Failed	User XXX
CICM639	/var/log/securitylog	LogoutSuccess	None	equipment	Logout Success	User XXX
CICM639	/var/log/securitylog	LoginSuccess	None	equipment	Login Success	User XXX
CICM641	/var/log/securitylog	ChangePassword	None	equipment	Change Password Attempt	User XXX
CICM642	/var/log/securitylog	ReleaseAuth	None	equipment	Release Authentication	
CICM643	/var/log/customerlog	InvalidFirmwareProt	None	equipment	Invalid Firmware Protocol	Invalid FirmwareProtocol for TerminalType= XXX
CICM644	/var/log/customerlog	InvalidFWLevel	None	equipment	Invalid Firmware Level	Invalid Firmware level for TerminalType= XXX
CICM645	/var/log/customerlog	NoFWLevel	None	equipment	No Firmware Level	Terminal has no firmware level recorded in the MIB
CICM646	/var/log/customerlog	InvalidUFTHost	None	equipment	Invalid UFTP Host	Invalid UFTP host port
CICM647	/var/log/customerlog	InvalidUnistimHost	None	equipment	Invalid Unistim Host	Invalid Unistim host address
CICM648	/var/log/customerlog	InvalidFWTFTPAddr	None	equipment	Invalid Firmware TFTP Address	Invalid Firmware TFTP Address for TerminalType=XXX
CICM649	/var/log/auditlog	ConfigDataChange	None	processingError	Config Data Change.	Admin reports a configuration data change.
CICM650	/var/log/auditlog	InitialisingAsMaster	None	communications	Initialising as master	Initialising as master
CICM650	/var/log/auditlog	InitialisingAsMasterNoSlave	None	communications	Initialising as master (no slave)	Initialising as master (no slave)
CICM650	/var/log/auditlog	InitialisingAsSlave	None	communications	Initialising as slave	Initialising as slave
CICM650	/var/log/auditlog	StartingTakeover	None	communications	Starting takeover	Starting takeover
CICM650	/var/log/auditlog	TakeoverSucceededNowSlave	None	communications	Takeover succeeded, now slave	Takeover succeeded, now slave
CICM650	/var/log/auditlog	TakeoverSucceededNowMaster	None	communications	Takeover succeeded, now Master	Takeover succeeded, now Master
CICM650	/var/log/auditlog	ForcingTransitionFromSlaveToMaster	None	communications	Forcing transition from slave to master	Forcing transition from slave to master
CICM650	/var/log/auditlog	ForcingTransitionFromMasterToSlave	None	communications	Forcing transition from master to slave	Forcing transition from master to slave
CICM650	/var/log/auditlog	MateNodeRecoveredForcingtransitionFromSlaveToMaster	None	communications	Mate Node Recovered - Forcing transition from slave to master	Mate Node Recovered - Forcing transition from slave to master
CICM650	/var/log/auditlog	ProcessingSwact	None	communications	Processing Swact	Processing Swact request
CICM652	/var/log/auditlog	addGateway	None	communications	Adding a gateway	Gateway XXX has been added.
CICM653	/var/log/auditlog	deleteGateway	None	communications	Deleting a gateway	Deleting gateway XXX

CICM654	/var/log/auditlog	addProfile	None	communications	Adding a profile	Adding a XXX profile for gateway XXX
CICM655	/var/log/auditlog	delProfile	None	communications	Deleting a profile	Deleting XXX profile for gateway XXX
CICM656	ALARM_TRAP_to_IEMS	maxRxRateExceeded	Minor	processingError	Max Rx Rate Exceeded.	Max rx rate of XXX has been exceeded by rate XXX.
CICM656	ALARM_TRAP_to_IEMS	maxRxRateExceededClear	None	processingError	Max Rx Rate Exceeded.	Clear max rx rate of XXX has been exceeded.
CICM657	ALARM_TRAP_to_IEMS	maxCreateAttempts	Minor	communications	Max Creation Attempts.	Reached the max creation attempts for the session.
CICM657	ALARM_TRAP_to_IEMS	maxCreateAttemptsClear	None	communications	Max Creation Attempts.	Reached the max creation attempts for the session.
CICM658	/var/log/auditlog	MateNodeRecovered	None	communications	Mate node recovered	Mate node recovered
CICM659	/var/log/auditlog	SlaveAdapterRecovered	None	communications	Slave adapter recovered	Slave adapter XXX recovered
CICM660	/var/log/securitylog	SuccessfulPAMAuthentication	None	environmental	Successful PAM Authentication.	User XXX has started a session on the CICM-EM
CICM661	/var/log/securitylog	PAMAuthenticationFailure	None	processingError	PAM Authentication Failure.	User XXX authentication failure
CICM662	/var/log/securitylog	UserRevoked	None	environmental	User Privileges Revoked.	Privileges revoked
CICM663	/var/log/securitylog	UserUpgraded	None	environmental	User Privileges upgraded.	Privileges upgraded
CICM664	/var/log/securitylog	InactiveUserTMO	None	environmental	Inactive User Timeout.	User XXX is no longer active on the CICM-EM
CICM665	/var/log/auditlog	NetworkElementHasRecovered	None	communications	Network Element recovered	Network Element XXX recovered
CICM668	ALARM_TRAP_to_IEMS	MaxNoSessions	Warning	processingError	Reached the maximum number of sessions.	Current number of active sessions has reached the maximum of XXX.
CICM668	ALARM_TRAP_to_IEMS	MaxNoSessionsClear	None	processingError	Reached the maximum number of sessions.	Current number of active sessions is below the maximum of XXX.
CICM680	/var/log/auditlog	RegisterGatewaySucceeded	None	communications	Register Gateway Succeeded	Register Gateway XXX Succeeded
CICM681	/var/log/auditlog	ConfigurationChange	None	communications	Configuration change	XXX
CICM682	/var/log/auditlog	ProvisioningChange	None	communications	Provisioning change	XXX
CICM749	/var/log/securitylog	AccountDisabled	None	equipment	Account Disabled	User XXX
CICM750	/var/log/securitylog	ChangePasswordFail	None	equipment	Change Password Attempt	User XXX

Succession

SN07 OSS Guide (IP)

Advance Feature Guide

Copyright © 2004 Nortel Networks,
All Rights Reserved

NORTEL NETWORKS CONFIDENTIAL: The information contained herein is the property of Nortel Networks and is strictly confidential. Except as expressly authorized in writing by Nortel Networks, the holder shall keep all information contained herein confidential, shall disclose the information only to its employees with a need to know, and shall protect the information, in whole or in part, from disclosure and dissemination to third parties with the same degree of care it uses to protect its own confidential information, but with no less than reasonable care. Except as expressly authorized in writing by Nortel Networks, the holder is granted no rights to use the information contained herein.

Nortel Networks, the Nortel Networks logo, the Globemark, How the World Shares Ideas, and Unified Networks are trademarks of Nortel Networks.

Publication number: PLN-07IP-OSS
Product release: SN07
Document release: Standard 01.04
Date: December 2004
United States of America