

(I)SN09FF OSS Guide

Advance Feature Guide

(I)SN09FF Standard 01.06 June 2006

(I)SN09FF OSS Guide

Advance Feature Guide

Publication number: PLN-i09FF-OSS
Product release: (I)SN09FF
Document release: Standard 01.06
Date: June 2006

Copyright © 2006 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

June 2005

Standard release 01.06 of this document for (I)SN09FF, re-release of Standard due to CR content. The following update has been made:

- Per CR Q01374755, updated Chapter 2, IEMS Functionality, to reflect changes in the XML and CSV reports generated by IEMS.

Note: Publication History for International features appears at the start of Chapter 4.

May 2005

Standard release 01.05 of this document for (I)SN09FF, re-release of Standard due to CR content. The following updates have been made:

- Per CR Q01333369, added a section under Feature Deltas on activating/deactivating T.38 in TGCP gateways.
- Per CR Q01360938, updated A00012905 with corrected ERS8600 log information. Also updated Appendix G, ERS8600 Trap List.

April 2006

Standard release 01.04 of this document for (I)SN09FF, re-release of Standard for Customer Ready due to churn. The following features and CRs have been added since the last Standard release:

- Per CR Q01210435-03, added log GWC322 to the New and Changed section and the Baseline section.
- Per CR Q01060433-03, added log VMG313 to the New and Changed section and the Baseline section.
- A00012183, Public Key Manager
- A00012215, Global Line Card Field Programmable Gate Array download
- A00012242, TME-CD with GSM Wireless Client, Phase-1

- A00012310, Hunt, SCMP, and CWT variant support for SIP Lines
- A00012349, U3WC Support for SIP Lines
- A00012385, SIP Lines MADN Support
- A00012402, 911 Hold/Ringback Support on SIP Lines

The following feature has been deferred to a later release, so it has been removed from this version of the document: A00012893, BCP 7200 VLAN Tagging.

January 2006

Standard release 01.03 of this document for (I)SN09FF. The following features not previously identified as OSS-impacting have been added since the last Preliminary release:

- A00009026, RMGC Security
- A00010880, ABI SMU Support
- A00012183, Public Key Manager
- A00012215, Global Line Card Field Programmable Gate Array download
- A00012242, TME-CD with GSM Wireless Client, Ph-1
- A00012349, U3WC Support for SIP Lines
- A00012385, SIP Lines MADN Support
- A00012478, Compact Call Agent: Geo Support for GigE
- A00012570, Disabling Non-Secure Network Services in SSPFS
- A00012735, Session Server Fault Handling Enhancements
- A00012843, IEMS support for MDM security Interface changes
- A00012905, ERS8600 Alarm Mapping Correction in IEMS
- A00014049, GWC and SESM support of AAL2-G726-32 codec in IP network

The following feature has been deferred to a later release, so it has been removed from this version of the document: A00012893, BCP 7200 VLAN Tagging.

Note: Publication History for International features appears at the start of Chapter 4.

November 2005

Preliminary release 01.02 of this document for (I)SN09FF. The following updates have been made:

- Chapter 2, IEMS Functionality, of the document is updated to provide more accurate examples of logs in SNMP format.
- A00013063 is updated to reflect actual functionality.

November 2005

Preliminary release 01.01 of this document for (I)SN09FF. The document covers ATM solutions, IP solutions (Chapters 1-3), and International features (Chapter 4). The following sections are updated for this release:

- Mapping tables (ACTID-to-solutions; ACTID-to-OAM&P impacts). Two new reference lists have been added:
 - Features for IP solutions
 - Features for ATM solutions
- New or changed per release for both IP and ATM features
- IEMS Functionality for (I)SN09FF
- Feature descriptions by product/network element for both IP and ATM features
- International Features information, including the following:
 - Mapping tables (ACTID-to-solutions; ACTID-to-OAM&P impacts). A new reference list has been added: International Features List, which shows both International-only features as well as features that apply to the International and North American markets
 - New and changed for ISN09FF
 - ISN09FF Feature descriptions for CS2K International and World Trade
- Baseline information for Logs/Faults
- Baseline information for OMs/PMs
- Appendices of OMs/PMs and Logs/Faults

Table of Contents

Introduction and Mapping Tables	11
ISN09FF Activity mapping tables	12
Activity Mapping Table: Solutions Affected	13
Activity Mapping Table: Software object types or areas impacted	15
IP and ATM Features Lists	16

Chapter 1: New and Changed per Release	22
Logs/faults changes overview	22
Data Schema/MIBs changes overview	37
Commands and User Interface changes overview	40
Servord changes overview	50
Office Parameter changes overview	51
OM/PM changes overview	52
AMA/Billing changes overview	55
Software Optionality Control (SOC) changes overview	56

Chapter 2: IEEMS Functionality	57
IEEMS Northbound Interfaces	57
IEEMS Supported Devices	132
Call Agent Core	134
Call Agent Platform	138
Core Element Manager (CEM)	140
Centrex IP Call Manager (CICM)	147
Ethernet Routing Switch 8600 (formerly Passport 8600)	153
Gateway Controller (GWC)	190
Media Gateway 9000 (MG9000)	225
MultiService Switch 7400, 15000, 20000	296
MS2000 Series Node	303
Session Server Manager	313
SAM21 Shelf Controller	330
Storage Manager (STORM)	334
Universal Audio Server (UAS)	359
Universal Signaling Point (USP)	371
XACore	628
Platforms	632
Core Manager Platform	632
Succession Server Platform Foundation Software (SSPFS)	635
Element Managers	646
CS2000 Core Manager	646
Centrex IP Call Manager (CICM Manager)	649
GWC Manager	658

Integrated Element Management System (IEMS)	661
MG9000 Manager	686
Multi-Service Data Manager (MDM)	690
SAM21 Element Manager	704
Applications	708
Audio Provisioning Server (APS)	708
Line Maintenance Manager (LMM)	714
Network Patch Manager (NPM)	714
OSSGate	716
QoS Collector Application (QCA)	717
Trunk Maintenance Manager (TMM)	721
Non-Topology Elements	722
Data Audit System	722
IW-SPM IP	724
MG9000 Manager Mid-Tier	727
OM Collector	729
V5.2 Data Audit	731
References	735
IEMS Appendix 1: Northbound OSS Configurations	737
IEMS Appendix 2: Nortel Alarm Extension MIB	739
Chapter 3: (I)SN09FF Features	759
Product = CS 2000	759
A00009026--RMGC Security	759
A00010880--ABI SMU Support	762
A00012109--Session Server Shared Library Replacement (SLR) Patching	766
A00012349 -- U3WC Support for SIP Lines	777
A00012478--Compact Call Agent: Geo Support for GigE	780
A00012526--TDM Call Recording Feature	800
A00012527--Provisioning of CS2K trunks on GW and Carrier basis	821
A00012569--NI2 PRI/ ISUP UII over SCAI	836
A00012570-- Disabling Non-secure Network Services in SSPFS	865
A00012735 -- Session Server Fault Handling Enhancements	871
A00012889 -- Passphrase Protected Keys for SSH	885
CR Q01333369 -- Triggering gateway capabilities audit while changing T.38 network option on CS2K with TGCP gateways	906
Product = CS2K Management Tools	907
A00009576--RASless Provisioning	907
A00010742--GWC EM Enhancements to support SIREN	927
A00011827--GWC Autonomous SWACT	935
A00012183--Public Key Manager	965
A00012223, A00012217, A00012225--SESM Support for SIP Lines, Part 2	1103
A00012310--Hunt, SCMP, and CWT variant support for SIP Lines	1157
A00012974--Correct Execdata mismatch between GWC EM and Core	1161

A00014049--GWC and SESM support for AAL2-G726-32 codec in IP Network . .	1165
Product = IEMS	1167
A00011281--MS2000 IPSec Configuration Via IEMS	1167
A00012001--IEMS Call Server 2000 SIP Integration	1175
A00012843--IEMS Support for MDM Security Interface Changes.	1203
A00012905--ERS8600 Alarm Mapping Correction in IEMS	1207
A00013508--System Manager Auto-failover Support	1315
Product = MCS	1323
A00012242--TME-CD with GSM Wireless Client, Ph-1: "Mobility for Converged Desktop - MCD"	1323
A00012273--SIP Lines: Call Forwarding Indication	1395
A00012385--SIP Lines MADN Support	1398
A00012506--Border Control Point (BCP) Operational Measurement (OM) Enhancements	1410
A00012538, A00012537, A00012539--SIP Lines features	1425
A00012622--Platform HW Alarm Reporting	1432
A00013063 -- PacketCable Multimedia for MCS and Carrier Grade	1441
Product = MG 9000	1453
A00007814--REX testing for MG9000 from Element Manager	1453
A00012198--GLC12 Coin Card Support from EM	1473
A00012199--MG9K EM CPR Robustness	1482
A00012215--Global Line Card Field Programmable Gate Array download	1492
A00012386--Media Gateway 9000 Public Key Infrastructure	1503
Product = SIP Lines	1508
A00012326--SIP Lines: Authentication and Authorization account codes	1508
A00012402--911 Hold/Ringback support on SIP Lines.	1513
A00012403--Data Protection for SIP Lines	1524
Chapter 4: International-only features	1533
ISN09FF Activity mapping tables	1536
Activity Mapping Table: Solutions Affected	1537
Activity Mapping Table: Software object types or areas impacted	1537
International Features List	1538
New and Changed for ISN09FF	1539
Office Parameter changes overview	1539
Logs/faults changes overview	1540
Operational Measurements/Performance Measurement changes overview	1540
Data Schema tables/MIBs changes overview	1541
User Interface (commands) changes overview.	1541
Service Order changes overview	1542
AMA/billing changes overview	1542
Software Optionality Control (SOC) changes overview	1542
ISN09FF Feature Descriptions	1543
Product = Call Server 2000	1543

A00009297 -- QoS Reporting: QoS Collector Application	1543
A00013275 -- SESM Flex Large Line GWC Profile Support - Phase 1	1615
A00013286 -- Core Flex Large Line GWC Profile - Phase 1	1645
Product = World Trade	1648
A00009037 -- Core Enhanced ESA for International MG9000	1648
Chapter 5: Logs/faults and OMs/PMs	1661
Logs/Faults information	1661
Audio Codes Media Server (AMS)--available logs/faults	1668
Audio Provisioning Server (APS)--available logs/faults	1668
Compact Call Agent (CCA)--available logs/faults	1668
CS2000--available logs/faults	1670
CS2000 Core Manager--available logs/faults	1698
ERS8600 (previously Passport 8600)--available traps/faults	1704
MCS Manager Logs/Faults	1711
MG9000--available logs/faults	1718
MG15000 (previously PVG) Logs/Faults	1733
Multiservice Data Manager logs/faults	1733
NPM--available logs/faults	1733
QCA Logs/Faults	1734
SAM21--available logs/faults	1735
SPM--available logs/faults	1741
Stormia (STM)-available logs/faults	1749
UAS--available logs/faults	1749
USP Logs/Faults	1759
Operational measurements/performance measurements	1760
OMs/PMs collection and delivery	1760
Available OMs/ PMs	1760
CS 2000 Core OMs/PMs	1760
Performance Measurements	1783
Audio codes Media Servers (AMS) Performance Measurements	1783
Ethernet Routing Switch 8600 (formerly Passport 8600) PMs	1789
GWC Performance Measurements	1790
IEMS Performance Measurements	1794
MCS, RTP Media Portal, and MAS Performance Measurements	1796
MG 3200 Performance Measurements	1798
MG 9000 Performance Measurements	1799
Media Gateway 15000 OMs/PMs and Passport 15000/Multiservice Switch OMs/PMs	1802
MS 2000 Series Node OMs/PMs	1803
Session Server Manager OMs/PMs	1804
SAM21 OMs/PMs	1804
STORM OMs/PMs	1804
UAS OMs/PMs	1804
USP OMs/PMs	1806

Appendices for Logs/Faults and OMs/PMs

Appendix A: Ethernet Routing Switch 8600 Performance Metrics

Appendix B: MG 9000 MIB OMs/PMs

Appendix C: MSS15000, MG15000, and MDM Alarm Log Summary

Appendix D: USP Operational Measurements

Appendix E: MG 9000 Report Alarms, Event Logs, Audit Logs

Appendix F: CICM Logs and Alarms

Appendix G: Ethernet Routing Switch 8600 Trap List

Appendix H: IEMS Fault Transparency with SDM/CBM

Appendix I: MCS Alarms and Logs

Appendix J: MCS Operational Measurements



About this document

When to use this document

This document supports the (I)SN09 release of Carrier VoIP Solutions. It provides (I)SN09 design documents that contain Operations Support Systems (OSS) information. It also provides information on what is new and changed in (I)SN09, 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 Carrier VoIP, 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 (I)SN09. **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 and Feature Lists
 - Mapping network elements to ACTIDs to solutions
 - Mapping network elements to ACTIDs to OAM&P documentation elements
 - Features for IP solutions
 - Features for ATM solutions
- New/changed information for (I)SN09
 - Logs and faults
 - Data Schema/MIBs
 - Commands/User Interface
 - Service Order
 - Office Parameters
 - Operational Measurements/Performance Measurements
 - AMA/Billing
 - Software Optionality Control (SOC)
- (I)SN09 features for IP and ATM solutions, organized by network element
- ISN09 International features information, including the following:
 - Mapping tables (ACTID-to-solutions; ACTID-to-OAM&P impacts). A new reference list has been added: International Features List, which shows both International-only features as well as features that apply to the International and North American markets.
 - New and changed for ISN09
 - ISN09 Feature descriptions for CS2K International and World Trade
- Baseline information
 - Logs/faults available, organized by network element
 - OMs/PMs available, organized by network element
- Appendix A: Ethernet Routing Switch 8600 Performance Metrics
- Appendix B: MG9000 MIB OMs/PMs
- Appendix C: Media Gateway 15000 and MDM Alarm Log Summary
- Appendix D: USP OMs/PMs
- Appendix E: MG9000 Alarms, Event Logs, Audit Logs

- Appendix F: CICM Logs and Alarms
- Appendix G: Ethernet Routing Switch 8600 Trap List
- Appendix H: IEMS Fault Transparency with SDM/CBM
- Appendix I: MCS Alarms and Logs
- Appendix J: MCS Operational Measurements

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 may refer to the following Nortel Networks publications:

- 297-8001-840, *NA DMS-100 Log Report Reference Manual*
- 297-2621-840, *DMS-250 Logs Reference Manual*
- NN10021-111, *cCS 2000 Product and Technology Fundamentals*
- NN10408-900, *ATM/IP Solution-level Fault Management*
- NN10409-500, *ATM/IP Solution-level Configuration Management*
- NN10401-700, *ATM/IP Solution-level Performance Management*
- NN10334-911, *IEMS Fault Management*
- NN10330-511, *IEMS Configuration Management*
- NN10327-711, *IEMS Performance Management*
- NN10324-509, *Carrier Voice over IP Operational Configuration: Data Schema Reference*
- NN10264-709, *Carrier VoIP Performance Management Operational Measurements Reference*
- NN10025-111, *SAM21 Product and Technology Fundamentals*
- NN10089-911, *SAM21 Fault Management*
- NN10111-511, *SAM21 Configuration Management*
- NN10155-711, *SAM21 Performance Management*
- NN10083-911, *CS 2000 Fault Management*
- NN10188-511, *CS 2000 Configuration Management*
- NN10149-711, *CS 2000 Performance Management*
- NN10275-909, *Carrier Voice over IP Fault Management: Logs Reference*
- NN10090-911, *GWC Fault Management*
- NN10012-111, *SPM Product and Technology Fundamentals*
- NN10075-911, *SPM Fault Management*
- NN10097-511, *SPM Configuration Management*
- NN10141-711, *SPM Performance Management*
- NN10079-911, *DPT-SPM (IP) Fault Management*
- NN10078-911, *IW-SPM (IP) Fault Management*
- NN10073-911, *UAS Fault Management*

- NN10139-711, *UAS Performance Management*
- NN10085-911, *cCS 2000 Fault Management*
- NN10082-911, *CS 2000 Core Manager Fault Management*
- NN10104-511, *CS 2000 Core Manager Configuration Management*
- NN10148-711, *CS 2000 Core Manager Performance 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*
- NN10088-911, *STORM Fault Management*
- NN10110-511, *STORM Configuration Management*
- NN10154-711, *STORM PerformanceManagement*
- NN10074-911, *MG 9000 Fault Management*
- NN10096-511, *MG 9000 Configuration Management*
- NN10140-711, *MG 9000 PerformanceManagement*
- NN10087-911, *Call Agent Fault Management*
- NN10109-511, *Call Agent ConfigurationManagement*
- NN10153-711, *Call Agent PerformanceManagement*
- NN10202-911, *Gateway Controller Fault Management*
- NN10205-511, *Gateway Controller ConfigurationManagement*
- NN10208-711, *Gateway Controller PerformanceManagement*
- NN10145-711, *DPT-SPM (IP) Performance*
- NN10144-711, *IW-SPM (IP) Performance*
- NN10071-911, *USP Fault Management*
- NN10137-711, *USP Performance Management*
- NN10351-911, *Core and Billing Manager 850 Fault Management*
- NN10361-711, *Core and Billing Manager 850 Performance Management*
- NN10076-911, *MG 4000 Fault Management*
- NN10142-711, *MG 4000 Performance Management*
- NN10080-911, *DPT SPM-ATM Fault Management*
- NN10146-711, *DPT SPM-ATM Performance Management*

- NN10077-911, *IW SPM-ATM Fault Management*
- NN10143-711, *IW SPM-ATM Performance Management*
- NN10328-911, *Media Server 2000 Series Fault Management*
- NN10331-711, *Media Server 2000 Performance Management*
- NN10438-911, *Policy Controller Fault Management*
- NN10439-711, *Policy Controller Performance Management*
- NN10332-911, *Session Server Fault Management*
- NN10342-711, *Session Server Performance Management*

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

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



Introduction and Mapping Tables

Overview

This document supports Nortel's Carrier VoIP Solutions ISN09FF release for North American and International markets. The features described in Chapter 4 apply to International solutions only. This document describes ISN09FF features that affect inputs to or outputs from the solutions. These changes, therefore, affect the use of the Operations Support System (OSS) for ISN09FF. The document includes copies of feature descriptions used in software design.

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 ISN09FF. DO NOT use this document to make changes to existing software.

How the North American section is organized

This portion of the document is divided into the following areas:

- *North American activities mapping tables.* These tables relate the activity identifier associated with each feature to:
 - the product/application/network element affected
 - affected software object types (data schema, for example)
- *North American features lists by solution type.* This part has two lists:
 - Features for IP solutions. This list includes all IP-solutions-related features. Features associated with the following solutions may be found here: PT-IP, UA-IP, IAC, IAW, CHS, MCS, and DMS. It also identifies features associated with the PT-AAL2 solution. (The main difference between IP solutions and the ATM AAL2 solution is that the Media Gateways are setup to transport the bearer path using ATM AAL2 instead of IP.)
 - Features for ATM solutions. This list includes all ATM-solutions-related features. Features associated with the following solutions may be found here: PT-AAL1, UA-AAL1.

- *Chapter 1, New and changed for (I)SN09 (North American).* This section provides a table for each software object type, as follows:
 - Logs and alarms
 - Data Schema tables or MIBs
 - User Interface (commands)
 - Service Orders (Servord+)
 - Office parameters
 - Operational and Performance Measurements (OMs and PMs)
 - AMA/billing
 - Software Optionality Control (SOC)

Each table gives a summary of the changes caused per feature. Within each table, features are arranged by product/application, network element and then in numeric order by the ACTID of the feature which creates new information or causes the change.

- *Chapter 2, IEMS Functionality for (I)SN09.* This chapter provides information on fault management and performance management for all network elements regarding their interaction with IEMS.
- *Chapter 3, Feature descriptions (North American and some International).* This section provides feature descriptions, based on design documents. These are organized by product/application/network element and then in numeric order by ACTID.

The features that apply to both North American and International markets are located in this chapter, while the International-only features are located in Chapter 4.

ISN09FF Activity mapping tables

Introduction

This document contains advance information about differences in operations, administration, maintenance, and provisioning (OAM&P) for (I)SN09. The purpose of this document is to provide early information about new, modified or deleted items related to OSS-impacting areas.

The table below shows the mapping from the activity identifier (ACTID) associated with each new feature to the following:

- the associated product, application, or network element

- the solution that the feature affects, of the following:
 - PT-IP
 - UA-IP
 - IAW
 - IAC
 - DMS
 - MCS
 - CHS
 - AAL2
 - UA-AAL1
 - PT-AAL1
- the software object type or area that the feature affects, of the following:
 - Logs/faults
 - Data schema tables/MIBs
 - Office parameters
 - Service orders (ServOrd)
 - User interface/human-machine interface
 - Operational and performance measurements (OMs/PMs)
 - Automatic Message Accounting (AMA)/billing
 - Software Optionality Control (SOC)

Activity Mapping Table: Solutions Affected

		(I)SN09FF Solutions											
PRODUCT or APPLICATION	ACTID	PT-IP	UA-IP	IAW	IAC	DMS	MCS	CHS	AAL2	UA-AAL1	PT-AAL1		
CS 2000	A00009026				X								
CS 2000	A00010880									X			
CS 2000	A00012109	X											
CS 2000	A00012349							X					
CS 2000	A00012478	X	X	X	X			X					
CS 2000	A00012526	X	X										

		(I)SN09FF Solutions											
PRODUCT or APPLICATION	ACTID	PT-IP	UA-IP	IAW	IAC	DMS	MCS	CHS	AAL2	UA-AAL1	PT-AAL1		
CS 2000	A00012527	X											
CS 2000	A00012569	X											
CS 2000	A00012570					X	X						
CS 2000	A00012735	X											
CS 2000	A00012889					X							
CS2K Mgmt. Tools	A00009576							X					
CS2K Mgmt. Tools	A00010742	X	X	X	X		X						
CS2K Mgmt. Tools	A00011827		X										
CS2K Mgmt. Tools	A00012183		X							X			
CS2K Mgmt. Tools	A0001223, 12217, 12225						X						
CS2K Mgmt. Tools	A00012310							X					
CS2K Mgmt. Tools	A00012974		X							X			
CS2K Mgmt. Tools	A00014049	X											
IEMS	A00011281		X										
IEMS	A00012001		X										
IEMS	A00012843		X										
IEMS	A00012905		X										
IEMS	A00013508		X										
MCS	A00012242						X						
MCS	A00012273							X					
MCS	A00012385						X						
MCS	A00012506						X						
MCS	A00012538, 12537, 12539						X						
MCS	A00012622						X						
MCS	A00013063				X								
MG 9000	A00007814							X					
MG 9000	A00012198		X							X			
MG 9000	A00012199		X							X			
MG 9000	A00012215		X							X			
MG 9000	A00012386		X										
SIP Lines	A00012326							X					
SIP Lines	A00012402							X					
SIP Lines	A00012403							X					

Activity Mapping Table: Software object types or areas impacted

(I)SN09FF Solutions		Documentation Elements							
PRODUCT	ACTID	Logs/Faults	Data Schema	Office Parms	Service Orders	Commands/User Interf/HMI	OMs/PMs	AMA/Billing	Optionality
CS 2000	A00009026					X			
CS 2000	A00010880		X						
CS 2000	A00012109						X		
CS 2000	A00012349						X	X	
CS 2000	A00012478	X				X			
CS 2000	A00012526	X	X						X
CS 2000	A00012527		X						
CS 2000	A00012569		X		X		X		X
CS 2000	A00012570					X			
CS 2000	A00012735	X							
CS 2000	A00012889					X			
CS2K Mgmt. Tools	A00009576		X			X			
CS2K Mgmt. Tools	A00010742					X			X
CS2K Mgmt. Tools	A00011827	X	X			X			
CS2K Mgmt. Tools	A00012183	X	X			X			
CS2K Mgmt. Tools	A0001223, 12217, 12225				X	X			
CS2K Mgmt. Tools	A00012310					X			
CS2K Mgmt. Tools	A00012974					X			
CS2K Mgmt. Tools	A00014049					X			
IEMS	A00011281					X			
IEMS	A00012001					X			
IEMS	A00012843					X			
IEMS	A00012905	X							
IEMS	A00013508	X							
MCS	A00012242						X		
MCS	A00012273				X				
MCS	A00012385				X				
MCS	A00012506						X		
MCS	A00012538, 12537, 12539					X			
MCS	A00012622	X							
MCS	A00013063					X			
MG 9000	A00007814	X	X			X			

(I)SN09FF Solutions		Documentation Elements							
PRODUCT	ACTID	Logs/Faults	Data Schema	Office Params	Service Orders	Commands/User Interf/HMI	OMS/PMs	AMA/Billing	Optionality
MG 9000	A00012198					X			
MG 9000	A00012199	X	X			X			
MG 9000	A00012215					X			
MG 9000	A00012386					X			
SIP Lines	A00012326	X							
SIP Lines	A00012402		X						
SIP Lines	A00012403	X							

IP and ATM Features Lists

Introduction

This section consists of two tables: Features for IP solution, and Features for ATM solutions. The first table shows all features in numeric order by ACTID that are applicable to the various VoIP solutions:

- PT-IP
- UA-IP
- IAW
- IAC
- DMS
- MCS
- CHS

Features for IP solutions

ACTID	Feature Title	IP Solution
A89007814	REX testing for MG9000 from Element Manager	CHS
A00009026	RMGC Security	IAC

ACTID	Feature Title	IP Solution
A00009576	RASless Provisioning	CHS
A00010742	GWC EM Enhancements to support SIREN	PT-IP, UA-IP, IAW, IAC, MCS
A00011281	MS2000 IPSec Configuration Via IEMS	UA-IP
A00011827	GWC Autonomous SWACT	UA-IP
A00012001	IEMS Call Server 2000 SIP Integration	UA-IP
A00012109	Session Server Shared Library Replacement (SLR) Patching	PT-IP
A00012183	Public Key Manager	UA-IP
A00012198	GLC12 Coin Card Support from EM	UA-IP
A00012199	MG9K EM CPR Robustness	UA-IP
A00012215	Global Line Card Field Programmable Gate Array download	UA-IP
A0001223, 12217, 12225	SESM Support for SIP Lines, Part 2	MCS
A00012242	TME-CD with GSM Wireless Client, Ph-1	MCS
A00012273	SIP Lines: Call Forwarding Indication	CHS
A00012310	Hunt, SCMP, and CWT variant support for SIP Lines	CHS
A00012326	SIP Lines: Authentication and Authorization Codes	CHS
A00012349	U3WC Support for SIP Lines	CHS
A00012385	SIP Lines MADN Support	CHS
A00012386	Media Gateway 9000 Public Key Infrastructure	UA-IP
A00012402	Hold/Ringback support on SIP Lines	CHS
A00012403	Data Protection for SIP Lines	CHS
A00012478	Compact Call Agent: Geo Support for GigE	PT-IP, UA-IP, IAW, IAC, CHS
A00012506	Border Control Point (BCP) Operational Measurement (OM) Enhancements	MCS
A00012526	TDM Call Recording Feature	PT-IP, UA-IP
A00012527	Provisioning of CS2K trunks on GW and Carrier basis	PT-IP

ACTID	Feature Title	IP Solution
A00012538, 12537, 12539	SIP Lines features	MCS
A00012569	NI2 PRI/ ISUP UUI over SCAI	PT-IP
A00012570	Disabling Non-Secure Network Services in SSPFS	DMS, MCS
A00012622	Platform HW Alarm Reporting	MCS
A00012735	Session Server Fault Handling Enhancements	PT-IP
A00012843	IEMS support for MDM security Interface changes	UA-IP
A00012889	Passphrase Protected Keys for SSH	DMS
A00012905	ERS8600 Alarm Mapping Correction in IEMS	UA-IP
A00012974	Correct Execdata mismatch between GWC EM and Core	UA-IP
A00013063	PacketCable Multimedia for MCS and Carrier Grade	IAC
A00013508	System Manager Auto-failover Support	UA-IP
A00014049	GWC and SESM support of AAL2-G726-32 in IP network	PT-IP

Features for ATM solutions

This table shows all features in numeric order by ACTID that are applicable to the various VoATM solutions:

- PT-AAL1
- UA-AAL1
- PT-AAL2

ACTID	Feature Title	ATM Solution
A00010880	ABI SMU Support	UA-AAL1
A00012183	Public Key Manager	PT-AAL1
A00012198	GLC12 Coin Card Support from EM	UA-AAL1
A00012199	MG9K EM CPR Robustness	PT-AAL1
A00012215	Global Line Card Field Programmable Gate Array download	UA-AAL1

ACTID	Feature Title	ATM Solution
A00012889	Passphrase Protected Keys for SSH	DMS
A00012974	Correct Execdata mismatch between GWC EM and Core	UA-AAL1



Chapter 1: New and changed

New or changed for (I)SN09FF

This section of the document contains tables which give an overview of the feature-based changes occurring in the (I)SN09FF release for the following categories:

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

Within each table, the changes are arranged by associated product, and then in numeric order by the ACTID of the feature which creates new information or causes the change.

Solutions Application

This OSS Guide includes both IP solutions and ATM solutions. The ATM AAL2 solution differs from IP solutions in that the ATM AAL2 solution has Media Gateways set up to transport the bearer path using ATM AAL2 instead of IP. The signaling functionality for both ATM AAL2 and IP solutions is the same.

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 (I)SN09FF. They also appear in the logs-by-product tables in the Baseline section of this document with descriptions/cause for generation. This section also offers general log changes. Additional information is available in the Feature Deltas section of this document.

Summary of new or changed Logs/Faults for (I)SN09FF

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
Product = CS 2000		
CCA logs (changed)	All CCA logs	Feature A00012478 (applies only to the CS2100 for the Enterprise market) for CCA logs and alarms renames all the appearances of "FC" to "SL."
SCAI log (new)	SCAI600	Feature A00012526 (PT-IP, UA-IP, Int'l UA-IP) creates new log SCAI600. When TDM Call Recording TRNKINFO criteria is met, if the trunk information is not accessible by SCAI, the new parameter, TRNKINFO, will not be sent and SCAI600 will be generated.
SCAI log (new)	SCAI304	Feature A00012569 (PT-IP, SE10) creates new log SCAI304. If the total size of the outgoing ICM message with UUI exceeds the maximum supported size of outgoing ICM message then the UUI IE is discarded and LOG SCAI 304 is generated.

Summary of new or changed Logs/Faults for (I)SN09FF

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
XTS logs (new)	XTS382	Feature A00012735 (PT-IP) creates the following alarms and logs:
	XTS383	XTS382 - When a sensor reports a failure condition, an XTS382 alarm is raised on the Alarms panel of the NCGL Session Server unit. An XTS382 log is generated.
	XTS682	XTS383 - When one or more sensors report failure conditions with either power supply module A or B, an XTS383 alarm is raised on the Alarms panel of the NCGL Session Server unit. An XTS383 log is generated.
	XTS683	- XTS682 - When XTS382 Chassis Sensor fault condition and alarm is cleared, an alarm trap and INFO log XTS682 are generated. - XTS683 - When XTS383 Minor/Major Power Supply Sensor Fault alarm condition clears, INFO alarm/log XTS683 is generated.
SDM log (new)	SDM666	Feature A00012889 (DMS) introduces INFO log SDM666, created if there is a failure to generate cryptographic keys for the user.
GWC log (new)	GWC321	CR Q01163024 creates new alarm log GWC321 to indicate that Auto-negotiation is disabled on the ethernet link for the GWC card.
GWC log (new)	GWC322	CR Q01210435 creates new log GWC322 to indicate that GWC's SNMP message rate exceeded the recommended maximum. A minor alarm is raised on crossing the Panic Levels and a warning alarm is raised on crossing the Warning Levels.
GWC log (new)	GWC603	CR Q01221814 creates new INFO log GWC603 to indicate that a netfail event occurred from the GW and was reported to the connection broker. The log shows on which GWC the problem occurred, the Gateway name, IP address of the GW, the Endpoint name, the terminal ID, and the reason for the netfail event.
GWC log (new)	GWC604	CR Q01221822 creates new INFO log GWC604 to indicate that a connection broker exception occurred from the GW and was reported. The log shows on which GWC the problem occurred, the Gateway name, IP address of the GW, the Endpoint name, the terminal ID, and the reason for the exception
Product = CSK Management Tools		

Summary of new or changed Logs/Faults for (I)SN09FF

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
GWC logs (new)	GWC318 GWC319 (corresponding clear log for these two is GWC 399)	Feature A00011827 (UA-IP) introduces two new logs and modifies another: - GWC318 is associated with a critical alarm which indicates an autonomous SWACT is initiated due to a loss of communication to all the associated media gateways. - GWC319 is associated with a critical alarm that indicates communication with the GWC's associated gateways is down.
PM log (changed)	PM181	Feature A00011827 (UA-IP) introduces two new logs and modifies another: PM181--this existing log is used to report a GWC SWACT has occurred. The Autonomous SWACT activity adds a new reason to the PM181 log to indicate the cause of the autonomous SWACT. In this case, the reason indicates that a SWACT has occurred due to loss of communication with all associated media gateways.
CMT alarms (new)	GWC communication loss with associated media gateway(s) Autonomous SWACT initiated	Feature A00011827 (UA-IP) introduces two new critical CMT alarms to identify the following: - GWC communication loss with associated media gateway(s), raised if communication to the GWC's associated gateways is lost. This alarm is cleared when communication is detected with at least one associated gateway. It is also cleared when the GWC is manually or automatically SWACT and is raised again on the newly active unit if communication is still lost with all the associated gateways. Associated with log GWC319. The corresponding clear log is GWC399. - Autonomous SWACT initiated, raised when an autonomous SWACT is initiated due to a loss of communication to all the associated media gateways. This alarm indicates that the system has taken action in an attempt to restore communication. This alarm remains active until manually cleared or gets automatically cleared when the GWC is SWACT back to the original active unit. Associated with log GWC318. The corresponding clear log is GWC399.

Summary of new or changed Logs/Faults for (I)SN09FF

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
GWC EM alarm (new)	Failure to retrieve the certificate	Feature A00012183 (UA-AAL1, UA-IP) creates GWC EM "failure to retrieve the certificate" Critical Alarm when GWCEM fails to retrieve the certificates from the PKBClient.
MGEM audit log (new)	MGEM715	Feature A00012183 (UA-AAL1, UA-IP) creates the MGEM715 audit log whenever a user initiates a certificate download request for the NE.
PKManager Security logs and alarms (new)	(Refer to next column)	Feature A00012183 (UA-AAL1, UA-IP) creates PKManager logs for the following events: • creation of a certificate request for export • reception of a certificate request from integrated client applications • successful creation of an X509 certificate • successful delivery of an X509 certificate • invalid and rejected certificate requests • revocation of certificates • X509 certificate replacement requests • certificates that fail validation • certificates approaching expiration in advance of expiration as configured in the system. • a final notice in advance of expiration as configured in the system • when new certificates have been sent from PKManager for replacement on the application client box • new certificates have been received and are ready to be replaced by the crafts person • PKM300 is a Major Alarm log that indicates failure to create an X509 certificate. PKM300 also functions as a clear log. • PKM301 is a Major Alarm log that indicates an attempt to deliver a certificate to an application for a device failed. PKM301 also functions as a clear log. • PKM302 is a Critical Alarm log that indicates an X509 certificate has expired. PKM302 also functions as a clear log. • PKM303 is a Major Alarm log that is the last forewarning of an impending certificate expiration. PKM303 also functions as a clear log.

Summary of new or changed Logs/Faults for (I)SN09FF

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
(continued) PKManager Security logs and alarms (new)	(Refer to next column)	(continued) Feature A00012183 (UA-AAL1, UA-IP) creates PKManager logs for the following events: - PKM304 is a Minor Alarm log that is the initial forewarning of an impending certificate expiration. PKM304 also functions as a clear log. - PKM305 is a Major Alarm log that indicates a certificate used for OAM&P functions has expired. PKM305 also functions as a clear log.
MG9K EM alarms (new)	IPSC307 IPSC308 IPSC309 IPSC310 IPSC311 IPSC312 IPSC313 IPSC314	Feature A00012183 (UA-AAL1, UA-IP) -- The following alarms are raised or cleared when the Mg9kEM receives the "nnIpsecCertifFault" trap from the gateway: - IPSC307 indicates certificate has expired - IPSC308 indicates certificate is about to expire in 4 days - IPSC309 indicates certificate has invalid from date - IPSC310 indicates certificate not installed - IPSC311 indicates remote certificate verification failed - IPS 312 indicates certificate is missing Subject Alt. Name - IPSC313 indicates certificate processing failed - IPSC314 is raised when the EM attempts but fails to deliver certificates to the gateway. This alarm is cleared when a subsequent delivery attempt succeeds.
GWC EM alarm (new)	CMT304	Feature A00012183 (UA-AAL1, UA-IP) creates this Critical alarm when the GWCEM fails to retrieve the certificates from the PKBClient.
Product = IEMS		
ERS8600 Faults (changed)	(Refer to the next column)	Feature A00012905 (UA-IP) corrects the mapping severity for certain ERS8600 traps. See the Logs/Faults chapter and Appendix G for corrections.

Summary of new or changed Logs/Faults for (I)SN09FF

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
ERS8600 Faults	(Refer to the next column)	The Fault Management section of feature A00012905 (UA-IP) describes ERS8600 faults. The following list gives a brief description: • PP310 rising alarm is triggered when the alarm value rises above the threshold value. A clear alarm is triggered when the alarm value falls below the threshold value. • PP311 falling alarm is generated when an alarm entry crosses its falling threshold. • PP313 signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered. • PP315 signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered. • PP317 means the SNMPv2 entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to transition into the down state. • PP318 signifies that the SNMPv2 entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links has transitioned out of the down state. • PP319 signifies an authenticationFailure on the device. • PP322 signifies that 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. • PP323 signifies that 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. • PP324 signifies that 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. • PP325 signifies that 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 up state.

Summary of new or changed Logs/Faults for (I)SN09FF

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
(continued) ERS8600 Faults	(Refer to the next column)	(continued) The Fault Management section of feature A00012905 (UA-IP) describes ERS8600 faults. The following list gives a brief description: • PP326 signifies that 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. • PP327 signifies that 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. • PP328 signifies that the SNMPv2 entity, acting in an agent role, has detected the chassis is over-heating. • PP329 signifies that the SNMPv2 entity, acting in an agent role, has detected that an error condition has occurred. • PP330 means the SNMPv2 entity, acting in an agent role, has detected an excessive number of link state transitions on the specified port. • PP331 signifies that the SNMPv2 entity, acting in an agent role, has received a PDU with an invalid source MAC address. • PP332 signifies that the SNMPv2 entity, acting in an agent role, has detected a change of status on a Sonet port. • PP333 signifies that 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. • PP334 signifies that the SNMPv2 entity, acting in an agent role, has detected that the Spanning Tree Protocol has gone due to a topology change event. • PP335 signifies that the SNMPv2 entity, acting in an agent role, has detected that the Spanning Tree Protocol has gone due to a topology change event. • PP336 signifies that the SNMPv2 entity, acting in an agent role, has detected that the rc2kAtmPvcOamVcStatus object for one of PVC is about to transition into different state, either from up to down or from down to up.

Summary of new or changed Logs/Faults for (I)SN09FF

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
(continued) ERS8600 Faults	(Refer to the next column)	(continued) The Fault Management section of feature A00012905 (UA-IP) describes ERS8600 faults. The following list gives a brief description: • PP337 signifies that the split MLT link is from down to up. • PP338 signifies that the split MLT link is from up to down. • PP339 signifies that the split SMLT link is up. • PP340 signifies that the split SMLT link is down. • PP341 signifies that the SNMPv2 entity, acting in an agent role, has detected that the one of the cli password is changed. • PP342 signifies that the SNMPv2 entity, acting in an agent role, has detected that the PCMCIA card is being removed. • PP343 signifies that the cpld timer fired. • PP344 signifies that the cpld is not up to date. • PP345 signifies that the lgap accounting time-out Log File reached the maximum. • PP346 signifies that the cp limit for the port is shutting down. • PP347 signifies that the SSH server is enabled. • PP348 signifies that the SSH server is disabled. • PP349 signifies that there is a SSH session login. • PP350 signifies that there is a SSH session logout. • PP351 signifies that an unauthorized access has occurred. • PP352 signifies the state of the HA-CPU. • PP353 signifies insufficient memory on CPU blade for proper operation. • PP354 signifies that the switch run time or boot configuration is being saved. • PP355 signifies that a loop has been detected on a port. The vlan on that port will be disabled.

Summary of new or changed Logs/Faults for (I)SN09FF

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
(continued) ERS8600 Faults	(Refer to the next column)	(continued) The Fault Management section of feature A00012905 (UA-IP) describes ERS8600 faults. The following list gives a brief description: • PP356 signifies that a state transition has occurred on a particular vrrp interface. • PP357 signifies that the SNMPv2 entity, acting in an agent role, has detected Em error. • PP358 signifies that there has been a change in the state of an OSPF virtual interface. • PP359 signifies that there has been a change in the state of a non-virtual OSPF neighbor. • PP360 signifies that there has been a change in the state of an OSPF virtual neighbor. • PP361 signifies that a packet has been received on a non-virtual interface from a router whose configuration parameters conflict with this router's configuration parameters. • PP362 signifies that a packet has been received on a virtual interface from a router whose configuration parameters conflict with this router's configuration parameters. • PP363 signifies that a packet has been received on a non-virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type. • PP364 signifies that a packet has been received on a virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type. • PP365 signifies that there has been a change in the state of a non-virtual OSPF interface. • PP366 signifies that 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. • PP367 signifies that 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. • PP368 is generated when the BGP FSM enters the ESTABLISHED state.

Summary of new or changed Logs/Faults for (I)SN09FF

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
(continued) ERS8600 Faults	(Refer to the next column)	(continued) The Fault Management section of feature A00012905 (UA-IP) describes ERS8600 faults. The following list gives a brief description: • PP369 is generated when the BGP FSM moves from a higher numbered state to a lower numbered state. • PP370 is generated when the operational state of the aggregator changes from down to up. • PP371 is generated when the operational state of the aggregator changes from up to down. • PP372 signifies that a new member has come on an interface. • PP373 signifies that a group member has been lost on an interface. • PP374 signifies that a new querier has come up on an interface. • PP375 signifies that the querier has changed. • PP376 signifies that there has been a change in the state of a DVMRP interface. • PP377 signifies that a new neighbor has come up on a DVMRP interface. • PP378 signifies that a new neighbor has gone down on a DVMRP interface. • PP379 signifies that the system has violated the user configured limit for total number of fdb-entries learned on that port. • PP380 whether or not the number of repetitions of the particular Log message has exceeded the particular frequency/count or not. • PP381 signifies that either the runtime config or the boot config has been saved on the switch. • PP382 signifies that the switch had sent a query to the DNS server or it had received a successful response from the DNS Server. • PP383 is generated when a probe failure is detected when the corresponding pingCtlTrapGeneration object is set to probeFailure(0) subject to the value of pingCtlTrapProbeFailureFilter.

Summary of new or changed Logs/Faults for (I)SN09FF

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
(continued) ERS8600 Faults	(Refer to the next column)	(continued) The Fault Management section of feature A00012905 (UA-IP) describes ERS8600 faults. The following list gives a brief description: • PP384 is generated when a ping test is determined to have failed when the corresponding pingCtlTrapGeneration object is set to testFailure(1). • PP385 is generated at the completion of a ping test when the corresponding pingCtlTrapGeneration object is set to testCompletion(4). • PP386 signifies that the path to a target has changed. • PP387 signifies that the system could not determine the path to a target. • PP388 signifies that the path to a target has just been determined. • PP389 signifies that the UDPEap session has ended. • PP390 signifies that the UDPEap session has started. • PP391 signifies that a duplicate IP address is detected on the subnet. • PP392 signifies that a loop has been detected on a port and the port is going to shut down.
EMJS log (new)	EMJS351	Feature A00013508 (UA-IP) creates EMJS351 in two possible instances: • the user configured in the indicated Job Instance does not have the privileges required to rename an OM file on the specified device. • the IEMS is not able to login to the System Manager with the configured Username and the password details. The same log is also used as a Clear when either problem is resolved.

Summary of new or changed Logs/Faults for (I)SN09FF

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
EMJS log (changed)	EMJS350	CR Q01282151 modifies this raise/clear log to make the structure and content of the Location & Component ID fields consistent. The raise indicates that the system is not able to establish the SFTP connection with the device <IP address>. The clear indicates that the system has successfully established the SFTP connection with the device <IP address >.
IEMS log (new)	IEMS616	CR Q01267955 creates new INFO log IEMS616 to indicate an SNMP protocol authentication failure with the MS2010/MS2020.
Product = MCS		

Summary of new or changed Logs/Faults for (I)SN09FF

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
Alarms and logs for hardware faults (new)	HWER701 HWER702	Feature A00012622 (PT-IP, IAC) provides the capability for the MCS System Manager to monitor HP CC3310 servers, IBM blade servers, and the IBM BladeCenter chassis for hardware faults. Alarms are generated for four kinds of hardware faults. A log is generated whenever an alarm is raised or cleared. • HWER 701 - Cooling Device Malfunction — For the BC-T platform, derived from the monitors.blowers table. The alarm is raised when one or more blowers have any state value other than “good”. The alarm severity is Critical if both blowers are faulty, otherwise the severity is Major. — For the Langley platform, derived from the tCoolingDevice and tOperationalState tables. The alarm is raised when one or more cooling devices have an operational state not equal to vEnabled. The alarm severity is Critical if any of the faulty cooling devices are unspared, otherwise the severity is Major. • HWER 702 - Power Supply Malfunction — For the BC-T platform, derived from the powerModuleHealthTable table. The alarm is raised when one or more power modules have a state not equal to “good”. The alarm severity is Critical if any of the faulty power modules are unspared, otherwise the severity is Major. — For the Langley platform, derived from the tPowerSupply and tOperationalState tables. The alarm is raised when one or more power supplies have an operational state not equal to vEnabled. The alarm severity is Critical if any of the faulty power supplies are unspared, otherwise the severity is Major.

Summary of new or changed Logs/Faults for (I)SN09FF

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
(continued) Alarms and logs for hardware faults (new)	(continued) HWER703 HWER704	(continued) Feature A00012622 (PT-IP, IAC) provides the capability for the MCS System Manager to monitor HP CC3310 servers, IBM blade servers, and the IBM BladeCenter chassis for hardware faults. Alarms are generated for four kinds of hardware faults. A log is generated whenever an alarm is raised or cleared. • HWER 703 - Temperature Threshold Exceeded — For the BC-T platform, derived from the bladeTemperaturesTable and bladeTemperatureThresholdsTable tables. The alarm is raised when one or more blade SensorNTemp probes report a value greater than the corresponding warning threshold. The sensor value table in the report text consists an inequality ("actual > expected" and the sensor name for each sensor out of spec. The alarm severity is Major. — For the Langley platform, derived from the tTemperatureProbe table. The alarm is raised when one or more temperature probes report that a55TemperatureStatus is any value other than vOk. The sensor value table in the report text consists of the a55TemperatureStatus and the a55TemperatureProbeDescription variables for each sensor out of spec. The alarm severity is Major. • HWER 704 - Processor Malfunction — For the BC-T platform: HWER 704 is not reported for BC-T. — For the Langley platform, derived from the tProcessor and tOperationalState tables. The alarm is raised when one or more processors have an operational state not equal to vEnabled. The alarm severity is Major.
Product = MG 9000		

Summary of new or changed Logs/Faults for (I)SN09FF

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
REX logs (new)	REX 600 REX 601 REX 602	Feature A00007814 (UA-AAL1, UA-IP) creates the following logs related to ITP, ITX and DCC cards: - REX 600 indicates the start or completion of REX on a card/card-pair. - REX 601 indicates the success or failure of REX on a card/card-pair. - REX 602 indicates that the REX for the card/card-pair under consideration has been skipped.
VMG log	VMG313 (new in SN09)	Feature A00008718 and CR Q01060433-03 (UA-AAL1, UA-IP) create this new Major alarm log which indicates an equipment malfunction due to a DSP resource overload. During the alarm state, new requests are diverted from the overloaded DSP to the other DSPs until the overloaded DSP recovers from the overload condition.
NE log (new)	NE606	Feature A00012199 (UA-AAL1, UA-IP) creates new log NE606, generated each time a user clicks on "Clear persist and discover" button in NE Discovery View.
Product = SIP Lines		
IBN log (changed)	IBN110	Feature A00012326 (CHS) modifies IBN110 by adding the following reasons: - AUTH_ACCT_ON_MULTIPLE_SESSIONS: It is generated when Multiple sessions are present while invoking the Acct/Auth codes flash entry feature. - BLV_IN_PROGRESS: It is generated if the invoker of ACCT/AUTH or the connected party is being verified by the Operator.
AUD log and TRMT log (changed)	AUD501 TRMT22	Feature A00012403 (CHS) modifies the following logs: - AUD501 is generated when there is a data dump for a local test desk (LTD) extension block. The log is encountered when performing a test against a line with NDC option. - TRMT22 is generated when Busy Verify fails because there is no double connection call. The log is encountered when performing a test against a line with NDC option.

Data Schema/MIBs changes overview

The following Data Schema tables or MIBs are new or changed for (I)SN09FF. More complete descriptions will appear in the Feature Deltas section of this document.

Summary of new/changed Data Schema/MIBs information for (I)SN09FF

Table or MIB name	New or changed	Description
Product = Call Server 2000		
LTCINV	Changed	Feature A00010880 (UA-AAL1) modifies the OPTATTR field so it is now valid to enter EXTDS512 as an value in the OPTATTR field for SMU XPM.
SCAISSRV	Changed	Feature A00012526 (PT-IP, UA-IP, Int'l UA-IP) modifies table SCAISSRV by adding new field TRKINFO under the function CALLOFFR for these categories: RESEVENT, CTXEVENT and ACDEVENT, also under the function CALLQUED for category ACDEVENT.
GATWYINV	Changed	Feature A00012527 (PT-IP, Int'l UA-IP) modifies the GTWYNAME field so it now supports PVG and GW profiles through changes to field GTWYPRFL.
GWEPCARR	New	Feature A00012527 (PT-IP, Int'l UA-IP) creates GWEPCARR to hold the mapping from GW and carrier number to the TID range used by trunks on the carrier. The key to table GWEPCARR is the GW type and number and the carrier number. The number of channels on a carrier is restricted to 24 for North America and 31 for International. The table will also hold the carrier name information. Only Add and Delete operations will be supported on table GWEPCARR.

Summary of new/changed Data Schema/MIBs information for (I)SN09FF

Table or MIB name	New or changed	Description
SCAISSRV	Changed	Feature A00012569 (PT-IP, SE10) modifies SCAISSRV to provide subscription to receive ICM messages with the new parameter. The changes in table SCAISSRV are made for the following SCAI messages: - DV_Call_Received_C - DV_Call_Queued_U - DV_Call_Offered_U - DV_Call_Released_U An optional parameter UUI is added to the existing parameters in the function CALLQUED, CALLOFFR, CALLRECD and CALLREL which are present in the following categories: CTXEVENT, RESEVENT, ROUTING and ACDEVENT messages in table SCAISSRV.
Product = CS2K Management Tools		
GWC-APP-DATA-MIB	New	Feature A00009576 (CHS) creates this MIB to convey optional application specific data to the GWC.
GWC Maintenance Controls MIB GWC.GWCMTCCONTROLS table	New	Feature A00011827 (UA-IP) introduces a new MIB and a new table: - GWC Maintenance Controls MIB contains timers and other maintenance-related controls that are provisioned in CMT and are needed in the GWC. - GWC.GWCMTCCONTROLS table contains timers and other maintenance-related controls that are provisioned in CMT.
ikepreferenceentry connectionpolicyentry certificatefileentry	Changed	Feature A00012183 (UA-AAL-1, UA-IP) modifies the following tables: - ikepreferenceentry stores the ike preference configuration by the customer. It removes the field "ikeprefauthmethod." - connectionpolicyentry stores the connection policy configuration by the customer. It removes the field "IPSECCONNIKEREMGWID" and "IPSECCONNIKEPREFLISTID." It adds new fields "IPSECCONNFLAGV1" (not currently used) and "IPSECCONNIKEAUTHMETHODIDV1." - certificatefileentry stores the certificates file data.

Summary of new/changed Data Schema/MIBs information for (I)SN09FF

Table or MIB name	New or changed	Description
MIB GWC-SPD-MIB: ikeAuthenticationTable ikeauthenticationentry certificateFileTableV1 privatekeyFileTableV1 privatekeyfileentry	New	Feature A00012183 (UA-AAL-1, UA-IP) creates the following new tables: - MIB GWC- SPD-MIB stores the certificates. - ikeAuthenticationTable to store the ike authentication method setting. - ikeauthenticationentry stores the ike authentication configuration by the customer. - certificateFileTableV1 stores the certificates. - privatekeyFileTableV1 stores the device private key. - privatekeyfileentry stores the private key file data.
Product = MG 9000		
REX_SCHEDULE	Changed	Feature A00007814 (UA-AAL1, UA-IP) creates table REX_SCHEDULE to store the schedule information for the NEs that have to execute REX.
NORTEL-UEMG-NODE-MIB	Changed	Feature A00012199 (UA-AAL1, UA-IP) modifies NORTEL-UEMG-NODE-MIB by adding two scalar MIB variables. One MIB variable will store slot 10 out of band IP and another MIB variable will store slot 11 out of band IP. One additional MIB will be introduced for clear persist and discover functionality.
Product = SIP Lines		
Table TRKGRP (changed)	IBN110	Feature A00012402 (CHS) modifies table TRKGRP to allow the ORIGHOLD subfield to be provisionable on the E911 incoming trunks to the E911 Tandem. Both MF and ISUP IT with the E911 Option trunks provide the support for Network Hold.

Commands and User Interface changes overview

The following Commands and/or User Interface are new or changed for (I)SN09FF. More complete descriptions appear in the Feature Deltas section of this document.

Affected Area	Command/User Interface Description
Product = CS 2000	
Provisioning RMGC	Feature A00009026 (IAC, Int'l IAC) describes provisioning of an RMGC as very similar to that of a CallP GWC in that Kerberos and Connection Policies must be created. The only change is when a connection policy is created there is a limitation for the IPSec SA lifetime. This value must be between an upper and lower limit (10 seconds to 20 seconds). Any other value will not be accepted.
CCA MTC	Feature A00012478 (applies only to the CS2100 for the Enterprise market) creates the following changes in CCA MTC: - The "FC" for the carrier sparing state is replaced by "SL." - There is a new query util "QuerySL" in CCAMTC slot 16 all mtc levels to query the type is sparing link.
SAM21EM GUI	Feature A00012478 (applies only to the CS2100 for the Enterprise market) creates a new tab window for the 905 card for the customer to choose which sparing link to use, "Fiber Channel" or "Gigbit Ethernet."
CktLoc Command (changed)	Feature A00012527 (PT-IP, Int'l UA-IP) modifies the CktLoc command to support GWC trunks to allow display of carrier information for the trunk member currently being posted.
SSPFS cli configuration tool (changed)	Feature A00012570 (DMS, MCS) introduces new sub-menu items into the " Security Services Configuration " layer within the configuration panel for SSPFS cli configuration tool. Refer to the Configuration section of this feature for additional details.
SBA User Interface (changed)	Feature A00012889 (DMS) enhances the existing secure outbound file transfer functionality by introducing the key-based (public key) authentication. The key-based authentication mechanism is provided as an additional option for the user. Hence, the user can select to use either the password-based or the key-based authentication while adding and changing the secure file transfer schedules in the SBA (billmtc) or OMDD (omui) user interface programs.
SDM OM User Interface (changed)	Feature A00012889 (DMS) modifies the Add, List and Modify File Transfer Destination menus of OMUI. The "Add File Transfer Destination" menu 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.
Activating T.38 on BTX-4K	CR Q01333369 provides the steps for activating and deactivating T.38 on a BTX-4K controlled by a CS2K.

Affected Area	Command/User Interface Description
Product = CS2K Management Tools	
CS2K Management Tools GUI (changed)	Feature A00009576 (CHS) updates the associate gateway operation with the ability to configure the optional RAS-less capability. The RASLess option is displayed as part of the GWC Provisioning Panel of the CMT (CS2K Management Tools) GUI. The “Details” button of the Gateway tab has been updated to display the RASLess option configuration setting. A new optional gateway data application panel has been added to the associate gateway dialog box. The optional “RAS-less” data is presented as part of the new optional gateway data choices.
assocMG and queryMG of OSSGate XML interface (changed)	Feature A00009576 (CHS) modifies the assocMG and queryMG operations of the OSSGate interface to support the optional RAS-less configuration data. The optional RAS-less data is only applicable to H.323 gateways/gatekeepers.
GWC EM GUI (changed) and OSSGate XML schema (changed)	Feature A00010742 (PT-IP, UA-IP, IAW, IAC, MCS, Int'l IAW, Int'l IAC, Int'l PT-IP, Int'l UA-IP) creates the following interface changes in the GWC EM GUI: • In Siren configuration, the ability to bring up the SAM21 card view of the GWC card is removed, and the warm and cold swact buttons are replaced with a single ‘swact’ button. There is no change for Carrier VoIP installations. • In both Siren and Succession configurations, the ‘Add GWC’ dialog box will now prompt only for GWC name and not the IP address. The IP addresses will be determined internally by the hardware management software. The GWC names are listed in a pulldown menu for selection. This list contains GWCs that are provisioned in the hardware manager (SAM21EM for Succession, CLI on Typhoon for Siren), but not yet provisioned in the EM. • In OSSGate, the add GWC (addGWCtoCS) operation, the GWC IP address will now be looked up using the GWC name (gwcUIName). Therefore, the active IP address (gwcActvIp) is no longer required by the EM software and is being made optional. Note that this parameter may still be specified, but it will be ignored.

Affected Area	Command/User Interface Description
Change GWC Auto Swact Dialog (new) Controller Panel (changed)	Feature A00011827 (UA-IP) creates one new GUI and modifies another: - Change GWC Auto Swact Dialog contains a check box for enabling the control and a timer where the user can enter an integer between 0 and 300 seconds. The timer cannot be filled in if GWC Autonomous SWACT is not enabled. This dialog appears whenever the GWC Autonomous SWACT button is selected on the Controller Panel. The current status of the control and timer for the selected GWC is displayed. - Controller Panel GUI is modified to also contain GWC Autonomous SWACT information, as well as an additional Change button to change the state of the control and/or timer and to make a request to the GWC to do a clear of the Swact Alarm.
MG9K GUI (changed)	Feature A00012183 (UA-AAL-1, UA-IP) modifies the following GUIs: - LCI IPsec Control GUI allows the user to select authentication type of pre-shared key or Digital Certificate on the DCC card of the MG9K. - LCI OAMP Control GUI allows the user to configure a preshared encryption key used to encrypt/decrypt sensitive data transferred between the MG9K and its element manager.
MG9K EM GUIs (changed)	Feature A00012183 (UA-AAL-1, UA-IP) modifies the following GUIs: - MG9000 Provisioning View is updated to include a new "Download Digital Certificates" option. Using this option, during the initial NE commissioning, the user can download the certificates that the gateway needs to secure the OAMP channel. - NE Properties View is updated to include a new "Download Certificates" button. The user can use this view to download the certificates that the gateway needs to secure the OAMP channel. Four additional display fields are added to Properties View: — Gateway Authentication Method — Managing Gateway Certificate — Last Pushed Certificate — Last Pulled Certificate - GW Security Config panel is updated to include a new "Security Infrastructure" selector where the user can specify whether the VMG intends to use certificate or preshared key for securing its callp link. It also contains a new option to allow the user to explicitly trigger a certificate download request. This panel will become a required step during VMG provisioning.

Affected Area	Command/User Interface Description
PKManager Web Application GUIs (new)	Feature A00012183 (UA-AAL1, UA-IP) provides the following set of user screens for certificate administration and management tasks: • PK Manager Home • Broker Configuration Menu • Import/Export Menu allows the user to manually import/export certificates for expiration monitoring for a supported device. Certificates to be imported for integrated devices must be matched with a corresponding CSR from the database. • Revoke Certificate Menu • Browser menu (read-only) • Modify Broker Defaults is accessed from the Broker Configuration link in the menu panel on the left side of the Home page. This menu will be displayed as the top-level or entry screen to the application. This screen is intended for use during initial setup of the PKBroker application on SSPFS and allows the user to set default values for PKBroker parameters used throughout the PKGUI implementation. • Configure Entity Defaults allows the user to change the default Distinguished Name components used by the PKManager to generate certificates and requests. This screen is intended for use during initial setup of the PKBroker application on SSPFS and allows the user to set default values for Distinguished Name parameters used for certificate management and generation. • Generate CSR for Export allows the user to generate a certificate request for submission to an external certificate authority. • Import Certificate allows the user to manually import certificates for expiration monitoring for a supported device. Most fields on this screen are common for both integrated and non-integrated devices. • Create Integrated/Non-Integrated Certificate for Export allows the user to generate a private key and certificate for use with a supported device. The operation integration "type" will be determined by the EntityType selected by the user and set appropriately in the PKBRequest object passed to the server. • Inherit Certificate is used to manually import a WebPKProxy certificate generated by a commercial or external certificate authority. By doing so the certificate management and monitoring services of the PKManager are obtained. This enables a purchased and the valid certificate to continue to be used.

Affected Area	Command/User Interface Description
(continued) PKManager Web Application GUIs (new)	(continued) Feature A00012183 (UA-AAL1, UA-IP) provides the following set of user screens for certificate administration and management tasks: • Revoke Certificate allows the user to manually revoke any certificate that is monitored by the PKManager. Integrated device certificates that are revoked result in creation and delivery of replacement certificates to their original downstream clients. • Revoke CA Certificate is used to immediately revoke a CA certificate that is monitored by the PKManager. This operation should be used with extreme caution as it will cause the PKManager to initiate certificate replacements for ALL certificates generated and managed by the Certificate Manager. • View Certificates provides the user with the ability to browse certificates according to their entity type (device) hierarchy. The user has the ability to choose one or more entity types from which a database query will be launched to retrieve the associated data. • View Certificate Details displays a form containing a detailed listing of a specified certificate's fields. • View Alarms provides a summary listing of the current outstanding alarms generated by the PKManager. The alarm content will be displayed in the "body" portion of the standard screen layout. • View Alarm Details displays a form containing a detailed listing of a specified alarm's fields.
GWC EM GUIs (changed)	Feature A00012183 (UA-AAL-1, UA-IP) modifies the following GUIs: • IKE Preference Panel deletes the column "Authentication method." • Add/Change IKE Preference dialog deletes the parameter "Authentication method." • Connection Policy Panel deletes the columns "IKE remote gateway" and "IKE preference list" and adds new column "IKE Authentication." • Add/Change Connection Policy dialog removes the area "IKE Preshared Key Data" and adds a new drop down selector "IKE Authentication."

Affected Area	Command/User Interface Description
GWC EM GUIs (new)	Feature A00012183 (UA-AAL-1, UA-IP) creates the following new GUIs: • IKE Authentication panel displays the IKE authentication configuration data. It includes 4 columns, plus Add/Change/Delete buttons. • Add/Change IKE Authentication dialog shows the IKE authentication configuration parameter list and is used to configure these parameters. It has the following fields: — IKE remove gateway — IKE preference list cl — Authentication Method (1) — Authentication Method (2) • PKI certificate panel displays the entire chain (root, intermediate, device certs + private key) in a single row with one piece of info (maybe subject name) on each certificate. • IKE preference panel displays the entire chain with more information.
Server Security Manager Enhancements (new)	Feature A00012183 (UA-AAL-1, UA-IP) creates this web interface to define security parameters to secure communications into and out from the SSPFS Machine. This includes MG9000 Element Manager to MG9000 OAM&P communications. It has the following areas: • Two tables represent currently provisioned security parameters, one for IPSec parameters and one for IKE parameters. Add and delete options are available. • The IPSec Entries page allows retrieval and manipulation of IPSec policies for a host server. Once the policies are configured, all outbound and inbound datagrams are subject to policy checks as they exit and enter the host server. If no entry is found, no policy checks will be completed, and all the traffic will pass through. Depending upon the match of the policy entry, a specific action will be taken. • The IKE Entries page allows retrieval and manipulation of Internet Key Exchange policies for a host server. Once a policy is configured, the IKE daemon running on the host server discovers a remote host's public encryption key. The local system can then encrypt messages destined for the remote host whose public key it has discovered. • A new "Transforms" button on the IKE Entries page allows the craftperson to enter and view multiple transforms per IKE entry. • A new "Certificates" link is on the navigation bar on the left. This will access the SSPFS Machine's certificates, with options to request and delete certificates.

Affected Area	Command/User Interface Description
LMM CLUI (new)	Feature A00012225 (MCS) creates this CLUI to replace the LMM GUI and eventually the LTP (Lines Test Position) level of the MAPCI. For the introduction, this CLUI will allow the user to post Succession and non-Succession lines (TDM) and perform functions similar to that of the LTP level.
Line Data audit GUI (changed)	Feature A00012217 (MCS) makes the following changes: • The Line Audit will add auditing coverage of SIP line data on the SS-EM. The data to be audited on the SS-EM includes the Directory Number (DN), the termination name, the Virtual Media Gateway (VMG), and the HUNT/MADN group name information. • The audit GUI look and feel does not change, except that a few checks are added to warn the user of system load. Also the audit output file (both valid and problem files) will have extra information pertaining to the Session Server audit.
Hunt Groups for SIP Lines (changed)	Feature A00012310 (CHS) provides support for network based hunting, series completion and call waiting services for SIP user agents as part of the CS2K SIP Lines program.
GWC EM GUI (changed)	Feature A00012974 (UA-AAL1, UA-IP) modifies this GUI by adding a new function that allows customers to change the execdata of an existing GWC. If the execdata of a GWC is changed, then both the SESM database table and Core table will be updated. After successfully changing the execdata, BSY/RTS operations are needed to make the new configuration valid on the GWC pair.
SESM GUI (changed)	Feature A00014049 (PT-IP) modifies this GUI so that when provisioning a codec profile for an IP network, the codec list will include AAL2-G726-32. It replaces the existing iLBC codec.
Product = IEMS	
IEMS - MS2000 Node Configuration (changed)	Feature A00011281 (UA-IP) extends the existing GUI to include configuration of the IPSec and IKE parameters that are needed to allow for secure messaging between the IEMS and the MS2000 as well as between the MS2000 and the GWC.

Affected Area	Command/User Interface Description
MCS GUIs (changed)	Feature A00012001 (UA-IP) provides rebranding and proxying of the MCS GUIs through the IEMS. The functionality of handling faults and provisioning data remains unchanged. • When adding the SSLines device, an SSLines Mgr is added instead of an MCS Mgr or RTP Media Portal. • SStrunks is the SN10 rebranded name of the Session Server. • The Media Proxy NE type has been changed to Media Portal. • The launch of a command line has been modified in that it is now possible to launch a command line to any platform that is configured. • A user can now configure all the platforms associated with an MCS/SSLines deployment from the map reference of the SSLines EM. • From the EM or NE it is possible to launch the Provisioning client GUI.
Remove Radius Secret GUIs (changed)	Per feature A00012843 (UA-IP) MDM client is moving from a PAM Radius client to a PAM IS Client, so it will no longer require a Radius secret configuration in IEMS. This feature describes the following GUI changes: • Remove the Radius Secret field from the MDM Mgr Addition wizard when adding a new SN09 or later MDM Element Manager. • Disable the Update Radius Secret menu item from the MDM Element Manager's menu when it is a SN09 or later MDM Element Manager.
Product = MCS	
SIP Line Data audit OPI web service (changed)	Feature A00012538, 12537, 12539 (MCS) introduces new methods for auditing SIP lines provisioning data from the client: • <code>public int getUserCountInSubDomain(String subDomainName) throws ProvisionException.</code> The output is the number of users in the actual domain specified. • <code>public int getUserCountInDomain(String domainName) throws ProvisionException.</code> Returns user count in the domain tree starting with the specified domain.

Affected Area	Command/User Interface Description
SIPLines web service (new)	Feature A00012538, 12537, 12539 (MCS) introduces the new SIPLines web service which used these methods: • public String[] getDomainsForVMG(String vmgName) throws ProvisionException • public String[] getVMGForDomain(String subDomainName) throws ProvisionException • public SipLineAuditData[] getSIPLineAuditDataByDomain (String domainName, int start, int stop) throws ProvisionException. Returns the users available in the actual domain specified. • public SipLineAuditData[] getSIPLineAuditDataByDomainByVMG(String domainName, String vmgName, int start, int stop) throws ProvisionException. Returns the users available in the actual domain specified. • public String[] getUsersByRegistrationState(String domainName, boolean registered). Returns the usernames in the actual domain specified. • public String[] getUsersByRegistrationState(String domainName, boolean registrationState, String clientType). Returns the same list as in the previous method, except that it is also filtered by the client Type. The client type check is done against the provisioned data and has no bearing to what client actually registered.
VersionService web service (new)	Feature A00012538, 12537, 12539 (MCS) introduces the new web service "VersionService" to run on the SM and Prov Mgr. This service would be used by OPI and OMI clients to handle versions for maintenance releases. The Method: getLoadVersion() returns Version.
MCP System Management Console (changed)	Feature A00013063 (IAC) modifies this GUI to allow customers to configure the video codec Flow/Spec mappings through the "Network Data and Mtc" folder and through expanding the "Codec" folder. This GUI may also be used to delete a video codec or to modify a PCMM codec.
Product = MG 9000	
MG9KEM GUI (new GUI added)	Feature A00007814 (UA-AAL1, UA-IP) creates new GUI REX NE View introduced under the submenu option MG9KEM NE Specific Desktop view ->Configuration. This GUI allows the user to schedule REX and also view the progress details on the selected NE.
MG9KEM GUI (changed)	Feature A00007814 (UA-AAL1, UA-IP) modifies the NE Specific Desktop View GUI. The configuration submenu of this view contains a new menu item "REX NE" which enables the user to launch REX GUI. Also, a new tab is introduced on the left panel of NE Specific Desktop View to display the status of REX on the current NE.

Affected Area	Command/User Interface Description
GLC12 card replaces the SAA12 card (changed)	Feature A00012198 (UA-AAL1, UA-IP) describes the GUI interface of the new GLC12 card. When the user opens the GLC12 card view, the GLC12 card details will be displayed and with twelve port graphics for the GLCports (The GLC12 card has twelve ports). When the user double clicks on the port icon, the GLC circuit view will be displayed. The GLC12 circuit view will display circuit details. There are no new views added for this feature.
NE Discovery View (changed)	Feature A00012199 (UA-AAL1, UA-IP) modifies the NE Discovery View to show one more button for “Clear persist and discover” functionality. The following panels are added: • Subnet Configuration menu--LCI session will be invoked through a new submenu in configuration menu of subnet view. • Launch LCI View--After clicking on “Launch LCI Session”, a new view will be invoked for launching LCI. This view will give user option of connecting to LCI either inband or out of band.
NY53BA card replaces the POTS-32 and GLC-32 cards (changed)	Feature A00012215 (UA-AAL1, UA-IP) modifies the following GUIs to enable the NY53BA card: • GLC card View--the Actions Menu adds a new Software Download Manager menu selection for GLC cards. This brings up the existing software download GUI view. Also, new field FGPA Configuration Load displays the FPGA load on the GLC card. • GLC circuit diagnostic View--the Diagnostic Type field adds new subfield Controller Diagnostic to reveal if the controller for this line circuit and the other 3 line circuits on this controller needs to be reloaded and it reloads if appropriate. • Upgrade View from Frame View--clicking on Configure opens an upgrade wizard. The user selects complete upgrade, clicks Next, and Card Type Selection options appear. The user may choose GLC-32 BA Cards or GLC-12 CA Cards.
MG9K OAMP IPsec Provisioning	Feature A00012386 (UA-IP) modifies the Local Craft Interface (LCI) screens to allow the user to select the authentication method, the options being Pre-shared key and Digital certificate, when configuring IPsec on the DCC cards. A similar change was made to the MG9K EM VMG security view.

Servord changes overview

The following Service Order items are new or changed for (I)SN09FF. More complete descriptions appear in the Feature Deltas section of this document.

Area	New or changed	ServOrd Description
Product = CS2K Management Tools		
SIP_DATA option	New	Feature A00012223 (MCS) provides a richer set of SERVORD+ and query commands will be supported for SIP lines. Some of the newly supported commands will trigger flow through of new data to the Session Server Element Manager (SS-EM). The support of HUNT and MADN commands will entail new flow through logic for group information to the SS-EM. For SIP Line clients, the NEW, OUT and CHF commands are currently supported. A new suboption SIP_SUBDOMAIN for the SIP_DATA option is defined which can be used in NEW/CHF/EST/ADD commands applicable to SIP lines hosted off of Session ServerVMG.
Product = MCS		
Call Forwarding for SIP lines	Changed	A00012273 (CHS) provides the CS2K support for Call Forwarding Indicator and Call Forwarding Reminder for SIP agents that interface to the CS2K. Call Forwarding Indicator is provisioned using option CFIND. The SIP client provides a special dialtone (sometimes called "stuttered dialtone") to a subscriber who goes offhook when the subscriber has had call forwarding activated.
Product = SIP Lines		
Query commands for SIP lines	Changed	A00012385 (CHS) enables a specific set of SIP clients with IBN/RES network-based Multiple Appearance Directory Number (MADN) Single Call Arrangement (SCA) features. It includes the following query commands: • qdn <DN> • qlen <LEN> • qsip <DN,LEN>

Office Parameter changes overview

The following office parameters are new or changed for (I)SN09FF. More complete descriptions will appear in the Feature Deltas section of this document.

Summary of new/changed Office Parameters for (I)SN09FF

Status	Name	Description
Product = CS 2000		
	(None)	

OM/PM changes overview

The following OMs/PMs are new or changed for (I)SN09FF. 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 (I)SN09FF

OM Group or PM name	New or Changed	Description
Product = Call Server 2000		
NGSS SIPGW OM groups	Changed	Feature A00012109 (PT-IP) adds five spare registers to each of the NGSS SIPGW OM groups listed below: • SIPGW_CALLP • SIPGW_SERVICES • SIPGW_MISC • SIPGW_TLS • SIPGW_OVERLOAD • SIPGW_OOB • SIPGW_NCAS
U3WC OM group	(not pegged)	Feature A00012349 (CHS) explains why some OMs are not pegged. For DPL case, the conferencing service is provided by the UA or the CS2K SS and the conference notification from User Agent or CS2K SS is not available to the core. Hence for DPL, it is not possible to peg the U3WCCONF register. If the other two registers are pegged, it could lead to an imbalance over time. For this reason, none of the U3WC OM registers will be pegged for the DPL case.
Product = MCS		
CONVERGED DESKTOP3_SERVICE OM Group	New	Feature A00012242 (MCS) creates this new OM group with the following 12 registers: • CDC2C - Counts the number click-to-call originations that were placed from a MCD PC Client. • CDANSPAD - Counts the number call attempts that were answered on the CD Mobile (PAD). • CDANSPCC - Counts the number call attempts that were answered on the MCD PC Client. • CDCOG - Counts the number call-of-grace terminations that were attempted on a MCD PC Client. • CDPXYCALL - Counts the number call attempts that were proxied back to the CS2000.

Summary of new or changed OMs/PMs for (I)SN09FF

OM Group or PM name	New or Changed	Description
(continued) CONVERGED DESKTOP3_S ERVICE OM Group	(continued) New	(continued) Feature A00012242 (MCS) creates this new OM group with the following 12 registers: • CDCATTEXP - Counts the number of termination attempts presented to MCD PC Client, where the call attempt timer expired. • CDDECLINE - Counts the number of declined termination attempts that were presented to MCD PC Client. • CDIGNORE - Counts the number of ignored termination attempts presented to MCD PC Client. • CDHLDRT - Counts the number of hold/retrieve attempts managed by the CD3 service. • CDXFER - Counts the number of call transfers managed by the CD3 service. • CDCONF - Counts the number of conference calls managed by the CD3 service. • CDREG - Counts the number of register messages that are sent by the MCD PC Client during Login, updates, and Presence state changes.
Ports OM Group	New	Feature A00012506 (MCS) creates a new OM group due to the large number of registers already existing in the MPCP OM Group, and two existing registers ("rtpMpPortUsage" and "connMapEntries") are moved from MPCP to Ports. Four new registers are added to Ports: • sampledRtpMpPortUsage--Provides the summing of the in use ports every 100 seconds. • portUsageSampleCnt--The number of 100 second samples taken during this collection interval contributing to the averaged report. • connMapEntriesHWM--Highest number of simultaneous ports detected to be in use during this collection interval. • connMapEntriesLWM--Lowest number of simultaneous ports detected to be in use during this collection interval.

Summary of new or changed OMs/PMs for (I)SN09FF

OM Group or PM name	New or Changed	Description
Media Portal OM Group	Changed	Feature A00012506 (MCS) adds three new registers: - mediaPortalCount – the number of BCPs configured to support this Session Manager from the Management Console. This counter will be updated when BCPs are added or removed via the Management Console. - sesmSuccessCalls - the number of calls that were successfully setup using any available BCP on this Session Manager in the last collection period. - sesmFailedCalls - the number of failed attempts to setup a call on any available BCP on this Session Manager in the last collection period.
MediaPortalInstance	New	Feature A00012506 (MCS) creates a new OM group for registers that are per-BCP. For each BCP configured to support this Session Manager, an OM Row is created. It has the following registers: - sesmSuccessStreams - the number of stream setups that were successfully processed by this Media Portal Instance. - sesmFailedStreams - the number of stream setups that were not successfully processed by this Media Portal Instance. - rSipReceivedCount - the number of RSIP messages received from this Media Portal Instance. - createConnectionCount - the number of CRCX messages sent to this Media Portal Instance. - modifyConnectionCount - the number of MDCX messages sent to this Media Portal Instance. - deleteConnectionCount - the number of DLCX messages sent to this Media Portal Instance. - CRCXErrorCount - the number of CRCX error response messages received from this Media Portal Instance. - CRCXTimeOutCount - the number of CRCX time out (no response) from this Media Portal Instance. - MDCXErrorCount - the number of MDCX error response messages received from this Media Portal Instance. - MDCXTimeOutCount - the number of MDCX time out (no response) from this Media Portal Instance. - DLCXTimeOutCount - the number of MDCX time out (no response) from this Media Portal Instance.

Summary of new or changed OMs/PMs for (I)SN09FF

OM Group or PM name	New or Changed	Description

AMA/Billing changes overview

The following AMA/Billing information is new or changed for (I)SN09FF. 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		
DPL U3WC billing record	Changed	Per feature A00012349 (CHS), each time DPL U3WC is invoked, a billing record based on Structure Code 00001 with Call Type of 048 and Service Feature of 018 is created. For DPL, the conferencing is done at the client or on ad-hoc basis at the CS2K SS and hence no conference resources are used in the core. Also, the conference notification from User Agent is not being implemented as part of this activity. Therefore, the DPL U3WC billing record will be made always consistent with the TOTAL_DURATION setting of the U3WC_ELAPSED_TIME, irrespective of this parm being set to any other values. Also the billing record will be generated for every successful U3WC consult call termination, regardless of whether a conference is ever established. The module code 260 will be appended to the DPL U3WC billing records to indicate that they pertain to SIP lines, when the RECORD_MC260 tuple is set to ON in table AMAOPTS.

Software Optionality Control (SOC) changes overview

The following SOC information is new or changed for (I)SN09FF. More complete descriptions appear in the Feature Deltas section of this document.

Summary of new or changed SOC information for (I)SN09FF

SOC code	New or Changed	Description
Product = CS 2000		
ICM00085	New	Feature A00012526 (PT-IP, UA-IP, Int'l UA-IP) creates SOC option TDM Call Recording. With the SOC turned on, the new parameter added to indicate the trunk information will be sent in the two existing messages, dv_call_queued_U, and dv_call_offered_U, provided the new parameter is subscribed for these messages and the call is coming in from a trunk.
ICM00083	New	Feature A00012569 (PT-IP, SE10) creates this SOC option to control the UUI IE data delivery to SCAI. The UUI IE data is delivered to the SCAI host only if the SOC is turned on and the sub service supporting UUI is subscribed.



Chapter 2: IEMS Functionality

IEMS Northbound Interfaces

General Information

The IEMS provides a consolidated location to manage the Fault, Configuration, Performance Collection and Security account domains for devices (Network Elements, Element Managers, Management Applications and Platforms) in a CS 2000 central office. A brief description of its capabilities include the following:

- **Topology:** The IEMS provides a graphical representation of the managed devices in a central office. The IEMS client comes with default views (Network Elements, Element Managers, Applications and Platforms) of the managed network and provides flexible interfaces that allow a craftsperson to create customized views of the network. The alarm state of each of the managed devices in the IEMS topology is dynamically depicted by the associated background color (Red= Critical, Red=Major, Amber=Minor, Yellow=Warning, Green=Clear) of the managed device.
- **Fault:** The IEMS aggregates the event streams received from the various EMSs, NEs, applications, and platforms that it manages. It normalizes the events received from these streams and forwards the events over its northbound interfaces (such as SCC2, NTSTD, SNMP, and SYSLOG). The IEMS alarm and event browsers provide a consolidated real-time and historical view of the events that have occurred in a CS 2000 central office. It provides tools to view and page through the events and alarms in a common graphical interface. The Alarm and event browsers provide a wide range of features to manage, sort, filter and view events in a single centralized location. For detailed information on the IEMS fault management features please refer to the IEMS Fault Management document (NN10334-911).
- **Performance:** The IEMS provides a centralized location for collecting, storing and forwarding performance data in a CS 2000 central office. Its performance collection sub-system provides some basic tools for viewing and graphing the collected performance attributes. In addition, it does provide interfaces to configure the generation of threshold alarms for the

collected Operation Measurement data. For detailed information on the IEMS performance management features please refer to the IEMS Performance Management document (NN10327-711).

- **Configuration:** The IEMS provides a centralized location to launch the various Succession Configuration management interfaces. For detailed information on the IEMS configuration management features please refer to the IEMS Configuration Management document (NN10330-511).
- **Security:** The IEMS provides a centralized graphical interface to configure and manage the user accounts in a Succession Central Office. The IEMS Security subsystem provides centralized authentication and authorization server for many of its managed devices. It also provides centralized security logging for successful and failed authentications. In addition it provides Single Sign-on support enabling a user to log in to the IEMS client once and access multiple Succession Management interfaces without requiring the user to re-enter a userid and password. For detailed information on the IEMS Security management features please refer to the IEMS Security and Administration document (NN10336-611).

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 SN09 Devices

	NB format -> Device/EM	Documentation Log Key	Document Reference
1	<i>“Audio Provisioning Server (APS)”</i>	Log name and number	NN10328-911 MS 2000 Series Fault Management

	NB format -> Device/EM	Documentation Log Key	Document Reference
2	“Call Agent Core”	Log name and number	see “Fault documentation for Call Agent Core:”
3	“Call Agent Platform”	Log name and number	NN10087-911 Call Agent Fault Management
4	CBM See “CS2000 Core Manager”	Log name and number	See “CS2000 Core Manager”
5	CEM	Log value from the CEM logs	NN10334-911 IEMS Fault Management
6	“Centrex IP Call Manager (CICM)”	Log name and number	NN10334-911 IEMS Fault Management
7	“CS2000 Core Manager”	Log name and number	NN10082-911 CS 2000 Core Manager Fault Management
8	“Gateway Controller (GWC)”	Log name and number	NN10202-911 GWC Fault Management
9	“GWC Manager”	Log name and number	PLN-i09-OSS (I)SN09 OSS Guide
10	Keymile UNEM and UMUX	Log name and number	Keymile UMUX User's Guide and Keymile UNEM User's Guide
11	“Media Application Server (MAS)”	Log name and number from the specific problem	NN10375-113 MAS Unified Communications Service Guide
12	“Multimedia Communication Server (MCS)”	Log name and number	NN10030-111 System Manager Basics
13	Media Gateway 3200 (MG 3200)	Log name and number	LTRT-72704: MG3200 H.248 User Manual
14	“Multi-Service Data Manager (MDM)”	faultCode (specificProblem)	241-6001-500, <i>MDM Alarms Reference</i> , and 241-6001-011, <i>MDM Fault Management Tools</i> .

	NB format -> Device/EM	Documentation Log Key	Document Reference
15	MDM for BSC see “Multi-Service Data Manager (MDM)”	faultCode (specificProblem)	see “ Multi-Service Data Manager (MDM) ”
16	MDM - carrier see “Multi-Service Data Manager (MDM)”	faultCode (specificProblem)	see “ Multi-Service Data Manager (MDM) ”
17	MDM Client-Server see “Multi-Service Data Manager (MDM)”	faultCode (specificProblem)	see “ Multi-Service Data Manager (MDM) ”
18	“MultiService Switch 7400, 15000, 20000”	Log name and number	NN10600-500 Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference NN10600-520 Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management MSS 15000, MG 15000 & MDM Fault Overview
19	“Media Gateway 9000 (MG9000)”	Log name and number	NN10074-911 MG9000 Fault Management
20	“MG9000 Manager”	Log name and number	NN10074-911 MG9000 Fault Management
21	“MS2000 Series Node”	Log name and number	NN10328-911 MS2000 Series Fault Management
22	“Network Patch Manager (NPM)”	Log name and number	N10408-900 ATM/IP Solution-level Fault Management
23	“Ethernet Routing Switch 8600 (formerly Passport 8600)”	Log name and number	241-6003-110 Passport 8600 Device Integration Cartridge User Guide
24	“QoS Collector Application (QCA)”	Log name and number	NN10083-911 Communication Server 2000 Fault Management

	NB format -> Device/EM	Documentation Log Key	Document Reference
25	<i>“SAM21 Element Manager”</i>	Log name and number	NN10089-911 SAM21 Shelf Controller Fault Management
26	<i>“SAM21 Shelf Controller”</i>	Log name and number	NN10089-911 SAM21 Shelf Controller Fault Management
27	<i>“Core Manager Platform”</i> <i>See “CS2000 Core Manager”</i>	Log name and number	NN10082-911 CS 2000 Core Manager Fault Management
28	<i>“Session Server Manager”</i>	Log name and number	NN10332-911 Session Server Fault Management
29	<i>“Succession Server Platform Foundation Software (SSPFS)”</i>	Log name and number	NN10408-900 ATM/IP Solution-level Fault Management
30	<i>“Storage Manager (STORM)”</i>	Log name and number	NN10088-911 Storm Fault Management
31	<i>“Universal Audio Server (UAS)”</i>	Log name and number	NN10275-909 v3 Succession Fault Management Logs Reference NN10073-911 UAS Fault Management
32	<i>“Universal Signaling Point (USP)”</i>	Specific Problem: Log Group=<text> & Log Number=<number> Note: Log GroupID is not used	NN10071-911 USP Fault Management
33	<i>“XACore”</i>	Log name and number	297-8991-510 XA-Core Maintenance Manual

IEMS Northbound Fault Specifications

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.

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	ASCII stream over TCP, push	OSS IP address or hostname
SCC2	8556	Incoming. IEMS waits for connection by remote host	ASCII 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.	SNMP trap events (UDP), push	IP address and port of listener on OSS

- 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'

Fld	Name	Description	Example
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'
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', 'PSY', '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...#cccdeeeefff\ggghh\ii:jj:kk\1111\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

Fld	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.	'SCP 2B'

Fld	Name	Description	Example
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.	' *'
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, (i.e. 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'

Fld	Name	Description	Example
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'
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	Equipment Identifier	A conditional equipment identifier determined by the application. It is a variable length character string.	'LIU7348'
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	~~ MGEM3 02 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, (i.e. 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'

Name	Description	Example
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'
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.	' 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'

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 72.

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. Note that some Solaris applications forward security logs to authlog (/varlog/authlog). Sample content of each follow:

Audit log sample (/var/log/auditlog):

```
Jan 16 10:37:55 sspfs_svr ID[SUNWcluster.pmf.1020]: "CorbaNotification" requeued
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]: "ompush" 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
```


Security log sample (/var/log/securitylog):

```
Dec 15 06:48:37 comp5iems su: 'su oracle' succeeded for root on /dev/???
Dec 15 06:48:56 comp5iems sshd[12755]: Accepted publickey for root from 192.168.47.2 port 64329
ssh2
Dec 15 08:42:36 comp5iems su[1200]: 'su root' failed for maint on /dev/pts/4
Dec 15 08:42:53 comp5iems su[2685]: 'su root' succeeded for maint on /dev/pts/4
```

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 /var/log/authlog/, auth (facility)	local3
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 an 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.

MIB Loading Sequence

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-CONF	(Not required by the IEMS server)
2	SNMPv2-SMI	/opt/nortel/iems/current/mibs
3	SNMPv2-TC	/opt/nortel/iems/current/mibs
4	SNMPv2-MIB	/opt/nortel/iems/current/mibs SNMPv2-MIB.txt
5	SNMP-FRAMEWORK-MIB	/opt/net-snmp/share/snmp/mibs/ SNMP-FRAMEWORK-MIB.txt
6	INET-ADDRESS-MIB	/opt/net-snmp/share/snmp/mibs/ INET-ADDRESS-MIB.txt
7	RFC1212	(Not required by the IEMS server)
8	RFC1155-SMI	/opt/nortel/iems/current/mibs
9	RFC1213-MIB	/opt/nortel/iems/current/mibs RFC1213-MIB.txt
10	RMON-MIB	/opt/nortel/iems/current/mibs/cicm RMON-MIB.txt
11	TOKEN-RING-RMON-MIB	/opt/nortel/iems/current/mibs/cicm TOKEN-RING-RMON-MIB.txt
12	RMON2-MIB	/opt/nortel/iems/current/mibs/cicm RMON2-MIB.txt
13	ALARM-MIB	/opt/nortel/iems/current/mibs/usp/ ALARM-MIB-disman-18.txt
14	IANA-ITU-ALARM-TC	/opt/nortel/iems/current/mibs/usp/ IANA-ITU-ALARM-TC-disman-18.txt

Load Order	MIB Name	IEMS Server File location
15	ITU-ALARM-TC	/opt/nortel/iems/current/mibs/usp/ ITU-ALARM-TC-disman-18.txt
16	ITU-ALARM-MIB	/opt/nortel/iems/current/mibs/usp/ ITU-ALARM-MIB-disman-18.txt
17	ITU-IANA-ALARM-TC	/opt/nortel/iems/current/mibs/usp/ ITU-IANA-ALARM-TC-disman- 04.txt
18	NOTIFICATION-LOG-MIB	/opt/nortel/iems/current/mibs/usp/ NOTIFICATION-LOG-MIB- rfc3014.txt
19	NORTEL-MIB	/opt/nortel/iems/current/mibs/usp/nort el.mib
20	NORTEL-GENERIC-MIB	/opt/nortel/iems/current/mibs/usp/ nortelGenericMIBs-smi2.mib
21	ENTITY-MIB	/opt/nortel/iems/current/mibs/usp/ ENTITY-MIB-entmib-03.txt
22	ENTITY-STATE-MIB	/opt/nortel/iems/current/mibs/usp/ ENTITY-STATE-MIB-entmib-01.txt
23	NORTEL-ALARM-EXT-MIB	/opt/nortel/iems/current/mibs/usp/ nortel_alarm_ext_smi.txt
24	NORTEL-NMI-MIB	/opt/nortel/iems/current/mibs/usp/ nortelNMI-smi2.smi
25	NORTEL-NMI-ALARM-CLEAR-MIB	/opt/nortel/iems/current/mibs/usp/ nortelNMIALarmClear_smi.txt

Support for the IETF Alarm MIB is new to IEMS. 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 “IEMS 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 IEMS.

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 IEMS. 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 79.

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 IEMS.

The instance array of the Table is created used a readable string format of the AlarmActiveDateAndTime index value, not the OCTET STRING representation of it.

Limitations

If the OSS requires the AlarmActiveTable to be traversed, the OSS should issue sequential SNMP GETNEXT requests starting from the first column till the response reaches the end of the Table. The OSS will not be able to retrieve the values by giving incomplete instance values to query this table. If one uses a incomplete instance value to query a column, the response value will have the first row of the next immediate column in the AlarmActiveTable which will not be expected by the OSS. For example, the OSS will not be able to query the Table such that it can retrieve the Active Alarm List after a particular date by giving the instance value accordingly.

Walking the AlarmActiveTable

To walk the alarmActiveTable, for example, an OSS can send a snmp getnext pdu with the individual column varbinds of interest (i.e.):

Getnext:

```
.iso.org.dod.internet.mgmt.mib-  
2.alarmMIB.alarmObjects.alarmActive.alarmActiveTable  
e.alarmActiveEntry.alarmActiveEngineID  
  
iso.org.dod.internet.mgmt.mib-  
2.alarmMIB.alarmObjects.alarmActive.alarmActiveTable  
e.alarmActiveEntry.alarmActiveEngineAddressType  
  
iso.org.dod.internet.mgmt.mib-  
2.alarmMIB.alarmObjects.alarmActive.alarmActiveTable  
e.alarmActiveEntry.alarmActiveEntry.alarmActiveEngineAddress  
  
..  
..  
  
iso.org.dod.internet.mgmt.mib-  
2.alarmMIB.alarmObjects.alarmActive.alarmActiveTable  
e.alarmActiveEntry.alarmActiveSpecificPointer
```

This would result in the IEMS agent returning the first instance of these columns in the alarmActiveTable. The returned instance values varbinds in turn can be used in the subsequent getnext messages from the manager to traverse the associated columns in this table. This can be used until the IEMS agent returns that last instance (i.e., last row) in the associated table.

This can be identified by parsing the OID in the response varbind, reaching the next column or the next group if that is the last column in the table.

Table walk Limitations:

Due to limitations with using a DateAndTime value octet string as a table index, the IEMS agent does not support the ability to use partial indexes to walk the alarmActiveTable. The alarmActiveTable, for example, has a 3-part

index (alarmListName, alarmActiveDateAndTime, and alarmActiveDateAndTime). Beyond the initial getnext to get the first instance (i.e., first row) in this table, all getnext requests must include all 3 index instances to lexicographically step through the columns in this table. For example, a user can **not** do the following to attempt to get the next alarmActiveEngineID instance that is lexicographically greater than the provided date.

Example (Wrong request)

Getnext:

```
alarmActiveEngineID.alarmListName.alarmActiveDateAndTime
```

Instead of returning the next alarmActiveEngineID, the IEMS northbound SNMP agent will return the first instance in the next column (In this example it would be the alarmActiveEngineAddressType).

Indexes into this table are: *alarmListName*, *alarmActiveDateAndTime*, *alarmActiveIndex*. AlarmListName matches the index nlmLogName for nlmLogTable 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

Sequence Field	Default Value
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.)

The instance array of the Table is created used a readable string format of the AlarmActiveDateAndTime index value, not the OCTET STRING representation of it.

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
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

Alarm Active Variable Entry	Notification Varbind	Default Value
alarmActiveVariableIndex 10	nnExtAlarmActiveResource Description	none
alarmActiveVariableIndex 11	nnExtAlarmActiveManualClear	none
alarmActiveVariableIndex 12	nnExtAlarmActiveSequence Number	none

ALARM CLEAR TABLE

Not supported.

Manual clears are performed with SNMP SET operations using the alarmActiveIndex of the alarm to be cleared. See section “Manual Clear” on page 95 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 IEMS 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 93 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 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 Probable Causes

Each alarm notification and record in the alarm table includes event type and probable cause. Values for these fields are defined 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), lowTemperatue (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), underlayingResourceUnavailable (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), ouputDeviceError (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
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
10.	Equipment Identifier	Location:	Location:	Location:	Not supported

Northbound Fault Format Summary

Row#	IEMS Schema	SYSLOG	NTSTD	SCC2	SNMP
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 Note: Specific Problem is now a part of the nnExtAlarmActiveAdditionalText VarBind.				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	The mmessage or the description of the event

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 84.
- 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 *nmlLogTable* and *nmlLogVariableTable* 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 84. 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

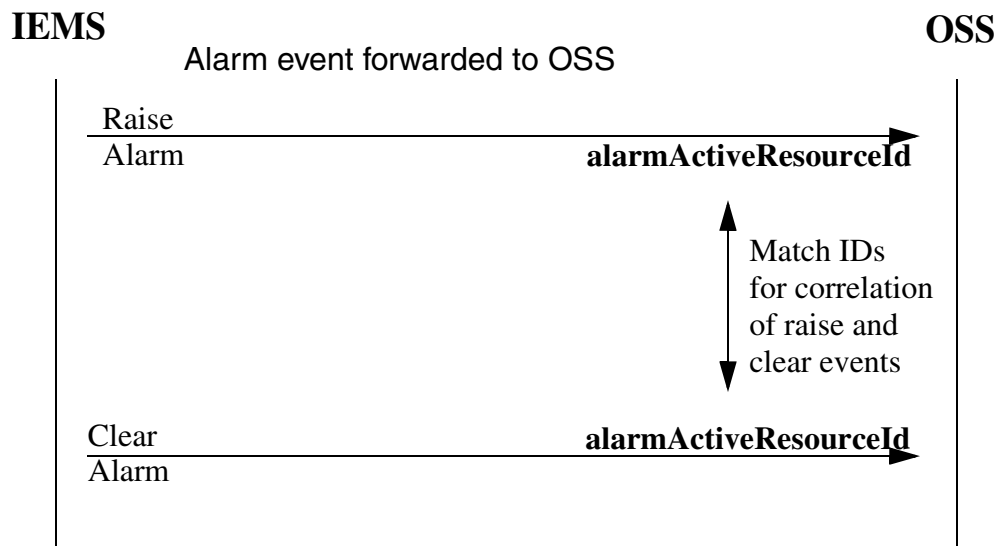
nnExtAlarmActiveTable

An entry is made in the log notification tables for the CLEAR event.

nlmLogTable

nlmLogVariableTable

Alarm Raise & Clear Correlation



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

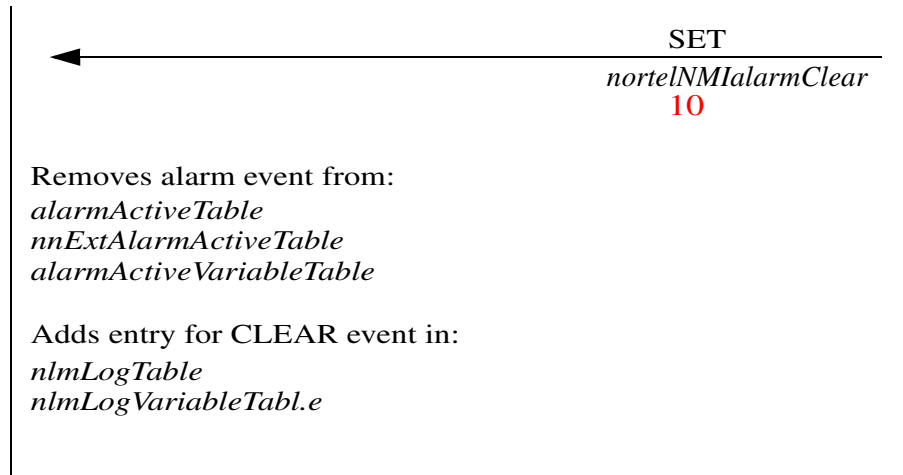
alarmActiveIndex:**10**

The resulting *alarmActiveResourceId* will be:

alarmActiveResourceId.**12.78.111.114.116.101.108.95.102.97.117.108.116.25.50.48.48.52.45.49.45.56.44.51.58.50.49.58.53.55.46.49.44.43.48.53.58.51.48.10**

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:

$$(\text{sysUpTime of current event}) < (\text{sysUpTime of previous event})$$

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 97](#) 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:

$$\begin{aligned}
 &(\text{sequence\# of latest event}) - (\text{sequence\# of missing event}) \\
 &\leq \text{nlmConfigGlobalEntryLimit (default = 25)}
 \end{aligned}$$

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 97.

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 *nImLogTable*. 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 97. 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
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 *nlmLogVariableTable* (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 *nlmStatsLogNotificationsLogged*. 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 (.1.3.6.1.4.1.562.29.6.1.0.302)

nnExtAlarmMinor (.1.3.6.1.4.1.562.29.6.1.0.303)

nnExtAlarmMajor (.1.3.6.1.4.1.562.29.6.1.0.304)

nnExtAlarmCritical (.1.3.6.1.4.1.562.29.6.1.0.305)

Table , “nlmLogVariableTable varbinds for recovery of lost CLEAR notification,” on page 101 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.

nlmLogVariableTable varbinds for recovery of lost RAISE notification

nlmLogVariableTable Index Variable	OID (<i>nlmLogName</i> = “Nortel_fault” (encoded) Sequence# = 1390 Index = 1 - 12)	Notification Varbind Represented
nlmLogVariableIndex 1	nlmLogVariableTimeTicksVal.12.78.111.114.116.101.108.95.102.97.117.108.116.1390.1	sysUpTime
nlmLogVariableIndex 2	nlmLogVariableOidVal.12.78.111.114.116.101.108.95.102.97.117.108.116.1390.2	snmpTrapOID
nlmLogVariableIndex 3	nlmLogVariableOctetStringVal.12.78.111.114.116.101.108.95.102.97.117.108.116.1390.3	alarmActiveResourceId

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 4	nImLogVariableOctetStringVal. 12.78.111.114.116.101.1 08.95.102.97.117.108.116.1 390.4	alarmActiveDescription
nImLogVariableIndex 5	nImLogVariableOctetStringVal. 12.78.111.114.116.101.1 08.95.102.97.117.108.116.1 390.5	alarmActiveDateAndTime
nImLogVariableIndex 6	nImLogVariableInteger32Val. 12.78.111.114.116.101.108 .95.102.97.117.108.116.139 0.6	ituAlarmEventType
nImLogVariableIndex 7	nImLogVariableInteger32Val. 12.78.111.114.116.101.108 .95.102.97.117.108.116.139 0.7	ituAlarmProbableCause
nImLogVariableIndex 8	nImLogVariableOctetStringVal. 12.78.111.114.116.101.1 08.95.102.97.117.108.116.1 390.8	ituAlarmAdditionalText
nImLogVariableIndex 9	nImLogVariableOctetStringVal. 12.78.111.114.116.101.1 08.95.102.97.117.108.116.1 390.9	nnItuAlarmActiveDocumentationPointer
nImLogVariableIndex 10	nImLogVariableOctetStringVal. 12.78.111.114.116.101.1 08.95.102.97.117.108.116.1 390.10	nnItuAlarmActiveResourceDescription
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

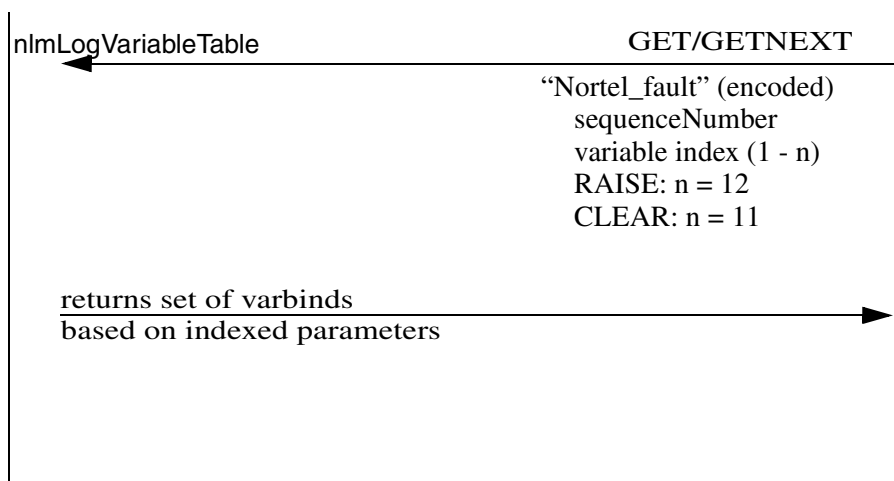
nImLogVariableTable Index Variable	OID (nImLogName = "Nortel_fault" (encoded) Sequence# = 1390 Index = 1 - 11)	Notification Varbind Represented
nImLogVariableIndex 1	nImLogVariableTimeTicksVal.12.78.111.114.116.101.1 08.95.102.97.117.108.116.1 390.1	sysUpTime
nImLogVariableIndex 2	nImLogVariableOidVal.12.7 8.111.114.116.101.108.95.1 02.97.117.108.116.1390.2	snmpTrapOID
nImLogVariableIndex 3	nImLogVariableOctetStringVal.12.78.111.114.116.101.1 08.95.102.97.117.108.116.1 390.3	alarmActiveResourceId
nImLogVariableIndex 4	nImLogVariableOctetStringVal.12.78.111.114.116.101.1 08.95.102.97.117.108.116.1 390.4	alarmActiveDescription
nImLogVariableIndex 5	nImLogVariableOctetStringVal.12.78.111.114.116.101.1 08.95.102.97.117.108.116.1 390.5	alarmActiveDateAndTime
nImLogVariableIndex 6	nImLogVariableInteger32Val .12.78.111.114.116.101.108 .95.102.97.117.108.116.139 0.6	ituAlarmEventType
nImLogVariableIndex 7	nImLogVariableInteger32Val .12.78.111.114.116.101.108 .95.102.97.117.108.116.139 0.7	ituAlarmProbableCause
nImLogVariableIndex 8	nImLogVariableOctetStringVal.12.78.111.114.116.101.1 08.95.102.97.117.108.116.1 390.8	ituAlarmAdditionalText
nImLogVariableIndex 9	nImLogVariableOctetStringVal.12.78.111.114.116.101.1 08.95.102.97.117.108.116.1 390.9	nnItuAlarmActiveDocumentationPointer
nImLogVariableIndex 10	nImLogVariableOctetStringVal.12.78.111.114.116.101.1 08.95.102.97.117.108.116.1 390.10	nnItuAlarmActiveResourceDescription

nImLogVariableTable Index Variable	OID (nImLogName = "Nortel_fault" (encoded) Sequence# = 1390 Index = 1 - 11)	Notification Varbind Represented
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 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 SN09 release, ERS8600, STORM, MS2000, Session Server-Trunks (platform PMs only), MAS, MCS, MCS Mgr, FPM, MG15000, SAM21, IEMS, UAS, GWC, USP, MG9K, and SSPFS.

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 XML Format

For examples of each of the supported PM files, refer to the section in this chapter entitled “IEMS Supported Devices” on page 132.

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

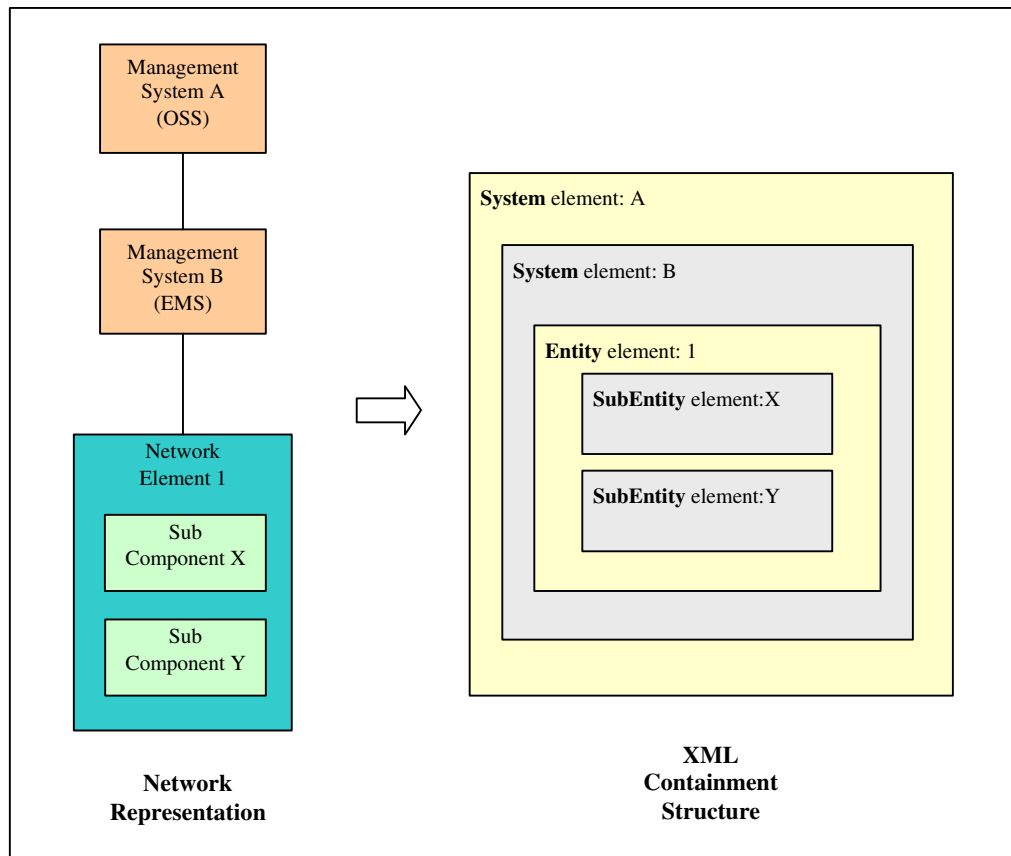
SubEntity element.

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.

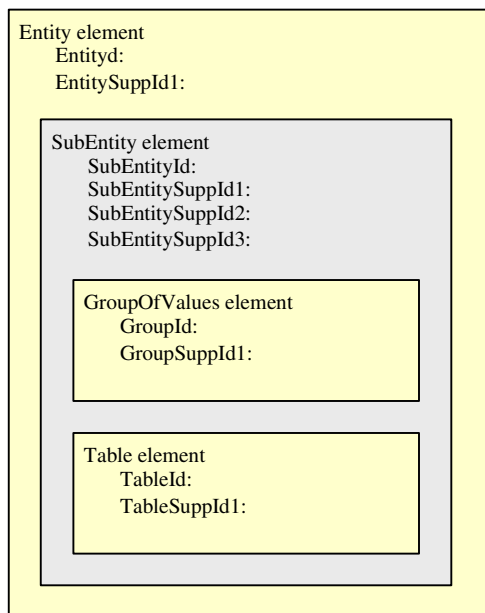
In the case of an *Entity* element (which is used to hold measurements for a particular NE), there are two identifiers: an EntityId (Entity Identifier) and an EntitySuppId (Entity Supplementary Identifier).

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 114](#) for more information.

Example of Identifiers and Supplementary Identifiers



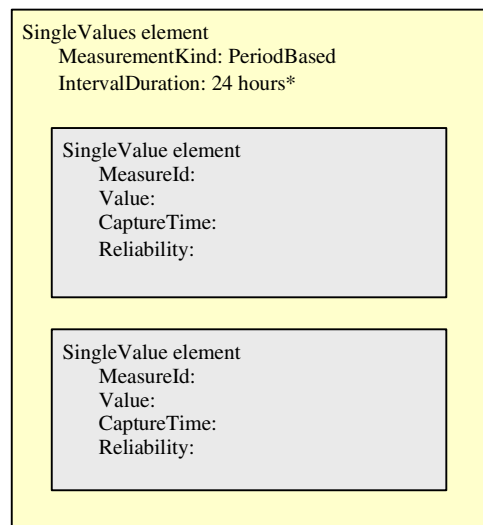
Measurement Elements

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

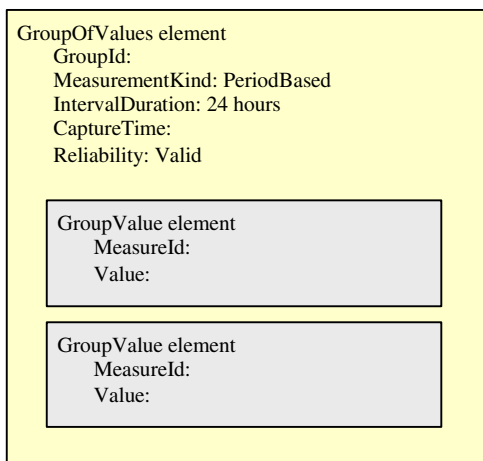
With this approach each performance measurement is considered as a standalone value with no explicit relationship to any other measurement value which may accompany it. Each measurement is encoded in a *SingleValue* element. One or more *SingleValue* elements are contained in a *SingleValues* element 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



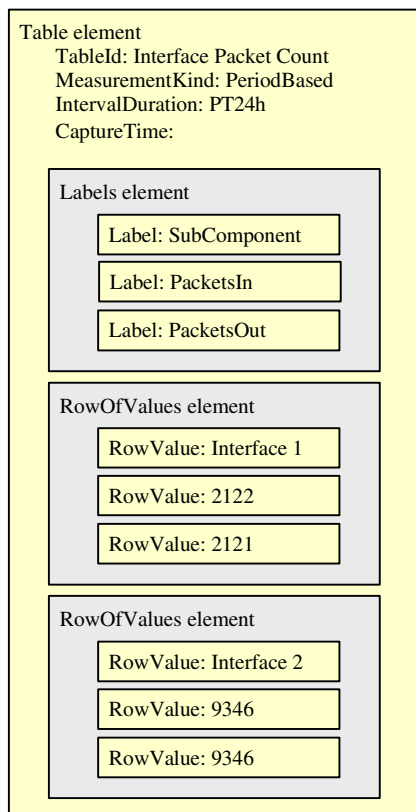
Group Values Approach

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

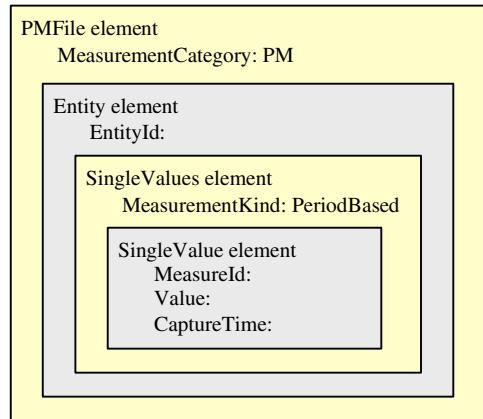
Labels Element: N/A

Label Element: N/A

RowOfValues Element: N/A

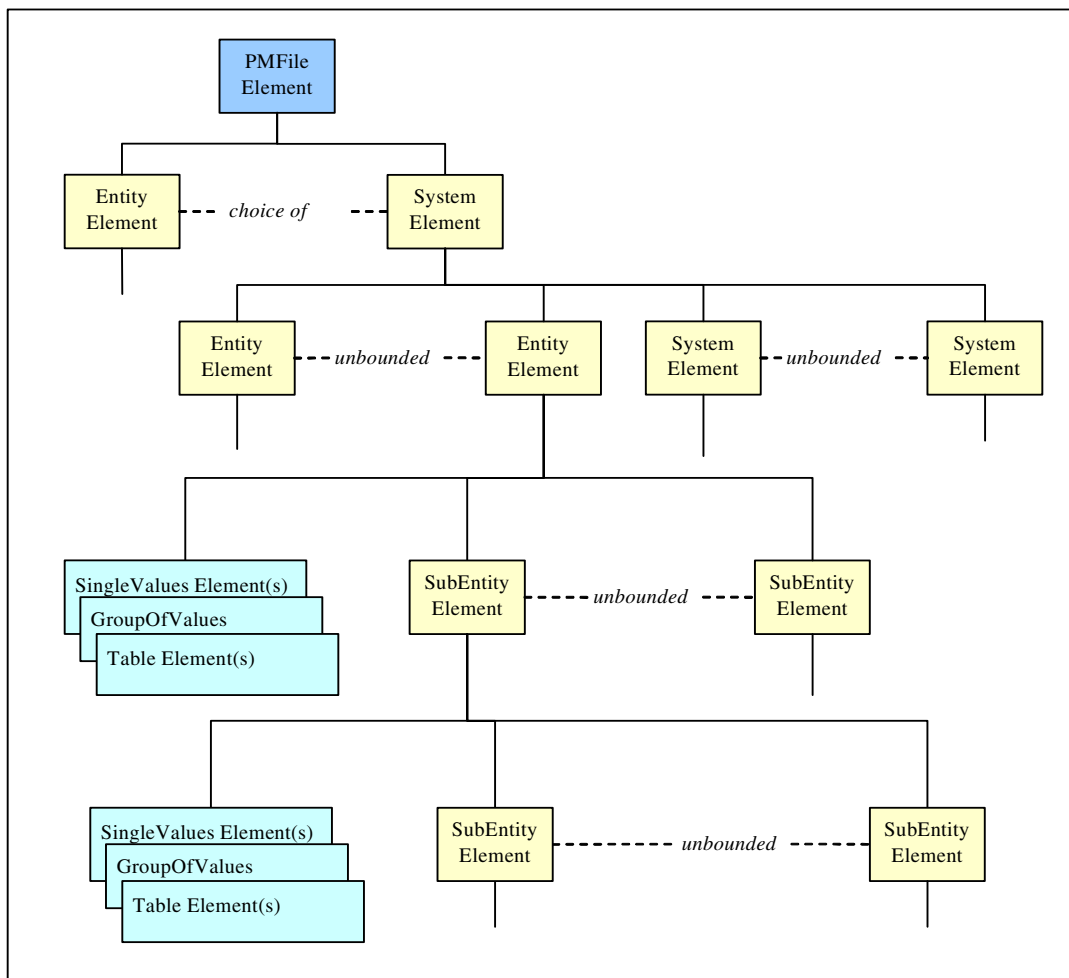
RowValue Element: Value

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>		LastRecord									
LastRecord											
<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>		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
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>		GroupId	GroupSuppId1	CaptureTime	LastRecord	Reliability					
GroupId											
GroupSuppId1											
CaptureTime											
LastRecord											
Reliability											
<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>		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				
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>		TableId	CaptureTime	LastRecord	Reliability						
TableId											
CaptureTime											
LastRecord											
Reliability											
<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>		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>						
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>										
<table border="1"> <tr> <td colspan="2"> RowOfValues <table border="1"> <tr> <td colspan="2"> RowValue <table border="1"> <tr> <td>Value</td> <td>ResetTime</td> </tr> </table> </td> </tr> </table> </td> </tr> </table>		RowOfValues <table border="1"> <tr> <td colspan="2"> RowValue <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				
RowOfValues <table border="1"> <tr> <td colspan="2"> RowValue <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

For examples of each of the supported PM files, refer to the section in this chapter entitled “IEMS Supported Devices” on page 132.

Note: The SNMP PM Poller is not supported for (I)SN09.

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.

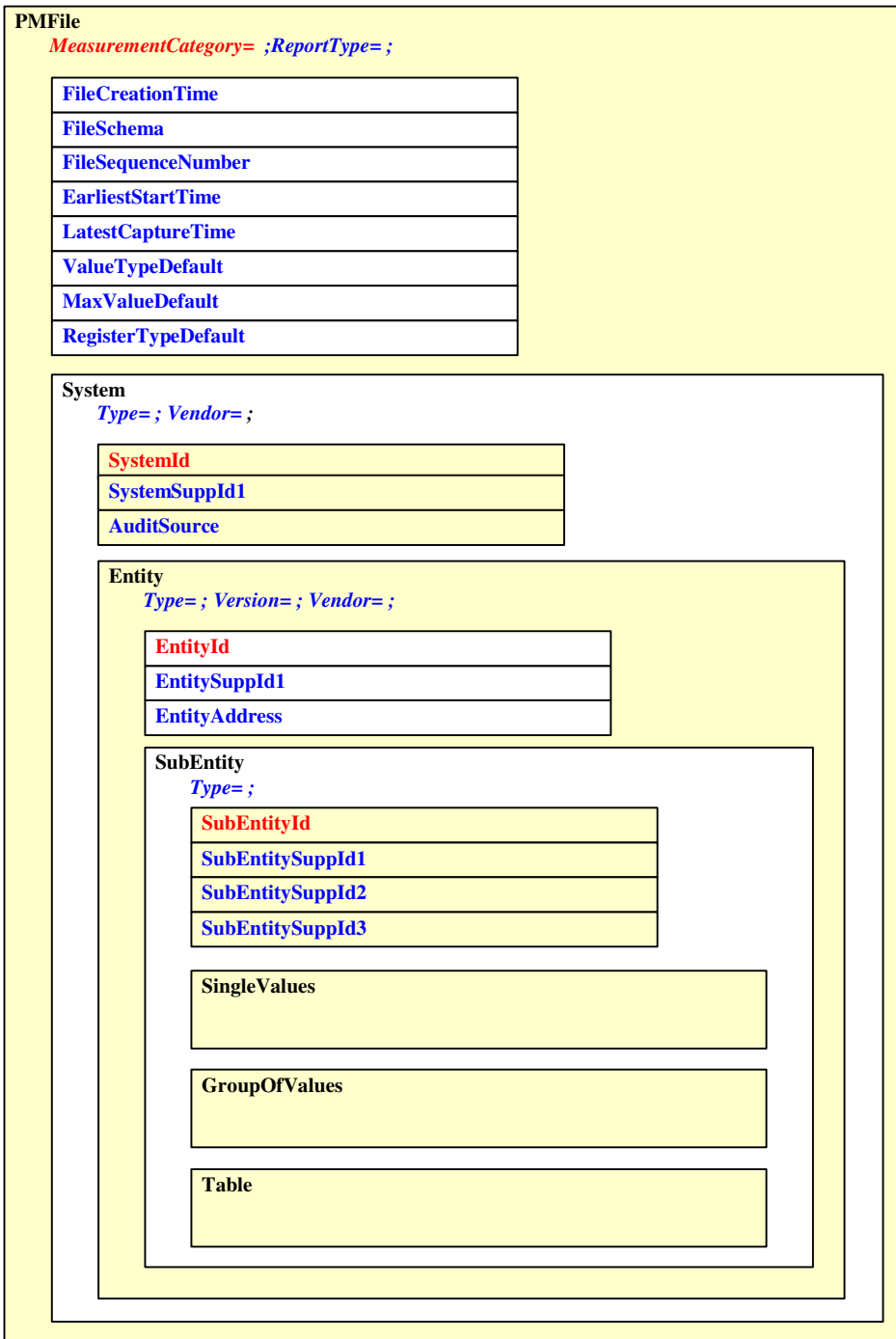
Element blocks and identifiers

Element	Block?	Identifier
PMFile	Y	MeasurementCategory
System	Y	SystemId
Entity	Y	EntityId
SubEntity	Y	SubEntityId
Table	Y	TableId

Element	Block?	Identifier
Labels	N	Label
RowOfValues	N	RowValue/Value
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

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> </table> <table border="1"> <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> </table> <table border="1"> <tr><td>ResetTime</td></tr> </table> </td></tr> </table>	RowValue	<table border="1"> <tr><td>Value</td></tr> </table> <table border="1"> <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> </table> <table border="1"> <tr><td>ResetTime</td></tr> </table> </td></tr> </table>	RowValue	<table border="1"> <tr><td>Value</td></tr> </table> <table border="1"> <tr><td>ResetTime</td></tr> </table>	Value	ResetTime							
RowValue	<table border="1"> <tr><td>Value</td></tr> </table> <table border="1"> <tr><td>ResetTime</td></tr> </table>	Value	ResetTime								
Value											
ResetTime											

CSV Table example

```

PMFile=Begin
PM,commonPerfRecord_V2.0.xsd,2004-06-
  23T13:01:14EST

System=Begin
NortelNetworks/IEMS

Entity=Begin
Entity Id
47.165.168.120

Table=Begin
.iso.org.dod.internet.mgmt.mib-
  2.rmmon.usrHistory.usrHistoryControlTable.usrHistoryControlEntry,Snapshot,5,2004-06-
  23T13:00:00EST
usrHistoryControlInterval,usrHistoryControlIndex,usrHistoryControlStatus,usrHistoryControlOwner
900,5,1,CICM-120A
Table=End

Table=Begin
.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelPerfRefMIB.nnPerfMetricReferenceTable.nnPerfMetricReferenceEntry,Snapshot,5,2004-06-23T13:00:02EST
nnPerfMetricValue,nnPerfMetricSources,nnPerfMetricDataType,nnPerfMetricGroup,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

```

}	Table attributes & text elements values
}	Labels attributes & text elements values
}	Row Of Values attributes & text elements

CSV SingleValues example

```

PMFile=Begin
PM,commonPerfRecord_V2.0.xsd,2004-06-23T17:30:21EST

System=Begin
NortelNetworks/IEMS

Entity=Begin
Entity Id
47.174.74.179

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 SN09 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,commonPerfRecord_V2.0.xsd,2004-06-23T12:45:04EST
System=Begin
SystemId
NortelNetworks/IEMS
Entity=Begin
EntityId
47.165.168.120
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,usrHistoryContr
olOwner
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

The IEMS 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 - IEMS Configuration Management

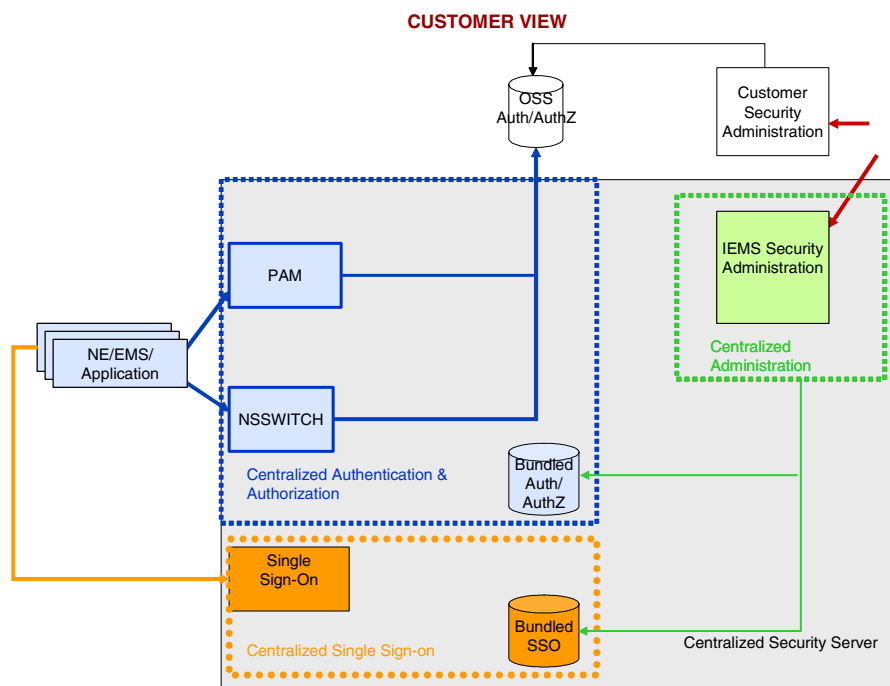
Network Security

Centralized Security Administration (Network Security)

Overview

The IEMS 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 and user groups
- Support for central authentication: authentication of centrally administered user accounts is performed by the IEMS Security Server.
- Support for central authorization: authorization information needed to support user access control is securely managed and provided by the IEMS Security Server.
- 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 on IEMS. Client authentication and authorization information are provided by the customer's security backend via the IEMS Security Server.

The following table lists the 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	USP Security and Administration, NN10159-611
ERS 8600 (formerly Passport 8600)	Radius	Configuring and Managing Security, 314724-B
SSPFS CS 2000 Management Tools (ossgate, sam2em, gwcem, uasem, apsem, lmm, tmm, Audio Provisioning Server (APS) Network Patch Manager (NPM) MG 9000 Manager	Radius	ATM/IP Solution-level Security and Administration, NN10402-600
IEMS	HTTPS	IEMS Security and Administration, NN10336-611
GWC	PAM Proxy	?
IEMS	HTTPS	IEMS Security and Administration, NN10336-611
CICM Manager	HTTPS	IEMS Security and Administration, NN10336-611
SDM	Radius	?
MDM and MDM Operator Client, PAM and Sun ONEIS	Radius	?
MG15000 (previously PVG)	Radius	?
CEM	PAM Proxy	?
MG9K	Radius	?

The following table lists IEMS single sign-on launch points.

IEMS single sign-on launch points

Network element/EMS platform/application	IEMS launch point
USP	USP Command Line USP Manager
ERS 8600 (formerly Passport 8600)	ERS8600 Command Line
SSPFS	CS 2000 Management Tools
CS 2000 Management Tools	
Audio Provisioning Server (APS)	
Network Patch Manager (NPM)	
MG 9000 Manager	
SAM21 Manager	SAM21 Manager
UAS Manager	UAS Manager
LMM	LMM
TMM	TMM
OSSGate	OSSGate BPT Servlet BPT Command Line
MG9000 Manager	MG9000 Manager
MG9000 Mid-Tier	
APS	APS Manager APS Application
NPM	NPM NPM Command Line
QOS	QOS Command Line
CEM	CEM
SSPFS	SSPFS

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. When customers use the PAM services provided by the IEMS Security Server, the user accounts are managed via the IEMS security and administration GUI.

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 via the IEMS security and administration GUI. 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)

For more information on adding a centrally managed user, refer to the “Adding New Users” section of *IEMS Administration and Security*.

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 Supported 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=nc0rtp2127.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	.1.3.6.1.2.1.118.1.2.2.1.10
Short name	alarmActiveDateAndTime

Long name	alarmMIB.alarmObjects.alarmActive.alarmActiveTable.alarmActiveEntry.alarmActiveDateAndTime
OID	.1.3.6.1.2.1.118.1.2.2.1.2
Short name	alarmActiveDescription
Long name	alarmMIB.alarmObjects.alarmActive.alarmActiveTable.alarmActiveEntry.alarmActiveDescription
OID	.1.3.6.1.2.1.118.1.2.2.1.11
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:

- NN10087-911 - Call Agent Fault Management
- NN10275-909 - Carrier VoIP Fault Management Logs Reference
- NN10083-911 - Communication Server 2000 Fault Management

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
- NN10087-911 - Call Agent Fault Management
- NN10264-709 - Carrier VoIP Performance Management Operational Measurements Reference

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

- NN10448-111 - Communication Server 2000 Basics
- NN10188-511 - Communication Server 2000 Configuration Management
- NN10083-911 - Communication Server 2000 Fault Management
- NN10149-711 - Communication Server 2000 Performance Management
- NN10171-611 - Communication Server 2000 Security and Administration
- 297-8403-901 - Operator Services System Advanced Intelligent Network (OSSAIN) User's Guide
- NN10324-509 - Carrier Voice over IP Operational Configuration: Data Schema Reference Vol. 1-2
- 297-8021-808 - DMS-100 SERVORD Reference Manual Vol. 1-2
- NN10264-709 - Carrier Voice over IP Performance Management Operational Measurements Reference Vol. 1-4
- NN10275-909 - Carrier Voice over IP Fault Management Logs Reference Vol. 1-6
- 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.

Note: All Call Agent logs are treated as INFO events by the IEMs and are associated to the CS2000 Manager when the CS2000 Manager is configured in IEMs.

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 =>
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.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 Security and Administration

Related documents

- NN10023-111 - Call Agent Basics
- NN10109-511 - Call Agent Configuration Management

Core Element Manager (CEM)

This section contains IEMS Northbound log samples and device documentation references for the Core Element Manager.

CEM Fault Interface

This section provides references to customer documentation for Fault Management for CEM.

Fault documentation for CEM:

The document that describes CEM faults is IEMS Fault Management, NN10334-911.

Fault Mapping for CEM

The following criteria can be used for looking up information on specific faults for CEM.

Table 1 Fault Correlation for CEM

NB format ->	SCC2	NTStd	SNMP	Syslog	Document Reference
Device/EM					
CEM	Description log name and log number	Description log name and log number	Device specific info	Description log name and log number	NN10334-911

Northbound Fault Formats for CEM

SCC2

The following is an example of a CEM log in SCC2 format:

info event:

```
58 CSEM600 0069 INFO Log
Equip Id: 250Q C7SP
Notification Id: 0000042693
Category: communications
Cause: unableToSSTreply
ComponentId: C7SP
LogKey: CCS224
Description:
"RTPU08AZI | | ICCS224|JAN19|13:57:30|8844|INFO|No reply SST Invd CGPA

SSN = 100,
CGPA: VALID  ANSI7  43 0 1 ANSI7 252 050 006
GTNAME: INVALID UNKNOWN 208 164 94 00 OCTET
DIGITS:
|1106161126"
```

alarm raise or clear:

```
* 00 CSEM300 0083 TBL Alarm set
Equip Id: 250Q SDM-0
Notification Id: 0000042700
Category: processingError
Cause: applStatusChange
ComponentId: SDM-0
LogKey: SDM550
Description:
"RTPU08AZI |** | |SDM550|JAN19|13:59:04|8861|INFO|Node Status Change
Node:  SDM 0
Status: ** ISTb   from ** ISTb
Reason: DCE unavailable alarm
|1106161220"
```

NTStd

The following is an example of a CEM log in NTStd format:

info event:

```
znc0s0jh  CSEM600 JAN19 13:58:58 0071 INFO Log
Equip Id: 250Q MPC-1
Notification Id: 0000042694
Category: equipment
Cause: mpcINFO
ComponentId: MPC-1
LogKey: MPC101
Description:
"RTPU08AZI | | IMPC101|JAN19|13:57:43|8845|INFOIMPC_INFORMATION_REPORT
  REASON = 19
  UNABLE TO DOWNLOAD MPC. FILE-ID NOT FOUND.
  MPC = 1

|1106161138"
```

alarm raise or clear:

```
znc0s0jh  * CSEM300 JAN19 14:00:20 0083 TBL Alarm set
Equip Id: 250Q SDM-0
Notification Id: 0000042700
Category: processingError
Cause: applStatusChange
ComponentId: SDM-0
LogKey: SDM550
Description:
"RTPU08AZI |** | |SDM550|JAN19|13:59:04|8861|INFOINode Status Change
  Node: SDM 0
  Status: ** ISTb from ** ISTb
  Reason: DCE unavailable alarm

|1106161220"
```

SNMP

The following is an example of a CEM log in SNMP format for **event**:

info event:

sysUpTime. => 1:56:59

snmpTrapOID. => nnExtAlarmMessage

nnExtAlarmMessageResource => .0.0

nnExtAlarmMessageResourceDescription =>
IEMS=250Q@rtpu@47.142.94.68;MPC-1

nnExtAlarmMessageDateAndTime => 2005-1-19,1:58:58.0

nnExtAlarmMessageDocumentationPointer => MPC101

nnExtAlarmMessageInfo => 58 CSEM600 0071 INFO Log

"RTPU08AZ| | |
|MPC101|JAN19|13:57:43|8845|INFO|MPC_INFORMATION_REPORT
REASON = 19

UNABLE TO DOWNLOAD MPC. FILE-ID NOT FOUND.

MPC = 1

|110616

clear alarm:

sysUpTime. => 4:50:21

snmpTrapOID. => nnExtAlarmClear

mib-2. =>
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.11
6.20.50.48.48.53.45.49.45.49.57.44.49.58.53.51.58.53.50.46.48.44.45906

mib-2. => 54

mib-2. => DeviceSpecificInfo="RTPU08AZ| |** |
|SDM550|JAN19|13:52:37|8807|INFO|Node Status Change

Node: SDM 0

Status: ** ISTb from ** ISTb

Reason: DCE unavailable alarm

|1106160832"

nnExtAlarmActiveEventType => 3

nnExtAlarmActiveProbableCause => 118

nnExtAlarmActiveAdditionalText =>

nnExtAlarmActiveDocumentationPointer =>

nnExtAlarmActiveResourceDescription =>
IEMS=250Q@rtpu@47.142.128.85;

nnExtAlarmActiveSequenceNumber => 4629

minor alarm:

sysUpTime. => 1:58:22

snmpTrapOID. => nnExtAlarmMinor

mib-2. =>

.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.11
6.19.50.48.48.53.45.49.45.49.57.44.50.58.48.58.50.48.46.48.44.2

mib-2. => Õ

mib-2. => DeviceSpecificInfo=applStatusChange;"RTPU08AZ| |** |
|SDM550|JAN19|13:59:04|8861|INFO|Node Status Change

Node: SDM 0

Status: ** ISTb from ** ISTb

Reason: DCE unavailable alarm

|1106161220"

nnExtAlarmActiveEventType => 3

nnExtAlarmActiveProbableCause => 118

nnExtAlarmActiveAdditionalText =>

nnExtAlarmActiveDocumentationPointer => SDM550

nnExtAlarmActiveResourceDescription =>
IEMS=250Q@rtpu@47.142.94.68;SDM-0

nnExtAlarmActiveManualClear => 2

nnExtAlarmActiveSequenceNumber => 3

major alarm:

sysUpTime. => 4:50:22

snmpTrapOID. => nnExtAlarmMajor

mib-2. =>
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.11
6.19.50.48.48.53.45.49.45.49.57.44.50.58.48.58.50.49.46.48.44.45917

mib-2. => Õ

mib-2. => DeviceSpecificInfo=sdmBaseMaintenance;"RTPU08AZ| |** |
|SDM317|JAN19|14:00:19|8862|TBL | SDM Base Maintenance

DCE problem detected

Reason: sec client service failed: Waited for 5 minutes and DCED had
not initia

nnExtAlarmActiveEventType => 3

nnExtAlarmActiveProbableCause => 118

nnExtAlarmActiveAdditionalText =>

nnExtAlarmActiveDocumentationPointer => SDM317

nnExtAlarmActiveResourceDescription =>
IEMS=250Q@rtpu@47.142.128.85;SDM-0

nnExtAlarmActiveManualClear => 4

nnExtAlarmActiveSequenceNumber => 4630

critical alarm:

Syslog

The following is an example of a CEM log in Syslog format:

info event:

```
Aug 1 18:30:17 znc0s0jh IEMS:
_V2_~I=~H=znc0s0jh~A=IEMS~S=0444~~ CSEM600 NONE INFO
Log^M Equip Id: 250Q C7SP^M Notification Id: 0000048176^M
Category: communications^M Cause: unableToSSTreply^M
ComponentId: C7SP^M LogKey: CCS224^M Description:^M
"RTPU08AZI| | |CCS224|JAN20|00:32:43|8642|INFO|No reply SST Invd
CGPA^M ^M SSN = 100,^M CGPA: VALID ANSI7
43 0 1 ANSI7 252 050 006 ^M GTNAME: INVALID
UNKNOWN 208 164 94 00 OCTET ^M DIGITS: ^M
|1106199239"
```

alarm raise or clear:

```
Aug 1 18:30:27 znc0s0jh IEMS:
_V2_~I=~H=znc0s0jh~A=IEMS~S=0451~~ CSEM300 MINOR TBL Alarm
set^M Equip Id: 250Q SDM-0^M Notification Id: 0000048178^M
Category: processingError^M Cause: applStatusChange^M
ComponentId: SDM-0^M LogKey: SDM550^M Description:^M
"RTPU08AZI|**||SDM550|JAN20|00:32:53|8644|INFO|Node Status Change
^M Node: SDM 0^M Status: ** ISTb from ** ISTb
^M Reason: DCE unavailable alarm^M |1106199249"
```

Performance

OM and PM Documentation references for CEM

- Not supported in SN09

Northbound OM/PM Formats

N/A

GUI/CLUI Documentation for CEM

GUI Launching and User procedures

- Adding a Core Element Manager - IEMS Configuration Management NN10330-511
- Launching a Core Element Manager - IEMS Basics, NN10329-111
- CEM Overview and GUI description - IEMS Basics, NN10329-111

Related documents

- Adding a Core Element Manager - IEMS Configuration Management NN10330-511
- Launching a Core Element Manager - IEMS Basics, NN10329-111
- CEM Logs and OMs - IEMS Fault Management, NN10334-911-
- CEM Overview and GUI description - IEMS Basics, NN10329-111
- CEM Restore - ATM/IP Solution level Security and Administration, NN10402-600
- Synchronous Backup Manager procedures - ATM/IP Solution level Security and Administration, NN10402-600

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  ** CICM500 JUN17 09:02:08 0005 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

test  ** CICM339 JUN17 09:02:13 0006 FLT  CICM 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. => 19:40:37
snmpTrapOID. => 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
.48.52.45.54.45.50.57.44.49.48.58.50.57.58.48.46.52.44.11925
alarmActiveDateAndTime => 2004-6-29,10:29:0.4
alarmActiveDescription => DeviceSpecificInfo=softwareProgramError(48);Backup
Fail.
nnExtAlarmActiveEventType => 4
nnExtAlarmActiveProbableCause => 1024
nnExtAlarmActiveAdditionalText => Scheduled/on-demand backup failed during
last iteration.
nnExtAlarmActiveDocumentationPointer => C1CM341
nnExtAlarmActiveResourceDescription => IEMS=47.142.86.95-C1CM-
Mgr_Card_A;C1CM=C1CMEM-000-A;NodeType=Platform
nnExtAlarmActiveSequenceNumber => 1

```

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 CICM

- N10327-711 - IEMS Performance Management

Northbound OM/PM Formats

Performance measurements for CICM are available only from the CICM Manager interface. See NN10327-711 - IEMS Performance Management for more information.

XML

The following is an example of Performance data for CICM 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="commonPerfRecord_V2.0.xsd" MeasurementCategory="PM">
<FileCreationTime>2004-06-23T12:30:00EST</FileCreationTime>
_ <System>
<SystemId>NortelNetworks/IEMS</SystemId>
_ <Entity>
<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

The following is an example of Performance data for CICM in CSV format:

```

PMFile=Begin
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonPerfRecord_V2.0.xsd,2005-03-28T17:30:02EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId
47.165.168.125

Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
.iso.org.dod.internet.mgmt.mib-
2.rmon.usrHistory.usrHistoryControlTable.usrHistoryControlEntry,Snapshot,5,2005-03-
28T17:30:00EST
Label,Label,Label,Label
usrHistoryControlIndex,usrHistoryControlInterval,usrHistoryControlOwner,usrHistoryCo
ntrolStatus
Value,Value,Value,Value
5,900,CICM-120B,1
Table=End

Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime

```

```
.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelPerfRefMIB.  
nnPerfMetricReferenceTable.nnPerfMetricReferenceEntry, Snapshot, 5, 2005-03-  
28T17:30:00EST
```

```
Label, Label, Label, Label, Label, Label
```

```
nnPerfMetricRefIndex, nnPerfMetricName, nnPerfMetricGroup, nnPerfMetricDataType, nnPerfM  
etricSources, nnPerfMetricValue
```

```
Value, Value, Value, Value, Value, Value
```

```
5, ActiveConnections, CICM, 1, 2, 0
```

```
4, PercentageCpuUsed, CICM, 1, 2, 0
```

```
3, PercentageMemoryUsed, CICM, 1, 2, 38
```

```
2, NumberOfLogs, CICM, 1, 2, 0
```

```
1, ActiveSessions, CICM, 1, 2, 671047275
```

```
Table=End
```

```
Entity=End
```

```
System=End
```

```
PMFile=End
```

GUI/CLUI Documentation for CICM

GUI Launching and User procedures

Related documents

Ethernet Routing Switch 8600 (formerly Passport 8600)

This section contains IEMS Northbound log samples and device documentation references for the ERS 8600.

ERS 8600 Fault Interface

Fault documentation for ERS 8600:

- 241-6001-011 Multiservice Data Manager Fault Management Tools
- 241-6001-501 Multiservice Data Manager Alarms Reference

Fault Mapping for ERS 8600

The following criteria can be used for looking up information on specific faults for ERS 8600.

Fault Correlation for ERS 8600

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
ERS 8600	logname and number	logname and number	logname and number	logname and number	241-6001-500 Multiservice Data Manager Alarms Reference

Northbound Fault Formats for Ethernet Routing Switch 8600

SCC2

The following is an example of an ERS 8600 log in SCC2 format:

```

**59 PP  330 0010 TBL  PP Fault
Location: pp8600;47.142.106.1
State: Raised
Category: equipment
Cause: Link Oscillation detected
Time: Aug 09 15:59:14 2004
Component ID: ERS8600=47.142.106.1; portIndex=198
Specific Problem: RC Link Oscillation
Description: LinkOscillation: portIndex = 198
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.8
.1.3.6.1.2.1.1.3.0: 50 days, 17 hours, 4 minutes, 39 seconds.

03 PP  318 0011 INFO PP Fault
Location: pp8600;47.142.106.1
State: Cleared
Category: communications
Cause: communication regained
Time: Aug 09 16:03:38 2004
Component ID: ERS8600=47.142.106.1; ifIndex=89
Specific Problem: Generic Link Status
Description: Link Up: ifIndex = 89( AdminStatus = up OperationStatus = u

```

p)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.4.0
.1.3.6.1.2.1.1.3.0: 50 days, 17 hours, 9 minutes, 3 seconds

NTSTD

The following is an example of an ERS 8600 log in NTSTD format:

```
MY_OFFICE  **    PP330 AUG09 15:59:14 0010 TBL  PP Fault
Location: pp8600;47.142.106.1
State: Raised
Category: equipment
Cause: Link Oscillation detected
Time: Aug 09 15:59:14 2004
Component ID: ERS8600=47.142.106.1; portIndex=198
Specific Problem: RC Link Oscillation
Description: LinkOscillation: portIndex = 198
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.8
.1.3.6.1.2.1.1.3.0: 50 days, 17 hours, 4 minutes, 39 seconds.

MY_OFFICE      PP318 AUG09 16:03:38 0011 INFO PP Fault
Location: pp8600;47.142.106.1
State: Cleared
Category: communications
Cause: communication regained
Time: Aug 09 16:03:38 2004
Component ID: ERS8600=47.142.106.1; ifIndex=89
Specific Problem: Generic Link Status
Description: Link Up: ifIndex = 89( AdminStatus = up OperationStatus = u
p)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.4.0
.1.3.6.1.2.1.1.3.0: 50 days, 17 hours, 9 minutes, 3 seconds.
```

SNMP

The following is an example of an ERS 8600 log in SNMP format:

```
sysUpTime.0 => 2:55:28
```



```

snmpTrapOID.0 => nnExtAlarmMajor
alarmActiveResourceId =>
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48
.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 317
nnExtAlarmActiveResourceDescription => IEMS=47.142.130.66-PP8600;3
nnExtAlarmActiveSequenceNumber => 2709

```

Syslog

The following is an example of an ERS 8600 log in Syslog format:

```

Aug 9 15:58:57 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=3342~~ PP317 MAJOR TBL
PP Fault^M Location: pp8600;47.142.106.1^M State: Raised^M Category:
com
munications^M Cause: loss of communication^M Time: Aug 09 15:58:56 2004^M
Component ID: ERS8600=47.142.106.1; ifIndex=89^M Specific Problem: Generic Li
nk Status^M Description: Link Down: ifIndex = 89( AdminStatus = down
OperationStatus^M = down)^M .1.3.6.1.6.3.1.1.4.1.0:
.1.3.6.1.6.3.1.1.5.3.0^M .1.
3.6.1.2.1.1.3.0: 50 days, 17 hours, 4 minutes, 22 seconds.

Aug 9 15:59:14 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=3343~~ PP318 NONE INFO
PP Fault^M Location: pp8600;47.142.106.1^M State: Cleared^M Category:
co
mmunications^M Cause: communication regained^M Time: Aug 09 15:59:14
2004^M Component ID: ERS8600=47.142.106.1; ifIndex=198^M Specific Problem:
Generic
Link Status^M Description: Link Up: ifIndex = 198( AdminStatus = up
OperationStatus = ^M up)^M .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.4.0^M
.1.3.
6.1.2.1.1.3.0: 50 days, 17 hours, 4 minutes, 39 seconds.

```

Performance

OM and PM Documentation references for ERS 8600

- 241-6001-031, Multiservice Data 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 ERS 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="commonPerfRecord_V2.0.xsd" MeasurementCategory="PM">
<FileCreationTime>2004-06-23T17:35:01EST</FileCreationTime>
_ <System>
<SystemId>NortelNetworks/IEMS</SystemId>
_ <Entity>
<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.snmpMPDMIBObject
s.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 ERS 8600 in CSV format:

Note: The following CSV output file are captured using ERS8600_IP_30_minute_data.xml template.

```

PMFile=Begin
MeasurementCategorynoNamespaceSchemaLocationFileCreationTime
PM commonPerfRecord_V2.0.xsd2005-12-20T21:48:39EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId
47.142.86.32

Table=Begin
TableIdMeasurementKindIntervalDurationCaptureTime
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcStat.rcStatTable.rcStat
EntrySnapshot52005-12-20T21:37:19EST
LabelLabelLabelLabelLabel
rcStatPortIndexrcStatRouteInDiscardsrcStatStgForwardTransitionsrcStatFrameTooShorts
rcStatBridgeInDiscards
ValueValueValueValueValue
70 0 0 0 0
2650 0 0 0
2640 0 0 0
2630 0 0 0
2620 0 0 0

```

2610	0	0	0
2600	0	0	0
4590	0	0	0
4580	0	0	0
69	0	0	0
4570	0	0	0
68	0	0	8 1292802
4560	0	0	0
67	0	0	0
4550	0	0	0
66	0	0	0
4540	0	0	0
65	0	0	0
4530	0	0	0
64	0	0	0 11534
2590	0	0	0
4520	0	0	0
2580	0	0	0
4510	0	0	0
2570	0	0	0
4500	0	0	0
2560	0	0	0
4490	0	0	0
4480	0	0	0
2390	0	0	0
2380	0	0	0
2370	0	0	0
2360	0	0	0
2350	0	0	0
2340	0	0	0
2330	0	0	0
2320	0	0	0
2310	0	2	0
1990	0	0	0
2300	0	2	0
1980	0	0	0
1970	0	0	0
1960	0	0	0

1950	0	0	0
1940	0	0	0
1930	0	0	0
1920	0	0	0
2290	0	0	0
5830	0	0	0
2280	0	0	0
5820	0	0	0
2270	0	0	0
5810	0	0	0
2260	0	0	0
5800	0	0	0
2250	0	0	0
2240	0	0	0
2230	0	0	0
2220	0	0	0
2210	0	0	0
2200	0	0	0
5790	0	0	0
5780	0	0	2561114
5770	0	0	0
5760	0	0	10984
2190	0	0	0
2180	0	0	0
2170	0	0	0
2160	0	0	0
2150	0	0	0
2140	0	0	0
2130	0	0	0
2120	0	0	0
2110	0	0	0
2100	0	0	0
2090	0	0	0
2080	0	0	0
2070	0	0	0
2060	0	0	0
2050	0	0	0
2040	0	0	0

2030	0	0	0
2020	0	0	0
2010	0	0	0
2000	0	0	0
1610	0	0	0
1600	0	0	0
5590	0	0	0
5580	0	0	0
5570	0	0	0
5560	0	0	0
5550	0	0	0
5540	0	0	0
5530	0	0	0
5520	0	0	0
5510	0	0	0
5500	0	0	0
1590	0	0	0
1580	0	0	0
1570	0	0	0
1560	0	0	0
1550	0	0	0
1540	0	2	0
1530	0	0	0
1520	0	0	0
1510	0	0	0
1500	0	0	0
5490	0	0	0
5480	0	0	0
5470	0	0	0
5460	0	0	0
5450	0	0	0
5440	0	0	0
5430	0	0	0
5420	0	0	0
5410	0	0	0
5400	0	0	0
1490	0	0	0
1480	0	0	0

1470	0	0	0
1460	0	0	0
1450	0	0	0
1440	0	0	0
1430	0	0	0
1420	0	0	0
1410	0	0	0
1400	0	0	0
5390	0	0	0
5380	0	0	0
5370	0	0	8
5360	0	0	0
5350	0	0	0
5340	0	0	0
5330	0	4	0
5320	0	0	0
5310	0	0	0
5300	0	0	0
4950	0	0	0
4940	0	0	0
1390	0	0	0
4930	0	0	0
1380	0	0	0
4920	0	0	0
1370	0	0	0
2990	0	0	0
4910	0	0	0
1360	0	0	0
2980	0	0	0
4900	0	0	0
1350	0	0	0
2970	0	0	0
1340	0	0	0
2960	0	0	0
1330	0	0	0
2950	0	0	0
1320	0	0	0
2940	0	0	0

1310	0	0	0
2930	0	0	0
1300	0	0	0
2920	0	0	0
2910	0	0	0
2900	0	0	0
5290	0	0	0
5280	0	0	0
5270	0	0	3
5260	0	0	0
5250	0	0	0
5240	0	0	0
5230	0	1	0
5220	0	0	0
5210	0	0	0
5200	0	0	0
4890	0	0	0
4880	0	0	0
4870	0	0	0
4860	0	0	0
4850	0	0	0
4840	0	0	3709801
1290	0	32	163
4830	0	0	0
1280	0	0	115
4820	0	0	0
2890	0	0	0
4810	0	0	0
2880	0	0	0
4800	0	0	0
2870	0	230966142	
2860	0	0	0
2850	0	9	0
2840	0	801180	
2830	0	22634230	
2820	0	22930420	
2810	0	7	0
2800	0	23074430	

5190	0	0	0
5180	0	0	0
5170	0	0	0
5160	0	0	0
5150	0	0	0
5140	0	0	0
5130	0	0	0
5120	0	0	0
4790	0	0	0
4780	0	0	0
4770	0	0	0
4760	0	0	0
4750	0	0	0
4740	0	0	0
4730	0	0	3
4720	0	0	0
2790	0	0	0
4710	0	0	0
2780	0	0	0
4700	0	0	0
2770	0	0	0
2760	0	0	0
2750	0	1	0
2740	0	29	0
2730	0	0	0
2720	0	0	0
2710	0	0	0
2700	0	0	0
4690	0	0	0
4680	0	0	0
4670	0	0	0
4660	0	0	0
4650	0	0	0
3030	0	0	0
4640	0	0	0
3020	0	0	0
4630	0	0	0
3010	0	0	0

```
4620 0 0 0
2690 0 0 0
3000 0 0 0
4610 0 0 0
2680 0 0 0
2670 0 0 0
4600 0 0 0
71 0 0 0 0
2660 0 0 0
```

```
Table=End
```

```
" "
```

```
Table=Begin
```

```
TableIdMeasurementKindIntervalDurationCaptureTime
```

```
.iso.org.dod.internet.mgmt.mib-2.ospf.ospfIfTable.ospfIfEntrySnapshot52005-12-20T21:37:12EST
```

```
LabelLabelLabel
```

```
ospfIfIpAddressospfIfEventsospfAddressLessIf
```

```
ValueValueValue
```

```
10.56.131.110
```

```
172.20.2.19510
```

```
172.16.0.310
```

```
172.16.128.310
```

```
172.30.252.310
```

```
47.142.85.13110
```

```
10.56.130.110
```

```
47.142.85.19500
```

```
172.16.109.110
```

```
172.30.242.16610
```

```
47.142.86.3210
```

```
172.30.252.1010
```

```
10.60.127.310
```

```
192.168.223.11050
```

```
10.10.3.310
```

```
172.16.17.3710
```

```
172.30.252.5110
```

```
10.10.0.310
```

```
Table=End
```

```
" "
```

Table=Begin

TableIdMeasurementKindIntervalDurationCaptureTime

.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcStg.rcStgPortTable.rcStgPortEntrySnapshot52005-12-20T21:38:14EST

LabelLabel

rcStgPortrcStgPortForwardTransitions

ValueValue

2350

5770

1440

4860

2330

1420

4840

1295

2310

2180

1400

2890

4690

1980

2160

5580

4800

2870

4670

1960

2140

5560

2850

4650

3030

1940

2120

5540

2830

4630

3010

1920
2100
5520
5390
2810
4610
2680
4480
5500
5370
71 0
2660
5350
2640
5330
2620
1580
5310
5180
2600
1560
5160
1540
5140
1520
4940
1390
5120
5830
2280
1500
4920
1370
2990
4790
5810
2260
4900

1350
2970
4770
2240
1330
2950
4750
2220
2090
2930
1310
4730
2200
2070
5490
2910
4710
2780
4580
2050
5470
2760
68 48
4560
2030
5450
2740
66 0
4540
2010
5430
2720
64 0
2590
4520
5410
5280
2700

2570
4500
5260
5240
1490
5220
2380
1600
1470
5200
4890
2360
57848
1450
4870
2340
5760
1430
4850
2320
2190
1410
4830
1280
1990
2300
2170
5590
4810
2880
4680
1970
2150
5570
2860
4660
1950
2130

5550
2840
4640
3020
1930
2110
5530
2820
4620
2690
3000
4490
5510
5380
2800
2670
4600
5360
70 0
2650
5340
2630
1590
5320
5190
2610
1570
5300
5170
1550
5150
1530
4950
5130
2290
1510
4930
1380

5820
2270
4910
1360
2980
4780
5800
2250
1340
2960
4760
2230
2940
1320
4740
2210
2080
2920
1300
4720
2790
4590
2060
5480
2900
4700
2770
69 0
4570
2040
2750
67 0
4550
2020
5440
2730
65 0
4530

2000

5420

5290

2710

2580

4510

5400

5270

2560

5250

5230

2392

1610

1480

5210

2370

5790

1460

4880

Table=End

" "

Table=Begin

TableIdMeasurementKindIntervalDurationCaptureTime

.iso.org.dod.internet.mgmt.mib-2.ospf.ospfNbrTable.ospfNbrEntrySnapshot52005-12-20T21:37:15EST

LabelLabelLabel

ospfNbrIpAddressospfNbrAddressLessIndexospfNbrEvents

ValueValueValue

172.30.252.105

172.30.252.1105

172.30.242.16505

172.30.252.205

Table=End

" "

Table=Begin

TableIdMeasurementKindIntervalDurationCaptureTime

.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcStat.rcStatGigTable.rcStatGigEntrySnapshot52005-12-20T21:37:40EST

LabelLabelLabelLabelLabel

rcStatGigPortIndexrcStatGigLinkFailuresrcStatGigPacketErrorsrcStatGigCarrierErrors
rcStatGigLinkInactiveErrors

ValueValueValueValueValue

70 0 0 0 0

2651 0 0 0

2641 0 0 0

2631 0 0 0

2621 0 0 0

2611 0 0 0

2601 0 0 0

4591 0 0 0

4581 0 0 0

69 24 0 0 0

4571 0 0 0

68 34 0 0 0

4561 0 0 0

67 0 0 0 0

4551 0 0 0

66 0 0 0 0

4541 0 0 0

65 0 0 0 0

4531 0 0 0

64 0 0 0 0

2591 0 0 0

4521 0 0 0

2581 0 0 0

4511 0 0 0

2571 0 0 0

4501 0 0 0

2562 0 0 0

4491 0 0 0

4482 0 0 0

2394 0 0 0

2381 0 0 0

2371 0 0 0

2363 0 0 0

2351	0	0	0
2341	0	0	0
2331	0	0	0
2321	0	0	0
2311220	0	0	
1991	0	0	0
2301210	0	0	
1981	0	0	0
1971	0	0	0
1961	0	0	0
1951	0	0	0
1941	0	0	0
1931	0	0	0
1921	0	0	0
2291	0	0	0
5830	0	0	0
2281	0	0	0
5820	0	0	0
2271	0	0	0
5810	0	0	0
2261	0	0	0
5803	0	0	0
2251	0	0	0
2242	0	0	0
2231	0	0	0
22212	0	0	0
2211	0	0	0
2201	0	0	0
5792	0	0	0
57838	0	0	0
5771	0	0	0
5761	0	0	0
2191	0	0	0
2181	0	0	0
2171	0	0	0
2161	0	0	0
2151	0	0	0
2141	0	0	0

2131	0	0	0
2121	0	0	0
2111	0	0	0
2101	0	0	0
2091	0	0	0
2081	0	0	0
2071	0	0	0
2061	0	0	0
2051	0	0	0
2041	0	0	0
2031	0	0	0
2021	0	0	0
2011	0	0	0
2001	0	0	0
1611	0	0	0
1601	0	0	0
5595	0	0	0
5581	0	0	0
5571	0	0	0
5561	0	0	0
5555	0	0	0
5541	0	0	0
5531	0	0	0
5521	0	0	0
5511	0	0	0
5501	0	0	0
1591	0	0	0
1581	0	0	0
1571	0	0	0
1561	0	0	0
1551	0	0	0
1542	0	0	0
1531	0	0	0
1521	0	0	0
1513	0	0	0
1501	0	0	0
5491	0	0	0
5481	0	0	0

5475	0	0	0
5462	0	0	0
5453	0	0	0
5442	0	0	0
5431	0	0	0
5421	0	0	0
5411	0	0	0
5401	0	0	0
1491	0	0	0
1481	0	0	0
1471	0	0	0
1461	0	0	0
1451	0	0	0
14410050	0	0	0
1431	0	0	0
1421	0	0	0
1411	0	0	0
1401	0	0	0
5391	0	0	0
5381	0	0	0
53751	0	0	0
5361	0	0	0
5351	0	0	0
5341	0	0	0
53316	0	0	0
5321	0	0	0
5311	0	0	0
5301	0	0	0
4954	0	0	0
4944	0	0	0
1391	0	0	0
4931	0	0	0
1383	0	0	0
4921	0	0	0
1371	0	0	0
2991	0	0	0
4911	0	0	0
1361	0	0	0

2981	0	0	0
4901	0	0	0
1351	0	0	0
2971	0	0	0
1341	0	0	0
2962	0	0	0
1331	0	0	0
2951	0	0	0
1321	0	0	0
2941	0	0	0
1311	0	0	0
2931	0	0	0
1301	0	0	0
2921	0	0	0
2911	0	0	0
2901	0	0	0
5291	0	0	0
5281	0	0	0
5271	0	0	0
5261	0	0	0
5251	0	0	0
5241	0	0	0
52351	0	0	0
5221	0	0	0
5211	0	0	0
5201	0	0	0
4891	0	0	0
4881	0	0	0
4871	0	0	0
4861	0	0	0
4851	0	0	0
4848	0	0	0
1297	0	0	0
4831	0	0	0
1283	0	0	0
4823	0	0	0
2891	0	0	0
4811	0	0	0

2881	0	0	0
4801	0	0	0
2873710	0	0	
2861	0	0	0
2857	0	0	0
2845200	0	0	
28312	0	0	0
28214	0	0	0
28112	0	0	0
28012	0	0	0
5191	0	0	0
5181	0	0	0
5171	0	0	0
5161	0	0	0
5151	0	0	0
5141	0	0	0
5131	0	0	0
5121	0	0	0
4791	0	0	0
4781	0	0	0
4771	0	0	0
4761	0	0	0
4751	0	0	0
4741	0	0	0
4738	0	0	0
4721	0	0	0
2791	0	0	0
4711	0	0	0
2782	0	0	0
4701	0	0	0
2778	0	0	0
2767	0	0	0
2759	0	0	0
2749	0	0	0
2738	0	0	0
27211	0	0	0
2711	0	0	0
2701	0	0	0


```
4691 0 0 0
4681 0 0 0
4671 0 0 0
4661 0 0 0
4657 0 0 0
3033 0 0 0
4641 0 0 0
3023 0 0 0
4632 0 0 0
3011 0 0 0
4622 0 0 0
2691 0 0 0
3001 0 0 0
4611 0 0 0
2681 0 0 0
2671 0 0 0
4601 0 0 0
71 0 0 0
2661 0 0 0
```

Table=End

" "

Table=Begin

TableIdMeasurementKindIntervalDurationCaptureTime

.iso.org.dod.internet.mgmt.mib-
2.vrrp.vrrpMIB.vrrpStatistics.vrrpRouterStatsTable.vrrpRouterStatsEntrySnapshot5
2005-12-20T21:39:22EST

LabelLabelLabel

vrrpStatsIfIndexvrrpStatsVrIdvrrpStatsBecomeMaster

ValueValueValue

21777 1

208710129

20951401

20911201

20851001

21116 1

2083601

2185511

20891101

```

21072468
20971501
20931301
2055111
21052458
Table=End

```

" "

```

Table=Begin
TableIdMeasurementKindIntervalDurationCaptureTime
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntrySnapshot52005-12-
20T21:38:29EST
LabelLabelLabelLabelLabelLabelLabelLabel
ifIndexifInOctetsifInDiscardsifInErrorsifOutOctetsifOutDiscardsifDescrifOutErrors
ValueValueValueValueValueValueValueValue
70 2746910380031133788801000GbicLx Port 1/7 Name ToM40-00
2650 0 0 0 0 10/100BaseTX Port 4/10 Name GWC_41_Unit10
2640 0 0 0 0 10/100BaseTX Port 4/9 Name GWC_40_Unit10
2630 0 0 0 0 10/100BaseTX Port 4/8 Name 0
2620 0 0 0 0 10/100BaseTX Port 4/7 Name GWC_42_Unit10
2610 0 0 0 0 10/100BaseTX Port 4/6 Name 0
2600 0 0 0 0 10/100BaseTX Port 4/5 Name GWC_36_Unit10
4590 0 0 0 0 10/100BaseTX Port 7/12 Name 0
4580 0 0 0 0 10/100BaseTX Port 7/11 Name 0
69 99691800 42110163601000GbicSx Port 1/6 Name IW-SPM0
4570 0 0 0 0 10/100BaseTX Port 7/10 Name 0
68 1094059809129280210261630683301000GbicLx Port 1/5 Name Acme-Enterprise0
4560 0 0 0 0 10/100BaseTX Port 7/9 Name 0
67 310185076005358195201000GbicSx Port 1/4 Name 0
4550 0 0 0 0 10/100BaseTX Port 7/8 Name 0
66 24118836580022314805001000GbicSx Port 1/3 Name Alteon 6614_1 Port 100
4540 0 0 0 0 10/100BaseTX Port 7/7 Name 0
65 2954334964009322455701000GbicLx Port 1/2 Name 0
4530 0 0 0 0 10/100BaseTX Port 7/6 Name 0
64 167780539911534089979341201000GbicSx Port 1/1 Name IST0
2590 0 0 0 0 10/100BaseTX Port 4/4 Name GWC_35_Unit10
4520 0 0 0 0 10/100BaseTX Port 7/5 Name 0
2580 0 0 0 0 10/100BaseTX Port 4/3 Name GWC_34_Unit10
4510 0 0 0 0 10/100BaseTX Port 7/4 Name 0

```

```
2570 0 0 0 0 10/100BaseTX Port 4/2 Name GWC_33_Unit10
4500 0 0 0 0 10/100BaseTX Port 7/3 Name 0
25680000 0 443328010/100BaseTX Port 4/1 Name GWC_32_Unit12
4490 0 0 0 0 10/100BaseTX Port 7/2 Name 0
4480 0 0 2107090800100BaseTX Port 7/1 Name AMS_0_11
2392005591721001904915850100BaseTX Port 3/48 Name 5
2380 0 0 522442880100BaseTX Port 3/47 Name a802996
2370 0 0 0 0 10/100BaseTX Port 3/46 Name 0
2360 0 0 69359133010/100BaseTX Port 3/45 Name 7
2350 0 0 0 0 10/100BaseTX Port 3/44 Name SDM0
2340 0 0 0 0 10/100BaseTX Port 3/43 Name HIOP0
2330 0 0 0 0 10/100BaseTX Port 3/42 Name 0
2320 0 0 0 0 10/100BaseTX Port 3/41 Name 0
23112842784180225430916660100BaseTX Port 3/40 Name CICM-2_Callp143
1990 0 0 0 0 10/100BaseTX Port 3/8 Name GWC_07_Unit10
2305733126250228419564420100BaseTX Port 3/39 Name CICM-2_OAM123
1980 0 0 0 0 10/100BaseTX Port 3/7 Name 0
1970 0 0 0 0 10/100BaseTX Port 3/6 Name GWC_05_Unit10
1960 0 0 0 0 10/100BaseTX Port 3/5 Name GWC_04_Unit10
1950 0 0 0 0 10/100BaseTX Port 3/4 Name GWC_03_Unit10
1940 0 0 0 0 10/100BaseTX Port 3/3 Name GWC_02_Unit10
1930 0 0 0 0 10/100BaseTX Port 3/2 Name GWC_01_Unit10
1920 0 0 0 0 10/100BaseTX Port 3/1 Name GWC_00_Unit10
2290 0 0 0 0 10/100BaseTX Port 3/38 Name 0
5830 0 0 0 0 Gbic1000BaseT Port 9/8 Name 0
2280 0 0 0 0 10/100BaseTX Port 3/37 Name SAM21-8_SC10
5820 0 0 0 0 Gbic1000BaseT Port 9/7 Name 0
2270 0 0 0 0 10/100BaseTX Port 3/36 Name SAM21-01_SC10
5810 0 0 0 0 1000Gbic Port 9/6 Name 0
2260 0 0 0 0 10/100BaseTX Port 3/35 Name SAM21-01_SC00
5800 0 0 20933896001000GbicSx Port 9/5 Name 0
2250 0 0 0 0 10/100BaseTX Port 3/34 Name SAM21-03_SC10
22429873800056841591010/100BaseTX Port 3/33 Name SAM21-03_SC01
2230 0 0 0 0 10/100BaseTX Port 3/32 Name GWC_31_Unit10
22212796670066058705010/100BaseTX Port 3/31 Name GWC_30_Unit114
2210 0 0 0 0 10/100BaseTX Port 3/30 Name GWC_29_Unit10
2200 0 0 0 0 10/100BaseTX Port 3/29 Name GWC_28_Unit10
5790 0 0 3479974401000GbicSx Port 9/4 Name 0
```

```
5781034892122256111474767941301000GbicLx Port 9/3 Name 0
577623963920030626144401000GbicSx Port 9/2 Name OM3500 OAM0
5761772578177109840338634257001000GbicSx Port 9/1 Name IST-OM35000
2190 0 0 0 0 10/100BaseTX Port 3/28 Name GWC_27_Unit10
2180 0 0 0 0 10/100BaseTX Port 3/27 Name GWC_26_Unit10
2170 0 0 0 0 10/100BaseTX Port 3/26 Name GWC_25_Unit10
2160 0 0 0 0 10/100BaseTX Port 3/25 Name GWC_24_Unit10
2150 0 0 0 0 10/100BaseTX Port 3/24 Name GWC_23_Unit10
2140 0 0 0 0 10/100BaseTX Port 3/23 Name GWC_22_Unit10
2130 0 0 0 0 10/100BaseTX Port 3/22 Name GWC_21_Unit10
2120 0 0 0 0 10/100BaseTX Port 3/21 Name GWC_20_Unit10
2110 0 0 0 0 10/100BaseTX Port 3/20 Name 0
2100 0 0 0 0 10/100BaseTX Port 3/19 Name GWC_18_Unit10
2090 0 0 0 0 10/100BaseTX Port 3/18 Name GWC_17_Unit10
2080 0 0 0 0 10/100BaseTX Port 3/17 Name GWC_16_Unit10
2070 0 0 0 0 10/100BaseTX Port 3/16 Name GWC_15_Unit10
2060 0 0 0 0 10/100BaseTX Port 3/15 Name GWC_14_Unit10
2050 0 0 0 0 10/100BaseTX Port 3/14 Name 0
2040 0 0 0 0 10/100BaseTX Port 3/13 Name GWC_12_Unit10
2030 0 0 0 0 10/100BaseTX Port 3/12 Name 0
2020 0 0 0 0 10/100BaseTX Port 3/11 Name GWC_10_Unit10
2010 0 0 0 0 10/100BaseTX Port 3/10 Name 0
2000 0 0 0 0 10/100BaseTX Port 3/9 Name 0
1610 0 0 0 0 1000GbicSx Port 2/34 Name IST-OM35000
1600 0 0 0 0 1000GbicSx Port 2/33 Name IST0
5592308201 2693490010/100BaseTX Port 8/48 Name CABLE_RKS3
5580 0 0 0 0 10/100BaseTX Port 8/47 Name CABLE_RKS0
5570 0 0 0 0 10/100BaseTX Port 8/46 Name CABLE_RKS0
5560 0 0 0 0 10/100BaseTX Port 8/45 Name 0
55517629900 2183427010/100BaseTX Port 8/44 Name 6
5540 0 0 0 0 10/100BaseTX Port 8/43 Name 0
5530 0 0 0 0 10/100BaseTX Port 8/42 Name 0
5520 0 0 0 0 10/100BaseTX Port 8/41 Name 0
5510 0 0 0 0 10/100BaseTX Port 8/40 Name 0
5500 0 0 0 0 10/100BaseTX Port 8/39 Name 0
159141147710002759673440100BaseTX Port 2/32 Name S1K_TLAN-test8
158126470588002168021760100BaseTX Port 2/31 Name S1K_ELAN-test9
1570 0 0 0 0 10/100BaseTX Port 2/30 Name 0
```

15612189830285922752790770100BaseTX Port 2/29 Name 0
1550 0 0 28763139860100BaseTX Port 2/28 Name 0
15412063940277022751913990100BaseTX Port 2/27 Name 1
1530 0 0 28763567200100BaseTX Port 2/26 Name 0
1520 0 0 0 0 10/100BaseTX Port 2/25 Name 0
151897297728052233722196010BaseTX Port 2/24 Name MCS0
150657886958002266133378010BaseTX Port 2/23 Name MCS0
5490 0 0 0 0 10/100BaseTX Port 8/38 Name 0
5480 0 0 0 0 10/100BaseTX Port 8/37 Name 0
54720512038000023647058810100BaseTX Port 8/36 Name RTP4-SPC-U1-LinkB4
54647476549098285987770010/100BaseTX Port 8/35 Name 1
54515106049180422106739520100BaseTX Port 8/34 Name RTP4-SPC-U0-LinkB2
5440 0 0 348216320100BaseTX Port 8/33 Name 1
5430 0 0 0 0 10/100BaseTX Port 8/32 Name 0
5420 0 0 0 0 10/100BaseTX Port 8/31 Name 0
5410 0 0 0 0 10/100BaseTX Port 8/30 Name 0
5400 0 0 0 0 10/100BaseTX Port 8/29 Name 0
149658218816002265777538010BaseTX Port 2/22 Name MCS0
1481363957033002682961418010BaseTX Port 2/21 Name MCS0
147658135680002410568386010BaseTX Port 2/20 Name MCS0
146658162368002265778754010BaseTX Port 2/19 Name MCS0
14523831136000271308760958010BaseTX Port 2/18 Name MCS0
14495633079801102702144086010BaseTX Port 2/17 Name MCS0
1430 0 0 0 0 10/100BaseTX Port 2/16 Name 0
1420 0 0 0 0 10/100BaseTX Port 2/15 Name OLD_CMT_T14000
1410 0 0 0 0 10/100BaseTX Port 2/14 Name 0
1400 0 0 0 0 10/100BaseTX Port 2/13 Name 0
5390 0 0 0 0 10/100BaseTX Port 8/28 Name 3PC_temp0
5380 0 0 0 0 10/100BaseTX Port 8/27 Name 0
537279942083893872407583010/100BaseTX Port 8/26 Name 3PC53
5360 0 0 0 0 10/100BaseTX Port 8/25 Name 0
5350 0 0 0 0 10/100BaseTX Port 8/24 Name 0
5340 0 0 0 0 10/100BaseTX Port 8/23 Name 0
53310445302805118280440010/100BaseTX Port 8/22 Name 21
5320 0 0 0 0 10/100BaseTX Port 8/21 Name 0
5310 0 0 0 0 10/100BaseTX Port 8/20 Name 0
5300 0 0 0 0 10/100BaseTX Port 8/19 Name CBM 1 Port 30
4950 0 0 287232010/100BaseTX Port 7/48 Name 2

```
4940 0 0 59714390010/100BaseTX Port 7/47 Name NGSS_line_reserved2
1390 0 0 0 0 10/100BaseTX Port 2/12 Name 0
4930 0 0 0 0 10/100BaseTX Port 7/46 Name 0
1382152769280029279520280100BaseTX Port 2/11 Name 2
4920 0 0 0 0 10/100BaseTX Port 7/45 Name NGSS_line_reserved0
137577866200022742349800100BaseTX Port 2/10 Name 0
2990 0 0 0 0 10/100BaseTX Port 4/44 Name 0
4910 0 0 0 0 10/100BaseTX Port 7/44 Name 0
1360 0 0 0 0 10/100BaseTX Port 2/9 Name 0
2980 0 0 28764616160100BaseTX Port 4/43 Name MCS-Media1
4900 0 0 0 0 10/100BaseTX Port 7/43 Name NGSS_lines0
1350 0 0 0 0 10/100BaseTX Port 2/8 Name 0
2970 0 0 0 0 10/100BaseTX Port 4/42 Name MCS-Media0
13414639863920013311197110100BaseTX Port 2/7 Name 0
2965551239610127934463120100BaseTX Port 4/41 Name MCS-Media11
1330 0 0 0 0 10/100BaseTX Port 2/6 Name 0
2950 0 0 0 0 10/100BaseTX Port 4/40 Name MCS-Media0
1320 0 0 0 0 10/100BaseTX Port 2/5 Name 0
2940 0 0 0 0 10/100BaseTX Port 4/39 Name MCS-Media0
1314339107290026227101200100BaseTX Port 2/4 Name 0
2930 0 0 0 0 10/100BaseTX Port 4/38 Name NGSS-Port0
1300 0 0 0 0 10/100BaseTX Port 2/3 Name 0
2920 0 0 0 0 10/100BaseTX Port 4/37 Name NGSS-Port0
2910 0 0 0 0 10/100BaseTX Port 4/36 Name 0
2900 0 0 0 0 10/100BaseTX Port 4/35 Name SAM21-07_SC00
5290 0 0 0 0 10/100BaseTX Port 8/18 Name 0
5280 0 0 0 0 10/100BaseTX Port 8/17 Name CBM 0 Port 30
52735034479703020473726450100BaseTX Port 8/16 Name cs2kprovEMS1-link10
52626185383960013267709500100BaseTX Port 8/15 Name cs2kprovEMS0-link10
5250 0 0 0 0 10/100BaseTX Port 8/14 Name 0
5240 0 0 0 0 10/100BaseTX Port 8/13 Name 0
5230 0 1 168960 10/100BaseTX Port 8/12 Name 90
5220 0 0 348595840100BaseTX Port 8/11 Name 1
5210 0 0 0 0 10/100BaseTX Port 8/10 Name 0
5200 0 0 0 0 10/100BaseTX Port 8/9 Name 0
4890 0 0 0 0 10/100BaseTX Port 7/42 Name 0
4880 0 0 0 0 10/100BaseTX Port 7/41 Name NGSS_lines0
4870 0 0 0 0 10/100BaseTX Port 7/40 Name NGSS_trunks_reserved0
```

4860 0 0 0 0 10/100BaseTX Port 7/39 Name STORM-XTS_interlink0
4850 0 0 0 0 10/100BaseTX Port 7/38 Name NGSS_trunks_reserved0
48423744070437100110348256000100BaseTX Port 7/37 Name STORM-XTS_interlink7
12910490712521633327784217310100BaseTX Port 2/2 Name MG9K_EM476
4830 0 0 0 0 10/100BaseTX Port 7/36 Name RTP4-SPC-U1-Link10
128210873511503466113010/100BaseTX Port 2/1 Name 1
482660889650023749128010/100BaseTX Port 7/35 Name STORM-XTS6
2890 0 0 0 0 10/100BaseTX Port 4/34 Name SAM21-06_SC10
4810 0 0 0 0 10/100BaseTX Port 7/34 Name RTP4-SPC-U0-Link10
2880 0 0 0 0 10/100BaseTX Port 4/33 Name SAM21-06_SC00
4800 0 0 0 0 10/100BaseTX Port 7/33 Name STORM-XTS0
287330069782642233356833032511380100BaseTX Port 4/32 Name 428
2860 0 0 0 0 10/100BaseTX Port 4/31 Name 0
2855957699109947487316010/100BaseTX Port 4/30 Name 22
2840 0 801182880138010/100BaseTX Port 4/29 Name 27211
2837183456802286853949204604010/100BaseTX Port 4/28 Name 35
2827179367102316780945642174010/100BaseTX Port 4/27 Name 20
2817176224308945507165010/100BaseTX Port 4/26 Name 13
2807173795902331332947420628010/100BaseTX Port 4/25 Name GWC_PUBLIC_KEYMILE20
5190 0 0 0 0 10/100BaseTX Port 8/8 Name 0
5180 0 0 0 0 10/100BaseTX Port 8/7 Name 0
51764 0 0 4846230540100BaseTX Port 8/6 Name cs2kssNE1-link10
51631013431840010392294360100BaseTX Port 8/5 Name cs2kssNE1-link00
5150 0 0 4858527430100BaseTX Port 8/4 Name cs2kssNE2-link10
5141958019447003794189240100BaseTX Port 8/3 Name cs2kssNE2-link00
5130 0 0 0 0 10/100BaseTX Port 8/2 Name Alteon OAM firewall_10
51216013313090034372148060100BaseTX Port 8/1 Name AMS_0_10
4790 0 0 0 0 10/100BaseTX Port 7/32 Name MC0
4780 0 0 0 0 10/100BaseTX Port 7/31 Name CMT_interlink0
4770 0 0 0 0 10/100BaseTX Port 7/30 Name MC0
4760 0 0 0 0 10/100BaseTX Port 7/29 Name 0
4750 0 0 0 0 10/100BaseTX Port 7/28 Name 3PC0
4740 0 0 0 0 10/100BaseTX Port 7/27 Name CMT0
473868624600313533207924857010/100BaseTX Port 7/26 Name 3PC8
4720 0 0 0 0 10/100BaseTX Port 7/25 Name 0
2790 0 0 0 0 10/100BaseTX Port 4/24 Name 0
4710 0 0 0 0 10/100BaseTX Port 7/24 Name NFS0
27815537230173603922010/100BaseTX Port 4/23 Name GWC_60_Unit10

```

4700 0 0 0 0 10/100BaseTX Port 7/23 Name CBM_interlink0
2777179925300943314829010/100BaseTX Port 4/22 Name 8
2767070262100910419026010/100BaseTX Port 4/21 Name 12
2757169427501943525849010/100BaseTX Port 4/20 Name 6
2741311870029960339889010/100BaseTX Port 4/19 Name 8
2737164854900941680405010/100BaseTX Port 4/18 Name 6
2727149273200941113294010/100BaseTX Port 4/17 Name 10
2710 0 0 0 0 10/100BaseTX Port 4/16 Name GWC_47_Unit10
2700 0 0 0 0 10/100BaseTX Port 4/15 Name GWC_46_Unit10
4690 0 0 0 0 10/100BaseTX Port 7/22 Name USPc0
4680 0 0 0 0 10/100BaseTX Port 7/21 Name 0
4670 0 0 0 0 10/100BaseTX Port 7/20 Name 3PC_SC10
4660 0 0 0 0 10/100BaseTX Port 7/19 Name CBM 1 Port 10
465705637601754645230010/100BaseTX Port 7/18 Name 3PC_SC08
30313214587790035459601760100BaseTX Port 4/48 Name CICM_Client5
4640 0 0 0 0 10/100BaseTX Port 7/17 Name CBM 0 Port 10
30214207148600018449664380100BaseTX Port 4/47 Name CICM_Client3
4630 0 0 22370932150100BaseTX Port 7/16 Name cs2kprovEMS1-link01
3010 0 0 0 0 10/100BaseTX Port 4/46 Name CICM_EM0
4620 0 0 22370842230100BaseTX Port 7/15 Name cs2kprovEMS0-link03
2690 0 0 0 0 10/100BaseTX Port 4/14 Name GWC_45_Unit10
3000 0 0 0 0 10/100BaseTX Port 4/45 Name Acme_01_OAM0
4610 0 0 0 0 10/100BaseTX Port 7/14 Name MC0
2680 0 0 0 0 10/100BaseTX Port 4/13 Name GWC_44_Unit10
2670 0 0 0 0 10/100BaseTX Port 4/12 Name GWC_43_Unit10
4600 0 0 0 0 10/100BaseTX Port 7/13 Name 0
71 0 0 0 0 1000Gbic Port 1/8 Name Acme-Carrier0
2660 0 0 0 0 10/100BaseTX Port 4/11 Name 0

```

Table=End

" "

SingleValues=Begin

MeasurementKindIntervalDuration

Snapshot5

MeasureIdCaptureTimeMeasureSuppId1ValueReliability

rcStatSmltIstDownCnt2005-12-20T21:38:07EST

.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcStat.rcStatMlt1Valid

rcStatSmltSmltDownRxMsgCnt2005-12-20T21:38:07EST

.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcStat.rcStatMlt2Valid


```
sysObjectID2005-12-20T21:38:24EST.iso.org.dod.internet.mgmt.mib-2.system
.iso.org.dod.internet.private.enterprises.rapidCity.rcA8610Valid
sysDescr2005-12-20T21:38:24EST.iso.org.dod.internet.mgmt.mib-2.systemPassport-8610
(3.7.2.2)Valid
sysLocation2005-12-20T21:38:24EST.iso.org.dod.internet.mgmt.mib-2.system4655 Great
America Parkway Santa Clara CA 95054Valid
sysUpTime2005-12-20T21:38:24EST.iso.org.dod.internet.mgmt.mib-2.system2790795Valid
sysName2005-12-20T21:38:24EST.iso.org.dod.internet.mgmt.mib-2.systemSuperman-C2Valid
ipOutRequests2005-12-20T21:39:16EST.iso.org.dod.internet.mgmt.mib-2.ip103000479Valid
ipInReceives2005-12-20T21:39:16EST.iso.org.dod.internet.mgmt.mib-2.ip2639631467Valid
ipInDiscards2005-12-20T21:39:16EST.iso.org.dod.internet.mgmt.mib-2.ip0Valid
ipOutDiscards2005-12-20T21:39:16EST.iso.org.dod.internet.mgmt.mib-2.ip0Valid
snmpInvalidMsgs2005-12-20T21:37:07EST
.iso.org.dod.internet.snmpV2.snmpModules.snmpMPDMIB.snmpMPDMIBObjects.snmpMPDStats0
Valid
snmpOutPkts2005-12-20T21:37:08EST.iso.org.dod.internet.mgmt.mib-2.snmp4685310Valid
snmpOutTraps2005-12-20T21:37:08EST.iso.org.dod.internet.mgmt.mib-2.snmp0Valid
snmpInTotalSetVars2005-12-20T21:37:08EST.iso.org.dod.internet.mgmt.mib-2.snmp0Valid
snmpInPkts2005-12-20T21:37:08EST.iso.org.dod.internet.mgmt.mib-2.snmp4685410Valid
snmpInTotalReqVars2005-12-20T21:37:08EST.iso.org.dod.internet.mgmt.mib-2.snmp
20367670Valid
snmpInASNParseErrs2005-12-20T21:37:08EST.iso.org.dod.internet.mgmt.mib-2.snmp0Valid
snmpInBadVersions2005-12-20T21:37:08EST.iso.org.dod.internet.mgmt.mib-2.snmp0Valid
snmpInBadCommunityUses2005-12-20T21:37:08EST.iso.org.dod.internet.mgmt.mib-2.snmp0
Valid
rcSysBufferUtilPeakTime2005-12-20T21:37:17EST
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcSystem0Valid
rcSysSwitchFabricUtil2005-12-20T21:37:17EST
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcSystem0Valid
rcSysNVRamUsed2005-12-20T21:37:17EST
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcSystem0Valid
rcSysBufferUtilPeak2005-12-20T21:37:17EST
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcSystem0Valid
rcSysCpuUtil2005-12-20T21:37:17EST
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcSystem11Valid
rcSysBufferUtil2005-12-20T21:37:17EST
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcSystem0Valid
rcStatSmltSmltDownTxMsgCnt2005-12-20T21:38:07EST
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcStat.rcStatMlt2Valid
rcStatSmltSmltUpRxMsgCnt2005-12-20T21:38:07EST
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcStat.rcStatMlt18Valid
rcStatSmltSmltUpTxMsgCnt2005-12-20T21:38:07EST
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcStat.rcStatMlt18Valid
SingleValues=End
```

```
Entity=End  
System=End  
PMFile=End
```

GUI/CLUI Documentation for ERS 8600

GUI Launching and User procedures

- 316341-B Rev 00 - Installing and Using Device Manager
- 314723-C - Configuring Network Management

Related documentation

- 314724-C - Configuring and Managing Security
- 314997-C - Read Me for Security
- 316341-B - Installing and Using Device Manager
- 313189-D - Getting Started
- 315545-C - Managing Platform Operations and Using Diagnostics Tools
- 314723-C - Configuring Network Management
- 314721-C - Configuring BGP Services
- 316433-C - Configuring QoS and IP Filtering
- 314720-D - Configuring IP Routing Operations
- 314725-C - Configuring Layer 2 Operations: “VLANs,” Spanning “Tree,” Multilink Trunking
- 314719-C - Configuring IP Multicast Routing Protocols
- 316343-B - Configuring IGMP for User Authentication (IGAP)
- 314722-B - Configuring IPX Routing Operations
- 314995-B - Configuring the Web Switching Module with Device Manager
- 315015-C - System Messaging Platform Reference Guide
- 315023-C - 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:

- NN10202-911 - 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	NN10202-911 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 => Communication with a gateway is down.
nnExtAlarmActiveEventType => 2
nnExtAlarmActiveProbableCause => 554
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => GWC304
nnExtAlarmActiveResourceDescription => IEMS=0x00000063000000a1ac101127-GWC-
19-UNIT-1;GWC=GWC-19-UNIT-1;Version=GN090CD;Unit=unit_1;Software=SSC
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          Category: Communications^M      Cause: Communications subsystem
failure^M        Time: Jan 23 15:15:59 2004^M      Component Id: GWC=GWC-2-UNIT-
0;Version=PGC92BA;Unit=unit_0;Software=NODE^M      MTC^M      Specific Problem: EM
not responding, provisioned data loaded from local^M      Flash^M      Description:
Element Manager communication failure.^M
```

Performance

OM and PM Documentation references for GWC

- NN10208-711 - 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:

```
<TableId>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelPerfRefMIB.nnPerfMetricReferenceTable.nnPerfMetricReferenceEntry</TableId>
<CaptureTime>2004-12-15T00:11:58EST</CaptureTime>
_ <Labels>
<Label>nnPerfMetricRefIndex</Label>
<Label>nnPerfMetricName</Label>
<Label>nnPerfMetricGroup</Label>
<Label>nnPerfMetricDataType</Label>
<Label>nnPerfMetricSources</Label>
<Label>nnPerfMetricValue</Label>
</Labels>
_ <RowOfValues>
_ <RowValue>
<Value>13</Value>
</RowValue>
_ <RowValue>
<Value>Peer connections attempted during interval</Value>
</RowValue>
_ <RowValue>
<Value>Measurement</Value>
</RowValue>
_ <RowValue>
```

```
<Value>1</Value>
</RowValue>
_ <RowValue>
<Value>1</Value>
</RowValue>
_ <RowValue>
<Value>2937</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>4</Value>
</RowValue>
_ <RowValue>
<Value>Total Gateways Provisioned</Value>
</RowValue>
_ <RowValue>
<Value>Measurement</Value>
</RowValue>
_ <RowValue>
<Value>1</Value>
</RowValue>
_ <RowValue>
<Value>1</Value>
</RowValue>
_ <RowValue>
<Value>10</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>12</Value>
</RowValue>
_ <RowValue>
<Value>Peer connections completed during interval</Value>
</RowValue>
_ <RowValue>
<Value>Measurement</Value>
```

```
</RowValue>
_ <RowValue>
<Value>1</Value>
</RowValue>
_ <RowValue>
<Value>1</Value>
</RowValue>
_ <RowValue>
<Value>2936</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>11</Value>
</RowValue>
_ <RowValue>
<Value>Peer connections failed during interval</Value>
</RowValue>
_ <RowValue>
<Value>Communications</Value>
</RowValue>
_ <RowValue>
<Value>1</Value>
</RowValue>
_ <RowValue>
<Value>1</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>1</Value>
</RowValue>
_ <RowValue>
<Value>Large GWs in Disabled State</Value>
</RowValue>
```

```
_ <RowValue>
<Value>Communications</Value>
</RowValue>
_ <RowValue>
<Value>1</Value>
</RowValue>
_ <RowValue>
<Value>1</Value>
</RowValue>
_ <RowValue>
<Value>8</Value>
</RowValue>
</RowOfValues>
</Table>
```

CSV

The following is an example of performance data for GWC in CSV format:

PMFile=Begin
 MeasurementCategory noNamespaceSchemaLocation FileCreationTime
 PM commonPerfRecord_V2.0.xsd 2005-06-29T06:30:06EST

System=Begin
 SystemId
 NortelNetworks/IEMS

Entity=Begin
 EntityId
 47.165.172.140-GWC-212

TableId	MeasurementKind	IntervalDuration	CaptureTime
.iso.org.dod.internet.private.e nterprises.nortel.nortelGener icMIBs.nortelPerfRefMIB.nn PerfMetricReferenceTable.n	Snapshot	5	2005-06-29T06:30:01EST
Label	Label	Label	Label
nnPerfMetricRefIndex	nnPerfMetricName	nnPerfMetricGroup	nnPerfMetricValue
Value	Value	Value	Value
	17 Calls failed for MP: MP2	Measurement	0
	16 Calls passed for MP: MP2	Measurement	0
	15 Total Media Proxies Provisioned	Measurement	1
	14 Media Proxies in Disabled State	Communications	0
	Media Proxy calls failed during		
	97 interval for GWC	Measurement	0
	4 Total Gateways Provisioned	Measurement	2
	Media Proxy calls passed during		
	96 interval for GWC	Measurement	0
	2 Trunk GWs in Disabled State	Communications	0

Table=End

Entity=End

System=End

PMFile=End

GUI/CLUI Documentation for GWC

GUI Launching and User procedures

- NN10189-111 - GWC Basics
- NN10205-511 - GWC Configuration Management
- NN10213-611 - GWC Security and Administration

Related documents

Keymile UNEM and UMUX

Keymile UNEM and UMUX Fault Interface

This section provides references to customer documentation for Fault, Performance, Topology, GUI/CLUI, and Security for Keymile UNEM and UMUX.

Fault documentation for Keymile UNEM and UMUX:

- KEYMILE001, Keymile Documentation and Support

Fault Mapping for Keymile UNEM and UMUX

The following criteria can be used for looking up information on specific faults for Keymile UNEM and UMUX devices.

Table 1 Fault Correlation for Keymile Traps

Trap Name	Log Name & No.	Document Reference
alarmRaisedTrap (communicationAlarm)	UMUX300 UNEM300	Keymile UMUX User's Guide Keymile UNEM User's Guide
alarmRaisedTrap (equipmentAlarm)	UMUX301 UNEM301	Keymile UMUX User's Guide Keymile UNEM User's Guide
alarmRaisedTrap (environmentalAlarm)	UMUX302 UNEM302	Keymile UMUX User's Guide Keymile UNEM User's Guide
alarmRaisedTrap (processingErrorAlarm)	UMUX303 UNEM303	Keymile UMUX User's Guide Keymile UNEM User's Guide
alarmRaisedTrap (qualityOfServiceAlarm)	UMUX304 UNEM304	Keymile UMUX User's Guide Keymile UNEM User's Guide
alarmClearedTrap	UMUX500 UNEM500	Keymile UMUX User's Guide Keymile UNEM User's Guide
neOpStatModified trap	UMUX501	Keymile UNEM User's Guide
nePollStatModified	UMUX502	Keymile UNEM User's Guide
alarmAckTrap	UMUX600 UNEM600	Keymile UMUX User's Guide Keymile UNEM User's Guide

Trap Name	Log Name & No.	Document Reference
neAdded	UMUX601	Keymile UNEM User's Guide
neDeleted	UMUX602	Keymile UNEM User's Guide
neNameModified	UMUX603	Keymile UNEM User's Guide
cardAdded	UMUX604	Keymile UMUX User's Guide
cardDeleted	UMUX605	Keymile UMUX User's Guide

Northbound Fault Formats for Keymile

SCC2

The following is an example of a Keymile log in SCC2 format:

```
54 UMUX601 0023 INFO UMUX Added
    Location: OTT_UMUX_TESTING
    State: INFO
    Time: Mar 31 03:54:48 2005
    Component Id: OTT_UMUX_TESTING 47.134. 44.110
    Description: OTT_UMUX_TESTING NE Added
```

```
**46 UMUX300 0009 TBL UMUX FLT
    Location: OTT_UMUX_1200
    Notification ID: 0
    State: Raised
    Category: communication
    Cause: others
    Time: Mar 17 13:46:27 2005
    Component Id: LOMIF <12> 2Mbit/s-1 / E12
    Specific Problem: others
    Description: Loss of Signal
```

NTSTD

The following is an example of a Keymile log in NTSTD format:

```
wnc0s0jn UMUX601 MAR29 05:35:35 INFO UMUX Added
    Location: OTT_UMUX_1200_Test
```

```

State: INFO
Time: Mar 29 05:35:35 2005
Component Id: OTT_UMUX_1200_Test797322492
Description: OTT_UMUX_1200_Test NE Added

```

```
wnc0s0jn *** UMUX300 MAR29 05:09:44 0482 TBL UMUX FLT
```

```

Location: OTT_UMUX_1200
Notification ID: 0
State: Raised
Category: communication
Cause: others
Time: Mar 29 05:09:44 2005
Component Id: LOMIF <12> 2Mbit/s-1 / E12
Specific Problem: others
Description: AIS Received

```

SNMP

The following is an example of a Keymile log in SNMP format:

```

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 2 hours, 48 minutes, 38
seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.306:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.1: STRING: .0.0:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.2: STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-37;;
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.3: STRING: ^G^E,^F^B:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.4: STRING: UMUX601:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.5: STRING: 44 UMUX601 0047 INFO UMUX
Added :
UMUX_TESTING( 10. 10. 1. 1) NE Added :

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 3 hours, 11 minutes, 8
seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.305:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.10: STRING:
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.18.50.48.48.53.45.5
2.45.56.44.54.58.51.52.58.48.46.48.44.23905:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.12: 07 d5 04 08 06 22 00 00:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.11: STRING: DeviceSpecificInfo=;AIS Received:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.1: INTEGER: 5:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.2: INTEGER: 1024:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.3: STRING: :
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.4: STRING: UMUX300:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.5: STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-15;;

```

```
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.6:  INTEGER:  1:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.7:  INTEGER: 16:
```

Syslog

The following is an example of a Keymile log in Syslog format:

```
Apr  8 00:59:37 wnc0s0jn IEMS: _V2_~I=~H=wnc0s0jn~A=IEMS~S=9434~~ UMUX601 NONE INFO
UMUX Added^M      Location: MYTest^M      State: INFO^M      Time: Apr 08 00:59:37
2005^M            Component Id: MYTest 10.  1.  5.  1^M      Description: MYTest NE Added
```

```
Apr  8 01:27:24 wnc0s0jn IEMS: _V2_~I=~H=wnc0s0jn~A=IEMS~S=9447~~ UMUX300 CRIT TBL
UMUX FLT^M        Location: OTT_UMUX_1200^M      Notification ID: 0^M      State:
Raised^M          Category: communication^M      Cause: others^M      Time: Apr 08
01:54:45 2005^M    Component Id: LOMIF <12> 2Mbit/s-1 / E12^M      Specific
Problem:  others^M      Description: AIS Received
```

Performance

Performance metrics are not available through the IEMS. Please refer to the Keymile UNEM User's Guide.

GUI Documentation for Keymile

GUI Launching and User procedures

- Keymile UNEM UNEM User's Guide
- Keymile UCST System Operation Basics

Media Application Server (MAS)

MAS Fault Interface

This section provides references to customer documentation for Fault Management for MAS.

Fault documentation for MAS:

- NN10383-900 - Fault Management: Alarm and Logs
- NN10375-113 - MAS Unified Communications Service Guide

- NN100388-111 - MAS Ad Hoc Audio Conferencing Service Guide
- NN10433-111 - MAS Meet Me Audio Conferencing Service Guide
- NN10429-113 - MAS IM Chat Service Guide
- NN10430-113 - MAS Music On Hold Service Guide
- NN10428-113 - MAS Announcements Service Guide

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	NN10383-900 - Fault Manage- ment: Alarm and Logs Also refer to the documents listed above

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 =>
```

```
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48  
.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

- NN10384-700 - Performance Management: OM

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,commonPerfRecord_V2.0.xsd,2004-07-02T05:55:54EST
System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId
47.104.11.120

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

- NN10006-100 - MCS 5200 Basics

Related Documents

None

Multimedia Communication Server (MCS)

MCS Fault Interface

This section provides references to customer documentation for Fault Management for MCS.

Fault documentation for MCS:

- NN10383-900, Fault Management: Alarm and Log

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	Event Id Logname and Log number	Event Id Logname and Log number	Event Id Logname and Log number	Event Id Logname and Log number	NN10383-900, Fault Management: Alarm and Log

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 failu
re;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 => 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.Service
s.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

- NN10384-700 - Performance Management: OM

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 MAS in CSV format:

Not available at time of publication

GUI/CLUI Documentation for MCS

GUI Launching and User procedures

- NN10006-100 - MCS 5200 Basics
- NN10247-111 - Multimedia Communication Server 5200 System Management Console User Guide

Related Documents

None

Media Gateway 3200 (MG 3200)

MG3200 Fault Interface

This section provides references to customer documentation for Fault Management for MG 3200.

Fault documentation for MG3200:

LTRT-72704: Media Gateway MG3200 H.248 User's Manual

Fault Mapping for MG3200

The following criteria can be used for looking up information on specific faults for MG3200.

Fault Correlation for MG 3200

Trap Name	LogKey	Customer Doc Ref (Media Gateway MG3200 H.248 User's Manual: LTRT-72704)
acBoardFatalError	MGTH301	Appendix I
acBoardConfigurationError	MGTH302	Appendix I
acBoardTemperatureAlarm	MGTH303	Appendix I
acBoardEvBoardStarted	MGTH500	Appendix I
acBoardEvResettingBoard	MGTH300	Appendix I
acgwAdminStateChange	MGTH501	Appendix I
acBoardEthernetLinkAlarm	MGTH307	Appendix I
acActiveAlarmTableOverflow	MGTH309	Appendix I
acOperationalStateChange	MGTH312	Appendix I
acKeepAlive	MGTH313	Appendix I
acNATTraversalAlarm	MGTH314	Appendix I
acEnhancedBITStatus	MGTH600	Appendix I
acPerformanceMonitoringThresholdCrossing	MGTH800	Appendix I
dsx1LineStatusChange	MGTH601	Appendix I

coldStart	Will not be sent to NB All prior alarms from the device will be cleared and "Re-sync" operation will be invoked as the device has been reset.	Appendix I
authenticationFailure	Will not be sent to NB	Appendix I

Northbound Fault Formats for MG 3200

SCC2

The following is an example of a MG 3200 Board Resetting log in SCC2 format:

*C36 MGTH300 0123 FLT MG3200 INFO

Location: mg32;47.142.106.106

State: Raised

Category: equipment

Cause: outOfService

Time: Mar 05 21:36:09 2000

Component Id: Board#1

Trap Name: 4

Description: User resetting board

NTStd

The following is an example of a MG 3200 Board Resetting Alarm log in NTStd format:

wnc0s0jn *** MGTH300 MAR05 21:40:04 0003 FLT MG3200 INFO

Location: mg32;47.142.106.106

State: Raised

Category: equipment

Cause: outOfService

Time: Mar 05 21:40:04 2000

Component Id: Board#1

Trap Name: 4

Description: User resetting board

SNMP

The following is an example of a MG 3200 Board Resetting Alarm log in SNMP format:

```
.1.3.6.1.2.1.1.3.0: 2 hours, 42 minutes, 17 seconds. ,
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.562.29.6.1.0.305,
.1.3.6.1.2.1.118.1.2.2.1.10:
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48.48.48.45.51.45
.53.44.56.58.51.52.58.53.49.46.48.44.4433,
.1.3.6.1.2.1.118.1.2.2.1.2: 7 d0 3 5 8 22 33 0 ,
.1.3.6.1.2.1.118.1.2.2.1.11: User resetting board,
.1.3.6.1.4.1.562.29.6.1.1.1.1: 4,
.1.3.6.1.4.1.562.29.6.1.1.1.2: 612,
.1.3.6.1.4.1.562.29.6.1.1.1.3: ,
.1.3.6.1.4.1.562.29.6.1.1.1.4: MGTH300 ,
.1.3.6.1.4.1.562.29.6.1.1.1.5: IEMS=47.142.106.106-MG_3200;Board#1,
.1.3.6.1.4.1.562.29.6.1.1.1.6: 4,
.1.3.6.1.4.1.562.29.6.1.1.1.7: 645
```

Syslog

The following is an example of a MG 3200 Board Started log in Syslog format:

```
Apr 13 11:16:37 wnc0s0jn IEMS: _V2_~I=~H=wnc0s0jn~A=IEMS~S=5565~~ MGTH300
CRIT F
```

```
LT MG3200 FAULT^M      Location: mg32;47.142.106.106^M      State: Raised^M
      Category: equipment^M      Cause: outOfService^M      Time: Mar 05 2
1:45:21 2000^M      Component Id: Board#1^M      Trap Name: 4^M      Descr
ption: User resetting board
```

The following is an example of a MG 3200 dsx1LineStatusChange log in Syslog format:

```
Apr 13 10:39:07 wnc0s0jn IEMS: _V2_~I=~H=wnc0s0jn~A=IEMS~S=2520~~ MGTH601
NONE I
```

NFO ^M Location: 47.142.106.106^M Event: .1.3.6.1.2.1.10.18.15.0.
 1^M Varbind0: .1.3.6.1.2.1.1.3.0: 382^M Varbind1: .1.3.6.1.6.3.1.1
 .4.1.0: .1.3.6.1.2.1.10.18.15.0.1^M Varbind2: .1.3.6.1.2.1.10.18.6.1.10.5
 : 2

Performance

OM and PM Documentation references for MG 3200

LTRT-72704: Media Gateway MG3200 H.248 User's Manual

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 3200 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="commonPerfRecord_V2.0.xsd" MeasurementCategory="PM">
<FileCreationTime>2005-05-13T11:53:53EST</FileCreationTime>
_ <System>
<SystemId>NortelNetworks/IEMS</SystemId>
_ <Entity>
<EntityId>47.142.106.106</EntityId>
_ <SingleValues MeasurementKind="Snapshot" IntervalDuration="1440">
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>snmpOutPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>6399</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>sysDescr</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.system</MeasureSuppId1>
<Value>Product: Mediant 2000;SW Version: 4.60D.007.002</Value>
```

```
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>snmpInBadVersions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>snmpInBadCommunityNames</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>snmpInTotalReqVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>7415</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>snmpOutTraps</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>1140</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>snmpInBadCommunityUses</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
```

```
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>snmpInPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>5260</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>snmpInTotalSetVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>82</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>snmpInASNParseErrs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>tcpOutSegs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.tcp</MeasureSuppId1>
<Value>21</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>tcpInSegs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.tcp</MeasureSuppId1>
<Value>26</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>udpOutDatagrams</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.udp</MeasureSuppId1>
```

```
<Value>54156</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>udpInDatagrams</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.udp</MeasureSuppId1>
<Value>901</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>snmpSilentDrops</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfCpMessageSendSuccesses</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfCp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfCpMessagesFromUntrustedSources</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfCp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfCpMessageRetransmissions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfCp</MeasureSuppId1>
<Value>292690</Value>
```

```
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfCpMessageSendErrors</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfCp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfCpMessageMaxRetransmissionsExceeded</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfCp</MeasureSuppId1>
<Value>41812</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfCpMessageReceiveSuccesses</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfCp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfCpNumDupsForCompletedTransactions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfCp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfCpMessageReceiveErrors</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfCp</MeasureSuppId1>
<Value>0</Value>
```

```
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfCpNumDupsForOutstandingTransactions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfCp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfCpProtocolSyntaxErrors</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfCp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpSimplexInSessionsCurrent</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpReceiverOctets</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpSimplexOutSessionsTotal</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
```



```
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpRcvrLostPackets</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpSimplexOutSessionsCurrent</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpSenderPackets</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpFailedDueToLackOfResources</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpDuplexSessionsTotal</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
```

```
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpSenderOctets</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpSimplexInSessionsTotal</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpDuplexSessionsCurrent</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpReceiverPackets</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfSystemPacketEndpoints</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfSystem</MeasureSuppId1>
<Value>300</Value>
```

```

<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfSystemPacketEndpointsInUse</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfSystem</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
</SingleValues>
</Entity>
</System>
</PMFile>

```

CSV

The following is an example of Performance data for MG 3200 in CSV format:

```

PMFile=Begin
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonPerfRecord_V2.0.xsd,2005-05-13T11:52:35EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId
47.142.106.106

SingleValues=Begin
MeasurementKind,IntervalDuration
Snapshot,1440
MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability
snmpOutPkts,2005-05-13T11:52:33EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,6391,Valid
sysDescr,2005-05-13T11:52:32EST,.iso.org.dod.internet.mgmt.mib-
2.system,Product: Mediant 2000;SW Version: 4.60D.007.002,Valid
snmpInBadVersions,2005-05-13T11:52:33EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid
snmpInBadCommunityNames,2005-05-
13T11:52:33EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid

```

snmpInTotalReqVars, 2005-05-13T11:52:33EST, .iso.org.dod.internet.mgmt.mib-2.snmp, 7376, Valid
snmpOutTraps, 2005-05-13T11:52:33EST, .iso.org.dod.internet.mgmt.mib-2.snmp, 1140, Valid
snmpInBadCommunityUses, 2005-05-13T11:52:33EST, .iso.org.dod.internet.mgmt.mib-2.snmp, 0, Valid
snmpInPkts, 2005-05-13T11:52:33EST, .iso.org.dod.internet.mgmt.mib-2.snmp, 5252, Valid
snmpInTotalSetVars, 2005-05-13T11:52:33EST, .iso.org.dod.internet.mgmt.mib-2.snmp, 82, Valid
snmpInASNParseErrs, 2005-05-13T11:52:33EST, .iso.org.dod.internet.mgmt.mib-2.snmp, 0, Valid
tcpOutSegs, 2005-05-13T11:52:33EST, .iso.org.dod.internet.mgmt.mib-2.tcp, 21, Valid
tcpInSegs, 2005-05-13T11:52:33EST, .iso.org.dod.internet.mgmt.mib-2.tcp, 26, Valid
udpOutDatagrams, 2005-05-13T11:52:33EST, .iso.org.dod.internet.mgmt.mib-2.udp, 54145, Valid
udpInDatagrams, 2005-05-13T11:52:33EST, .iso.org.dod.internet.mgmt.mib-2.udp, 901, Valid
snmpSilentDrops, 2005-05-13T11:52:34EST, .iso.org.dod.internet.mgmt.mib-2.snmp, 0, Valid
acPerfCpMessageSendSuccesses, 2005-05-13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp, 0, Valid
acPerfCpMessagesFromUntrustedSources, 2005-05-13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp, 0, Valid
acPerfCpMessageRetransmissions, 2005-05-13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp, 292674, Valid
acPerfCpMessageSendErrors, 2005-05-13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp, 0, Valid
acPerfCpMessageMaxRetransmissionsExceeded, 2005-05-13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp, 41810, Valid
acPerfCpMessageReceiveSuccesses, 2005-05-13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp, 0, Valid
acPerfCpNumDupsForCompletedTransactions, 2005-05-13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp, 0, Valid
acPerfCpMessageReceiveErrors, 2005-05-13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp, 0, Valid

acPerfCpNumDupsForOutstandingTransactions, 2005-05-
13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfCp, 0, Valid
acPerfCpProtocolSyntaxErrors, 2005-05-
13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfCp, 0, Valid
acPerfRtpSimplexInSessionsCurrent, 2005-05-
13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp, 0, Valid
acPerfRtpReceiverOctets, 2005-05-
13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp, 0, Valid
acPerfRtpSimplexOutSessionsTotal, 2005-05-
13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp, 0, Valid
acPerfRtpRcvrLostPackets, 2005-05-
13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp, 0, Valid
acPerfRtpSimplexOutSessionsCurrent, 2005-05-
13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp, 0, Valid
acPerfRtpSenderPackets, 2005-05-
13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp, 0, Valid
acPerfRtpFailedDueToLackOfResources, 2005-05-
13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp, 0, Valid
acPerfRtpDuplexSessionsTotal, 2005-05-
13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp, 0, Valid
acPerfRtpSenderOctets, 2005-05-
13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp, 0, Valid
acPerfRtpSimplexInSessionsTotal, 2005-05-
13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp, 0, Valid
acPerfRtpDuplexSessionsCurrent, 2005-05-
13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp, 0, Valid
acPerfRtpReceiverPackets, 2005-05-
13T11:52:34EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp, 0, Valid
acPerfSystemPacketEndpoints, 2005-05-
13T11:52:35EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfSystem, 300, Valid

```
acPerfSystemPacketEndpointsInUse,2005-05-  
13T11:52:35EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor  
mances.acPerfMediaGateway.acPerfSystem,0,Valid  
SingleValues=End
```

```
Entity=End
```

```
System=End
```

```
PMFile=End
```

GUI/CLUI Documentation for MG 3200

Reference the LTRT-72704: Media Gateway MG3200 H.248 User's Manual for information about launching the MG 3200 configuration GUI. GUI Launching and User procedures

Related documents

Other customer documents related to the MG 3200 are:

- LTRT73804, MG 3200 H.248 SIP Fast Track Installation Guide
- LTRT72904, MG 3200 Configuration Guide

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
- NN10409-500 ATM/IP Solution-level 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	NN10074- 911 MG9000 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:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<PMFile xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonPerfRecord_V2.0.xsd" MeasurementCategory="PM">
<FileCreationTime>2005-01-18T15:45:34EST</FileCreationTime>
<System>
<SystemId>NortelNetworks/IEMS</SystemId>
<Entity>
<EntityId>172.31.125.226</EntityId>
<SubEntity>
<SubEntityId>172.31.125.226</SubEntityId>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnMegacoOMECANIntervalTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnMegacoOMECANnumResrceReq</Label>
<Label>nnMegacoOMECANnumResrceReqFail</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot17</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot5</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot13</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
```

```
<RowValue>
<Value>Frame008.Shelf1.Slot12</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnMegacoOMDSPIntervalTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnMegacoOMDSPnumCMRmodemReq</Label>
<Label>nnMegacoOMDSPnumCMRmodemReqFail</Label>
<Label>nnMegacoOMDSPnumToneGenReq</Label>
<Label>nnMegacoOMDSPnumToneGenReqFail</Label>
<Label>nnMegacoOMDSPnumToneRcvrReq</Label>
<Label>nnMegacoOMDSPnumToneRcvrReqFail</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot17</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot5</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowValue>
```

```
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot13</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot12</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnMegacoQoSIntervalTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnMegacoQoSIntervalBadCalls</Label>
<Label>nnMegacoQoSIntervalCalls</Label>
<Label>nnMegacoQoSIntervalJitter</Label>
<Label>nnMegacoQoSIntervalLatency</Label>
<Label>nnMegacoQoSIntervalPktLossPct</Label>
<Label>nnMegacoQoSIntervalPktsLost</Label>
<Label>nnMegacoQoSIntervalPktsRecvd</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4.Port1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16.Port1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
```



```
<RowValue>
<Value>Frame008.Shelf1.Slot12.Port1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnIpsecOmIntervalTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnIpsecConfigInterfaceId</Label>
<Label>nnIpsecConfigSecLinkId</Label>
<Label>nnIpsecOmIntervalPacketsDiscardedIn</Label>
<Label>nnIpsecOmIntervalPacketsDiscardedOut</Label>
<Label>nnIpsecOmIntervalPacketsRx</Label>
<Label>nnIpsecOmIntervalPacketsTx</Label>
</Labels>
```

```
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot17</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot5</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
```

```
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot13</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot12</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot11</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot10</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnPmOvldRscIntervTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
```

```
<Label>nnPmOvldRscIntervChvMsgRAvg</Label>
<Label>nnPmOvldRscIntervChvMsgRPeak</Label>
<Label>nnPmOvldRscIntervConQDelAvg</Label>
<Label>nnPmOvldRscIntervConQDelPeak</Label>
<Label>nnPmOvldRscIntervCpuUtilAvg</Label>
<Label>nnPmOvldRscIntervCpuUtilPeak</Label>
<Label>nnPmOvldRscIntervPduRateAvg</Label>
<Label>nnPmOvldRscIntervPduRatePeak</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot17</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>514</Value>
</RowValue>
<RowValue>
<Value>552</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>6</Value>
</RowValue>
</RowOfValues>
```

```
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>494</Value>
</RowValue>
<RowValue>
<Value>498</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot5</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1</Value>
```



```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>435</Value>
</RowValue>
<RowValue>
<Value>449</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>6</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>451</Value>
```

```
</RowValue>
<RowValue>
<Value>476</Value>
</RowValue>
<RowValue>
<Value>6</Value>
</RowValue>
<RowValue>
<Value>8</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot13</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
<RowValue>
<Value>545</Value>
</RowValue>
<RowValue>
<Value>567</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>6</Value>
```

```
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot12</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>591</Value>
</RowValue>
<RowValue>
<Value>649</Value>
</RowValue>
<RowValue>
<Value>6</Value>
</RowValue>
<RowValue>
<Value>9</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot11</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>428</Value>
</RowValue>
<RowValue>
<Value>483</Value>
</RowValue>
<RowValue>
<Value>17</Value>
</RowValue>
<RowValue>
<Value>27</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot10</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>554</Value>
</RowValue>
<RowValue>
<Value>995</Value>
</RowValue>
<RowValue>
<Value>17</Value>
</RowValue>
<RowValue>
<Value>25</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnBwShelfIntervalSloaBandwResrvdTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnBwShelfIntervalSloaBandwReserved</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1</Value>
</RowValue>
<RowValue>
<Value>897</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>sonetPathIntervalTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>sonetPathIntervalCVs</Label>
<Label>sonetPathIntervalESs</Label>
<Label>sonetPathIntervalSEs</Label>
```

```
<Label>sonetPathIntervalUASs</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot11.Port1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot10.Port1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
```

```
<TableId>nnBwAbiIntervalBandwResrvdEntry</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnBwAbiIntervalBandwReserved</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot17</Value>
</RowValue>
<RowValue>
<Value>6000</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16</Value>
</RowValue>
<RowValue>
<Value>7000</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot5</Value>
</RowValue>
<RowValue>
<Value>6612</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4</Value>
</RowValue>
<RowValue>
<Value>7000</Value>
</RowValue>
</RowOfValues>
```

```
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnPmUtilOmIntervTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnPmUtilIntervChanAvg</Label>
<Label>nnPmUtilIntervChanPeak</Label>
<Label>nnPmUtilIntervCpuAvg</Label>
<Label>nnPmUtilIntervCpuPeak</Label>
<Label>nnPmUtilIntervFlashAvg</Label>
<Label>nnPmUtilIntervFlashPeak</Label>
<Label>nnPmUtilIntervRamAvg</Label>
<Label>nnPmUtilIntervRamPeak</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot5</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>4</Value>
</RowValue>
<RowValue>
<Value>4</Value>
</RowValue>
<RowValue>
<Value>17</Value>
</RowValue>
<RowValue>
<Value>17</Value>
</RowValue>
<RowValue>
```



```
<Value>32</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>17</Value>
</RowValue>
<RowValue>
<Value>17</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot17</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>6</Value>
</RowValue>
<RowValue>
<Value>17</Value>
</RowValue>
<RowValue>
<Value>17</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>5</Value>
```

```
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>17</Value>
</RowValue>
<RowValue>
<Value>17</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot15</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>19</Value>
</RowValue>
<RowValue>
<Value>19</Value>
```

```
</RowValue>
<RowValue>
<Value>36</Value>
</RowValue>
<RowValue>
<Value>36</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot14</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>18</Value>
</RowValue>
<RowValue>
<Value>18</Value>
</RowValue>
<RowValue>
<Value>36</Value>
</RowValue>
<RowValue>
<Value>36</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
```

```
<RowValue>
<Value>Frame008.Shelf1.Slot13</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>6</Value>
</RowValue>
<RowValue>
<Value>24</Value>
</RowValue>
<RowValue>
<Value>24</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot12</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>6</Value>
</RowValue>
<RowValue>
<Value>6</Value>
</RowValue>
<RowValue>
<Value>24</Value>
</RowValue>
<RowValue>
<Value>24</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot11</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>4</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>47</Value>
</RowValue>
```

```
<RowValue>
<Value>47</Value>
</RowValue>
<RowValue>
<Value>37</Value>
</RowValue>
<RowValue>
<Value>37</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot10</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>6</Value>
</RowValue>
<RowValue>
<Value>10</Value>
</RowValue>
<RowValue>
<Value>23</Value>
</RowValue>
<RowValue>
<Value>23</Value>
</RowValue>
<RowValue>
<Value>38</Value>
</RowValue>
<RowValue>
<Value>38</Value>
</RowValue>
```

```
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnRelMsgSctpAssocOmIntervTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnRelMsgSctpAscIntervAbort</Label>
<Label>nnRelMsgSctpAscIntervClosed</Label>
<Label>nnRelMsgSctpAscIntervCongCleared</Label>
<Label>nnRelMsgSctpAscIntervCongCount</Label>
<Label>nnRelMsgSctpAscIntervDiscPacks</Label>
<Label>nnRelMsgSctpAscIntervInPacks</Label>
<Label>nnRelMsgSctpAscIntervOutPacks</Label>
<Label>nnRelMsgSctpAscIntervRetranPacks</Label>
<Label>nnRelMsgSctpAscIntervT1expires</Label>
<Label>nnRelMsgSctpAscIntervT2expires</Label>
<Label>nnRelMsgSctpAscIntervT3expires</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot17</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```



```
<RowValue>
<Value>467</Value>
</RowValue>
<RowValue>
<Value>487</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowValue>
```

```
<RowValue>
<Value>465</Value>
</RowValue>
<RowValue>
<Value>485</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot5</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>761</Value>
</RowValue>
<RowValue>
<Value>697</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowValue>
```

```
<RowValue>
<Value>792</Value>
</RowValue>
<RowValue>
<Value>726</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>sonetLineIntervalTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>sonetLineIntervalCVs</Label>
<Label>sonetLineIntervalESS</Label>
<Label>sonetLineIntervalSESS</Label>
<Label>sonetLineIntervalUASS</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot11.Port1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot10.Port1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnMegacoOMCESIntervalTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnMegacoOMCESnumChnlAllocInter</Label>
<Label>nnMegacoOMCESnumChnlAllocInterFail</Label>
<Label>nnMegacoOMCESnumChnlAllocIntra</Label>
<Label>nnMegacoOMCESnumChnlAllocIntraFail</Label>
</Labels>
<RowOfValues>
```

```
<RowValue>
<Value>Frame008.Shelf1.Slot17</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot5</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot13</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot12</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot11</Value>
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```



```
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot10</Value>
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnBwAbiCurrentBandwResrvdTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnBwAbiCapacityBandwReserved</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot17</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
```

```
<RowValue>
<Value>Frame008.Shelf1.Slot16</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot5</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>sonetSectionIntervalTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>sonetSectionIntervalCVs</Label>
<Label>sonetSectionIntervalESs</Label>
<Label>sonetSectionIntervalSEFSs</Label>
<Label>sonetSectionIntervalSESSs</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot11.Port1</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot10.Port1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnClkSyncRefTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnClkSyncRefId</Label>
<Label>nnClkSyncRefLossOfFrameCount</Label>
```

```
<Label>nnClkSyncRefLossOfSignalCount</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot13</Value>
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot12</Value>
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnBwShelfCurrentSloaBandwResrvdTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnBwShelfCapacitySloaBandwReserved</Label>
</Labels>
```

```
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1</Value>
</RowValue>
<RowValue>
<Value>48960</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>norCarrSonetMediumIntervalTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnorCarrSonetMedIntervalLBC</Label>
<Label>norCarrSonetMedIntervalOpt</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot11.Port1</Value>
</RowValue>
<RowValue>
<Value>106</Value>
</RowValue>
<RowValue>
<Value>99</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot10.Port1</Value>
</RowValue>
<RowValue>
<Value>103</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
```

```
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnPmOvldConnDenyIntervTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnPmOvldConnDenyIntervCount</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot17</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot5</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot13</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot12</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot11</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot10</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>apsChanStatusTable</TableId>
```

```
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>apsChanSignalDegrades</Label>
<Label>apsChanSignalFailures</Label>
<Label>apsChanSwitchovers</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot11.Port1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot10.Port1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnMegacoOMMedGwyIntervalTable</TableId>
```



```
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnMegacoOMMedGwyAvrgInMsgRate</Label>
<Label>nnMegacoOMMedGwyAvrgOutMsgRate</Label>
<Label>nnMegacoOMMedGwyMaxInMsgRate</Label>
<Label>nnMegacoOMMedGwyMaxOutMsgRate</Label>
<Label>nnMegacoOMMedGwyNumInMessages</Label>
<Label>nnMegacoOMMedGwyNumInOctets</Label>
<Label>nnMegacoOMMedGwyNumOutMessages</Label>
<Label>nnMegacoOMMedGwyNumOutOctets</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4.Port1</Value>
</RowValue>
<RowValue>
<Value>29</Value>
</RowValue>
<RowValue>
<Value>29</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>438</Value>
</RowValue>
<RowValue>
<Value>25752</Value>
</RowValue>
<RowValue>
<Value>438</Value>
</RowValue>
<RowValue>
```

```
<Value>36018</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16.Port1</Value>
</RowValue>
<RowValue>
<Value>29</Value>
</RowValue>
<RowValue>
<Value>29</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>440</Value>
</RowValue>
<RowValue>
<Value>25867</Value>
</RowValue>
<RowValue>
<Value>440</Value>
</RowValue>
<RowValue>
<Value>33229</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot12.Port1</Value>
</RowValue>
<RowValue>
<Value>53</Value>
```

```
</RowValue>
<RowValue>
<Value>53</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>805</Value>
</RowValue>
<RowValue>
<Value>50834</Value>
</RowValue>
<RowValue>
<Value>805</Value>
</RowValue>
<RowValue>
<Value>52001</Value>
</RowValue>
</RowOfValues>
</Table>
<SingleValues MeasurementKind="Snapshot" IntervalDuration="15">
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>snmpInvalidMsgs</MeasureId>
<MeasureSuppId1>Miscellaneous</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>snmpInBadCommunityNames</MeasureId>
<MeasureSuppId1>Miscellaneous</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
```

```
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>snmpInPkts</MeasureId>
<MeasureSuppId1>Miscellaneous</MeasureSuppId1>
<Value>124921</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnPmSnmpIntervReqPeak</MeasureId>
<MeasureSuppId1>nnPmSnmpOmIntervTable</MeasureSuppId1>
<Value>40</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnPmSnmpIntervReqAvg</MeasureId>
<MeasureSuppId1>nnPmSnmpOmIntervTable</MeasureSuppId1>
<Value>126</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnPmSnmpIntervNotifPeak</MeasureId>
<MeasureSuppId1>nnPmSnmpOmIntervTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnPmSnmpIntervNotifAvg</MeasureId>
<MeasureSuppId1>nnPmSnmpOmIntervTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
```

```
<MeasureId>nnClkSyncSignalId</MeasureId>
<MeasureSuppId1>nnClkSyncSignalTable</MeasureSuppId1>
<Value>5</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnClkSyncSignalLossOfSignalCount</MeasureId>
<MeasureSuppId1>nnClkSyncSignalTable</MeasureSuppId1>
<Value>3</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnClkSyncSignalLossOfFrameCount</MeasureId>
<MeasureSuppId1>nnClkSyncSignalTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwBandwUtilIntervalInCellRate</MeasureId>
<MeasureSuppId1>nnBwIntervalBandwUtilTable</MeasureSuppId1>
<Value>878</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwBandwUtilIntervalOutCellRate</MeasureId>
<MeasureSuppId1>nnBwIntervalBandwUtilTable</MeasureSuppId1>
<Value>936</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwBandwUtilIntervalInDslCellRate</MeasureId>
<MeasureSuppId1>nnBwIntervalBandwUtilTable</MeasureSuppId1>
<Value>0</Value>
```

```
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwBandwUtilIntervalOutDslCellRate</MeasureId>
<MeasureSuppId1>nnBwIntervalBandwUtilTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwQueueFillIntervalTotal</MeasureId>
<MeasureSuppId1>nnBwIntervalQueueFillTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwQueueFillIntervalCbr</MeasureId>
<MeasureSuppId1>nnBwIntervalQueueFillTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwQueueFillIntervalRtVbr</MeasureId>
<MeasureSuppId1>nnBwIntervalQueueFillTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwQueueFillIntervalNrtVbr</MeasureId>
<MeasureSuppId1>nnBwIntervalQueueFillTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
```

```

<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwQueueFillIntervalUbr</MeasureId>
<MeasureSuppId1>nnBwIntervalQueueFillTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwQueueFillIntervalUbrPlus</MeasureId>
<MeasureSuppId1>nnBwIntervalQueueFillTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwQueueFillIntervalControl</MeasureId>
<MeasureSuppId1>nnBwIntervalQueueFillTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
</SingleValues>
</SubEntity>
</Entity>
</System>
</PMFile>

```

CSV

The following is an example of Performance data for MG 9000 in CSV format:

```

PMFile=Begin
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonPerfRecord_V2.0.xsd,2005-03-22T15:37:33EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId
10.32.128.11

```

SubEntity=Begin

SubEntityId

10.32.128.11

Table=Begin

TableId,MeasurementKind,IntervalDuration,CaptureTime

nnPmUtilOmIntervTable,Snapshot,5,2005-03-22T15:35:00EST

Label,Label,Label,Label,Label,Label,Label,Label,Label

Source,nnPmUtilIntervChanAvg,nnPmUtilIntervChanPeak,nnPmUtilIntervCpuAvg,nnPmUtilIntervCpuPeak,nnPmUtilIntervFlashAvg,nnPmUtilIntervFlashPeak,nnPmUtilIntervRamAvg,nnPmUtilIntervRamPeak

Value,Value,Value,Value,Value,Value,Value,Value,Value

Frame011.Shelf0.Slot13,0,0,12,13,47,47,74,74

Frame011.Shelf0.Slot12,4,4,15,16,47,47,73,73

Frame011.Shelf1.Slot13,10,10,22,24,24,24,75,75

Frame011.Shelf1.Slot12,0,0,15,16,24,24,77,77

Frame011.Shelf2.Slot13,10,10,14,15,24,24,76,76

Frame011.Shelf2.Slot12,0,0,12,12,24,24,77,77

Frame013.Shelf0.Slot13,0,0,19,22,25,25,79,80

Frame013.Shelf0.Slot12,12,12,21,24,25,25,78,78

Frame011.Shelf3.Slot13,0,0,10,10,24,24,76,76

Frame011.Shelf3.Slot12,6,6,12,13,45,45,75,75

Frame013.Shelf1.Slot13,0,0,18,19,25,25,79,79

Frame013.Shelf1.Slot12,6,6,31,34,25,25,79,79

Frame010.Shelf0.Slot19,10,10,21,21,51,51,52,52

Frame010.Shelf0.Slot18,0,0,14,16,52,52,52,52

Frame010.Shelf0.Slot17,0,0,5,6,18,18,35,35

Frame010.Shelf0.Slot16,0,0,5,5,22,22,35,35

Frame010.Shelf0.Slot15,0,0,4,4,19,19,35,35

Frame010.Shelf0.Slot14,0,0,5,6,18,18,35,35

Frame013.Shelf2.Slot13,5,5,16,17,25,25,75,75

Frame010.Shelf0.Slot13,1,1,8,9,24,24,68,68

Frame013.Shelf2.Slot12,0,0,15,16,25,25,75,75

Frame010.Shelf0.Slot12,0,0,8,11,47,47,68,68

Frame010.Shelf0.Slot11,0,0,58,59,44,44,73,73

Frame010.Shelf0.Slot10,200,229,70,80,38,38,73,73

Frame013.Shelf3.Slot13,3,3,19,21,25,25,73,73

Frame010.Shelf1.Slot13,5,5,13,15,48,48,77,77


```
Frame013.Shelf3.Slot12,0,0,14,16,24,24,74,74
Frame010.Shelf1.Slot12,0,0,10,10,25,25,78,78
Frame010.Shelf2.Slot13,2,2,11,12,25,25,77,77
Frame010.Shelf2.Slot12,0,0,11,13,25,25,78,78
Frame012.Shelf0.Slot13,6,6,18,21,48,48,77,77
Frame010.Shelf3.Slot13,3,3,12,14,25,25,77,77
Frame012.Shelf0.Slot12,0,0,13,14,25,25,78,78
Frame010.Shelf3.Slot12,0,0,10,11,25,25,78,78
Frame012.Shelf1.Slot13,7,7,18,20,25,25,76,76
Frame012.Shelf1.Slot12,0,0,14,15,25,25,77,77
Frame012.Shelf2.Slot13,5,5,22,24,25,25,76,76
Frame012.Shelf2.Slot12,0,0,16,17,25,25,77,77
Frame010.Shelf0.Slot9,0,0,44,44,18,18,53,53
Frame010.Shelf0.Slot8,29,29,86,88,18,18,53,53
Frame010.Shelf0.Slot5,7,7,24,26,51,51,52,52
Frame010.Shelf0.Slot4,0,0,14,15,51,51,52,52
Frame010.Shelf0.Slot3,13,13,23,26,51,51,52,52
Frame012.Shelf3.Slot13,9,9,23,25,25,25,76,76
Frame010.Shelf0.Slot2,0,0,14,14,51,51,52,52
Frame012.Shelf3.Slot12,0,0,18,19,25,25,77,77
Table=End
```

Table=Begin

```
TableId,MeasurementKind,IntervalDuration,CaptureTime
nnBwAbiCurrentBandwResrvdTable,Snapshot,5,2005-03-22T15:35:00EST
Label,Label
Source,nnBwAbiCapacityBandwReserved
Value,Value
Frame010.Shelf0.Slot5,0
Frame010.Shelf0.Slot4,0
Frame010.Shelf0.Slot3,0
Frame010.Shelf0.Slot2,0
Frame010.Shelf0.Slot19,0
Frame010.Shelf0.Slot18,0
Frame010.Shelf0.Slot9,0
Frame010.Shelf0.Slot8,0
Table=End
```

Table=Begin

TableId,MeasurementKind,IntervalDuration,CaptureTime

nnMegacoOMDSPIntervalTable,Snapshot,5,2005-03-22T15:35:00EST

Label,Label,Label,Label,Label,Label,Label

Source,nnMegacoOMDSPnumCMRmodemReq,nnMegacoOMDSPnumCMRmodemReqFail,nnMegacoOMDSPnumToneGenReq,nnMegacoOMDSPnumToneGenReqFail,nnMegacoOMDSPnumToneRcvrReq,nnMegacoOMDSPnumToneRcvrReqFail

Value,Value,Value,Value,Value,Value,Value

Frame011.Shelf0.Slot13,0,0,69,0,46,0

Frame011.Shelf0.Slot12,0,0,69,0,46,0

Frame011.Shelf1.Slot13,0,0,69,0,93,0

Frame011.Shelf1.Slot12,0,0,69,0,93,0

Frame011.Shelf2.Slot13,0,0,12,0,33,0

Frame011.Shelf2.Slot12,0,0,12,0,33,0

Frame013.Shelf0.Slot13,0,0,22,0,51,0

Frame013.Shelf0.Slot12,0,0,22,0,51,0

Frame011.Shelf3.Slot13,0,0,10,0,24,0

Frame011.Shelf3.Slot12,0,0,10,0,24,0

Frame013.Shelf1.Slot13,0,0,175,0,0,0

Frame013.Shelf1.Slot12,0,0,175,0,0,0

Frame010.Shelf0.Slot19,0,0,0,0,0,0

Frame010.Shelf0.Slot18,0,0,0,0,0,0

Frame013.Shelf2.Slot13,0,0,11,0,28,0

Frame010.Shelf0.Slot13,0,0,9,0,0,0

Frame013.Shelf2.Slot12,0,0,11,0,28,0

Frame010.Shelf0.Slot12,0,0,9,0,0,0

Frame013.Shelf3.Slot13,0,0,3,0,9,0

Frame010.Shelf1.Slot13,0,0,8,0,18,0

Frame013.Shelf3.Slot12,0,0,3,0,9,0

Frame010.Shelf1.Slot12,0,0,8,0,18,0

Frame010.Shelf2.Slot13,0,0,3,0,9,0

Frame010.Shelf2.Slot12,0,0,3,0,9,0

Frame012.Shelf0.Slot13,0,0,39,0,57,0

Frame010.Shelf3.Slot13,0,0,4,0,9,0

Frame012.Shelf0.Slot12,0,0,39,0,57,0

Frame010.Shelf3.Slot12,0,0,4,0,9,0

Frame012.Shelf1.Slot13,0,0,25,0,35,0

```
Frame012.Shelf1.Slot12,0,0,25,0,35,0
Frame012.Shelf2.Slot13,0,0,50,0,88,0
Frame012.Shelf2.Slot12,0,0,50,0,88,0
Frame010.Shelf0.Slot9,0,0,0,0,0,0
Frame010.Shelf0.Slot8,0,0,0,0,0,0
Frame010.Shelf0.Slot5,0,0,0,0,0,0
Frame010.Shelf0.Slot4,0,0,0,0,0,0
Frame010.Shelf0.Slot3,0,0,0,0,0,0
Frame010.Shelf0.Slot2,0,0,0,0,0,0
Frame012.Shelf3.Slot13,0,0,62,0,91,0
Frame012.Shelf3.Slot12,0,0,62,0,91,0
Table=End
```

Table=Begin

TableId,MeasurementKind,IntervalDuration,CaptureTime

nnMegacoOMCESIntervalTable,Snapshot,5,2005-03-22T15:35:00EST

Label,Label,Label,Label,Label

Source,nnMegacoOMCESnumChnlAllocInter,nnMegacoOMCESnumChnlAllocInterFail,nnMegacoOMCESnumChnlAllocIntra,nnMegacoOMCESnumChnlAllocIntraFail

Value,Value,Value,Value,Value

```
Frame011.Shelf0.Slot13,53,0,46,0
Frame011.Shelf0.Slot12,53,0,46,0
Frame011.Shelf1.Slot13,120,0,50,0
Frame011.Shelf1.Slot12,120,0,50,0
Frame011.Shelf2.Slot13,48,0,18,0
Frame011.Shelf2.Slot12,48,0,18,0
Frame013.Shelf0.Slot13,66,0,36,0
Frame013.Shelf0.Slot12,66,0,36,0
Frame011.Shelf3.Slot13,30,0,12,0
Frame011.Shelf3.Slot12,30,0,12,0
Frame013.Shelf1.Slot13,135,0,64,0
Frame013.Shelf1.Slot12,135,0,64,0
Frame010.Shelf0.Slot19,149,0,168,0
Frame010.Shelf0.Slot18,149,0,168,0
Frame013.Shelf2.Slot13,33,0,13,0
Frame010.Shelf0.Slot13,0,0,0,0
Frame013.Shelf2.Slot12,33,0,13,0
Frame010.Shelf0.Slot12,0,0,0,0
```

```
Frame010.Shelf0.Slot11,3152,0,1216,0
Frame010.Shelf0.Slot10,3152,0,1216,0
Frame013.Shelf3.Slot13,24,0,1,0
Frame010.Shelf1.Slot13,12,0,24,0
Frame013.Shelf3.Slot12,24,0,1,0
Frame010.Shelf1.Slot12,12,0,24,0
Frame010.Shelf2.Slot13,12,0,3,0
Frame010.Shelf2.Slot12,12,0,3,0
Frame012.Shelf0.Slot13,26,0,74,0
Frame010.Shelf3.Slot13,15,0,3,0
Frame012.Shelf0.Slot12,26,0,74,0
Frame010.Shelf3.Slot12,15,0,3,0
Frame012.Shelf1.Slot13,66,0,24,0
Frame012.Shelf1.Slot12,66,0,24,0
Frame012.Shelf2.Slot13,177,0,7,0
Frame012.Shelf2.Slot12,177,0,7,0
Frame010.Shelf0.Slot9,1563,0,416,0
Frame010.Shelf0.Slot8,1563,0,416,0
Frame010.Shelf0.Slot5,288,0,86,0
Frame010.Shelf0.Slot4,288,0,86,0
Frame010.Shelf0.Slot3,238,0,120,0
Frame010.Shelf0.Slot2,238,0,120,0
Frame012.Shelf3.Slot13,130,0,53,0
Frame012.Shelf3.Slot12,130,0,53,0
Table=End
```

Table=Begin

TableId,MeasurementKind,IntervalDuration,CaptureTime

nnIpsecOmIntervalTable,Snapshot,5,2005-03-22T15:35:00EST

Label,Label,Label,Label,Label,Label,Label

Source,nnIpsecConfigInterfaceId,nnIpsecConfigSecLinkId,nnIpsecOmIntervalPacketsDiscardedIn,nnIpsecOmIntervalPacketsDiscardedOut,nnIpsecOmIntervalPacketsRx,nnIpsecOmIntervalPacketsTx

Value,Value,Value,Value,Value,Value,Value

Frame011.Shelf0.Slot13,1,1,0,0,0,0

Frame011.Shelf0.Slot12,1,1,0,0,1684,1795

Frame011.Shelf1.Slot13,1,1,0,0,2710,2884

Frame011.Shelf1.Slot12,1,1,0,0,0,0

Frame011.Shelf2.Slot13,1,1,0,0,1056,1119
Frame011.Shelf2.Slot12,1,1,0,0,0,0
Frame013.Shelf0.Slot13,1,1,0,0,0,0
Frame013.Shelf0.Slot12,1,1,0,0,1483,1585
Frame011.Shelf3.Slot13,1,1,0,0,0,0
Frame011.Shelf3.Slot12,1,1,0,0,885,936
Frame013.Shelf1.Slot13,1,1,0,0,0,0
Frame013.Shelf1.Slot12,1,1,0,0,4264,4469
Frame010.Shelf0.Slot19,1,1,0,0,7454,5419
Frame010.Shelf0.Slot18,1,1,0,0,0,1514
Frame013.Shelf2.Slot13,1,1,0,0,997,1046
Frame010.Shelf0.Slot13,1,1,0,0,210,210
Frame013.Shelf2.Slot12,1,1,0,0,0,0
Frame010.Shelf0.Slot12,1,1,0,0,0,0
Frame010.Shelf0.Slot11,1,1,0,0,0,0
Frame010.Shelf0.Slot10,1,1,0,0,362,381
Frame013.Shelf3.Slot13,1,1,0,0,501,521
Frame010.Shelf1.Slot13,1,1,0,0,717,756
Frame013.Shelf3.Slot12,1,1,0,0,0,0
Frame010.Shelf1.Slot12,1,1,0,0,0,0
Frame010.Shelf2.Slot13,1,1,0,0,442,460
Frame010.Shelf2.Slot12,1,1,0,0,0,0
Frame012.Shelf0.Slot13,1,1,0,0,1541,1640
Frame010.Shelf3.Slot13,1,1,0,0,480,501
Frame012.Shelf0.Slot12,1,1,0,0,0,0
Frame010.Shelf3.Slot12,1,1,0,0,0,0
Frame012.Shelf1.Slot13,1,1,0,0,1502,1599
Frame012.Shelf1.Slot12,1,1,0,0,0,0
Frame012.Shelf2.Slot13,1,1,0,0,2840,3028
Frame012.Shelf2.Slot12,1,1,0,0,0,0
Frame010.Shelf0.Slot9,1,1,0,0,0,8370
Frame010.Shelf0.Slot8,1,1,0,0,39696,24384
Frame010.Shelf0.Slot5,1,1,0,0,8884,5222
Frame010.Shelf0.Slot4,1,1,0,0,0,2451
Frame010.Shelf0.Slot3,1,1,0,0,8626,5080
Frame010.Shelf0.Slot2,1,1,0,0,0,2014
Frame012.Shelf3.Slot13,1,1,0,0,2689,2851
Frame012.Shelf3.Slot12,1,1,0,0,0,0

Table=End

Table=Begin

TableId, MeasurementKind, IntervalDuration, CaptureTime

nnPmOvldRscIntervTable, Snapshot, 5, 2005-03-22T15:35:00EST

Label, Label, Label, Label, Label, Label, Label, Label, Label

Source, nnPmOvldRscIntervChvMsgRAvg, nnPmOvldRscIntervChvMsgRPeak, nnPmOvldRscIntervConQDelAvg, nnPmOvldRscIntervConQDelPeak, nnPmOvldRscIntervCpuUtilAvg, nnPmOvldRscIntervCpuUtilPeak, nnPmOvldRscIntervPduRateAvg, nnPmOvldRscIntervPduRatePeak

Value, Value, Value, Value, Value, Value, Value, Value, Value

Frame011.Shelf0.Slot13, 34, 47, 25, 30, 1212, 1289, 1, 1

Frame011.Shelf0.Slot12, 34, 47, 94, 129, 1497, 1587, 7, 9

Frame011.Shelf1.Slot13, 61, 82, 231, 417, 2173, 2393, 12, 15

Frame011.Shelf1.Slot12, 61, 82, 38, 44, 1478, 1592, 1, 2

Frame011.Shelf2.Slot13, 19, 32, 188, 299, 1441, 1529, 5, 7

Frame011.Shelf2.Slot12, 21, 32, 22, 30, 1199, 1246, 1, 1

Frame013.Shelf0.Slot13, 38, 60, 38, 62, 1853, 2218, 1, 2

Frame013.Shelf0.Slot12, 35, 52, 408, 585, 2087, 2393, 8, 9

Frame011.Shelf3.Slot13, 13, 21, 17, 28, 1008, 1045, 1, 1

Frame011.Shelf3.Slot12, 13, 21, 88, 221, 1236, 1296, 4, 5

Frame013.Shelf1.Slot13, 63, 70, 25, 27, 1777, 1896, 1, 1

Frame013.Shelf1.Slot12, 61, 72, 361, 415, 3105, 3368, 17, 19

Frame010.Shelf0.Slot19, 104, 119, 593, 737, 2063, 2139, 37, 40

Frame010.Shelf0.Slot18, 107, 120, 39, 42, 1356, 1618, 24, 27

Frame013.Shelf2.Slot13, 11, 22, 198, 319, 1609, 1727, 4, 7

Frame010.Shelf0.Slot13, 0, 0, 0, 0, 762, 857, 1, 4

Frame013.Shelf2.Slot12, 11, 22, 24, 39, 1539, 1627, 1, 2

Frame010.Shelf0.Slot12, 0, 0, 0, 0, 823, 1123, 1, 2

Frame010.Shelf0.Slot11, 0, 0, 1395, 1567, 5813, 5904, 216, 247

Frame010.Shelf0.Slot10, 1474, 1526, 809, 900, 7014, 7904, 249, 279

Frame013.Shelf3.Slot13, 6, 13, 33, 59, 1870, 2108, 3, 4

Frame010.Shelf1.Slot13, 8, 14, 118, 232, 1335, 1496, 3, 4

Frame013.Shelf3.Slot12, 6, 12, 10, 23, 1438, 1589, 1, 2

Frame010.Shelf1.Slot12, 9, 14, 12, 20, 1012, 1039, 1, 2

Frame010.Shelf2.Slot13, 5, 12, 15, 33, 1103, 1181, 2, 3

Frame010.Shelf2.Slot12, 5, 12, 9, 24, 1063, 1260, 1, 2

Frame012.Shelf0.Slot13, 33, 52, 433, 1031, 1752, 2064, 7, 11

Frame010.Shelf3.Slot13, 7, 23, 37, 86, 1209, 1381, 3, 5

```
Frame012.Shelf0.Slot12,32,51,26,36,1260,1379,1,2
Frame010.Shelf3.Slot12,7,23,9,24,1017,1098,1,2
Frame012.Shelf1.Slot13,31,52,331,860,1818,2017,6,9
Frame012.Shelf1.Slot12,23,31,32,46,1376,1538,1,1
Frame012.Shelf2.Slot13,59,63,90,144,2245,2355,13,14
Frame012.Shelf2.Slot12,60,65,32,38,1630,1676,1,1
Frame010.Shelf0.Slot9,641,651,104,118,4376,4415,137,139
Frame010.Shelf0.Slot8,650,685,16644,21690,8520,8733,204,207
Frame010.Shelf0.Slot5,122,141,430,581,2401,2579,44,47
Frame010.Shelf0.Slot4,123,141,47,55,1399,1529,29,31
Frame010.Shelf0.Slot3,112,120,510,611,2329,2624,42,44
Frame010.Shelf0.Slot2,125,138,46,50,1365,1411,29,31
Frame012.Shelf3.Slot13,58,68,362,862,2264,2477,13,15
Frame012.Shelf3.Slot12,57,68,36,46,1805,1916,1,2
Table=End
```

Table=Begin

TableId,MeasurementKind,IntervalDuration,CaptureTime

nnRelMsgSctpAssocOmIntervTable,Snapshot,5,2005-03-22T15:35:00EST

Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label

Source,nnRelMsgSctpAscIntervAbort,nnRelMsgSctpAscIntervClosed,nnRelMsgSctpAscIntervC
ongCleared,nnRelMsgSctpAscIntervCongCount,nnRelMsgSctpAscIntervDiscPacks,nnRelMsgSct
pAscIntervInPacks,nnRelMsgSctpAscIntervOutPacks,nnRelMsgSctpAscIntervRetranPacks,nnR
elMsgSctpAscIntervT1expires,nnRelMsgSctpAscIntervT2expires,nnRelMsgSctpAscIntervT3ex
pires

Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value

Frame010.Shelf0.Slot5,0,0,0,0,0,4387,1816,0,0,0,0

Frame010.Shelf0.Slot4,0,0,0,0,0,1535,2398,0,0,0,0

Frame010.Shelf0.Slot3,0,0,0,0,0,4036,1838,0,0,0,0

Frame010.Shelf0.Slot2,0,0,0,0,0,1748,1736,0,0,0,0

Frame010.Shelf0.Slot19,0,0,0,0,0,3650,2193,0,0,0,0

Frame010.Shelf0.Slot18,0,0,0,0,0,755,1346,0,0,0,0

Frame010.Shelf0.Slot9,0,0,0,0,0,5141,8278,0,0,0,0

Frame010.Shelf0.Slot8,0,0,0,0,0,21327,8865,0,0,0,0

Table=End

Table=Begin

TableId,MeasurementKind,IntervalDuration,CaptureTime

nnBwAbiIntervalBandwResrvdEntry, Snapshot, 5, 2005-03-22T15:35:00EST

Label, Label

Source, nnBwAbiIntervalBandwReserved

Value, Value

Frame010.Shelf0.Slot5, 6000

Frame010.Shelf0.Slot4, 10078

Frame010.Shelf0.Slot3, 6000

Frame010.Shelf0.Slot2, 14900

Frame010.Shelf0.Slot19, 10993

Frame010.Shelf0.Slot18, 7000

Frame010.Shelf0.Slot9, 22013

Frame010.Shelf0.Slot8, 6000

Table=End

Table=Begin

TableId, MeasurementKind, IntervalDuration, CaptureTime

nnPmOvldConnDenyIntervTable, Snapshot, 5, 2005-03-22T15:35:00EST

Label, Label

Source, nnPmOvldConnDenyIntervCount

Value, Value

Frame011.Shelf0.Slot13, 0

Frame011.Shelf0.Slot12, 0

Frame011.Shelf1.Slot13, 0

Frame011.Shelf1.Slot12, 0

Frame011.Shelf2.Slot13, 0

Frame011.Shelf2.Slot12, 0

Frame013.Shelf0.Slot13, 0

Frame013.Shelf0.Slot12, 0

Frame011.Shelf3.Slot13, 0

Frame011.Shelf3.Slot12, 0

Frame013.Shelf1.Slot13, 0

Frame013.Shelf1.Slot12, 0

Frame010.Shelf0.Slot19, 0

Frame010.Shelf0.Slot18, 0

Frame013.Shelf2.Slot13, 0

Frame010.Shelf0.Slot13, 0

Frame013.Shelf2.Slot12, 0

Frame010.Shelf0.Slot12,0
Frame010.Shelf0.Slot11,0
Frame010.Shelf0.Slot10,0
Frame013.Shelf3.Slot13,0
Frame010.Shelf1.Slot13,0
Frame013.Shelf3.Slot12,0
Frame010.Shelf1.Slot12,0
Frame010.Shelf2.Slot13,0
Frame010.Shelf2.Slot12,0
Frame012.Shelf0.Slot13,0
Frame010.Shelf3.Slot13,0
Frame012.Shelf0.Slot12,0
Frame010.Shelf3.Slot12,0
Frame012.Shelf1.Slot13,0
Frame012.Shelf1.Slot12,0
Frame012.Shelf2.Slot13,0
Frame012.Shelf2.Slot12,0
Frame010.Shelf0.Slot9,0
Frame010.Shelf0.Slot8,0
Frame010.Shelf0.Slot5,0
Frame010.Shelf0.Slot4,0
Frame010.Shelf0.Slot3,0
Frame010.Shelf0.Slot2,0
Frame012.Shelf3.Slot13,0
Frame012.Shelf3.Slot12,0
Table=End

Table=Begin

TableId,MeasurementKind,IntervalDuration,CaptureTime

nnMegacoOMECANIntervalTable,Snapshot,5,2005-03-22T15:35:00EST

Label,Label,Label

Source,nnMegacoOMECANnumResrceReq,nnMegacoOMECANnumResrceReqFail

Value,Value,Value

Frame011.Shelf0.Slot13,99,0

Frame011.Shelf0.Slot12,99,0

Frame011.Shelf1.Slot13,171,0

Frame011.Shelf1.Slot12,171,0

Frame011.Shelf2.Slot13,66,0
Frame011.Shelf2.Slot12,66,0
Frame013.Shelf0.Slot13,102,0
Frame013.Shelf0.Slot12,102,0
Frame011.Shelf3.Slot13,45,0
Frame011.Shelf3.Slot12,45,0
Frame013.Shelf1.Slot13,199,0
Frame013.Shelf1.Slot12,199,0
Frame010.Shelf0.Slot19,317,0
Frame010.Shelf0.Slot18,317,0
Frame013.Shelf2.Slot13,49,0
Frame010.Shelf0.Slot13,0,0
Frame013.Shelf2.Slot12,49,0
Frame010.Shelf0.Slot12,0,0
Frame013.Shelf3.Slot13,25,0
Frame010.Shelf1.Slot13,36,0
Frame013.Shelf3.Slot12,25,0
Frame010.Shelf1.Slot12,36,0
Frame010.Shelf2.Slot13,15,0
Frame010.Shelf2.Slot12,15,0
Frame012.Shelf0.Slot13,98,0
Frame010.Shelf3.Slot13,18,0
Frame012.Shelf0.Slot12,98,0
Frame010.Shelf3.Slot12,18,0
Frame012.Shelf1.Slot13,90,0
Frame012.Shelf1.Slot12,90,0
Frame012.Shelf2.Slot13,184,0
Frame012.Shelf2.Slot12,184,0
Frame010.Shelf0.Slot9,1979,0
Frame010.Shelf0.Slot8,1979,0
Frame010.Shelf0.Slot5,374,0
Frame010.Shelf0.Slot4,374,0
Frame010.Shelf0.Slot3,358,0
Frame010.Shelf0.Slot2,358,0
Frame012.Shelf3.Slot13,179,0
Frame012.Shelf3.Slot12,179,0
Table=End

```
Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
nnBwShelfCurrentSloaBandwResrvdTable,Snapshot,5,2005-03-22T15:35:00EST
Label,Label
Source,nnBwShelfCapacitySloaBandwReserved
Value,Value
Frame012.Shelf2,27680
Frame012.Shelf1,27680
Frame012.Shelf0,27680
Frame011.Shelf3,27680
Frame011.Shelf2,27680
Frame011.Shelf1,27680
Frame010.Shelf3,27680
Frame011.Shelf0,27680
Frame010.Shelf2,27680
Frame010.Shelf1,27680
Frame010.Shelf0,27680
Frame013.Shelf3,27680
Frame013.Shelf2,27680
Frame013.Shelf1,27680
Frame013.Shelf0,27680
Frame012.Shelf3,27680
Table=End
```

```
Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
nnBwShelfIntervalSloaBandwResrvdTable,Snapshot,5,2005-03-22T15:35:00EST
Label,Label
Source,nnBwShelfIntervalSloaBandwReserved
Value,Value
Frame012.Shelf2,3351
Frame012.Shelf1,5950
Frame012.Shelf0,3864
Frame011.Shelf3,5232
Frame011.Shelf2,7182
Frame011.Shelf1,5745
```

```
Frame010.Shelf3,2872
Frame011.Shelf0,2770
Frame010.Shelf2,1846
Frame010.Shelf1,4035
Frame010.Shelf0,684
Frame013.Shelf3,2394
Frame013.Shelf2,4651
Frame013.Shelf1,4035
Frame013.Shelf0,8310
Frame012.Shelf3,6771
Table=End
```

```
SingleValues=Begin
MeasurementKind,IntervalDuration
Snapshot,5
MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability
nnBwBandwUtilIntervalInCellRate,2005-03-
22T15:35:00EST,nnBwIntervalBandwUtilTable,66409,Valid
nnBwBandwUtilIntervalOutCellRate,2005-03-
22T15:35:00EST,nnBwIntervalBandwUtilTable,66339,Valid
nnBwBandwUtilIntervalInDslCellRate,2005-03-
22T15:35:00EST,nnBwIntervalBandwUtilTable,0,Valid
nnBwBandwUtilIntervalOutDslCellRate,2005-03-
22T15:35:00EST,nnBwIntervalBandwUtilTable,0,Valid
nnBwQueueFillIntervalTotal,2005-03-22T15:35:00EST,nnBwIntervalQueueFillTable,0,Valid
nnBwQueueFillIntervalCbr,2005-03-22T15:35:00EST,nnBwIntervalQueueFillTable,0,Valid
nnBwQueueFillIntervalRtVbr,2005-03-22T15:35:00EST,nnBwIntervalQueueFillTable,0,Valid
nnBwQueueFillIntervalNrtVbr,2005-03-
22T15:35:00EST,nnBwIntervalQueueFillTable,0,Valid
nnBwQueueFillIntervalUbr,2005-03-22T15:35:00EST,nnBwIntervalQueueFillTable,0,Valid
nnBwQueueFillIntervalUbrPlus,2005-03-
22T15:35:00EST,nnBwIntervalQueueFillTable,0,Valid
nnBwQueueFillIntervalControl,2005-03-
22T15:35:00EST,nnBwIntervalQueueFillTable,0,Valid
SingleValues=End

SubEntity=End

Entity=End
```

System=End

PMFile=End

GUI/CLUI Documentation for MG 9000

GUI Launching and User procedures

- NN10096-511 MG9000 Configuration Management

Related documents

- NN10409-500 ATM/IP Solution-level Configuration Management

MultiService Switch 7400, 15000, 20000

This section contains IEMS Northbound log samples and device documentation references for the MSS 7400, 15000, 20000.

MSS 7400, 15000, 20000 Fault Interface

Fault documentation for MSS 7400, 15000, 20000 :

- NN10600-500 - Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference
- NN10600-715 - Nortel Networks Multiservice Switch 7400/15000/20000 ATM Fault and Performance Management
- NN10600-520 - Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting

Fault Mapping for MSS 7400, 15000, 20000

The following criteria can be used for looking up information on specific faults for MS 7400, 15000, 20000.

Fault Correlation for MS 7400, 15000, 20000

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
MS 7400, 15000, 20000	logname and number	logname and number	logname and number	logname and number	NN10600-715 - Nortel Networks Multiservice Switch 7400/ 15000/20000 ATM Fault and Performance Management

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:

```

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 => 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 => 70115203
nnExtAlarmActiveResourceDescription => IEMS=wnc0y0m3.us.nortel.com-MDM-
Mgr;EM MANTEO
LP 3 SONET 2
nnExtAlarmActiveManualClear => 1
nnExtAlarmActiveSequenceNumber => 1375

```

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

- NN10600-710 - Nortel Networks Multiservice Switch 7400/15000/20000 ATM Configuration Management
- NN10600-582 - Nortel Networks Multiservice Switch 7400/15000/20000 IP VPN Configuration Management
- NN10600-520 - Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting

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 693.*

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 703.

- NN10600-030 - Nortel Networks Multiservice Switch 7400/15000/20000 Overview
- 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 704.*

- 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
- 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
- NN10600-550 - Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures
- NN10600-551 - Nortel Networks Multiservice Switch 7400/15000/20000 FP Configuration Reference
- NN10600-560 - Nortel Networks Multiservice Switch 7400/15000/20000 Accounting
- NN10600-561 - Nortel Networks Multiservice Switch 7400/15000/20000 Data Management
- 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
- NN10600-700 - 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 - Multiservice Data Manager Management Data Provider
- 241-6001-806 - Multiservice Data Manager Management Data Provider Data Formats Reference for DPN
- 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 Media Server 2000 Series 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 Series 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 INFO
  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 INFO

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 INFO

Location: 47.142.134.127

State: Cleared

Time: 1086873672172

Nortel-JH ** AMS501 JUN10 09:21:12 5709 FLT MS2000 INFO

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 INFO

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

- NN10331-711 - Media Server 2000 Series 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 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="commonPerfRecord_V2.0.xsd" MeasurementCategory="PM">
<FileCreationTime>2004-06-23T17:40:01EST</FileCreationTime>
_ <System>
<SystemId>NortelNetworks/IEMS</SystemId>
_ <Entity>
<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,commonPerfRecord_V2.0.xsd,2004-06-23T17:25:50EST
System=Begin
NortelNetworks/IEMS
Entity=Begin
Entity Id
47.142.92.104
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.a
cPerfMediaGateway.acPerfCp,0,Valid
```

acPerfCpNumDupsForCompletedTransactions,2004-06-
23T17:24:11EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,0,Valid

acPerfCpMessageMaxRetransmissionsExceeded,2004-06-
23T17:24:11EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,0,Valid

acPerfCpMessageReceiveErrors,2004-06-
23T17:24:12EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,0,Valid

acPerfCpMessageRetransmissions,2004-06-
23T17:24:13EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,18,Valid

acPerfCpNumDupsForOutstandingTransactions,2004-06-
23T17:24:13EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,0,Valid

acPerfCpMessagesFromUntrustedSources,2004-06-
23T17:24:13EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,0,Valid

acPerfCpProtocolSyntaxErrors,2004-06-
23T17:24:13EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,0,Valid

acPerfRtpRcvrLostPackets,2004-06-
23T17:24:13EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfRtp,0,Valid

acPerfRtpFailedDueToLackOfResources,2004-06-
23T17:24:13EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfRtp,0,Valid

acPerfIvrPlayCollectRequests,2004-06-
23T17:24:14EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrPlayRequests,2004-06-
23T17:24:15EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,88,Valid

acPerfBctRequests,2004-06-
23T17:24:16EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfBct,0,Valid

acPerfIvrPlayCollectFailedDueToLackOfResources,2004-06-
23T17:24:15EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrPlaySegmentFailedDueToProvMismatch,2004-06-
23T17:24:15EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,9,Valid

acPerfIvrContDigitCollectRequests,2004-06-
23T17:24:15EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrPlayFailedDueToLackOfResources,2004-06-
23T17:24:15EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrPlayCollectFailedDueToProvMismatch,2004-06-
23T17:24:16EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

```
acPerfIvrContDigitCollectFailedDueToLackOfResources,2004-06-
23T17:24:16EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfBctFailedDueToLackOfResources,2004-06-
23T17:24:16EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfBct,0,Valid

acPerfConfRequests,2004-06-
23T17:24:16EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfConf,11,Valid

acPerfConfPlays,2004-06-
23T17:24:16EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfConf,36,Valid

acPerfConfAddFailedDueToLackOfResources,2004-06-
23T17:24:16EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfConf,0,Valid

acPerfConfFailedDueToLackOfResources,2004-06-
23T17:24:17EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfConf,0,Valid

acPerfTtFailedDueToLackOfResources,2004-06-
23T17:24:17EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfTt,0,Valid

acPerfTtRequests,2004-06-
23T17:24:17EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfTt,0,Valid

acPerfSystemPacketEndpointsInUse,2004-06-
23T17:24:17EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.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 Series Basics

Related documents

- NN10340-511 MS2000 Series Configuration Management
- NN10337-611 MS2000 Series Security and Administration

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:

- NN10332-911 - Session Server 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	NN10332-911 Session Server 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 => SIP Gateway Application Mtc Out Of Sync
nnExtAlarmActiveEventType => 1
nnExtAlarmActiveProbableCause => 2
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => SIPM302
nnExtAlarmActiveResourceDescription => IEMS=47.142.123.48-SP2000-Unit-
0;NCGL=RTPFSIP0;
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 Locationon: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 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="commonPerfRecord_V2.0.xsd"
MeasurementCategory="PM">
<FileCreationTime>2006-01-16T01:28:11PST</FileCreationTime>
<System>
<SystemId>NortelNetworks/IEMS</SystemId>
<Entity>
<EntityId>47.142.92.225-47.142.92.230-SS-Unit-0</EntityId>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>.iso.org.dod.internet.private.enterprises.ucdavis.laTable.laEntry</TableId>
<CaptureTime>2006-01-16T01:28:09PST</CaptureTime>
<Labels>
<Label>laNames</Label>
<Label>laLoad</Label>
<Label>laConfig</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Load-15</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>12</Value>
```



```
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Load-5</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>12</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Load-1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>12</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTable.hrStorageEntry</TableId>
<CaptureTime>2006-01-16T01:28:03PST</CaptureTime>
<Labels>
<Label>hrStorageIndex</Label>
<Label>hrStorageType</Label>
<Label>hrStorageAllocationUnits</Label>
<Label>hrStorageSize</Label>
<Label>hrStorageUsed</Label>
<Label>hrStorageAllocationFailures</Label>
</Labels>
<RowOfValues>
<RowValue>
```

```
<Value>9</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
<RowValue>
<Value>4096</Value>
</RowValue>
<RowValue>
<Value>129872</Value>
</RowValue>
<RowValue>
<Value>216</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>8</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
<RowValue>
<Value>4096</Value>
</RowValue>
<RowValue>
<Value>179024</Value>
</RowValue>
<RowValue>
<Value>343</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>7</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
<RowValue>
<Value>4096</Value>
</RowValue>
<RowValue>
<Value>259584</Value>
</RowValue>
<RowValue>
<Value>198685</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>6</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
<RowValue>
<Value>4096</Value>
</RowValue>
<RowValue>
<Value>129872</Value>
</RowValue>
<RowValue>
<Value>29952</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
<RowValue>
<Value>4096</Value>
</RowValue>
<RowValue>
<Value>31568</Value>
</RowValue>
<RowValue>
<Value>6701</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>4</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
<RowValue>
<Value>4096</Value>
</RowValue>
<RowValue>
<Value>129872</Value>
</RowValue>
```

```
<RowValue>
<Value>95674</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>103</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageOther</Value>
</RowValue>
<RowValue>
<Value>256</Value>
</RowValue>
<RowValue>
<Value>51218</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1026</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>3</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
<RowValue>
<Value>4096</Value>
</RowValue>
```

```
<RowValue>
<Value>179024</Value>
</RowValue>
<RowValue>
<Value>327</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>102</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageVirtualMemory</Value>
</RowValue>
<RowValue>
<Value>1024</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1025</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>12</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
```

```
<RowValue>
<Value>4096</Value>
</RowValue>
<RowValue>
<Value>129872</Value>
</RowValue>
<RowValue>
<Value>81</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>101</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageRam</Value>
</RowValue>
<RowValue>
<Value>1024</Value>
</RowValue>
<RowValue>
<Value>2097151</Value>
</RowValue>
<RowValue>
<Value>2097151</Value>
</RowValue>
<RowValue>
<Value>769</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
```

```
<Value>.iso.org.dod.internet.mgmt.mib-  
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>  
</RowValue>  
<RowValue>  
<Value>1024</Value>  
</RowValue>  
<RowValue>  
<Value>101018</Value>  
</RowValue>  
<RowValue>  
<Value>80797</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
</RowOfValues>  
<RowOfValues>  
<RowValue>  
<Value>11</Value>  
</RowValue>  
<RowValue>  
<Value>.iso.org.dod.internet.mgmt.mib-  
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>  
</RowValue>  
<RowValue>  
<Value>4096</Value>  
</RowValue>  
<RowValue>  
<Value>2561536</Value>  
</RowValue>  
<RowValue>  
<Value>12352</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
</RowOfValues>  
<RowOfValues>  
<RowValue>
```



```
<Value>1</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
<RowValue>
<Value>1024</Value>
</RowValue>
<RowValue>
<Value>62941</Value>
</RowValue>
<RowValue>
<Value>51218</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>10</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
<RowValue>
<Value>4096</Value>
</RowValue>
<RowValue>
<Value>382464</Value>
</RowValue>
<RowValue>
<Value>56117</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
</RowOfValues>
</Table>
<SingleValues MeasurementKind="Snapshot" IntervalDuration="5">
<SingleValue>
<CaptureTime>2006-01-16T01:28:01PST</CaptureTime>
<MeasureId>sysDescr</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.system</MeasureSuppId1>
<Value>Linux RTP7NGSS-0 2.4.22-ncgl-9.51.1.0 #1 Wed Dec 21 03:52:40 EST 2005
i686</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:02PST</CaptureTime>
<MeasureId>snmpOutPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>6433</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:02PST</CaptureTime>
<MeasureId>snmpInBadVersions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:02PST</CaptureTime>
<MeasureId>snmpInBadCommunityNames</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:02PST</CaptureTime>
<MeasureId>snmpInTotalReqVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>20058</Value>
<Reliability>Valid</Reliability>
```

```
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:02PST</CaptureTime>
<MeasureId>snmpOutTraps</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>31</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:02PST</CaptureTime>
<MeasureId>snmpInBadCommunityUses</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:02PST</CaptureTime>
<MeasureId>snmpInPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>6428</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:02PST</CaptureTime>
<MeasureId>snmpInTotalSetVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:02PST</CaptureTime>
<MeasureId>snmpInASNParseErrs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:03PST</CaptureTime>
```

```

<MeasureId>hrSystemDate</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.host.hrSystem</MeasureSuppId1>
<Value>2006-1-16,4:44:25.0,-5:0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:03PST</CaptureTime>
<MeasureId>hrSystemUptime</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.host.hrSystem</MeasureSuppId1>
<Value>229179</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:03PST</CaptureTime>
<MeasureId>hrSystemProcesses</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.host.hrSystem</MeasureSuppId1>
<Value>194</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:03PST</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
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonPerfRecord_V2.0.xsd,2006-01-12T02:12:02PST

```

System=Begin

SystemId

NortelNetworks/IEMS

Entity=Begin

EntityId

47.142.92.225-47.142.92.230-SS-Unit-0

Table=Begin

TableId, MeasurementKind, IntervalDuration, CaptureTime

.iso.org.dod.internet.private.enterprises.ucdavis.laTable.laEntry, Snapshot, 5, 2006-01-12T02:12:01PST

Label, Label, Label

laNames, laLoad, laConfig

Value, Value, Value

Load-15, 0, 12

Load-5, 0, 12

Load-1, 0, 12

Table=End

Table=Begin

TableId, MeasurementKind, IntervalDuration, CaptureTime

.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTable.hrStorageEntry, Snapshot, 5, 2006-01-12T02:11:57PST

Label, Label, Label, Label, Label, Label

hrStorageIndex, hrStorageType, hrStorageAllocationUnits, hrStorageSize, hrStorageUsed, hrStorageAllocationFailures

Value, Value, Value, Value, Value, Value

9, .iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk, 4096, 179024, 342, 0

8, .iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk, 4096, 179024, 342, 0

7, .iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk, 4096, 259584, 198668, 0

6, .iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk, 4096, 129872, 26027, 0

5, .iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk, 4096, 31568, 6701, 0

4, .iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk, 4096, 129872, 89138, 0

```
103,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageOther,256,48363,0,1026

3,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,4096,179024,322,0

102,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageVirtualMemory,1024,0,0,1025

12,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,4096,129872,90,0

101,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageRam,1024,2097151,1125972,769

2,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,1024,101018,80797,0

11,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,4096,2561536,11651,0

1,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,1024,62941,48363,0

10,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,4096,382464,55288,0

Table=End
```

SingleValues=Begin

MeasurementKind,IntervalDuration

Snapshot,5

MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability

sysDescr,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-2.system,Linux
RTP7NGSS-0 2.4.22-ncgl-cca_image_7.09.2.1 #1 Wed Jul 13 15:33:06 EDT 2005 i686,Valid

snmpOutPkts,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-2.snmp,1913,Valid

snmpInBadVersions,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid

snmpInBadCommunityNames,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-
2.snmp,1,Valid

snmpInTotalReqVars,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-
2.snmp,7179,Valid

snmpOutTraps,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-2.snmp,92,Valid

snmpInBadCommunityUses,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid

snmpInPkts,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-2.snmp,2034,Valid

snmpInTotalSetVars,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid

snmpInASNParseErrs,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid

hrSystemDate,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-
2.host.hrSystem,2006-1-12,5:28:17.0,-5:0,Valid

```
hrSystemUptime,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-  
2.host.hrSystem,56466,Valid  
  
hrSystemProcesses,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-  
2.host.hrSystem,178,Valid  
  
snmpSilentDrops,2006-01-12T02:11:57PST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,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 Basics

Related documents

- NN10338-511 - Session Server Configuration Management
- NN10346-611 - Session Server 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 for IP solutions, only for ATM solutions.
- NN10155-711 - SAM21 Shelf Controller Performance Management

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided (for ATM solutions only).

CSV

The following is an example of Performance for SAM21 Shelf Controller in CSV format.

```
PMFile=Begin
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonPerfRecord_V2.0.xsd,2005-03-16T10:55:01EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
```

```
EntityId
172.16.144.134

SingleValues=Begin
MeasurementKind, IntervalDuration
Snapshot, 5
MeasureId, CaptureTime, MeasureSuppId1, Value, Reliability
totalBytesRxed, 2005-03-
16T10:55:00EST, .iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceCont
rol.scu.scuMessaging.ipoaMIB, 14792, Valid
rxedTimeoutCount, 2005-03-
16T10:55:00EST, .iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceCont
rol.scu.scuMessaging.ipoaMIB, 0, Valid
bytesSentPerSec, 2005-03-
16T10:55:00EST, .iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceCont
rol.scu.scuMessaging.ipoaMIB, 24, Valid
cellDropCount, 2005-03-
16T10:55:00EST, .iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceCont
rol.scu.scuMessaging.ipoaMIB, 0, Valid
oversizedPDUCount, 2005-03-
16T10:55:00EST, .iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceCont
rol.scu.scuMessaging.ipoaMIB, 0, Valid
bytesRxedPerSec, 2005-03-
16T10:55:00EST, .iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceCont
rol.scu.scuMessaging.ipoaMIB, 24, Valid
totalBytesSent, 2005-03-
16T10:55:00EST, .iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceCont
rol.scu.scuMessaging.ipoaMIB, 16765, Valid
SingleValues=End

Entity=End

System=End
```

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

Related documents

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="commonPerfRecord_V2.0.xsd" MeasurementCategory="PM">
<FileCreationTime>2005-03-15T15:35:04EST</FileCreationTime>
_ <System>
<SystemId>NortelNetworks/IEMS</SystemId>
_ <Entity>
<EntityId>47.166.56.10</EntityId>
_ <Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTable.hrStorageEntry</TableId>
<CaptureTime>2005-03-15T15:35:01EST</CaptureTime>
_ <Labels>
<Label>hrStorageIndex</Label>
<Label>hrStorageType</Label>
<Label>hrStorageDescr</Label>
<Label>hrStorageAllocationUnits</Label>
<Label>hrStorageSize</Label>
<Label>hrStorageUsed</Label>
<Label>hrStorageAllocationFailures</Label>
</Labels>
```

```
_ <RowOfValues>
_ <RowValue>
<Value>14</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
_ <RowValue>
<Value>/nfsserv/3pc/5/cs</Value>
</RowValue>
_ <RowValue>
<Value>4096</Value>
</RowValue>
_ <RowValue>
<Value>924496</Value>
</RowValue>
_ <RowValue>
<Value>591998</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>13</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
_ <RowValue>
<Value>/nfsserv/3pc/4/mtc</Value>
</RowValue>
_ <RowValue>
<Value>4096</Value>
</RowValue>
_ <RowValue>
```

```
<Value>260944</Value>
</RowValue>
_ <RowValue>
<Value>71434</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>12</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
_ <RowValue>
<Value>/nfsserv/3pc/4/cs</Value>
</RowValue>
_ <RowValue>
<Value>4096</Value>
</RowValue>
_ <RowValue>
<Value>924496</Value>
</RowValue>
_ <RowValue>
<Value>505263</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>11</Value>
</RowValue>
_ <RowValue>
```



```
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
_ <RowValue>
<Value>/nfsserv/3pc/3/mtc</Value>
</RowValue>
_ <RowValue>
<Value>4096</Value>
</RowValue>
_ <RowValue>
<Value>260944</Value>
</RowValue>
_ <RowValue>
<Value>66727</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>10</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
_ <RowValue>
<Value>/nfsserv/3pc/3/cs</Value>
</RowValue>
_ <RowValue>
<Value>4096</Value>
</RowValue>
_ <RowValue>
<Value>924496</Value>
</RowValue>
_ <RowValue>
<Value>486565</Value>
</RowValue>
```

```
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>103</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageOther</Value>
</RowValue>
_ <RowValue>
<Value>Memory Buffers</Value>
</RowValue>
_ <RowValue>
<Value>256</Value>
</RowValue>
_ <RowValue>
<Value>53493</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
_ <RowValue>
<Value>1026</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>102</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageVirtualMemory</Value>
</RowValue>
_ <RowValue>
<Value>Swap Space</Value>
</RowValue>
```

```
_ <RowValue>
<Value>1024</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
_ <RowValue>
<Value>1025</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>101</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageRam</Value>
</RowValue>
_ <RowValue>
<Value>Real Memory</Value>
</RowValue>
_ <RowValue>
<Value>1024</Value>
</RowValue>
_ <RowValue>
<Value>514140</Value>
</RowValue>
_ <RowValue>
<Value>381396</Value>
</RowValue>
_ <RowValue>
<Value>769</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
```

```
<Value>22</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
_ <RowValue>
<Value>/nfsserv/3pc/8/mtc</Value>
</RowValue>
_ <RowValue>
<Value>4096</Value>
</RowValue>
_ <RowValue>
<Value>260944</Value>
</RowValue>
_ <RowValue>
<Value>39840</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>21</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
_ <RowValue>
<Value>/nfsserv/3pc/8/cs</Value>
</RowValue>
_ <RowValue>
<Value>4096</Value>
</RowValue>
_ <RowValue>
<Value>875344</Value>
</RowValue>
```

```
_ <RowValue>
<Value>639076</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>9</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
_ <RowValue>
<Value>/nfsserv/3pc/2/mtc</Value>
</RowValue>
_ <RowValue>
<Value>4096</Value>
</RowValue>
_ <RowValue>
<Value>260944</Value>
</RowValue>
_ <RowValue>
<Value>41542</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>20</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
```

```
_ <RowValue>
<Value>/nfsserv/3pc/7/mtc</Value>
</RowValue>
_ <RowValue>
<Value>4096</Value>
</RowValue>
_ <RowValue>
<Value>260944</Value>
</RowValue>
_ <RowValue>
<Value>37878</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>8</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
_ <RowValue>
<Value>/nfsserv/3pc/2/cs</Value>
</RowValue>
_ <RowValue>
<Value>4096</Value>
</RowValue>
_ <RowValue>
<Value>924496</Value>
</RowValue>
_ <RowValue>
<Value>627594</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
```

```
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>7</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
_ <RowValue>
<Value>/nfsserv/3pc/1/mtc</Value>
</RowValue>
_ <RowValue>
<Value>4096</Value>
</RowValue>
_ <RowValue>
<Value>260944</Value>
</RowValue>
_ <RowValue>
<Value>64177</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>6</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
_ <RowValue>
<Value>/nfsserv/3pc/1/cs</Value>
</RowValue>
_ <RowValue>
<Value>4096</Value>
</RowValue>
```

```
_ <RowValue>
<Value>924496</Value>
</RowValue>
_ <RowValue>
<Value>484559</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>5</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
_ <RowValue>
<Value>/nfsserv/3pc/0/mtc</Value>
</RowValue>
_ <RowValue>
<Value>4096</Value>
</RowValue>
_ <RowValue>
<Value>260944</Value>
</RowValue>
_ <RowValue>
<Value>41699</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>4</Value>
</RowValue>
_ <RowValue>
```



```
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
_ <RowValue>
<Value>/nfsserv/3pc/0/cs</Value>
</RowValue>
_ <RowValue>
<Value>4096</Value>
</RowValue>
_ <RowValue>
<Value>924496</Value>
</RowValue>
_ <RowValue>
<Value>667345</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>3</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
_ <RowValue>
<Value>/storm</Value>
</RowValue>
_ <RowValue>
<Value>4096</Value>
</RowValue>
_ <RowValue>
<Value>260944</Value>
</RowValue>
_ <RowValue>
<Value>298</Value>
</RowValue>
```

```
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>2</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
_ <RowValue>
<Value>/boot</Value>
</RowValue>
_ <RowValue>
<Value>1024</Value>
</RowValue>
_ <RowValue>
<Value>101018</Value>
</RowValue>
_ <RowValue>
<Value>58993</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>1</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
_ <RowValue>
<Value>/</Value>
</RowValue>
```

```
_ <RowValue>
<Value>1024</Value>
</RowValue>
_ <RowValue>
<Value>59301</Value>
</RowValue>
_ <RowValue>
<Value>53493</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>19</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
_ <RowValue>
<Value>/nfsserv/3pc/7/cs</Value>
</RowValue>
_ <RowValue>
<Value>4096</Value>
</RowValue>
_ <RowValue>
<Value>875344</Value>
</RowValue>
_ <RowValue>
<Value>551564</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
```

```
<Value>18</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
_ <RowValue>
<Value>/nfsserv/3pc/6/mtc</Value>
</RowValue>
_ <RowValue>
<Value>4096</Value>
</RowValue>
_ <RowValue>
<Value>260944</Value>
</RowValue>
_ <RowValue>
<Value>41900</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>17</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
_ <RowValue>
<Value>/nfsserv/3pc/6/cs</Value>
</RowValue>
_ <RowValue>
<Value>4096</Value>
</RowValue>
_ <RowValue>
<Value>875344</Value>
</RowValue>
```

```
_ <RowValue>
<Value>600004</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>16</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
_ <RowValue>
<Value>/nfsserv/usp</Value>
</RowValue>
_ <RowValue>
<Value>4096</Value>
</RowValue>
_ <RowValue>
<Value>514896</Value>
</RowValue>
_ <RowValue>
<Value>13871</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
_ <RowOfValues>
_ <RowValue>
<Value>15</Value>
</RowValue>
_ <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
```

```
_ <RowValue>
<Value>/nfsserv/3pc/5/mtc</Value>
</RowValue>
_ <RowValue>
<Value>4096</Value>
</RowValue>
_ <RowValue>
<Value>260944</Value>
</RowValue>
_ <RowValue>
<Value>37460</Value>
</RowValue>
_ <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
_ <SingleValues MeasurementKind="Snapshot" IntervalDuration="5">
_ <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
<MeasureId>sysDescr</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.system</MeasureSuppId1>
<Value>Linux langley40 2.4.19-xf8 #1 SMP Fri Nov 7 11:18:05 EST 2003 i686</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
<MeasureId>snmpOutPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>106051</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
<MeasureId>snmpInBadVersions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
```

```
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
<MeasureId>snmpInBadCommunityNames</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>7</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
<MeasureId>snmpInTotalReqVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>559860</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
<MeasureId>snmpOutTraps</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>13442</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
<MeasureId>snmpInBadCommunityUses</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
<MeasureId>snmpInPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>97188</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
```

```
<MeasureId>snmpInTotalSetVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
<MeasureId>snmpInASNParseErrs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
<MeasureId>snmpSilentDrops</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-03-15T15:35:01EST</CaptureTime>
<MeasureId>hrSystemDate</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.host.hrSystem</MeasureSuppId1>
<Value>2005-3-15,20:35:1.0,+0:0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-03-15T15:35:01EST</CaptureTime>
<MeasureId>hrSystemUptime</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.host.hrSystem</MeasureSuppId1>
<Value>1642231</Value>
<Reliability>Valid</Reliability>
</SingleValue>
_ <SingleValue>
<CaptureTime>2005-03-15T15:35:01EST</CaptureTime>
<MeasureId>hrSystemProcesses</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.host.hrSystem</MeasureSuppId1>
<Value>80</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
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonPerfRecord_V2.0.xsd,2005-03-15T15:10:04EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId
47.166.56.10

Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTable.hrStorageEntry,Snapshot,5,2005-03-15T15:10:01EST
Label,Label,Label,Label,Label,Label,Label,Label
hrStorageIndex,hrStorageType,hrStorageDescr,hrStorageAllocationUnits,hrStorageSize,h
rStorageUsed,hrStorageAllocationFailures
Value,Value,Value,Value,Value,Value,Value,Value
14,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/5/cs,4096,924496,591
998,0
13,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/4/mtc,4096,260944,71
427,0
12,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/4/cs,4096,924496,505
263,0

```

```
11,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/3/mtc,4096,260944,66
723,0

10,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/3/cs,4096,924496,486
565,0

103,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageOther,Memory Buffers,256,53462,0,1026

102,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageVirtualMemory,Swap Space,1024,0,0,1025

101,.iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTypes.hrStorageRam,Real
Memory,1024,514140,381096,769

22,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/8/mtc,4096,260944,39
834,0

21,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/8/cs,4096,875344,639
076,0

9,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/2/mtc,4096,260944,41
535,0

20,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/7/mtc,4096,260944,37
872,0

8,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/2/cs,4096,924496,627
594,0

7,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/1/mtc,4096,260944,64
173,0

6,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/1/cs,4096,924496,484
559,0

5,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/0/mtc,4096,260944,41
693,0

4,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/0/cs,4096,924496,667
345,0

3,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/storm,4096,260944,298,0

2,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/boot,1024,101018,58993,0

1,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/,1024,59301,53462,0

19,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/7/cs,4096,875344,551
564,0
```

```
18,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/6/mtc,4096,260944,41
895,0

17,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/6/cs,4096,875344,600
004,0

16,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/usp,4096,514896,13870,0

15,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/5/mtc,4096,260944,37
451,0
```

Table=End

SingleValues=Begin

MeasurementKind,IntervalDuration

Snapshot,5

MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability

sysDescr,2005-03-15T15:10:00EST,.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,2005-03-15T15:10:00EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,105897,Valid

snmpInBadVersions,2005-03-15T15:10:00EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid

snmpInBadCommunityNames,2005-03-15T15:10:00EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,7,Valid

snmpInTotalReqVars,2005-03-15T15:10:00EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,559127,Valid

snmpOutTraps,2005-03-15T15:10:00EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,13412,Valid

snmpInBadCommunityUses,2005-03-15T15:10:00EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid

snmpInPkts,2005-03-15T15:10:00EST,.iso.org.dod.internet.mgmt.mib-2.snmp,97059,Valid

snmpInTotalSetVars,2005-03-15T15:10:00EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid

snmpInASNParseErrs,2005-03-15T15:10:00EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid

snmpSilentDrops,2005-03-15T15:10:00EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid

hrSystemDate,2005-03-15T15:10:01EST,.iso.org.dod.internet.mgmt.mib-
2.host.hrSystem,2005-3-15,20:10:1.0,+0:0,Valid

hrSystemUptime,2005-03-15T15:10:01EST,.iso.org.dod.internet.mgmt.mib-
2.host.hrSystem,1640731,Valid

hrSystemProcesses,2005-03-15T15:10:01EST,.iso.org.dod.internet.mgmt.mib-
2.host.hrSystem,79,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

- NN10110-511 - STORM Configuration
- NN10054-711 - STORM Performance Management
- 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 NN10139-711 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:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<PMFile xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonPerfRecord_V2.0.xsd" MeasurementCategory="PM">
<FileCreationTime>2005-01-13T14:15:01EST</FileCreationTime>
<System>
<SystemId>NortelNetworks/IEMS</SystemId>
<Entity>
<EntityId>47.142.89.82</EntityId>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasResourceMan
agerObjects.norUasRequestStatsTable.norUasRequestStatsEntry</TableId>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<Labels>
<Label>norUasResourceName</Label>
<Label>norUasRequestCount</Label>
<Label>norUasRequestsFailed</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>EndpointIdPool5</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>EndpointIdPool4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>EndpointIdPool3</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>EndpointIdPool2</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>EndpointIdPool1</Value>
</RowValue>
<RowValue>
<Value>4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
```



```
<Value>EndpointIdPool0</Value>
</RowValue>
<RowValue>
<Value>103</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<SingleValues MeasurementKind="Snapshot" IntervalDuration="5">
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasMgcpMessageRetransmissionFailures</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>3771</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasAckfail</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasProterror</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasAudioSegmentFailed</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
```

```
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasCompeerror</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasProtocolSyntaxErrors</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:01EST</CaptureTime>
<MeasureId>norUasNumberOfPlayRecordErrors</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasIVRS
erviceObjects</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasConfLackOfResourceRejections</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasConf
ServiceObjects</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasConfTotal</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasConf
ServiceObjects</MeasureSuppId1>
```

```
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasConfPlays</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasConf
ServiceObjects</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:01EST</CaptureTime>
<MeasureId>norUasNumberOfPlayRecords</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasIVRS
erviceObjects</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasRestart</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasConndeleted</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasProtocolMessageValidationErrors</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
```

```
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasUdpReceiveErrors</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>10</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasNumDupsForOutstandingTransactions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasEndpointsInUse</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasTimeout</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>1256</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasNumDupsForCompletedTransactions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
```

```
<Value>3</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasUdpSendErrors</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasCallControlMessageSendFailures</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>1257</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasMgcpMessageRetransmissions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>3771</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasAudioSegmentPlayed</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>134</Value>
<Reliability>Valid</Reliability>
</SingleValue>
</SingleValues>
</Entity>
</System>
</PMFile>
```

CSV

The following is an example of performance data for UAS in CSV format:

```
PMFile=Begin
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonPerfRecord_V2.0.xsd,2005-03-17T16:30:01EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId
47.142.89.82

Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasResourceManagerOb
jects.norUasRequestStatsTable.norUasRequestStatsEntry,Snapshot,5,2005-03-
17T16:30:00EST
Label,Label,Label
norUasResourceName,norUasRequestCount,norUasRequestsFailed
Value,Value,Value
EndpointIdPool5,0,0
EndpointIdPool4,7,0
EndpointIdPool3,21,0
EndpointIdPool2,0,0
EndpointIdPool1,62,0
EndpointIdPool0,116,0
Table=End

SingleValues=Begin
MeasurementKind,IntervalDuration
Snapshot,5
MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability
norUasUdpSendErrors,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasNumDupsForCompletedTransactions,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,15,Valid
norUasCallControlMessageSendFailures,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,1,Valid
norUasMgcpMessageRetransmissions,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,4,Valid
norUasAudioSegmentPlayed,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,134,Valid
norUasTimeout,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasRestart,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasConndeleted,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
```

```
norUasProtocolMessageValidationErrors,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasUdpReceiveErrors,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,2,Valid
norUasNumDupsForOutstandingTransactions,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasEndpointsInUse,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasMgcpMessageRetransmissionFailures,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,3,Valid
norUasAckfail,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasProterror,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasAudioSegmentFailed,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasComperror,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasProtocolSyntaxErrors,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasConfLackOfResourceRejections,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
onfServiceObjects,0,Valid
norUasConfTotal,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
onfServiceObjects,10,Valid
norUasConfPlays,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
onfServiceObjects,2,Valid
norUasNumberOfPlayRecords,2005-03-
17T16:30:01EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasI
VRServiceObjects,0,Valid
norUasNumberOfPlayRecordErrors,2005-03-
17T16:30:01EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasI
VRServiceObjects,0,Valid
SingleValues=End
```

Entity=End

System=End

PMFile=End

GUI/CLUI Documentation for UAS

GUI Launching and User procedures

- NN10010-111 - UAS Basics

Related documents

- NTP NN10095-511 - Universal Audio Server Basics
- NN10095-511 - Universal Audio Server Configuration Management
- NN10161-611 - Universal Audio Server Security and Administration

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 :

- NN10071-911 - USP Fault Management
- NN10072-911 - 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	Refer to the .1.3.6.1.4.1.562.2 9.6.1.1.1.3 varbind: Log Group =<text> & Log Number =<number>.	Specific Problem: Log Group =<text> & Log Number=<number> <r> Note: Log GroupID is not used	NN10071-911 USP Fault Management

Note: All USP alarm raise events are mapped to a USP398 event in the IEMS. In addition, all USP alarm clear events are mapped to a USP399. Refer to the USP device documentation for a detailed description of these events.

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 are examples of a USP log in NTSTD format:

```
znc0s0jh * USP398 FEB17 01:09:59 0010 FLT  USP Fault
    Location: 47.142.87.127-Unit-0;47.142.87.127
    Notification Id: 1034
    State: Raised
    Category: communications
    Cause: communicationsSubsystemFailure
    Time: Feb 17 01:09:59 2006
    Component Id: USP=COMP4;Shelf=0;Slot=12;ContextID=0x1010101
    Specific Problem: Log GroupID=32;Log Group=Network;Log Number=0
    Description: Connectivity lost: 1 1.1.1.1
```

```
znc0s0jh  USP399 FEB17 01:10:21 0011 INFO USP Fault
    Location: 47.142.87.127-Unit-0;47.142.87.127
    Notification Id: 1029
    State: Cleared
```

Time: Feb 17 01:10:21 2006

Component Id: USP=COMP4;Shelf=0;Slot=15;ContextID=0x1010101

Description: netping entry deleted: 1 1.1.1.1

SNMP

The following is an example of a USP log alarm raise and log alarm clear in SNMP format:

USP 398: Alarm Raise

```
.1.3.6.1.2.1.1.3.0: TimeTicks: 2 hours, 13 minutes, 19 seconds.:
.1.3.6.1.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.303:
.1.3.6.1.2.1.118.1.2.2.1.10: Object ID:
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.28.50.4
8.48.54.45.48.50.45.49.55.44.48.49.58.48.57.58.53.57.46.48.44.45.48.53.58.48.48.2
80155:
.1.3.6.1.2.1.118.1.2.2.1.2: 07 d6 02 11 01 09 3b 00 2d 05 00:
.1.3.6.1.2.1.118.1.2.2.1.11: STRING: Connectivity lost: 1 1.1.1.1:
.1.3.6.1.4.1.562.29.6.1.1.1.1: INTEGER: 2:
.1.3.6.1.4.1.562.29.6.1.1.1.2: INTEGER: 505:
.1.3.6.1.4.1.562.29.6.1.1.1.3: STRING: Log GroupID=32;Log Group=Network;Log
Number=0:
.1.3.6.1.4.1.562.29.6.1.1.1.4: STRING: USP398:
.1.3.6.1.4.1.562.29.6.1.1.1.5: STRING: IEMS=USP-1349-Unit-
0;USP=COMP4;Shelf=0;Slot=12;ContextID=0x1010101:
.1.3.6.1.4.1.562.29.6.1.1.1.6: INTEGER: 2:
.1.3.6.1.4.1.562.29.6.1.1.1.7: INTEGER: 48:
```

USP 399: Alarm Clear

```
.1.3.6.1.2.1.1.3.0: TimeTicks: 2 hours, 13 minutes, 41 seconds.:
.1.3.6.1.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.301:
.1.3.6.1.2.1.118.1.2.2.1.10: Object ID:
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.28.50.4
8.48.54.45.48.50.45.49.55.44.48.49.58.49.48.58.50.49.46.48.44.45.48.53.58.48.48.2
80149:
.1.3.6.1.2.1.118.1.2.2.1.2: 07 d6 02 11 01 0a 15 00 2d 05 00:
.1.3.6.1.2.1.118.1.2.2.1.11: STRING: DeviceSpecificInfo=;netping entry deleted: 1
1.1.1.1:
.1.3.6.1.4.1.562.29.6.1.1.1.1: INTEGER: 2:
.1.3.6.1.4.1.562.29.6.1.1.1.2: INTEGER: 1024:
.1.3.6.1.4.1.562.29.6.1.1.1.3: STRING: :
.1.3.6.1.4.1.562.29.6.1.1.1.4: STRING: USP399:
.1.3.6.1.4.1.562.29.6.1.1.1.5: STRING: IEMS=USP-1349-Unit-
0;USP=COMP4;Shelf=0;Slot=15;ContextID=0x1010101:
.1.3.6.1.4.1.562.29.6.1.1.1.7: INTEGER: 49:
```

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

- NN10137-711 - USP Performance Management
- NN10138-711 - 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.

Note that for SN08, the OMs/PMs are provided in raw CSV format.

XML

The following is an example of performance data for USP 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="commonPerfRecord_V2.0.xsd"
MeasurementCategory="PM">
<FileCreationTime>2004-12-09T16:30:20EST</FileCreationTime>
<System>
<SystemId>NortelNetworks/IEMS</SystemId>
<Entity>
<EntityId>47.135.60.71</EntityId>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>Linkset Utilization</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Linkset Inactivity Duration</Label>
<Label>RST Received Count</Label>
<Label>RST Transmitted Count</Label>
<Label>TFA and TCA Received Count</Label>
<Label>TFA and TCA Transmitted Count</Label>
<Label>TFC Received Count</Label>
<Label>TFC Transmitted Count</Label>
<Label>TFP and TCP Received Count</Label>
<Label>TFP and TCP Transmitted Count</Label>
<Label>TFR and TCR Received Count</Label>
<Label>TFR and TCR Transmitted Count</Label>
<Label>UPU Received Count</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
```

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]


```
<Label>Sent MSUs Count</Label>
<Label>Terminated MSUs Count</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>8378</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</RowOfValues>
```

```
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>8378</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>8378</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>8378</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
```

```
<Value/>
</RowValue>
<RowValue>
<Value>8378</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>8378</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>8378</Value>
```

```
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>8376</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```



```
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value/>  
</RowValue>  
</RowOfValues>  
<RowOfValues>  
<RowValue>  
<Value/>  
</RowValue>  
<RowValue>  
<Value/>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value/>  
</RowValue>  
</RowOfValues>  
<RowOfValues>  
<RowValue>  
<Value/>  
</RowValue>  
<RowValue>  
<Value/>  
</RowValue>  
<RowValue>  
<Value/>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value/>  
</RowValue>  
<RowValue>  
<Value/>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value/>  
</RowValue>  
<RowValue>  
<Value/>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value/>  
</RowValue>  
<RowValue>  
<Value/>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value/>  
</RowValue>
```

```
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
```

```
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
```

```

<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>SCCP System Totals</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Conn-Orient IP Dist Viol Count</Label>
<Label>Conn-Orient Msg Handled Count</Label>
<Label>Conn-Orient Msg Rtg Fail Count</Label>
<Label>LU DT Msg Rcvd Count</Label>
<Label>LU DT Msg Sent Count</Label>
<Label>LU DT S Msg Sent Count</Label>
<Label>MSUs Disc-Unrec SCCP Msg Count</Label>
<Label>Msg Incompatibility</Label>
<Label>Msg too large for segmentation</Label>
<Label>Out of sequence SCCP msg count</Label>
<Label>Reassembly Timer Expired</Label>
<Label>Reassembly buffer unavailable</Label>
<Label>Reassembly failed</Label>
<Label>Routing Failure - Unequip.User</Label>
<Label>SCCP Routing Failure Count</Label>
<Label>SSA Received Count</Label>
<Label>SSA Transmitted Count</Label>
<Label>SSP Received Count</Label>
<Label>SSP Transmitted Count</Label>
<Label>SST Received Count</Label>
<Label>SST Transmitted Count</Label>
<Label>Segmentation failed</Label>
<Label>Total messages handled</Label>
<Label>UDT Msg Rcvd Count</Label>

```


[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>System Node State</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Disabled, Locked Duration</Label>
<Label>Disabled, Unlocked Duration</Label>
<Label>Enabled, Locked Duration</Label>
<Label>Enabled, Unlocked Duration</Label>
<Label>Locked, Off-line Duration</Label>
<Label>Percentage Enabled</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
```

```
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<Value>0</Value>
</RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<Value>0</Value>
</RowValue>
<Value>0</Value>
</RowValue>
<Value>0</Value>
</RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>SCTP Management/Traffic Counts</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Association Aborted Count</Label>
<Label>Association Establish Attempts</Label>
<Label>Association Terminated Count</Label>
<Label>Chunk Retransmitted Count</Label>
<Label>Chunks Received Count</Label>
<Label>Chunks Transmitted Count</Label>
<Label>Established Association Count</Label>
<Label>Out of Blue SCTP Packet</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
```



```
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>Gateway Screening Results</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Disallowed Cld Party Addr Count</Label>
<Label>Disallowed ISUP Count</Label>
<Label>Disallowed Trans Type Count</Label>
<Label>Invalid Affct Destination Count</Label>
<Label>Invalid Affct PC-SSN Count</Label>
<Label>Invalid Cng Party Addr Count</Label>
<Label>Invalid DPC Count</Label>
<Label>Invalid OPC Count</Label>
<Label>Invalid SIO Count</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

[illegible]

[illegible]

[illegible]

[illegible]


```
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>Task Management</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Collection Period Duration</Label>
<Label>Idle Task Duration</Label>
<Label>Level 0 Priority Task Duration</Label>
<Label>Level 1 Priority Task Duration</Label>
<Label>Level 2 Priority Task Duration</Label>
<Label>Level 3 Priority Task Duration</Label>
<Label>Level 4 Priority Task Duration</Label>
<Label>Level 5 Priority Task Duration</Label>
<Label>Level 6 Priority Task Duration</Label>
<Label>Level 7 Priority Task Duration</Label>
<Label>Level 8 Priority Task Duration</Label>
<Label>Level 9 Priority Task Duration</Label>
<Label>OS System Tasks Duration</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>300020</Value>
</RowValue>
<RowValue>
<Value>299580</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>18</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
<RowValue>
<Value>12</Value>
</RowValue>
<RowValue>
<Value>44</Value>
</RowValue>
<RowValue>
<Value>87</Value>
</RowValue>
<RowValue>
<Value>4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>93</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>143</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300020</Value>
</RowValue>
```

```
<RowValue>
<Value>299644</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>19</Value>
</RowValue>
<RowValue>
<Value>30</Value>
</RowValue>
<RowValue>
<Value>11</Value>
</RowValue>
<RowValue>
<Value>42</Value>
</RowValue>
<RowValue>
<Value>81</Value>
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>39</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>143</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300020</Value>
</RowValue>
<RowValue>
<Value>298200</Value>
</RowValue>
<RowValue>
<Value>23</Value>
</RowValue>
<RowValue>
<Value>140</Value>
</RowValue>
<RowValue>
<Value>256</Value>
</RowValue>
<RowValue>
<Value>95</Value>
</RowValue>
<RowValue>
<Value>381</Value>
</RowValue>
<RowValue>
<Value>320</Value>
</RowValue>
<RowValue>
<Value>29</Value>
```

```
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
<RowValue>
<Value>46</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>522</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300010</Value>
</RowValue>
<RowValue>
<Value>213491</Value>
</RowValue>
<RowValue>
<Value>29</Value>
</RowValue>
<RowValue>
<Value>199</Value>
</RowValue>
<RowValue>
<Value>942</Value>
</RowValue>
<RowValue>
<Value>131</Value>
</RowValue>
<RowValue>
<Value>419</Value>
</RowValue>
<RowValue>
<Value>83882</Value>
</RowValue>
<RowValue>
<Value>35</Value>
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
<RowValue>
<Value>53</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>820</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300000</Value>
</RowValue>
<RowValue>
<Value>293717</Value>
</RowValue>
<RowValue>
<Value>9</Value>
```

```
</RowValue>
<RowValue>
<Value>143</Value>
</RowValue>
<RowValue>
<Value>173</Value>
</RowValue>
<RowValue>
<Value>42</Value>
</RowValue>
<RowValue>
<Value>275</Value>
</RowValue>
<RowValue>
<Value>216</Value>
</RowValue>
<RowValue>
<Value>4563</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>241</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>616</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300000</Value>
</RowValue>
<RowValue>
<Value>268732</Value>
</RowValue>
<RowValue>
<Value>10</Value>
</RowValue>
<RowValue>
<Value>69</Value>
</RowValue>
<RowValue>
<Value>332</Value>
</RowValue>
<RowValue>
<Value>45</Value>
</RowValue>
<RowValue>
<Value>161</Value>
</RowValue>
<RowValue>
<Value>30313</Value>
</RowValue>
<RowValue>
<Value>15</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
```

```
<Value>28</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>290</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>299990</Value>
</RowValue>
<RowValue>
<Value>211715</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>3405</Value>
</RowValue>
<RowValue>
<Value>18873</Value>
</RowValue>
<RowValue>
<Value>790</Value>
</RowValue>
<RowValue>
<Value>12939</Value>
</RowValue>
<RowValue>
<Value>1461</Value>
</RowValue>
<RowValue>
<Value>219</Value>
</RowValue>
<RowValue>
<Value>38315</Value>
</RowValue>
<RowValue>
<Value>68</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>12200</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300000</Value>
</RowValue>
<RowValue>
<Value>211866</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>3381</Value>
</RowValue>
<RowValue>
```



```
<Value>18854</Value>
</RowValue>
<RowValue>
<Value>792</Value>
</RowValue>
<RowValue>
<Value>13024</Value>
</RowValue>
<RowValue>
<Value>1171</Value>
</RowValue>
<RowValue>
<Value>211</Value>
</RowValue>
<RowValue>
<Value>38497</Value>
</RowValue>
<RowValue>
<Value>68</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>12131</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300000</Value>
</RowValue>
<RowValue>
<Value>299319</Value>
</RowValue>
<RowValue>
<Value>7</Value>
</RowValue>
<RowValue>
<Value>48</Value>
</RowValue>
<RowValue>
<Value>89</Value>
</RowValue>
<RowValue>
<Value>34</Value>
</RowValue>
<RowValue>
<Value>137</Value>
</RowValue>
<RowValue>
<Value>128</Value>
</RowValue>
<RowValue>
<Value>11</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>26</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>196</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300020</Value>
</RowValue>
<RowValue>
<Value>299818</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>18</Value>
</RowValue>
<RowValue>
<Value>30</Value>
</RowValue>
<RowValue>
<Value>9</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>46</Value>
</RowValue>
<RowValue>
<Value>4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>40</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>42</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300020</Value>
</RowValue>
<RowValue>
<Value>299819</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>18</Value>
</RowValue>
<RowValue>
<Value>29</Value>
</RowValue>
<RowValue>
<Value>9</Value>
</RowValue>
```

```
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>46</Value>
</RowValue>
<RowValue>
<Value>4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>40</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>42</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300030</Value>
</RowValue>
<RowValue>
<Value>299600</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>18</Value>
</RowValue>
<RowValue>
<Value>31</Value>
</RowValue>
<RowValue>
<Value>11</Value>
</RowValue>
<RowValue>
<Value>43</Value>
</RowValue>
<RowValue>
<Value>79</Value>
</RowValue>
<RowValue>
<Value>4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>92</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>144</Value>
</RowValue>
</RowOfValues>
</Table>
```


[illegible]

```
<RowValue>
<Value>70</Value>
</RowValue>
<RowValue>
<Value>67022</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>8376</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1474484</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>134016</Value>
</RowValue>
<RowValue>
<Value>134016</Value>
</RowValue>
<RowValue>
<Value>67022</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

[illegible]


```
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
</RowOfValues>  
<RowOfValues>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value/>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value/>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>
```



```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>ISUP Received Message Counts</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>ACM Received Count</Label>
<Label>ALT Received Count</Label>
<Label>ANM Received Count</Label>
<Label>BLA Received Count</Label>
<Label>BLO Received Count</Label>
<Label>CCR Received Count</Label>
<Label>CFN Received Count</Label>
<Label>CGB Received Count</Label>
<Label>CGBA Received Count</Label>
<Label>CGU Received Count</Label>
<Label>CGUA Received Count</Label>
<Label>CMC Received Count</Label>
<Label>CMR Received Count</Label>
<Label>CMRJ Received Count</Label>
<Label>CON Received Count</Label>
<Label>COT Received Count</Label>
<Label>CPG Received Count</Label>
<Label>CQM Received Count</Label>
<Label>CQR Received Count</Label>
<Label>CRA Received Count</Label>
<Label>CRG Received Count</Label>
<Label>CRM Received Count</Label>
<Label>CSV Received Count</Label>
<Label>CSV Received Count</Label>
```


[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]


```
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
</RowOfValues>  
<RowOfValues>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
</RowOfValues>  
<RowOfValues>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
</RowOfValues>  
<RowOfValues>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
</RowOfValues>  
<RowOfValues>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>
```

[illegible]

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</RowOfValues>
```

```
<RowOfValues>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
</RowOfValues>  
<RowOfValues>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
</RowOfValues>  
<RowOfValues>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
</RowOfValues>  
<RowOfValues>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
</RowOfValues>  
<RowOfValues>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
<RowValue>  
<Value>0</Value>  
</RowValue>  
</RowOfValues>
```



```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>Link Management</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Changeover Procedure Count</Label>
<Label>Far End Mgmt Inhibit Count</Label>
<Label>Level 1 Congestion Count</Label>
<Label>Level 1 Congestion Duration</Label>
<Label>Level 2 Congestion Count</Label>
<Label>Level 2 Congestion Duration</Label>
<Label>Level 3 Congestion Count</Label>
<Label>Level 3 Congestion Duration</Label>
<Label>Link Available Duration</Label>
<Label>Link Deactivated Duration</Label>
<Label>Link Local Inhibit Duration</Label>
<Label>Link Remote Inhibit Duration</Label>
<Label>Near End Forced Unavailable Cou</Label>
<Label>RPO Count</Label>
<Label>RPO Cumulative Duration</Label>
<Label>Unavailable Duration</Label>
</Labels>
<RowOfValues>
<RowValue>
```

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]


```
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>BICC Received Message Counts</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>BICC Call P Received Count</Label>
<Label>BICC Error No OPC Route</Label>
<Label>BICC Error No Path</Label>
<Label>BICC Error No Route</Label>
<Label>BICC Maint Received Count</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```


[illegible]

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
```



```
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>ASP Path Management</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Path Down Time</Label>
<Label>Path Restore Time</Label>
<Label>Path Up Time</Label>
<Label>Path entered Down state</Label>
<Label>Path entered Restoring state</Label>
<Label>Path entered Up state</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</Table>
```

```
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</RowOfValues>
```

```
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>Carrier</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Far End Line - Errored Seconds</Label>
<Label>Far End P - Sev Err Frm/AIS Sec</Label>
<Label>Far End P - Severely Err Secs</Label>
<Label>Far End P - Unavailable Seconds</Label>
<Label>Far End Path - Code Violations</Label>
<Label>Far End Path - Controlled Slips</Label>
<Label>Far End Path - Errored Seconds</Label>
<Label>Far End Path - Failure Count</Label>
<Label>Line - Code Violations</Label>
<Label>Line - Errored Seconds</Label>
<Label>Line - Loss of Signal Seconds</Label>
<Label>Line - Severely Errored Seconds</Label>
<Label>P - Severely Err Frame/AIS Secs</Label>
<Label>Path - AIS Seconds</Label>
<Label>Path - Code Violations</Label>
<Label>Path - Errored Seconds</Label>
<Label>Path - Failure Count</Label>
<Label>Path - Severely Errored Seconds</Label>
<Label>Path - Unavailable Seconds</Label>
</Labels>
```



```
<Label>Plane 2 Messages Count</Label>
<Label>Raw Cell Count</Label>
<Label>Raw Message Count</Label>
<Label>SSCOP Message Count</Label>
<Label>Sequence Number Reset Count</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>1725</Value>
</RowValue>
<RowValue>
<Value>634</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1725</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1725</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1091</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>1730</Value>
</RowValue>
<RowValue>
<Value>634</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1730</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1730</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
```

```
<Value>1096</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>1721</Value>
</RowValue>
<RowValue>
<Value>634</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1721</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1721</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1087</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>24365</Value>
</RowValue>
<RowValue>
<Value>634</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>24365</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>24365</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>23731</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>1997</Value>
</RowValue>
<RowValue>
<Value>869</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1997</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1997</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1128</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>24364</Value>
</RowValue>
<RowValue>
<Value>634</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>24364</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>24364</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```



```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>1721</Value>
</RowValue>
<RowValue>
<Value>634</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1721</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1721</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1721</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1087</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>1114</Value>
</RowValue>
<RowValue>
<Value>34</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1114</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1114</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>1080</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>1114</Value>
</RowValue>
<RowValue>
<Value>34</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1114</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1114</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1080</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>1729</Value>
</RowValue>
<RowValue>
<Value>634</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1729</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1729</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```



```

<Label>Trans Type Not Found Count</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
</Entity>
</System>
</PMFile>

```

CSV

The following is an example of performance data for USP in CSV format:

```

NOA;Task Management;LINK_NODE_3_1;Level 0 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;23
NOA;Task Management;LINK_NODE_3_1;Level 1 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;128
NOA;Task Management;LINK_NODE_3_1;Level 2 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;348
NOA;Task Management;LINK_NODE_3_1;Level 3 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;105
NOA;Task Management;LINK_NODE_3_1;Level 4 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;377
NOA;Task Management;LINK_NODE_3_1;Level 5 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;345
NOA;Task Management;LINK_NODE_3_1;Level 6 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;33
NOA;Task Management;LINK_NODE_3_1;Level 7 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;3
NOA;Task Management;LINK_NODE_3_1;Level 8 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;149
NOA;Task Management;LINK_NODE_3_1;Level 9 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;LINK_NODE_3_1;OS System Tasks Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;542
NOA;Task Management;LINK_NODE_3_1;Collection Period Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300000
NOA;Task Management;LINK_NODE_4_1;Level 0 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;23
NOA;Task Management;LINK_NODE_4_1;Level 1 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;129
NOA;Task Management;LINK_NODE_4_1;Level 2 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;276
NOA;Task Management;LINK_NODE_4_1;Level 3 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;105
NOA;Task Management;LINK_NODE_4_1;Level 4 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;376

```

NOA;Task Management;LINK_NODE_4_1;Level 5 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;298
NOA;Task Management;LINK_NODE_4_1;Level 6 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;35
NOA;Task Management;LINK_NODE_4_1;Level 7 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;3
NOA;Task Management;LINK_NODE_4_1;Level 8 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;148
NOA;Task Management;LINK_NODE_4_1;Level 9 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;LINK_NODE_4_1;OS System Tasks Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;534
NOA;Task Management;LINK_NODE_4_1;Collection Period Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;299990
NOA;Task Management;CC_NODE_1_1;Level 0 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;CC_NODE_1_1;Level 1 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;3404
NOA;Task Management;CC_NODE_1_1;Level 2 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;18883
NOA;Task Management;CC_NODE_1_1;Level 3 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;794
NOA;Task Management;CC_NODE_1_1;Level 4 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;12846
NOA;Task Management;CC_NODE_1_1;Level 5 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;1479
NOA;Task Management;CC_NODE_1_1;Level 6 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;220
NOA;Task Management;CC_NODE_1_1;Level 7 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;38371
NOA;Task Management;CC_NODE_1_1;Level 8 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;70
NOA;Task Management;CC_NODE_1_1;Level 9 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;CC_NODE_1_1;OS System Tasks Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;12199
NOA;Task Management;CC_NODE_1_1;Collection Period Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;299990
NOA;Task Management;LINK_NODE_5_1;Level 0 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;23
NOA;Task Management;LINK_NODE_5_1;Level 1 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;137
NOA;Task Management;LINK_NODE_5_1;Level 2 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;402
NOA;Task Management;LINK_NODE_5_1;Level 3 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;109
NOA;Task Management;LINK_NODE_5_1;Level 4 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;380
NOA;Task Management;LINK_NODE_5_1;Level 5 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;378
NOA;Task Management;LINK_NODE_5_1;Level 6 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;34
NOA;Task Management;LINK_NODE_5_1;Level 7 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;3
NOA;Task Management;LINK_NODE_5_1;Level 8 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;148
NOA;Task Management;LINK_NODE_5_1;Level 9 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;LINK_NODE_5_1;OS System Tasks Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;540
NOA;Task Management;LINK_NODE_5_1;Collection Period Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;299990
NOA;Task Management;NODE_LINK_6_1;Level 0 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;22

NOA;Task Management;NODE_LINK_6_1;Level 1 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;148
NOA;Task Management;NODE_LINK_6_1;Level 2 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;399
NOA;Task Management;NODE_LINK_6_1;Level 3 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;109
NOA;Task Management;NODE_LINK_6_1;Level 4 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;383
NOA;Task Management;NODE_LINK_6_1;Level 5 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;382
NOA;Task Management;NODE_LINK_6_1;Level 6 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;35
NOA;Task Management;NODE_LINK_6_1;Level 7 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;3
NOA;Task Management;NODE_LINK_6_1;Level 8 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;148
NOA;Task Management;NODE_LINK_6_1;Level 9 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;NODE_LINK_6_1;OS System Tasks Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;542
NOA;Task Management;NODE_LINK_6_1;Collection Period Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;299990
NOA;Task Management;IP_LINK_NODE_9;Level 0 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;2
NOA;Task Management;IP_LINK_NODE_9;Level 1 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;26
NOA;Task Management;IP_LINK_NODE_9;Level 2 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;34
NOA;Task Management;IP_LINK_NODE_9;Level 3 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;13
NOA;Task Management;IP_LINK_NODE_9;Level 4 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;42
NOA;Task Management;IP_LINK_NODE_9;Level 5 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;418
NOA;Task Management;IP_LINK_NODE_9;Level 6 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;4
NOA;Task Management;IP_LINK_NODE_9;Level 7 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;IP_LINK_NODE_9;Level 8 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;41
NOA;Task Management;IP_LINK_NODE_9;Level 9 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;IP_LINK_NODE_9;OS System Tasks Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;225
NOA;Task Management;IP_LINK_NODE_9;Collection Period Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300010
NOA;Task Management;IP_LINK_NODE_10;Level 0 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;2
NOA;Task Management;IP_LINK_NODE_10;Level 1 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;24
NOA;Task Management;IP_LINK_NODE_10;Level 2 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;33
NOA;Task Management;IP_LINK_NODE_10;Level 3 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;13
NOA;Task Management;IP_LINK_NODE_10;Level 4 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;43
NOA;Task Management;IP_LINK_NODE_10;Level 5 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;415
NOA;Task Management;IP_LINK_NODE_10;Level 6 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;4
NOA;Task Management;IP_LINK_NODE_10;Level 7 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;IP_LINK_NODE_10;Level 8 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;42

NOA;Task Management;IP_LINK_NODE_10;Level 9 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;IP_LINK_NODE_10;OS System Tasks Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;224
NOA;Task Management;IP_LINK_NODE_10;Collection Period Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300010
NOA;Task Management;RTC_NODE_15;Level 0 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;3
NOA;Task Management;RTC_NODE_15;Level 1 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;45
NOA;Task Management;RTC_NODE_15;Level 2 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;58
NOA;Task Management;RTC_NODE_15;Level 3 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;13
NOA;Task Management;RTC_NODE_15;Level 4 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;99
NOA;Task Management;RTC_NODE_15;Level 5 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;130
NOA;Task Management;RTC_NODE_15;Level 6 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;1399
NOA;Task Management;RTC_NODE_15;Level 7 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;RTC_NODE_15;Level 8 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;119
NOA;Task Management;RTC_NODE_15;Level 9 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;RTC_NODE_15;OS System Tasks Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;131
NOA;Task Management;RTC_NODE_15;Collection Period Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;299990
NOA;Task Management;CC_NODE_1_18;Level 0 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;CC_NODE_1_18;Level 1 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;3410
NOA;Task Management;CC_NODE_1_18;Level 2 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;19067
NOA;Task Management;CC_NODE_1_18;Level 3 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;791
NOA;Task Management;CC_NODE_1_18;Level 4 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;12798
NOA;Task Management;CC_NODE_1_18;Level 5 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;1479
NOA;Task Management;CC_NODE_1_18;Level 6 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;226
NOA;Task Management;CC_NODE_1_18;Level 7 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;38371
NOA;Task Management;CC_NODE_1_18;Level 8 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;67
NOA;Task Management;CC_NODE_1_18;Level 9 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;CC_NODE_1_18;OS System Tasks Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;12207
NOA;Task Management;CC_NODE_1_18;Collection Period Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;299980
NOA;System Node State;CC_NODE_1_1;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;100
NOA;System Node State;LINK_NODE_3_1;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;100
NOA;System Node State;LINK_NODE_4_1;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;100
NOA;System Node State;LINK_NODE_5_1;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;100
NOA;System Node State;NODE_LINK_6_1;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;100

NOA;System Node State;IP_LINK_NODE_8;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;System Node State;IP_LINK_NODE_9;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;100
NOA;System Node State;IP_LINK_NODE_10;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;100
NOA;System Node State;IP_LINK_NODE_11;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;System Node State;RTC_NODE_12;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;100
NOA;System Node State;RTC_NODE_15;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;100
NOA;System Node State;CC_NODE_1_18;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;100
NOA;Task Management;RTC_NODE_12;Level 0 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;3
NOA;Task Management;RTC_NODE_12;Level 1 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;47
NOA;Task Management;RTC_NODE_12;Level 2 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;67
NOA;Task Management;RTC_NODE_12;Level 3 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;13
NOA;Task Management;RTC_NODE_12;Level 4 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;118
NOA;Task Management;RTC_NODE_12;Level 5 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;149
NOA;Task Management;RTC_NODE_12;Level 6 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;1554
NOA;Task Management;RTC_NODE_12;Level 7 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;RTC_NODE_12;Level 8 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;166
NOA;Task Management;RTC_NODE_12;Level 9 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;RTC_NODE_12;OS System Tasks Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;188
NOA;Task Management;RTC_NODE_12;Collection Period Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300000
ACC;System Node State;CC_NODE_1_18;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;CC_NODE_1_18;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;CC_NODE_1_18;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;CC_NODE_1_18;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;CC_NODE_1_18;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Log Server;RTC_NODE_12;Minor Alarms Cleared Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Log Server;RTC_NODE_12;Major Alarms Cleared Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Log Server;RTC_NODE_12;Critical Alarms Cleared Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Log Server;RTC_NODE_12;Minor Alarms Ack Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Log Server;RTC_NODE_12;Major Alarms Ack Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Log Server;RTC_NODE_12;Critical Alarms Ack Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0

ACC;Log Server;RTC_NODE_12;Minor Alarms Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Log Server;RTC_NODE_12;Major Alarms Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Log Server;RTC_NODE_12;Critical Alarms Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_12;Sequence Number Reset Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_12;Raw Cell Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_12;Raw Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_12;SSCOP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2930
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_12;IP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1392
ACC;ATM Driver Messaging;RTC_NODE_12;Duplicate Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;4322
ACC;ATM Driver Messaging;RTC_NODE_12;Plane 2 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;4322
ACC;ATM Driver Messaging;RTC_NODE_12;Plane 1 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;4322
ACC;ATM Driver Messaging;RTC_NODE_12;Plane 2 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_12;Plane 1 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_10;Association Terminated
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;MSUs Disc-Unrec SCCP Msg Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP GTT;USP:C7NETWRK1;Hop Counter Violation Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP GTT;USP:C7NETWRK1;Alt Routing on Cong Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP GTT;USP:C7NETWRK1;No Translation for Addr Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP GTT;USP:C7NETWRK1;Trans Type Not Found Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP GTT;USP:C7NETWRK1;GTT Performed Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;Conn-Orient IP Dist Viol Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;Conn-Orient Msg Rtg Fail Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;Conn-Orient Msg Handled Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;SCCP Routing Failure Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;Reassembly failed;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;Segmentation failed;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;Msg too large for segmentation;;03/24/2005
15:15:00;03/24/2005 15:20:00;0

```
ACC;SCCP System Totals;USP:C7NETWRK1;Reassembly Timer Expired;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;Reassembly buffer unavailable;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;Out of sequence SCCP msg count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;Msg Incompatibility;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;LUDTS Msg Sent Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;LUDT Msg Sent Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;LUDT Msg Rcvd Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;XUDTS Msg Rcvd Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;XUDT Msg Rcvd Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;XUDTS Msg Sent Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;XUDT Msg Sent Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;UDTS Msg Rcvd Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;UDT Msg Rcvd Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;UDTS Msg Sent Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;UDT Msg Sent Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;SST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;SST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;SSA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;SSA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;SSP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;SSP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_10;Association Aborted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_10;Established Association
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;6
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_10;Association Establish
Attempts;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_10;Chunk Retransmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_10;Chunks Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_10;Chunks Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_10;Out of Blue SCTP
Packet;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;IP_LINK_NODE_10;Sequence Number Reset Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;IP_LINK_NODE_10;Raw Cell Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;IP_LINK_NODE_10;Raw Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC14_PVG190A PID:1;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

ACC;ATM Driver Messaging;IP_LINK_NODE_10;SSCOP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;878
ACC;ATM Driver Messaging;IP_LINK_NODE_10;IP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;624
ACC;ATM Driver Messaging;IP_LINK_NODE_10;Duplicate Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1502
ACC;ATM Driver Messaging;IP_LINK_NODE_10;Plane 2 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1502
ACC;ATM Driver Messaging;IP_LINK_NODE_10;Plane 1 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1502
ACC;ATM Driver Messaging;CC_NODE_1_18;Plane 1 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_18;Plane 2 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_18;Plane 1 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3054
ACC;ATM Driver Messaging;CC_NODE_1_18;Plane 2 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3054
ACC;ATM Driver Messaging;CC_NODE_1_18;Duplicate Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3054
ACC;ATM Driver Messaging;CC_NODE_1_18;IP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3054
ACC;ATM Driver Messaging;CC_NODE_1_18;SSCOP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_18;Raw Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_18;Raw Cell Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_18;Sequence Number Reset Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;RTC Sanity;CC_NODE_1_18; RTC12 Passive Audit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;RTC Sanity;CC_NODE_1_18; RTC15 Passive Audit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPA_INTL SLC:0;B/TUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPA_INTL SLC:0;B/TUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000001 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000001 SLC:0;B/TUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000001 SLC:0;B/TUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STEPBOX01 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Pri 3 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Pri 2 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Pri 1 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0


```
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Pri 3 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Pri 2 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Pri 1 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_3_1;Plane 1 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_3_1;Plane 2 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_3_1;Plane 1 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2022
ACC;ATM Driver Messaging;LINK_NODE_3_1;Plane 2 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2022
ACC;ATM Driver Messaging;LINK_NODE_3_1;Duplicate Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2022
ACC;ATM Driver Messaging;LINK_NODE_3_1;IP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;624
ACC;ATM Driver Messaging;LINK_NODE_3_1;SSCOP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1398
ACC;ATM Driver Messaging;LINK_NODE_3_1;Raw Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_3_1;Raw Cell Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_3_1;Sequence Number Reset Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_3_1;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_3_1;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_3_1;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;LINK_NODE_3_1;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_3_1;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_4_1;Plane 1 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_4_1;Plane 2 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_4_1;Plane 1 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1798
ACC;ATM Driver Messaging;LINK_NODE_4_1;Plane 2 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1798
ACC;ATM Driver Messaging;LINK_NODE_4_1;Duplicate Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1798
ACC;ATM Driver Messaging;LINK_NODE_4_1;IP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;624
ACC;ATM Driver Messaging;LINK_NODE_4_1;SSCOP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1174
ACC;ATM Driver Messaging;LINK_NODE_4_1;Raw Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ATM Driver Messaging;LINK_NODE_4_1;Raw Cell Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_4_1;Sequence Number Reset Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_4_1;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_4_1;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_4_1;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;LINK_NODE_4_1;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_4_1;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_5_1;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_5_1;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_5_1;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;LINK_NODE_5_1;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_5_1;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_5_1;Plane 1 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_5_1;Plane 2 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_5_1;Plane 1 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2217
ACC;ATM Driver Messaging;LINK_NODE_5_1;Plane 2 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2217
ACC;ATM Driver Messaging;LINK_NODE_5_1;Duplicate Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2217
ACC;ATM Driver Messaging;LINK_NODE_5_1;IP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;624
ACC;ATM Driver Messaging;LINK_NODE_5_1;SSCOP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1593
ACC;ATM Driver Messaging;LINK_NODE_5_1;Raw Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_5_1;Raw Cell Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_5_1;Sequence Number Reset Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;NODE_LINK_6_1;Plane 1 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;NODE_LINK_6_1;Plane 2 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;NODE_LINK_6_1;Plane 1 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2221
ACC;ATM Driver Messaging;NODE_LINK_6_1;Plane 2 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2221
ACC;ATM Driver Messaging;NODE_LINK_6_1;Duplicate Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2221
ACC;ATM Driver Messaging;NODE_LINK_6_1;IP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;624
ACC;ATM Driver Messaging;NODE_LINK_6_1;SSCOP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1597
ACC;ATM Driver Messaging;NODE_LINK_6_1;Raw Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;NODE_LINK_6_1;Raw Cell Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;NODE_LINK_6_1;Sequence Number Reset Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

ACC;System Node State;NODE_LINK_6_1;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;NODE_LINK_6_1;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;NODE_LINK_6_1;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;NODE_LINK_6_1;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;NODE_LINK_6_1;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;RTC_NODE_12;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;RTC_NODE_12;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;RTC_NODE_12;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_15;Sequence Number Reset Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_15;Raw Cell Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_15;Raw Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_15;SSCOP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2300
ACC;ATM Driver Messaging;RTC_NODE_15;IP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1351
ACC;ATM Driver Messaging;RTC_NODE_15;Duplicate Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3651
ACC;ATM Driver Messaging;RTC_NODE_15;Plane 2 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3651
ACC;ATM Driver Messaging;RTC_NODE_15;Plane 1 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3651
ACC;ATM Driver Messaging;RTC_NODE_15;Plane 2 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_15;Plane 1 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;RTC_NODE_15;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;RTC_NODE_15;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;RTC_NODE_15;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;RTC_NODE_15;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;RTC_NODE_15;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_10;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_10;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_10;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;IP_LINK_NODE_10;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_10;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;IP_LINK_NODE_10;Plane 2 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;IP_LINK_NODE_10;Plane 1 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0

```
ACC;Linkset Utilization;LS:ITUCLKSET3;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:CATTBOX01 SLC:0;Disallowed ISUP
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC14_PVG190A PID:1;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC14_PVG190A PID:1;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC14_PVG190A PID:1;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC14_PVG190A PID:1;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC14_PVG190A PID:1;Invalid SIO
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC14_PVG190A PID:1;Invalid DPC
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Task Management;LINK_NODE_3_1;Idle Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;297941
ACC;TUP Received Message Counts;LS:C7LKSET2 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET2 SLC:0;B/TUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET2 SLC:0;B/TUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPB_INTL SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPB_INTL SLC:0;B/TUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPB_INTL SLC:0;B/TUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000002 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000002 SLC:0;B/TUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000002 SLC:0;B/TUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
MAX;Link Traffic;LS:C7LKSET2 SLC:0;Link utilization;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

ACC;Linkset Utilization;LS:C7LKSET1;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0


```
ACC;Linkset Utilization;LS:ST000001;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

ACC;Linkset Utilization;LS:STPB_INTL;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC15_PVG192A PID:0;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC15_PVG192A PID:0;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC15_PVG192A PID:0;DAUD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC15_PVG192A PID:0;DUNA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC15_PVG192A PID:0;DAVA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:0;Discarded MTP3b MSUs
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:0;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:0;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:0;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC14_PVG190A PID:0;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC14_PVG190A PID:0;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC14_PVG190A PID:0;DAUD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC14_PVG190A PID:0;DUNA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC14_PVG190A PID:0;DAVA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:0;Discarded MTP3b MSUs
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:0;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:0;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:0;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC14_PVG190A PID:1;Invalid OPC
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC13_PVG194A PID:1;Disallowed ISUP
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC13_PVG194A PID:1;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC13_PVG194A PID:1;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC13_PVG194A PID:1;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Gateway Screening Results;ASP:GWC13_PVG194A PID:1;Invalid Cng Party Addr Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Gateway Screening Results;ASP:GWC13_PVG194A PID:1;Invalid Affct Destination Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Gateway Screening Results;ASP:GWC13_PVG194A PID:1;Invalid SIO Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:0;Path Restore Time;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:0;Path Down Time;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:0;Path Up Time;;03/24/2005 15:15:00;03/24/2005 15:20:00;300

ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:0;Path entered Restoring state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:0;Path entered Down state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:0;Path entered Up state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:0;Path Restore Time;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:0;Path Down Time;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:0;Path Up Time;;03/24/2005 15:15:00;03/24/2005 15:20:00;300

ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:0;Path entered Restoring state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:0;Path entered Down state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:0;Path entered Up state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Gateway Screening Results;ASP:GWC13_PVG194A PID:1;Invalid DPC Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Gateway Screening Results;ASP:GWC13_PVG194A PID:1;Invalid OPC Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Utilization;ASP:RTPSSSP PID:1;DUPU Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Utilization;ASP:RTPSSSP PID:1;SCON Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Utilization;ASP:RTPSSSP PID:1;DAUD Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Utilization;ASP:RTPSSSP PID:1;DUNA Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Management;ASP:GWC9_PVG192B PID:0;Path Restore Time;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Management;ASP:GWC9_PVG192B PID:0;Path Down Time;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Management;ASP:GWC9_PVG192B PID:0;Path Up Time;;03/24/2005 15:15:00;03/24/2005 15:20:00;300

ACC;ASP Path Management;ASP:GWC9_PVG192B PID:0;Path entered Restoring state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Management;ASP:GWC9_PVG192B PID:0;Path entered Down state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Management;ASP:GWC9_PVG192B PID:0;Path entered Up state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Utilization;ASP:RTPSSSP PID:1;DAVA Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Traffic;ASP:RTPSSSP PID:1;Discarded MTP3b MSUs Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Traffic;ASP:RTPSSSP PID:1;Discarded MSUs Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Traffic;ASP:RTPSSSP PID:1;Received MSUs Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Traffic;ASP:RTPSSSP PID:1;Sent MSUs Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Traffic;ASP:RTPSSSP PID:1;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:0;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:0;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:0;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:0;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:0;Path entered Down
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:0;Path entered Up state;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTPC_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTPC_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTPC_RS;Routeset Unavailability
Dur.;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTPC_RS;Routeset Unavailability
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPFVME3_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPFVME3_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPFVME3_RS;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPFVME3_RS;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;RPO Cumulative Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;Far End Mgmt Inhibit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;Near End Forced Unavailable Cou;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;Changeover Procedure Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;Link Available Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;Level 1 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;Unavailable Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;Link Management;LS:RTPFVME3 SLC:0;Link Remote Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;Link Local Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;Link Deactivated Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:RTPFVME3 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:RTPFVME3 SLC:0;BICC Error No OPC
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:RTPFVME3 SLC:0;BICC Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:RTPFVME3 SLC:0;BICC Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:RTPFVME3 SLC:0;BICC Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:RTPFVME3 SLC:0;BICC Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;TUP Received Message Counts;LS:RTPFVME3 SLC:0;Wrong NE Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;TUP Received Message Counts;LS:RTPFVME3 SLC:0;B/TUP Error No AS for OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;TUP Received Message Counts;LS:RTPFVME3 SLC:0;B/TUP Error No Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;TUP Received Message Counts;LS:RTPFVME3 SLC:0;B/TUP Error No Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;TUP Received Message Counts;LS:RTPFVME3 SLC:0;B/TUP Error No OPC/CIC Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;TUP Received Message Counts;LS:RTPFVME3 SLC:0;BTUP Maint Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;TUP Received Message Counts;LS:RTPFVME3 SLC:0;BTUP Call P Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;TUP Received Message Counts;LS:RTPFVME3 SLC:0;TUP Maint Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;TUP Received Message Counts;LS:RTPFVME3 SLC:0;TUP Call P Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;Wrong NE Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;ISUP Error Unknown Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;ISUP Error No AS for OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;ISUP Error No OPC/CIC Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;ISUP Error No Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;ISUP Error No Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;USR Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;UPT Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;UPA Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;UCIC Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;UBL Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;UBA Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;SUS Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;SGM Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;SAM Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;RSC Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;RPM Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;RLC Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;RES Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;REL Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;PRG Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;PAM Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;NRM Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;LPA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;LOP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;IRS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;INR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;INF Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;IDR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;IAMN1 Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;IAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;GRS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;GRA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;FOT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;FRJ Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;FAR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;FAI Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;FAD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;FAC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;FAA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;EXM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;DRS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CVT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CVR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CSVS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CSVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CRM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CRG Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CRA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CQR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CQM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CPG Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;COT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CON Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0

ACC;Linkset Utilization;LS:ITUCLKSET3;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:RTPSSSP PID:1;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC9_PVG192B PID:1;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC9_PVG192B PID:1;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC9_PVG192B PID:1;DAUD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC9_PVG192B PID:1;DUNA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC9_PVG192B PID:1;DAVA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:1;Discarded MTP3b MSUs
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:0;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:0;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:0;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:0;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:0;Path entered Down
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:0;Path entered Up state;;03/24/2005
15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CMR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:1;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:1;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:1;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:1;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:1;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC2_PVG191_194 PID:1;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CMRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CMC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CGUA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CGU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CGBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CGB Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CFN Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;BLO Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;BLA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;ANM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;ALT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;ACM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Octets Requiring GTT Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;MSUs Requiring GTT Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:RTPFVME3 SLC:0;Disallowed ISUP Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0


```
ACC;Gateway Screening Results;LS:RTPFVME3 SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:RTPFVME3 SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:RTPFVME3 SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:RTPFVME3 SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:RTPFVME3 SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:RTPFVME3 SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:RTPFVME3 SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:RTPFVME3 SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
MAX;Link Traffic;LS:RTPFVME3 SLC:0;Link utilization;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC2_PVG191_194 PID:1;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC2_PVG191_194 PID:1;DAUD Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC2_PVG191_194 PID:1;DUNA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC2_PVG191_194 PID:1;DAVA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:1;Discarded MTP3b MSUs
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;AS Master;RTPSSP;Core Overload Duration;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;AS Master;RTPSSP;TUP Discard Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;AS Master;RTPSSP;BICC Discard Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;AS Master;RTPSSP;ISUP Discard Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;AS Master;RTPSSP;RANAP Discard Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;AS Master;RTPSSP;BSSAP Discard Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET2 SLC:0;Octets
Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET2 SLC:0;Number of negative
ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

ACC;Link Faults and Performance;LS:ITUCLKSET2 SLC:0;Number of SUs received in error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:ITUCLKSET2 SLC:0;SL alignment or proving failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:ITUCLKSET2 SLC:0;SL failure-Other reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:ITUCLKSET2 SLC:0;SL failure-Exc. duration of con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:ITUCLKSET2 SLC:0;SL failure-Excessive error rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:ITUCLKSET2 SLC:0;SL failure-Exc. delay of ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:1;Discarded MSUs Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:1;Received MSUs Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:1;Sent MSUs Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:1;Terminated MSUs Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:1;Originated MSUs Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Utilization;ASP:GWC1_PVG190_193 PID:1;DUPU Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Utilization;ASP:GWC1_PVG190_193 PID:1;SCON Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Utilization;ASP:GWC1_PVG190_193 PID:1;DAUD Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Utilization;ASP:GWC1_PVG190_193 PID:1;DUNA Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Utilization;ASP:GWC1_PVG190_193 PID:1;DAVA Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:1;Discarded MTP3b MSUs Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:1;Discarded MSUs Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:1;Received MSUs Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:1;Sent MSUs Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:1;Terminated MSUs Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:1;Originated MSUs Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Utilization;ASP:GWC15_PVG192A PID:1;DUPU Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Utilization;ASP:GWC15_PVG192A PID:1;SCON Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Utilization;ASP:GWC15_PVG192A PID:1;DAUD Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Utilization;ASP:GWC15_PVG192A PID:1;DUNA Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Utilization;ASP:GWC15_PVG192A PID:1;DAVA Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:1;Discarded MTP3b MSUs Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:1;Discarded MSUs Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:1;Received MSUs Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:1;Sent MSUs Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:1;Terminated MSUs Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Gateway Screening Results;LS:CATTBOX01 SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:CATTBOX01 SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:CATTBOX01 SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:CATTBOX01 SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:CATTBOX01 SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:CATTBOX01 SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:CATTBOX01 SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:CATTBOX01 SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET2 SLC:0;SL failure-Abnormal
FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET2 SLC:0;SL failure-All
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET3 SLC:0;Octets
Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET3 SLC:0;Number of negative
ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET3 SLC:0;Number of SUs received in
error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET3 SLC:0;SL alignment or proving
failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET3 SLC:0;SL failure-Other
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET3 SLC:0;SL failure-Exc. duration of
con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET3 SLC:0;SL failure-Excessive error
rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET3 SLC:0;SL failure-Exc. delay of
ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET3 SLC:0;SL failure-Abnormal
FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET3 SLC:0;SL failure-All
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:RTPFVME3 SLC:0;Octets
Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:RTPFVME3 SLC:0;Number of negative
ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:RTPFVME3 SLC:0;Number of SUs received in
error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:RTPFVME3 SLC:0;SL alignment or proving
failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;50
ACC;Link Faults and Performance;LS:RTPFVME3 SLC:0;SL failure-Other
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:RTPFVME3 SLC:0;SL failure-Exc. duration of
con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:RTPFVME3 SLC:0;SL failure-Excessive error
rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:RTPFVME3 SLC:0;SL failure-Exc. delay of
ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Level 3 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:1;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC14_PVG190A PID:1;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC14_PVG190A PID:1;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Utilization;ASP:GWC14_PVG190A PID:1;DAUD Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC14_PVG190A PID:1;DUNA Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:SIMTOOL RTESET;Routeset Man-busied Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:SIMTOOL RTESET;RouteSet Congested Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:SIMTOOL RTESET;Routeset Unavailability Dur.;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:SIMTOOL RTESET;Routeset Unavailability Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC14_PVG190A PID:1;DAVA Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Traffic;ASP:GWC14_PVG190A PID:1;Discarded MTP3b MSUs Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:RTPFVME3 SLC:0;SL failure-Abnormal FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:ITURTESET2;Routeset Man-busied Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:ITURTESET2;RouteSet Congested Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:ITURTESET2;Routeset Unavailability Dur.;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:ITURTESET2;Routeset Unavailability Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:RTPFVME3 SLC:0;SL failure-All reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:RTPSSSP PID:0;Path Restore Time;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:RTPSSSP PID:0;Path Down Time;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:RTPSSSP PID:0;Path Up Time;;03/24/2005 15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:RTPSSSP PID:0;Path entered Restoring state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:RTPSSSP PID:0;Path entered Down state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:RTPSSSP PID:0;Path entered Up state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;TFR and TCR Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:0;Path Restore Time;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:0;Path Down Time;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:0;Path Up Time;;03/24/2005 15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:0;Path entered Restoring state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:0;Path entered Down state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:0;Path entered Up state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;TFP and TCP Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;TFP and TCP Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;Linkset Inactivity Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CATTBOX_RS;Routeset Man-busied Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CATTBOX_RS;RouteSet Congested Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Route Set Management;RS:CATTBOX_RS;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CATTBOX_RS;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Level 2 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
MAX;Link Traffic;LS:CATTBOX01 SLC:0;Link utilization;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC13_PVG194A PID:0;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC13_PVG194A PID:0;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC13_PVG194A PID:0;DAUD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC13_PVG194A PID:0;DUNA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC13_PVG194A PID:0;DAVA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:0;Discarded MTP3b MSUs
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:0;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:0;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:0;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC9_PVG192B PID:0;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC9_PVG192B PID:0;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC9_PVG192B PID:0;DAUD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC9_PVG192B PID:0;DUNA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC9_PVG192B PID:0;DAVA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:0;Discarded MTP3b MSUs
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:0;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0

ACC;Linkset Utilization;LS:STEPBOX01;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:0;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:0;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Pri 3 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Pri 2 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Pri 1 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0

ACC;Link Management;LS:CATTBOX01 SLC:0;RPO Cumulative Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Far End Mgmt Inhibit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Near End Forced Unavailable
Cou;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Changeover Procedure Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Link Available Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Level 3 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Level 2 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Level 1 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Unavailable Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC2_PVG191_194 PID:0;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC2_PVG191_194 PID:0;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC2_PVG191_194 PID:0;DAUD Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC2_PVG191_194 PID:0;DUNA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC2_PVG191_194 PID:0;DAVA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:0;Discarded MTP3b MSUs
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:0;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:0;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:0;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC1_PVG190_193 PID:0;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC1_PVG190_193 PID:0;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Link Remote Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC1_PVG190_193 PID:0;DAUD Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC1_PVG190_193 PID:0;DUNA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:CATTBOX01 SLC:0;Octets
Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:CATTBOX01 SLC:0;Number of negative
ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:CATTBOX01 SLC:0;Number of SUs received in
error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC1_PVG190_193 PID:0;DAVA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:0;Discarded MTP3b MSUs
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

```
ACC;System Node State;IP_LINK_NODE_11;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;IP_LINK_NODE_11;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_11;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_11;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_11;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_8;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;IP_LINK_NODE_8;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_8;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_8;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_8;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTPRTPB_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTPRTPB_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTPRTPB_RS;Routeset Unavailability
Dur.;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTPRTPB_RS;Routeset Unavailability
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:0;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:0;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Link Local Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Link Deactivated Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:CATTBOX01 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:CATTBOX01 SLC:0;BICC Error No OPC
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:CATTBOX01 SLC:0;BICC Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:CATTBOX01 SLC:0;BICC Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:CATTBOX01 SLC:0;BICC Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CRES16A_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CRES16A_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CRES16A_RS;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CRES16A_RS;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPS_INTL_RTP6;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPS_INTL_RTP6;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPS_INTL_RTP6;Routeset Unavailability
Dur.;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPS_INTL_RTP6;Routeset Unavailability
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STEPBOX_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```



```
ACC;Route Set Management;RS:STEPBOX_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STEPBOX_RS;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STEPBOX_RS;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTP6_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTP6_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTP6_RS;Routeset Unavailability
Dur.;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTP6_RS;Routeset Unavailability
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STPB_INTL_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STPB_INTL_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STPB_INTL_RS;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STPB_INTL_RS;Routeset Unavailability
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STPA_INTL_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STPA_INTL_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STPA_INTL_RS;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STPA_INTL_RS;Routeset Unavailability
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTPI_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTPI_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTPI_RS;Routeset Unavailability
Dur.;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTPI_RS;Routeset Unavailability
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CRES58A_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CRES58A_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CRES58A_RS;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CRES58A_RS;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTP5_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTP5_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTP5_RS;Routeset Unavailability
Dur.;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTP5_RS;Routeset Unavailability
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPORTESET1;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPORTESET1;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPORTESET1;Routeset Unavailability
Dur.;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPORTESET1;Routeset Unavailability
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPSTPB;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

ACC;Route Set Management;RS:BNRRTPSTPB;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPSTPB;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPSTPB;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPSTPA;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPSTPA;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPSTPA;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPSTPA;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:C7RTESET2;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:C7RTESET2;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:C7RTESET2;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:C7RTESET2;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:C7RTESET1;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:C7RTESET1;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:C7RTESET1;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:C7RTESET1;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Task Management;RTC_NODE_12;Idle Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;297690
ACC;Task Management;CC_NODE_1_18;Idle Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;211558
ACC;Task Management;RTC_NODE_15;Idle Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;297990
ACC;BICC Received Message Counts;LS:CATTBOX01 SLC:0;BICC Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:CATTBOX01 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:0;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Task Management;IP_LINK_NODE_10;Idle Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;299204
ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:RTPSSSP PID:0;DUPU Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:RTPSSSP PID:0;SCON Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:CATTBOX01 SLC:0;B/TUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Task Management;IP_LINK_NODE_9;Idle Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;299199
ACC;Link Faults and Performance;LS:C7LKSET2 SLC:0;Octets
Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET2 SLC:0;Number of negative
ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET2 SLC:0;Number of SUs received in
error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET2 SLC:0;SL alignment or proving
failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:C7LKSET2 SLC:0;SL failure-Other reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:C7LKSET2 SLC:0;SL failure-Exc. duration of con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:C7LKSET2 SLC:0;SL failure-Excessive error rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:C7LKSET2 SLC:0;SL failure-Exc. delay of ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:C7LKSET2 SLC:0;SL failure-Abnormal FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:C7LKSET2 SLC:0;SL failure-All reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:STPB_INTL SLC:0;Octets Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:STPB_INTL SLC:0;Number of negative ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:STPB_INTL SLC:0;Number of SUs received in error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:STPB_INTL SLC:0;SL alignment or proving failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;24

ACC;Link Faults and Performance;LS:STPB_INTL SLC:0;SL failure-Other reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:STPB_INTL SLC:0;SL failure-Exc. duration of con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:STPB_INTL SLC:0;SL failure-Excessive error rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:STPB_INTL SLC:0;SL failure-Exc. delay of ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:STPB_INTL SLC:0;SL failure-Abnormal FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:STPB_INTL SLC:0;SL failure-All reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:ST000002 SLC:0;Octets Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:ST000002 SLC:0;Number of negative ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:ST000002 SLC:0;Number of SUs received in error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:ST000002 SLC:0;SL alignment or proving failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;24

ACC;Link Faults and Performance;LS:ST000002 SLC:0;SL failure-Other reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:ST000002 SLC:0;SL failure-Exc. duration of con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:ST000002 SLC:0;SL failure-Excessive error rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:ST000002 SLC:0;SL failure-Exc. delay of ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:ST000002 SLC:0;SL failure-Abnormal FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:ST000002 SLC:0;SL failure-All reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Task Management;NODE_LINK_6_1;Idle Task Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;297815

ACC;Link Faults and Performance;LS:C7LKSET1 SLC:0;Octets Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:C7LKSET1 SLC:0;Number of negative ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:C7LKSET1 SLC:0;Number of SUs received in error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:C7LKSET1 SLC:0;SL alignment or proving failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:C7LKSET1 SLC:0;SL failure-Other reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:C7LKSET1 SLC:0;SL failure-Exc. duration of con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET1 SLC:0;SL failure-Excessive error rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET1 SLC:0;SL failure-Exc. delay of ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET1 SLC:0;SL failure-Abnormal FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET1 SLC:0;SL failure-All reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPA_INTL SLC:0;Octets Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPA_INTL SLC:0;Number of negative ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPA_INTL SLC:0;Number of SUs received in error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPA_INTL SLC:0;SL alignment or proving failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;24
ACC;Link Faults and Performance;LS:STPA_INTL SLC:0;SL failure-Other reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPA_INTL SLC:0;SL failure-Exc. duration of con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPA_INTL SLC:0;SL failure-Excessive error rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPA_INTL SLC:0;SL failure-Exc. delay of ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPA_INTL SLC:0;SL failure-Abnormal FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPA_INTL SLC:0;SL failure-All reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000001 SLC:0;Octets Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000001 SLC:0;Number of negative ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000001 SLC:0;Number of SUs received in error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000001 SLC:0;SL alignment or proving failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;24
ACC;Link Faults and Performance;LS:ST000001 SLC:0;SL failure-Other reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000001 SLC:0;SL failure-Exc. duration of con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000001 SLC:0;SL failure-Excessive error rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000001 SLC:0;SL failure-Exc. delay of ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000001 SLC:0;SL failure-Abnormal FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
MAX;Link Traffic;LS:STPB_INTL SLC:0;Link utilization;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:CATTBOX01 SLC:0;B/TUP Error No Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:CATTBOX01 SLC:0;B/TUP Error No Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:CATTBOX01 SLC:0;B/TUP Error No OPC/CIC Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:CATTBOX01 SLC:0;BTUP Maint Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:CATTBOX01 SLC:0;BTUP Call P Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:CATTBOX01 SLC:0;TUP Maint Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:CATTBOX01 SLC:0;TUP Call P Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;Wrong NE Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:ST000001 SLC:0;SL failure-All reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Task Management;LINK_NODE_5_1;Idle Task Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;297830

ACC;Link Faults and Performance;LS:CATTBOX01 SLC:0;SL alignment or proving failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;24

ACC;Link Faults and Performance;LS:STEPBOX01 SLC:0;Octets Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:STEPBOX01 SLC:0;Number of negative ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:STEPBOX01 SLC:0;Number of SUs received in error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:STEPBOX01 SLC:0;SL alignment or proving failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;24

ACC;Link Faults and Performance;LS:STEPBOX01 SLC:0;SL failure-Other reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:STEPBOX01 SLC:0;SL failure-Exc. duration of con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:STEPBOX01 SLC:0;SL failure-Excessive error rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:STEPBOX01 SLC:0;SL failure-Exc. delay of ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:STEPBOX01 SLC:0;SL failure-Abnormal FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Faults and Performance;LS:STEPBOX01 SLC:0;SL failure-All reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Task Management;LINK_NODE_4_1;Idle Task Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;298056

ACC;TUP Received Message Counts;LS:STEPBOX01 SLC:0;B/TUP Error No AS for OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;TUP Received Message Counts;LS:STEPBOX01 SLC:0;B/TUP Error No Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

MAX;Link Traffic;LS:C7LKSET1 SLC:0;Link utilization;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

MAX;Link Traffic;LS:STPA_INTL SLC:0;Link utilization;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

MAX;Link Traffic;LS:ST000001 SLC:0;Link utilization;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;Wrong NE Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;SCCP System Totals;USP:C7NETWRK1;Total messages handled;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;SCCP System Totals;USP:C7NETWRK1;Routing Failure - Unequip.User;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

MAX;Link Traffic;LS:STEPBOX01 SLC:0;Link utilization;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

MAX;Link Traffic;LS:ST000002 SLC:0;Link utilization;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;TUP Received Message Counts;LS:C7LKSET1 SLC:0;Wrong NE Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;TUP Received Message Counts;LS:C7LKSET1 SLC:0;B/TUP Error No AS for OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;TUP Received Message Counts;LS:C7LKSET1 SLC:0;B/TUP Error No Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;TUP Received Message Counts;LS:STPA_INTL SLC:0;Wrong NE Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;ISUP Error Unknown Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;ISUP Error No AS for OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;ISUP Error No OPC/CIC Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;ISUP Error No Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;RPO Cumulative Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Far End Mgmt Inhibit Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Near End Forced Unavailable Cou;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Changeover Procedure Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Link Available Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;300
ACC;Link Management;LS:C7LKSET2 SLC:0;Level 3 Congestion Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Level 2 Congestion Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Level 1 Congestion Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Unavailable Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Link Remote Inhibit Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Link Local Inhibit Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Link Deactivated Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;RPO Cumulative Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Far End Mgmt Inhibit Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Near End Forced Unavailable Cou;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Changeover Procedure Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Link Available Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;300
ACC;Link Management;LS:C7LKSET1 SLC:0;Level 3 Congestion Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Level 2 Congestion Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Level 1 Congestion Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Unavailable Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Link Remote Inhibit Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Link Local Inhibit Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Link Deactivated Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET2 SLC:0;B/TUP Error No Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET2 SLC:0;B/TUP Error No OPC/CIC Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET2 SLC:0;BTUP Maint Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET2 SLC:0;BTUP Call P Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET2 SLC:0;TUP Maint Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;TUP Received Message Counts;LS:C7LKSET2 SLC:0;TUP Call P Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;ISUP Error Unknown Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;ISUP Error No AS for OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;ISUP Error No OPC/CIC Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;ISUP Error No Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;ISUP Error No Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;USR Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;UPT Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;UPA Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;UCIC Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;UBL Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;UBA Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;SUS Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;SGM Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;SAM Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;RSC Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;RPM Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;RLC Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;RES Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;REL Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;PRG Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;PAM Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;NRM Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;LPA Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;LOP Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;IRS Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;INR Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;INF Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;IDR Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;IAMN1 Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;IAM Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;GRS Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

[illegible]

ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;BLA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;ANM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;ALT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;ACM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET2 SLC:0;Disallowed ISUP Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET2 SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET2 SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET2 SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET2 SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET2 SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET2 SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET2 SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET2 SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Level 3 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Level 2 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Pri 3 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Pri 2 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Pri 1 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Pri 3 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Pri 2 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Pri 1 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0

ACC;Link Traffic;LS:C7LKSET2 SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET1 SLC:0;B/TUP Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET1 SLC:0;B/TUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET1 SLC:0;BTUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET1 SLC:0;BTUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET1 SLC:0;TUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET1 SLC:0;TUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;ISUP Error Unknown
Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;ISUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;ISUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;ISUP Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;ISUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;USR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;UPT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;UPA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;UCIC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;UBL Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;UBA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;SUS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;SGM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;SAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;RSC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;RPM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;RLC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;RES Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;REL Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;PRG Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;PAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;NRM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;LPA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0

[illegible]

ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CMC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CGUA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CGU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CGBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CGB Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CFN Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;BLO Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;BLA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;ANM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;ALT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;ACM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET1 SLC:0;Disallowed ISUP Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET1 SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET1 SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET1 SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET1 SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET1 SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET1 SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET1 SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET1 SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Level 3 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Level 2 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;RTC_NODE_12;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;RTC_NODE_12;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_9;Association Terminated
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_9;Association Aborted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_9;Established Association Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;6
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_9;Association Establish Attempts;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_9;Chunk Retransmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_9;Chunks Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_9;Chunks Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_9;Out of Blue SCTP Packet;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;IP_LINK_NODE_9;Sequence Number Reset Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;IP_LINK_NODE_9;Raw Cell Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;IP_LINK_NODE_9;Raw Message Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;IP_LINK_NODE_9;SSCOP Message Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;878
ACC;ATM Driver Messaging;IP_LINK_NODE_9;IP Message Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;624
ACC;ATM Driver Messaging;IP_LINK_NODE_9;Duplicate Messages Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;1502
ACC;ATM Driver Messaging;IP_LINK_NODE_9;Plane 2 Messages Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;1502
ACC;ATM Driver Messaging;IP_LINK_NODE_9;Plane 1 Messages Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;1502
ACC;ATM Driver Messaging;IP_LINK_NODE_9;Plane 2 CRC Error Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;IP_LINK_NODE_9;Plane 1 CRC Error Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_9;Locked, Off-line Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_9;Enabled, Locked Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_9;Enabled, Unlocked Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;IP_LINK_NODE_9;Disabled, Locked Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_9;Disabled, Unlocked Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;MSUs Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;MSUs Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Octets Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Octets Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Pri 1 MSU Outbd Discard Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Pri 2 MSU Outbd Discard Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Pri 3 MSU Outbd Discard Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Pri 1 MSU Inbd Discard Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Pri 2 MSU Inbd Discard Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Traffic;LS:STEPBOX01 SLC:0;Pri 3 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Level 2 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Level 3 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STEPBOX01 SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STEPBOX01 SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STEPBOX01 SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STEPBOX01 SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STEPBOX01 SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STEPBOX01 SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STEPBOX01 SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STEPBOX01 SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STEPBOX01 SLC:0;Disallowed ISUP
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;MSUs Requiring GTT Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Octets Requiring GTT Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;ACM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;ALT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;ANM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;BLA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;BLO Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CCR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CFN Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CGB Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CGBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CGU Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

[illegible]

ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;IRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;LOP Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;LPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;NRM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;PAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;PRG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;REL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;RES Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;RLC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;RPM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;RSC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;SAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;SGM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;SUS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;UBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;UBL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;UCIC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;UPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;UPT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;USR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;ISUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;ISUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;ISUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;ISUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;ISUP Error Unknown
Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STEPBOX01 SLC:0;TUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STEPBOX01 SLC:0;TUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STEPBOX01 SLC:0;BTUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STEPBOX01 SLC:0;BTUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STEPBOX01 SLC:0;B/TUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STEPBOX01 SLC:0;B/TUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0


```
ACC;Link Traffic;LS:ST000001 SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Pri 1 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Pri 2 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Pri 3 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Pri 1 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Pri 2 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Pri 3 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Level 2 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Level 3 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Pri 1 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Pri 2 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Pri 3 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Pri 1 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Pri 2 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

ACC;Link Traffic;LS:STPA_INTL SLC:0;Pri 3 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Level 2 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Level 3 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000001 SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000001 SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000001 SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000001 SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000001 SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000001 SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000001 SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000001 SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000001 SLC:0;Disallowed ISUP Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPA_INTL SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPA_INTL SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPA_INTL SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPA_INTL SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPA_INTL SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPA_INTL SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPA_INTL SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPA_INTL SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPA_INTL SLC:0;Disallowed ISUP
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;MSUs Requiring GTT Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Octets Requiring GTT Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;ACM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0

[illegible]

ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;FRJ Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;FOT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;GRA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;GRS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;IAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;IAMN1 Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;IDR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;INF Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;INR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;IRS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;LOP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;LPA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;NRM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;PAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;PRG Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;REL Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;RES Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;RLC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;RPM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;RSC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;SAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;SGM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;SUS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;UBA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;UBL Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;UCIC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;UPA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;UPT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;USR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;ISUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;ISUP Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;ISUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

[illegible]

[illegible]

```
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;ISUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;ISUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;ISUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;ISUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;ISUP Error Unknown
Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Pri 1 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Pri 2 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Pri 3 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Pri 1 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Pri 2 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Pri 3 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Level 2 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Level 3 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

ACC;Link Traffic;LS:STPB_INTL SLC:0;Pri 1 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Pri 2 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Pri 3 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Pri 1 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Pri 2 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Pri 3 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Level 2 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Level 3 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000001 SLC:0;TUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000001 SLC:0;TUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000001 SLC:0;BTUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000001 SLC:0;BTUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000001 SLC:0;B/TUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000001 SLC:0;B/TUP Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPA_INTL SLC:0;TUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPA_INTL SLC:0;TUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPA_INTL SLC:0;BTUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPA_INTL SLC:0;BTUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPA_INTL SLC:0;B/TUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPA_INTL SLC:0;B/TUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000002 SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000002 SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000002 SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0

ACC;Gateway Screening Results;LS:ST000002 SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000002 SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000002 SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000002 SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000002 SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000002 SLC:0;Disallowed ISUP Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPB_INTL SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPB_INTL SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPB_INTL SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPB_INTL SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPB_INTL SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPB_INTL SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPB_INTL SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPB_INTL SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPB_INTL SLC:0;Disallowed ISUP
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;MSUs Requiring GTT Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Octets Requiring GTT Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;ACM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;ALT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;ANM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;BLA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;BLO Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CFN Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CGB Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CGBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CGU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CGUA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CMC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CMRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CMR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CON Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0

[illegible]

ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;PRG Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;REL Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;RES Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;RLC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;RPM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;RSC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;SAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;SGM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;SUS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;UBA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;UBL Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;UCIC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;UPA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;UPT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;USR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;ISUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;ISUP Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;ISUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;ISUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;ISUP Error Unknown
Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;ACM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;ALT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;ANM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;BLA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;BLO Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CCR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CFN Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CGB Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CGBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CGU Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CGUA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CMC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

[illegible]

ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;LPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;NRM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;PAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;PRG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;REL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;RES Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;RLC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;RPM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;RSC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;SAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;SGM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;SUS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;UBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;UBL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;UCIC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;UPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;UPT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;USR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;ISUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;ISUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;ISUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;ISUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;ISUP Error Unknown
Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000002 SLC:0;TUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000002 SLC:0;TUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000002 SLC:0;BTUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000002 SLC:0;BTUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000002 SLC:0;B/TUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000002 SLC:0;B/TUP Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPB_INTL SLC:0;TUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPB_INTL SLC:0;TUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPB_INTL SLC:0;BTUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;TUP Received Message Counts;LS:STPB_INTL SLC:0;BTUP Maint Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPB_INTL SLC:0;B/TUP Error No OPC/CIC Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPB_INTL SLC:0;B/TUP Error No Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Link Deactivated Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Link Local Inhibit Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Link Remote Inhibit Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Unavailable Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;300
ACC;Link Management;LS:ST000002 SLC:0;Level 1 Congestion Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Level 2 Congestion Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Level 3 Congestion Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Link Available Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Changeover Procedure Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Near End Forced Unavailable Cou;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Far End Mgmt Inhibit Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;RPO Cumulative Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Link Deactivated Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Link Local Inhibit Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Link Remote Inhibit Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Unavailable Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;300
ACC;Link Management;LS:STEPBOX01 SLC:0;Level 1 Congestion Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Level 2 Congestion Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Level 3 Congestion Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Link Available Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Changeover Procedure Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Near End Forced Unavailable Cou;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Far End Mgmt Inhibit Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;RPO Cumulative Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Link Deactivated Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Link Local Inhibit Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Link Remote Inhibit Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

```
ACC;Link Management;LS:ST000001 SLC:0;Unavailable Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;Link Management;LS:ST000001 SLC:0;Level 1 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Level 2 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Level 3 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Link Available Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Changeover Procedure Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Near End Forced Unavailable Cou;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Far End Mgmt Inhibit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;RPO Cumulative Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Link Deactivated Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Link Local Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Link Remote Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Unavailable Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;Link Management;LS:STPB_INTL SLC:0;Level 1 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Level 2 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Level 3 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Link Available Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Changeover Procedure Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Near End Forced Unavailable
Cou;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Far End Mgmt Inhibit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;RPO Cumulative Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Link Deactivated Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Link Local Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Link Remote Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Unavailable Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;Link Management;LS:STPA_INTL SLC:0;Level 1 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Level 2 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Level 3 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Link Available Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Changeover Procedure Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

ACC;Link Management;LS:STPA_INTL SLC:0;Near End Forced Unavailable
Cou;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Far End Mgmt Inhibit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;RPO Cumulative Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Link Faults and Performance;LS:CATTBOX01 SLC:0;SL failure-Other
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:CATTBOX01 SLC:0;SL failure-Exc. duration of
con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:CATTBOX01 SLC:0;SL failure-Excessive error
rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:CATTBOX01 SLC:0;SL failure-Exc. delay of
ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:CATTBOX01 SLC:0;SL failure-Abnormal
FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:CATTBOX01 SLC:0;SL failure-All
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Pri 3 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Pri 2 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Pri 1 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:RTPSSSP PID:0;DAUD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:RTPSSSP PID:0;DUNA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:RTPSSSP PID:0;DAVA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:RTPSSSP PID:0;Discarded MTP3b MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:RTPSSSP PID:0;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:RTPSSSP PID:0;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:RTPSSSP PID:0;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:RTPSSSP PID:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:RTPSSSP PID:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0

ACC;Linkset Utilization;LS:CATTBOX01;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:AUTORTESET;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:AUTORTESET;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:AUTORTESET;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:AUTORTESET;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;RPO Cumulative Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Far End Mgmt Inhibit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Near End Forced Unavailable
Cou;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Changeover Procedure Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Link Available Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Level 3 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Level 2 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Level 1 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Unavailable Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;Link Management;LS:AUTOLKSET SLC:0;Link Remote Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Link Local Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Link Deactivated Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:AUTOLKSET SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:AUTOLKSET SLC:0;BICC Error No OPC
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:AUTOLKSET SLC:0;BICC Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:AUTOLKSET SLC:0;BICC Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:AUTOLKSET SLC:0;BICC Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:AUTOLKSET SLC:0;BICC Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:AUTOLKSET SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:AUTOLKSET SLC:0;B/TUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:AUTOLKSET SLC:0;B/TUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;TUP Received Message Counts;LS:AUTOLKSET SLC:0;B/TUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:AUTOLKSET SLC:0;B/TUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:AUTOLKSET SLC:0;BTUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:AUTOLKSET SLC:0;BTUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:AUTOLKSET SLC:0;TUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:AUTOLKSET SLC:0;TUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;ISUP Error Unknown
Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;ISUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;ISUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;ISUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;ISUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;USR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;UPT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;UPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;UCIC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;UBL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;UBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;SUS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;SGM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;SAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;RSC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;RPM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;RLC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;RES Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;REL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;PRG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;PAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;NRM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;LPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;LOP Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;IRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

[illegible]

ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CGU Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CGBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CGB Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CFN Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CCR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;BLO Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;BLA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;ANM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;ALT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;ACM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:AUTOLKSET SLC:0;Disallowed ISUP
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:AUTOLKSET SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:AUTOLKSET SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:AUTOLKSET SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:AUTOLKSET SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:AUTOLKSET SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:AUTOLKSET SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:AUTOLKSET SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:AUTOLKSET SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Level 3 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Level 2 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
MAX;Link Traffic;LS:AUTOLKSET SLC:0;Link utilization;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Pri 3 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Pri 2 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0

```
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Pri 1 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Pri 3 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Pri 2 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Pri 1 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:AUTOLKSET SLC:0;Octets
Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:AUTOLKSET SLC:0;Number of negative
ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:AUTOLKSET SLC:0;Number of SUs received in
error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:AUTOLKSET SLC:0;SL alignment or proving
failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;24
ACC;Link Faults and Performance;LS:AUTOLKSET SLC:0;SL failure-Other
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:AUTOLKSET SLC:0;SL failure-Exc. duration of
con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:AUTOLKSET SLC:0;SL failure-Excessive error
rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:AUTOLKSET SLC:0;SL failure-Exc. delay of
ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:AUTOLKSET SLC:0;SL failure-Abnormal
FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;CC_NODE_1_1;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;CC_NODE_1_1;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;CC_NODE_1_1;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;CC_NODE_1_1;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;CC_NODE_1_1;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Task Management;CC_NODE_1_1;Idle Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;211720
ACC;RTC Sanity;CC_NODE_1_1; RTC15 Passive Audit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;RTC Sanity;CC_NODE_1_1; RTC12 Passive Audit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_1;Sequence Number Reset Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_1;Raw Cell Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_1;Raw Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_1;SSCOP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_1;IP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3054
```

ACC;ATM Driver Messaging;CC_NODE_1_1;Duplicate Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3054
ACC;ATM Driver Messaging;CC_NODE_1_1;Plane 2 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3054
ACC;ATM Driver Messaging;CC_NODE_1_1;Plane 1 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3054
ACC;ATM Driver Messaging;CC_NODE_1_1;Plane 2 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_1;Plane 1 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;UDP;CC_NODE_1_1;Full Socket Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;ISUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;USR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;UPT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;UPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;UCIC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;UBL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;UBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;SUS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;SGM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;SAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;RSC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;RPM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;RLC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;RES Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;REL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;PRG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;PAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;NRM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;LPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;LOP Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;IRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;INR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;INF Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;IDR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;IAMN1 Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;IAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

[illegible]

ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;BLO Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;BLA Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;ANM Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;ALT Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;ACM Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;TFC Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;TFC Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;RST Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;RST Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;TFA and TCA Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;TFA and TCA Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;TFR and TCR Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;TFR and TCR Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;TFP and TCP Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;TFP and TCP Transmitted Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;Linkset Inactivity Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;UDP;CC_NODE_1_18;Full Socket Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;UDP;RTC_NODE_15;Full Socket Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;UDP;RTC_NODE_12;Full Socket Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;UDP;IP_LINK_NODE_10;Full Socket Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;UDP;IP_LINK_NODE_9;Full Socket Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;UDP;NODE_LINK_6_1;Full Socket Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;UDP;LINK_NODE_5_1;Full Socket Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:AUTOLKSET SLC:0;SL failure-All reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;UDP;LINK_NODE_4_1;Full Socket Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;UDP;LINK_NODE_3_1;Full Socket Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:C7LKSET2 SLC:0;Wrong NE Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:C7LKSET2 SLC:0;BICC Error No OPC Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:C7LKSET2 SLC:0;BICC Error No Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:C7LKSET2 SLC:0;BICC Error No Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:C7LKSET2 SLC:0;BICC Maint Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:C7LKSET2 SLC:0;BICC Call P Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:STPB_INTL SLC:0;Wrong NE Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

[illegible]

ACC;BICC Received Message Counts;LS:STEPBOX01 SLC:0;BICC Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:STEPBOX01 SLC:0;BICC Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:STEPBOX01 SLC:0;BICC Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
MAX;Link Traffic;LS:ITUCLKSET2 SLC:0;Link utilization;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET2 SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET2 SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET2 SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET2 SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET2 SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET2 SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET2 SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET2 SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET2 SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET2 SLC:0;Disallowed ISUP
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:1;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:1;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:1;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:1;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:1;Path entered Down
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:1;Path entered Up
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

```
ACC;ASP Path Management;ASP:GWC9_PVG192B PID:1;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;ACM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;ALT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;ANM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;BLA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;BLO Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CCR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CFN Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CGB Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CGBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CGU Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CGUA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CMC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CMRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CMR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CON Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;COT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CPG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CQM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CQR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CRA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CRG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CRM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CSVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CSVS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CVT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;DRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;EXM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;FAA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;FAC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;FAD Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```


ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;FAI Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;FAR Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;FRJ Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;FOT Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;GRA Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;GRS Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;IAM Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;IAMN1 Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;IDR Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;INF Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;INR Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;IRS Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;LOP Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;LPA Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;NRM Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;PAM Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;PRG Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;REL Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;RES Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;RLC Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;RPM Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;RSC Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;SAM Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;SGM Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;SUS Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;UBA Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;UBL Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;UCIC Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;UPA Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;UPT Received
ACC;ISUP Received Count;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;USR Received
ACC;ISUP Received Route;;03/24/2005	Message Counts;LS:ITUCLKSET2 SLC:0;ISUP Error No

ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;ISUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;ISUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;ISUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;ISUP Error Unknown
Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC9_PVG192B PID:1;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC9_PVG192B PID:1;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:GWC9_PVG192B PID:1;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC9_PVG192B PID:1;Path entered Down
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC9_PVG192B PID:1;Path entered Up state;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:RTPSSSP PID:1;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:RTPSSSP PID:1;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:RTPSSSP PID:1;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:RTPSSSP PID:1;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:RTPSSSP PID:1;Path entered Down state;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:RTPSSSP PID:1;Path entered Up state;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:1;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:1;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:1;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:1;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:1;Path entered Down
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:1;Path entered Up state;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:1;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:1;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:1;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:1;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:1;Path entered Down
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:1;Path entered Up
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:1;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:1;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:1;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:1;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;ASP Path Management;ASP:GWC15_PVG192A PID:1;Path entered Down state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:1;Path entered Up state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:1;Path Restore Time;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:1;Path Down Time;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:1;Path Up Time;;03/24/2005 15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:1;Path entered Restoring state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:1;Path entered Down state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:1;Path entered Up state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC1_PVG190_193 PID:1;Disallowed ISUP Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC1_PVG190_193 PID:1;Disallowed Trans Type Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC1_PVG190_193 PID:1;Disallowed Cld Party Addr Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC1_PVG190_193 PID:1;Invalid Affct PC-SSN Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC1_PVG190_193 PID:1;Invalid Cng Party Addr Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC1_PVG190_193 PID:1;Invalid Affct Destination Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC1_PVG190_193 PID:1;Invalid SIO Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC1_PVG190_193 PID:1;Invalid DPC Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC1_PVG190_193 PID:1;Invalid OPC Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC15_PVG192A PID:1;Disallowed ISUP Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC15_PVG192A PID:1;Disallowed Trans Type Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC15_PVG192A PID:1;Disallowed Cld Party Addr Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC15_PVG192A PID:1;Invalid Affct PC-SSN Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC15_PVG192A PID:1;Invalid Cng Party Addr Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC15_PVG192A PID:1;Invalid Affct Destination Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC15_PVG192A PID:1;Invalid SIO Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC15_PVG192A PID:1;Invalid DPC Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC15_PVG192A PID:1;Invalid OPC Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC14_PVG190A PID:1;Disallowed ISUP Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET2 SLC:0;TUP Call P Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET2 SLC:0;TUP Maint Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET2 SLC:0;BTUP Call P Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET2 SLC:0;BTUP Maint Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET2 SLC:0;B/TUP Error No OPC/CIC Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;TUP Received Message Counts;LS:ITUCLKSET2 SLC:0;B/TUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET2 SLC:0;B/TUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET2 SLC:0;B/TUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET2 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET2 SLC:0;BICC Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET2 SLC:0;BICC Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET2 SLC:0;BICC Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET2 SLC:0;BICC Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET2 SLC:0;BICC Error No OPC
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET2 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:1;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:1;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:1;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET2 SLC:0;Link Deactivated Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET2 SLC:0;Link Local Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET2 SLC:0;Link Remote Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET2 SLC:0;Unavailable Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET2 SLC:0;Level 1 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET2 SLC:0;Link Available Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;Link Management;LS:ITUCLKSET2 SLC:0;Changeover Procedure Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET2 SLC:0;Near End Forced Unavailable
Cou;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET2 SLC:0;Far End Mgmt Inhibit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET2 SLC:0;RPO Cumulative Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET2 SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:1;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:1;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC13_PVG194A PID:1;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC13_PVG194A PID:1;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC13_PVG194A PID:1;DAUD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC13_PVG194A PID:1;DUNA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC13_PVG194A PID:1;DAVA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:ITURTESET3;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0

```
ACC;Route Set Management;RS:ITURTESET3;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:ITURTESET3;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:ITURTESET3;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:1;Discarded MTP3b MSUs
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:1;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:1;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:1;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:1;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:1;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
MAX;Link Traffic;LS:ITUCLKSET3 SLC:0;Link utilization;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET3 SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET3 SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET3 SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET3 SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET3 SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET3 SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET3 SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```


ACC;Gateway Screening Results;LS:ITUCLKSET3 SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET3 SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET3 SLC:0;Disallowed ISUP
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;ACM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;ALT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;ANM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;BLA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;BLO Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CCR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CFN Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CGB Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CGBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CGU Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CGUA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CMC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CMRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CMR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CON Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;COT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CPG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CQM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CQR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CRA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CRG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CRM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CSVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CSVS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CVT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;DRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;EXM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;FAA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

[illegible]

ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;USR Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;ISUP Error No Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;ISUP Error No Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;ISUP Error No OPC/CIC Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;ISUP Error No AS for OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;ISUP Error Unknown Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;Wrong NE Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET3 SLC:0;TUP Call P Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET3 SLC:0;TUP Maint Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET3 SLC:0;BTUP Call P Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET3 SLC:0;BTUP Maint Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET3 SLC:0;B/TUP Error No OPC/CIC Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET3 SLC:0;B/TUP Error No Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET3 SLC:0;B/TUP Error No Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET3 SLC:0;B/TUP Error No AS for OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET3 SLC:0;Wrong NE Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET3 SLC:0;BICC Call P Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET3 SLC:0;BICC Maint Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET3 SLC:0;BICC Error No Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET3 SLC:0;BICC Error No Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET3 SLC:0;BICC Error No OPC Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET3 SLC:0;Wrong NE Received Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET3 SLC:0;Link Deactivated Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET3 SLC:0;Link Local Inhibit Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET3 SLC:0;Link Remote Inhibit Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET3 SLC:0;Unavailable Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET3 SLC:0;Level 1 Congestion Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET3 SLC:0;Link Available Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;300
ACC;Link Management;LS:ITUCLKSET3 SLC:0;Changeover Procedure Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET3 SLC:0;Near End Forced Unavailable Cou;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET3 SLC:0;Far End Mgmt Inhibit Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET3 SLC:0;RPO Cumulative Duration;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

ACC;Link Management;LS:ITUCLKSET3 SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0

GUI/CLUI Documentation for USP

GUI Launching and User procedures

- NN10093-511 - USP Configuration Management
- NN10094-511 - USP-Compact Operational Configuration
- NN10159-611 - USP Security and Administration
- NN10160-611 - USP-Compact Security and Administration

Related documents

- NN10008-111 - USP Basics
- NN10045-461 - Upgrading the USP
- NN10009-111 - USP-Compact Basics

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
- NN10275-909 - Carrier VoIP Fault Management Logs Reference, volumes 1-6.
- NN10083-911 - Communication Server 2000 Fault Management

Fault Mapping for XACore

The following criteria can be used for looking up information on specific faults for XACore.

Note: All XA-Core Logs are treated as INFO Events by the IEMS and are associated to the CS2000 Manager when the CS2000 Manager is configured in IEMS.

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 SONENT 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
- NN10264-709 - Carrier VoIP Performance Management Operational Measurements Reference, volumes 1-4

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

- NN10448-111 - Communication Server 2000 Basics
- NN10171-611 - Communication Server 2000 Security and Administration
- NN10324-509 - Carrier VoIP Operational Configuration: Data Schema Reference, volumes 1-2
- NN10324-509 - Carrier VoIP Performance Management Operational Measurements Reference, volumes 1-4
- 297-8021-808P2 - DMS-100 SERVORD Reference Manual
- 297-8991-810 - XA-Core Reference Manual

Platforms

Core Manager Platform

This section contains IEMS Northbound log samples and device documentation references for the Core Manager Platform.

Core Manager Platform Fault Interface

Fault documentation for Core Manager Platform :

- NN10408-900 ATM/IP Solution-level Fault Management
- NN10082-911 CS2000 Core Manager Fault Management
- NN10351-911 Core and Billing Manager 850 Fault Management

Fault Mapping for Core Manager Platform

The following criteria can be used for looking up information on specific faults for Core Manager Platform.

Note: All SDM Logs are treated as INFO Events by the IEMS and are associated to the Core Manager when the Core Manager is configured in IEMS.

Fault Correlation for Core Manager Platform

NB format -> Device/EM	SCC2	NTSTD	Document Reference
AIX Platform	logname and number	logname and number	NN10082-911 CS2000 Core Manager Fault Management
SPFS	logname and number	logname and number	NN10351-911 Core and Billing Manager 850 Fault Management

Northbound Fault Formats for Core Manager Platform

SCC2

The following is an example of a Core Manager Platform log in SCC2 format:

```
* 52 2 317 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.
```

```
SEC Master Server 47.142.94.49 is down.
```

Performance

OM and PM Documentation references for Core Manager Platform

- NN10148-700 CS2000 Core Manager Performance Management
- NN10361-711 Core and Billing Manager 850 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 Core Manager 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 Core Manager Platform in CSV format:

***Note:** The IEMS northbound performance interface does not support this device.*

GUI/CLUI Documentation for Core Manager Platform

Core Manager Platform has a command line user interface that can be accessed via a secure shell.

GUI/CLUI Launching and User procedures

- NN10104-511 CS2000 Core Manager Configuration Management

Related documents

- NN10018-111 CS2000 Core Manager Basics
- NN10126-811 CS2000 Core Manager Accounting
- NN10170-611 CS2000 Core Manager Security and Administration
- NN10355-111 Core and Billing Manager 850 Basics
- NN10363-811 Core and Billing Manager 850 Accounting
- NN10358-611 Core and Billing Manager 850 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

- NN10440-450 - Upgrading a Carrier VoIP Network

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	NN10440-450 Upgrading a Carrier VoIP Network

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)
- Upgrading a Carrier VoIP Network, NN10440-450.

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:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<PMFile xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonPerfRecord_V2.0.xsd"
MeasurementCategory="PM">
<FileCreationTime>2004-12-14T13:20:20EST</FileCreationTime>
<System>
<SystemId>NortelNetworks/IEMS</SystemId>
<Entity>
<EntityId>47.142.106.220</EntityId>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>.iso.org.dod.internet.mgmt.mib-2.ip.ipAddrTable.ipAddrEntry</TableId>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<Labels>
<Label>ipAdEntAddr</Label>
<Label>ipAdEntIfIndex</Label>
<Label>ipAdEntNetMask</Label>
<Label>ipAdEntBcastAddr</Label>
<Label>ipAdEntReasmMaxSize</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>47.142.106.222</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>255.255.255.0</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>65535</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
```

```
<Value>47.142.106.220</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>255.255.255.0</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>65535</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>192.168.47.1</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>255.255.255.0</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>65535</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>127.0.0.1</Value>
</RowValue>
<RowValue>
<Value>6</Value>
</RowValue>
<RowValue>
<Value>255.0.0.0</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>65535</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>47.142.106.224</Value>
</RowValue>
<RowValue>
<Value>4</Value>
</RowValue>
<RowValue>
<Value>255.255.255.0</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>65535</Value>
```

```
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>47.142.106.223</Value>
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
<RowValue>
<Value>255.255.255.0</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>65535</Value>
</RowValue>
</RowOfValues>
</Table>
<SingleValues MeasurementKind="Snapshot" IntervalDuration="5">
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipInUnknownProtos</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipFragCreates</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>418461</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipOutRequests</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>19623971</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipInDelivers</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>21482658</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipOutNoRoutes</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipDefaultTTL</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>255</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
```

```
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipReasmReqds</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>137693</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipInHdrErrors</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipReasmFails</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipForwDatagrams</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipFragFails</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipInDiscards</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipOutDiscards</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>4</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipForwarding</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>2</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipReasmTimeout</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>60</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
```

```
<MeasureId>ipInReceives</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>17207338</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipReasmOKs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>137693</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipRoutingDiscards</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipInAddrErrors</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipFragOKs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>138590</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsIfInErrors</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsSystemProcessTime</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsIfCollisions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsDiskXfer1</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
```

```
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsVSwapIn</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsDiskXfer3</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsVIntr</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsVPagesIn</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsIfOutPackets</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsNiceModeTime</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsIfOutErrors</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsIdleModeTime</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
```

```

</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsVPagesOut</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsDiskXfer2</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsVSwapOut</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsDiskXfer4</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsIfInPackets</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsUserProcessTime</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
</SingleValues>
</Entity>
</System>
</PMFile>

```

CSV

The following is an example of performance data for SSPFS platform in CSV format:

```
PMFile=Begin
```

MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime

PM,commonPerfRecord_V2.0.xsd,2005-03-17T10:25:00EST

System=Begin

SystemId

NortelNetworks/IEMS

Entity=Begin

EntityId

47.142.128.112

Table=Begin

TableId,MeasurementKind,IntervalDuration,CaptureTime

.iso.org.dod.internet.mgmt.mib-2.ip.ipAddrTable.ipAddrEntry,Snapshot,5,2005-03-17T10:25:00EST

Label,Label,Label,Label,Label

ipAdEntAddr,ipAdEntIfIndex,ipAdEntNetMask,ipAdEntBcastAddr,ipAdEntReasmMaxSize

Value,Value,Value,Value,Value

47.142.128.112,1,255.255.255.128,1,65535

127.0.0.1,3,255.0.0.0,1,65535

47.142.128.115,2,255.255.255.128,1,65535

Table=End

SingleValues=Begin

MeasurementKind,IntervalDuration

Snapshot,5

MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability

ipInUnknownProtos,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid

ipFragCreates,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid

ipOutRequests,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,3525617,Valid

ipInDelivers,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,21811895,Valid

ipOutNoRoutes,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid

ipDefaultTTL,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,255,Valid

ipReasmReqds,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid

ipInHdrErrors,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid

ipReasmFails,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid

ipForwDatagrams,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid
ipFragFails,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid
ipInDiscards,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid
ipOutDiscards,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid
ipForwarding,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,2,Valid
ipReasmTimeout,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,60,Valid
ipInReceives,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-
2.ip,4673901,Valid
ipReasmOKs,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid
ipRoutingDiscards,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid
ipInAddrErrors,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid
ipFragOKs,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid
rsIfInErrors,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Valid
rsSystemProcessTime,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Valid
rsIfCollisions,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Valid
rsDiskXfer1,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Valid
rsVSwapIn,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Valid
rsDiskXfer3,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Valid
rsVIntr,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Valid
rsVPagesIn,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Valid
rsIfOutPackets,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Valid
rsNiceModeTime,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Valid
rsIfOutErrors,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Valid
rsIdleModeTime,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Valid

```
rsVPagesOut,2005-03-  
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Valid  
  
rsDiskXfer2,2005-03-  
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Valid  
  
rsVSwapOut,2005-03-  
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Valid  
  
rsDiskXfer4,2005-03-  
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Valid  
  
rsIfInPackets,2005-03-  
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Valid  
  
rsUserProcessTime,2005-03-  
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Valid  
  
SingleValues=End  
  
Entity=End  
  
System=End  
  
PMFile=End
```

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 - Carrier VoIP 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 Carrier VoIP 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. => 19:40:37
snmpTrapOID. => 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
.48.52.45.54.45.50.57.44.49.48.58.50.57.58.48.46.52.44.11925
alarmActiveDateAndTime => 2004-6-29,10:29:0.4
alarmActiveDescription => DeviceSpecificInfo=softwareProgramError(48);Backup
Fail
nnExtAlarmActiveEventType => 4
nnExtAlarmActiveProbableCause => 1024
nnExtAlarmActiveAdditionalText => Scheduled/on-demand backup failed during
last iteration.
nnExtAlarmActiveDocumentationPointer => CICM341
nnExtAlarmActiveResourceDescription => IEMS=47.142.86.95-CICM-
Mgr_Card_A;CICM=CICMEM-000-A;NodeType=Platform
nnExtAlarmActiveSequenceNumber => 1

```

Syslog

The following is an example of a CICM Manager log in Syslog format:

```

Jun 30 15:44:06 2004      ComponentId: 47.165.168.74-CICM-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-CICM-Mgr_Card_B      Specific
Problem: Connection Lost      Description: IEMS Unable to communicate with managed
device

```

Performance

OM and PM Documentation references for CICM Manager

- NN10327-711 - IEMS Performance Management

Northbound OM/PM Formats

Performance measurements for CICM Manager are available only from the CICM Manager interface. See NN10327-711 - IEMS Performance Management for more information.

XML

The following is an example of Performance data for CICM 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="commonPerfRecord_V2.0.xsd" MeasurementCategory="PM">
<FileCreationTime>2004-06-23T13:36:04EST</FileCreationTime>
_ <System>
<SystemId>NortelNetworks/IEMS</SystemId>
_ <Entity>
<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.

```

PMFile=Begin
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonPerfRecord_V2.0.xsd,2005-03-29T15:30:02EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId
47.165.168.252

```

```
Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
.iso.org.dod.internet.mgmt.mib-
2.rmon.usrHistory.usrHistoryControlTable.usrHistoryControlEntry,Snapshot,5,2005-03-
29T15:30:00EST
Label,Label,Label,Label
usrHistoryControlIndex,usrHistoryControlInterval,usrHistoryControlOwner,usrHistoryCo
ntrolStatus
Value,Value,Value,Value
9,900,CICMEM-070-B,1
Table=End
```

```
Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelPerfRefMIB.
nnPerfMetricReferenceTable.nnPerfMetricReferenceEntry,Snapshot,5,2005-03-
29T15:30:01EST
Label,Label,Label,Label,Label,Label
nnPerfMetricRefIndex,nnPerfMetricName,nnPerfMetricGroup,nnPerfMetricDataType,nnPerfM
etricSources,nnPerfMetricValue
Value,Value,Value,Value,Value,Value
9,TransmittedBytesPerSecond,CICM,1,2,0
8,ReceivedBytesPerSecond,CICM,1,2,0
7,LoggedInUsers,CICM,1,2,0
6,HalfCallAttempts,CICM,1,2,0
5,ActiveConnections,CICM,1,2,0
4,PercentageCpuUsed,CICM,1,2,1
3,PercentageMemoryUsed,CICM,1,2,18
2,NumberOfLogs,CICM,1,2,0
1,ActiveSessions,CICM,1,2,0
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 :

- NN10408-900 - ATM/IP Solution-level Fault Management
- NN10202-911 - Gateway Controller 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	NN10408- 900 - ATM/IP Solution-level Fault Management

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=LANError;GWC is inaccessible
from GWCEM
nnExtAlarmActiveEventType => 2
nnExtAlarmActiveProbableCause => 1024
nnExtAlarmActiveAdditionalText => GWCEM fail to ping both GWC units of GWC-50
nnExtAlarmActiveDocumentationPointer => CMT301
```



```
nnExtAlarmActiveResourceDescription =>IEMS=rtp4cmt-GWC-  
Mgr;SESM=GWCEMalarm;GWCEM=DeviceInAccessible;GWC=GWC-50-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.

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

- NN10409-500 - ATM/IP Solution-level Configuration Management

- NN10402-600 - ATM/IP Solution-level Administration and Security
- NN10408-900 - ATM/IP Solution-level 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 :

- NN10275-909v3: Carrier VoIP Fault Management Logs Reference Vol. 3
- 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	Log name and log number (Log Names: EMSS, IEMS, EMJS)	Log name and log number (Log Names: EMSS, IEMS, EMJS)	Log name and log number (Log Names: EMSS, IEMS, EMJS)	Log name and log number (Log Names: EMSS, IEMS, EMJS)	See references listed above.

Northbound Fault Formats for IEMS

SCC2

The following is an example of a IEMS log in SCC2 format:

Sample Raise:

```
*C55 IEMS398 0006 FLT Communication Lost
Location: 47.142.94.68
NotificationID: 0
State: Raised
Category: Communications
Cause: Communications subsystem failure
```

Time: Dec 13 13:55:15 2004
ComponentId: znc0s0jh-SSPFS-Unit-0
Specific Problem: Connection Lost
Description: IEMS Unable to communicate with managed device

Sample Clear:

55 IEMS399 0007 FLT Communication Regained
Location: 47.142.94.68
NotificationID: 0
State: Cleared
Category: Communications
Time: Dec 13 13:55:22 2004
ComponentId: znc0s0jh-SSPFS-Unit-0
Description: IEMS regained communication with the managed device

NTStd

The following is an example of a IEMS log in NTStd format:

Sample Raise:

office_name *** IEMS398 DEC13 13:55:15 0006 FLT Communication Lost
Location: 47.142.94.68
NotificationID: 0
State: Raised
Category: Communications
Cause: Communications subsystem failure
Time: Dec 13 13:55:15 2004
ComponentId: znc0s0jh-SSPFS-Unit-0
Specific Problem: Connection Lost
Description: IEMS Unable to communicate with managed device

Sample Clear:

office_name IEMS399 DEC13 13:55:22 0007 FLT Communication Regained
Location: 47.142.94.68
NotificationID: 0
State: Cleared
Category: Communications
Time: Dec 13 13:55:22 2004
ComponentId: znc0s0jh-SSPFS-Unit-0
Description: IEMS regained communication with the managed device

SNMP

The following is an example of a IEMS log in SNMP format:

Sample Raise:

```

system.sysUpTime.0 => 7:01:55
snmpTrapOID.0 => nnExtAlarmMajor
alarmActiveResourceId =>
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48
.48.52.45.49.50.45.49.51.44.50.58.52.58.56.46.51.44.649
alarmActiveDateAndTime => 2004-12-13,2:4:8.3,
alarmActiveDescription => IEMS Unable to communicate with managed device
nnExtAlarmActiveEventType => 1
nnExtAlarmActiveProbableCause => 6
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => IEMS398
nnExtAlarmActiveResourceDescription => IEMS=IEMS-Mgr;znc0s0jh-SSPFS-Unit-0
nnExtAlarmActiveManualClear => 2
nnExtAlarmActiveSequenceNumber => 7

```

Sample Clear:

```

system.sysUpTime.0 => 7:01:55
snmpTrapOID.0 => nnExtAlarmClear
alarmActiveResourceId =>
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48.48.52.45.49.50.45.49.51.44.50.58.52.5
8.50.50.46.48.44.649
alarmActiveDateAndTime => 2004-12-13,2:4:22.0,
alarmActiveDescription => DeviceSpecificInfo=;IEMS regained communication with the managed
device
nnExtAlarmActiveEventType => 1
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => IEMS399
nnExtAlarmActiveResourceDescription => IEMS=IEMS-Mgr;znc0s0jh-SSPFS-Unit-0
nnExtAlarmActiveSequenceNumber => 8

```

Syslog

The following is an example of a IEMS log in Syslog format:

Sample Raise:

```

Dec 13 13:55:15 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=4093~~ IEMS398 CRIT
FLT Communication Lost^M Location: 47.142.94.68^M NotificationID: 0^M State:
Raised^M Category: Communications^M Cause: Communications subsystem failure^M
Time: Dec 13 13:55:15 2004^M ComponentId: znc0s0jh-SSPFS-Unit-0^M Specific
Problem: Connection Lost^M Description: IEMS Unable to communicate with managed
device

```

Sample Clear:

```

Dec 13 13:55:22 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=4094~~ IEMS399
NONE FLT Communication Regained^M Location: 47.142.94.68^M NotificationID:
0^M State: Cleared^M Category: Communications^M Time: Dec 13 13:55:22
2004^M ComponentId: znc0s0jh-SSPFS-Unit-0^M Description: IEMS regained
communication with the managed device

```

Performance

OM and PM Documentation references for IEMS

- NN10327-711 IEMS 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 IEMS 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="commonPerfRecord_V2.0.xsd" MeasurementCategory="PM">
<FileCreationTime>2004-12-13T13:06:04EST</FileCreationTime>
<System>
<SystemId>NortelNetworks/IEMS</SystemId>
<Entity>
<EntityId>47.142.94.68</EntityId>
<Table MeasurementKind="Snapshot" IntervalDuration="30">
<TableId>fiveMinCollectionJobTable</TableId>
<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>
<Labels>
<Label>fiveMinCollectionJobID</Label>
<Label>fiveMinCollectionJobName</Label>
<Label>fiveMinCollectionJobStartTime</Label>
<Label>fiveMinCollectionJobExecutionTime</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>storm_collect</Value>
</RowValue>
<RowValue>
<Value>1102961130856</Value>
</RowValue>
```

```
<RowValue>
<Value>4586</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="30">
<TableId>thirtyMinCollectionJobTable</TableId>
<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>
<Labels>
<Label>thirtyMinCollectionJobID</Label>
<Label>thirtyMinCollectionJobName</Label>
<Label>thirtyMinCollectionJobStartTime</Label>
<Label>thirtyMinCollectionJobExecutionTime</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>iems_collect</Value>
</RowValue>
<RowValue>
<Value>1102961120556</Value>
</RowValue>
<RowValue>
<Value>2621</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="30">
<TableId>tableSpaceTable</TableId>
<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>
<Labels>
<Label>tableSpaceName</Label>
<Label>usedTableSpaceInBytes</Label>
<Label>usedTableSpaceInPercent</Label>
</Labels>
<RowOfValues>
```

```
<RowValue>
<Value>IEMS_TS</Value>
</RowValue>
<RowValue>
<Value>18808832</Value>
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>IEMS_EVENT_TS</Value>
</RowValue>
<RowValue>
<Value>5963776</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>IEMS_PERF_TS</Value>
</RowValue>
<RowValue>
<Value>1835008</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<SingleValues MeasurementKind="Snapshot" IntervalDuration="30">
<SingleValue>
<CaptureTime>2004-12-13T13:05:50EST</CaptureTime>
<MeasureId>systemRestartCount</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.system</MeasureSuppId1>
```

```
<Value>3</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:50EST</CaptureTime>
<MeasureId>numOfActiveClients</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.client</MeasureSuppId1>
<Value>3</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:50EST</CaptureTime>
<MeasureId>numOfEventsFromUnknownCustlogDevices</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event</MeasureSupp
Id1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:50EST</CaptureTime>
<MeasureId>eventQueueSize</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event</MeasureSupp
Id1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:50EST</CaptureTime>
<MeasureId>numOfEventsFromUnknownSNMPDevices</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event</MeasureSupp
Id1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:50EST</CaptureTime>
<MeasureId>avgEventThroughputRate</MeasureId>
```



```
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event</MeasureSupp
Id1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:50EST</CaptureTime>

<MeasureId>numOfEventsFromUnknownDevices</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event</MeasureSupp
Id1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:50EST</CaptureTime>

<MeasureId>maxEventThroughputRate</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event</MeasureSupp
Id1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>

<MeasureId>numOfDiscardedEvents</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event</MeasureSupp
Id1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>

<MeasureId>numOfEvents</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event</MeasureSupp
Id1>

<Value>6060</Value>

<Reliability>Valid</Reliability>

</SingleValue>
```

```
<SingleValue>
<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>
<MeasureId>numOfEventsAdded</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event</MeasureSupp
Id1>
<Value>5</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>
<MeasureId>numOfAlarmsCleared</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms</MeasureSup
pId1>
<Value>2</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>
<MeasureId>numOfMajorAlarms</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms</MeasureSup
pId1>
<Value>27</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>
<MeasureId>numOfWarningAlarms</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms</MeasureSup
pId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>
<MeasureId>numOfCriticalAlarms</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms</MeasureSup
pId1>
```

```
<Value>48</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>
<MeasureId>numOfAlarmsAdded</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms</MeasureSupp
pId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>
<MeasureId>numOfMinorAlarms</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms</MeasureSupp
pId1>
<Value>7</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>
<MeasureId>numOfActiveAlarms</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms</MeasureSupp
pId1>
<Value>82</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>
<MeasureId>numOfDBCcleanUpPolicyExecutions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.database</MeasureSuppId1
>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>
```

```
<MeasureId>numOfAttributesCollected</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance</MeasureSupp
Id1>
<Value>4146</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>
<MeasureId>numOfReportsJobsProvisioned</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance</MeasureSupp
Id1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>
<MeasureId>numOfTransferJobsProvisioned</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance</MeasureSupp
Id1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>
<MeasureId>numOfCollectionJobsProvisioned</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance</MeasureSupp
Id1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>
<MeasureId>numOfAttributesCollectedOverThisInterval</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance</MeasureSupp
Id1>
<Value>3342</Value>
<Reliability>Valid</Reliability>
```

```
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>
<MeasureId>numOfFailedReportJobs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance</MeasureSupp
Id1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>
<MeasureId>numOf24HrSuccessfulJobs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCo
llectionJobs</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>
<MeasureId>numOf30MinSuccessfulJobs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCo
llectionJobs</MeasureSuppId1>
<Value>1</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>
<MeasureId>numOf12HrSuccessfulJobs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCo
llectionJobs</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>
<MeasureId>numOf15MinSuccessfulJobs</MeasureId>
```

```
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCo
llectionJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf60MinSuccessfulJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCo
llectionJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf5MinSuccessfulJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCo
llectionJobs</MeasureSuppId1>

<Value>1</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf15MinPartialSuccessfulJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucce
ssfulCollectionJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf60MinPartialSuccessfulJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucce
ssfulCollectionJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>
```

```
<SingleValue>
<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>
<MeasureId>numOf5MinPartialSuccessfulJobs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucce
ssfulCollectionJobs</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>
<MeasureId>numOf24HrPartialSuccessfulJobs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucce
ssfulCollectionJobs</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>
<MeasureId>numOf30MinPartialSuccessfulJobs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucce
ssfulCollectionJobs</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>
<MeasureId>numOf12HrPartialSuccessfulJobs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucce
ssfulCollectionJobs</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>
<MeasureId>numOf24HrFailedCollectionJobs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollec
tionJobs</MeasureSuppId1>
```

```
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>
<MeasureId>numOf30MinFailedCollectionJobs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollec
tionJobs</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>
<MeasureId>numOf12HrFailedCollectionJobs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollec
tionJobs</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>
<MeasureId>numOf15MinFailedCollectionJobs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollec
tionJobs</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>
<MeasureId>numOf60MinFailedCollectionJobs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollec
tionJobs</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>
```



```
<MeasureId>numOf5MinFailedCollectionJobs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollec
tionJobs</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>
<MeasureId>numOf24HrFailedTransferJobs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransf
erJobs</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>
<MeasureId>numOf30MinFailedTransferJobs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransf
erJobs</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>
<MeasureId>numOf12HrFailedTransferJobs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransf
erJobs</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>
<MeasureId>numOf15MinFailedTransferJobs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransf
erJobs</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
```

```
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>
<MeasureId>numOf60MinFailedTransferJobs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransf
erJobs</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>
<MeasureId>numOf5MinFailedTransferJobs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransf
erJobs</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>
<MeasureId>numOfManagedObjects</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.topology</MeasureSuppId1
>
<Value>47</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>
<MeasureId>numOfDevicesInUnManagedState</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.topology</MeasureSuppId1
>
<Value>3</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>
<MeasureId>numOfAddedManagedObjects</MeasureId>
```

```
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.topology</MeasureSuppId1
>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>

<MeasureId>numOfDevicesInUnKnownState</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.topology</MeasureSuppId1
>

<Value>8</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>

<MeasureId>numOfUnKnownDeviceStateTransistions</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.topology</MeasureSuppId1
>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>

<MeasureId>numOfdeletedManagedObjects</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.topology</MeasureSuppId1
>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>

<MeasureId>numOfThrottledDeviceStateTransistions</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.topology</MeasureSuppId1
>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>
```

```

<SingleValue>
<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>
<MeasureId>numOfDevicesInThrottledState</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.topology</MeasureSuppId1
>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>
<MeasureId>numOfSystemUnManagedDeviceStateTransistions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.topology</MeasureSuppId1
>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>
<MeasureId>numOfDevicesInSystemUnManagedState</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.topology</MeasureSuppId1
>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
</SingleValues>
</Entity>
</System>
</PMFile>

```

CSV

The following is an example of Performance data for IEMS in CSV format:

```

PMFile=Begin
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonPerfRecord_V2.0.xsd,2005-03-17T13:00:02EST

System=Begin

```

SystemId

NortelNetworks/IEMS

Entity=Begin

EntityId

47.142.128.115

Table=Begin

TableId, MeasurementKind, IntervalDuration, CaptureTime

fiveMinCollectionJobTable, Snapshot, 5, 2005-03-17T13:00:02EST

Label, Label, Label, Label

fiveMinCollectionJobID, fiveMinCollectionJobName, fiveMinCollectionJobStartTime, fiveMinCollectionJobExecutionTime

Value, Value, Value, Value

1, IEMS5minCollection, 1111082100898, 2233

Table=End

Table=Begin

TableId, MeasurementKind, IntervalDuration, CaptureTime

tableSpaceTable, Snapshot, 5, 2005-03-17T13:00:01EST

Label, Label, Label

tableSpaceName, usedTableSpaceInBytes, usedTableSpaceInPercent

Value, Value, Value

IEMS_TS, 45875200, 44

IEMS_EVENT_TS, 134610944, 16

IEMS_PERF_TS, 13238272, 2

Table=End

Table=Begin

TableId, MeasurementKind, IntervalDuration, CaptureTime

fiveMinTransferJobTable, Snapshot, 5, 2005-03-17T13:00:02EST

Label, Label, Label, Label

fiveMinTransferJobID, fiveMinTransferJobName, fiveMinTransferJobStartTime, fiveMinTransferJobExecutionTime

Value, Value, Value, Value

1, IEMS5minTransfer, 1111082103882, 453

Table=End

```
Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
deviceEventRateTable,Snapshot,5,2005-03-17T13:00:01EST
Label,Label,Label,Label
deviceID,deviceName,eventRate,eventRateDetails
Value,Value,Value,Value
3,rtpo-mg9kem.us.nortel.com-MG9K-Mgr_7.0,0,106 events received in 298170
milliseconds.
2,wnc0s0pe.us.nortel.com-MG9K-Mgr_9.0,0,14 events received in 298170 milliseconds.
1,SYSLOG,0,6 events received in 298170 milliseconds.
Table=End
```

```
Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
fiveMinReportJobTable,Snapshot,5,2005-03-17T13:00:02EST
Label,Label,Label,Label
fiveMinReportJobID,fiveMinReportJobName,fiveMinReportJobStartTime,fiveMinReportJobEx
ecutionTime
Value,Value,Value,Value
1,IEMS5minReport,1111082100898,733
Table=End
```

```
SingleValues=Begin
MeasurementKind,IntervalDuration
Snapshot,5
MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability
systemRestartCount,2005-03-
17T13:00:00EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.system,2,Valid
numOfActiveClients,2005-03-
17T13:00:00EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.client,6,Valid
numOfEventsFromUnknownCustlogDevices,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,6,Valid
eventQueueSize,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,0,Valid
```

```
numOfEventsFromUnknownSNMPDevices,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,0,Valid

avgEventThroughputRate,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,0,Valid

numOfEventsFromUnknownDevices,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,6,Valid

maxEventThroughputRate,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,2,Valid

numOfDiscardedEvents,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,0,Valid

numOfEvents,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,150735,Valid

numOfEventsAdded,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,137,Valid

numOfAlarmsCleared,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,73,Valid

numOfMajorAlarms,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,263,Valid

numOfWarningAlarms,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,75,Valid

numOfCriticalAlarms,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,36,Valid

numOfAlarmsAdded,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,47,Valid

numOfMinorAlarms,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,74,Valid

numOfActiveAlarms,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,448,Valid

numOfDBCcleanUpPolicyExecutions,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.database,1,Valid

applicationHeapSize,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.memory,101923064,Valid

maxApplicationHeapSize,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.memory,139169296,Valid
```

```
numOfAttributesCollected,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,19411,Valid

numOfReportsJobsProvisioned,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,0,Valid

numOfTransferJobsProvisioned,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,0,Valid

numOfCollectionJobsProvisioned,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,0,Valid

numOfAttributesCollectedOverThisInterval,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,176,Valid

numOfFailedReportJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,0,Valid

numOf24HrSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,0,Valid

numOf30MinSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,0,Valid

numOf12HrSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,0,Valid

numOf15MinSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,0,Valid

numOf60MinSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,0,Valid

numOf5MinSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,1,Valid

numOf15MinPartialSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucces
sfulCollectionJobs,0,Valid

numOf60MinPartialSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucces
sfulCollectionJobs,0,Valid

numOf5MinPartialSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
```


rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSuccessfulCollectionJobs,0,Valid

numOf24HrPartialSuccessfulJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSuccessfulCollectionJobs,0,Valid

numOf30MinPartialSuccessfulJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSuccessfulCollectionJobs,0,Valid

numOf12HrPartialSuccessfulJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSuccessfulCollectionJobs,0,Valid

numOf24HrFailedCollectionJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollectionJobs,0,Valid

numOf30MinFailedCollectionJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollectionJobs,0,Valid

numOf12HrFailedCollectionJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollectionJobs,0,Valid

numOf15MinFailedCollectionJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollectionJobs,0,Valid

numOf60MinFailedCollectionJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollectionJobs,0,Valid

numOf5MinFailedCollectionJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollectionJobs,0,Valid

numOf24HrFailedTransferJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransferJobs,0,Valid

numOf30MinFailedTransferJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransferJobs,0,Valid

numOf12HrFailedTransferJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransferJobs,0,Valid

numOf15MinFailedTransferJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no

```
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransferJobs,0,Valid

numOf60MinFailedTransferJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransferJobs,0,Valid

numOf5MinFailedTransferJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransferJobs,0,Valid

numOfManagedObjects,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,345,Valid

numOfDevicesInUnManagedState,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,4,Valid

numOfAddedManagedObjects,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfDevicesInUnknownState,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,9,Valid

numOfUnknownDeviceStateTransitions,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfDeletedManagedObjects,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfThrottledDeviceStateTransitions,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfDevicesInThrottledState,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfSystemUnManagedDeviceStateTransitions,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfDevicesInSystemUnManagedState,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

SingleValues=End
```

GUI/CLUI Documentation for IEMS

GUI Launching and User procedures

- NN10329-111 - IEMS Basics

Related documents

- NN10334-911: IEMS Fault Management
- NN10330-511: IEMS Configuration Management
- NN10327-711: IEMS Performance Management
- NN10336-611: IEMS Security and Administration

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
- NN10408-900 ATM/IP Solution-level Fault Management
- NN10275-909 Carrier VoIP 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 been 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 been 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

- 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 MG9000 Mgr in XML format:

```

PMFile=Begin
MeasurementCategorynoNamespaceSchemaLocationFileCreationTime
PM commonPerfRecord_V2.0.xsd2004-11-18T15:45:53EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId
47.142.110.210

```

SubEntity=Begin

SubEntityId

CC04

SubEntity=End

" "

SubEntity=Begin

SubEntityId

CC03

SubEntity=End

" "

SubEntity=Begin

SubEntityId

CC02

SubEntity=End

" "

SubEntity=Begin

SubEntityId

Sefik_CC01

SubEntity=End

" "

SubEntity=Begin

SubEntityId

cco6

Table=Begin

TableIdMeasurementKindIntervalDurationCaptureTime

nnPmUtilOmIntervTableSnapshot52004-11-18T15:45:00EST

LabelLabelLabelLabelLabelLabelLabelLabelLabel

SourcennPmUtilIntervChanAvgnnPmUtilIntervChanPeaknnPmUtilIntervCpuAvg

nnPmUtilIntervCpuPeaknnPmUtilIntervFlashAvgnnPmUtilIntervFlashPeak

nnPmUtilIntervRamAvgnnPmUtilIntervRamPeak

ValueValueValueValueValueValueValueValueValueValue

Frame006.Shelf2.Slot1500000000

Frame006.Shelf2.Slot1400000000

Frame006.Shelf3.Slot1300000000

Frame006.Shelf2.Slot1300000000

Frame006.Shelf3.Slot1200000000

Frame006.Shelf2.Slot1200000000

Frame006.Shelf2.Slot1100000000

Frame006.Shelf2.Slot1000000000

Table=End

GUI/CLUI Documentation for MG9000 Mgr

GUI Launching and User procedures

- NN10096-511 MG9000 Configuration Management

Related documents

- NN10162-611 MG9000 Administration and Security
- NN10048-461 Upgrading the MG9000
- NN10409-500 ATM/IP Solution-level Configuration Management
- NN10408-900 ATM/IP Solution-level 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 - MDM Fault Management Tools
- NN10092-911 - MSS 15000, MG 15000 & MDM Fault Overview
- NN10600-500 - Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference
- NN10600-520 - Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference
- 241-6001-500 - MDM 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	241-6001-500 - MDM Alarms Reference Guide
301x	241-6001-500 - MDM Alarms Reference Guide
50xx	241-6001-500 - MDM Alarms Reference Guide
600x	241-6001-500 - MDM Alarms Reference Guide
A0xx	241-6001-500 - MDM Alarms Reference Guide
B000	241-6001-500 - MDM Alarms Reference Guide
CDxx	241-6001-500 - MDM 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 - MSS 15000, MG 15000 & MDM Fault Overview

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 MSS 15000, MG 15000 & MDM Fault Overview

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@rt pimdm 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@rt pimdm 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

- 241-6001-031 - Multiservice Data Manager Performance Management Tools
- 241-6001-032 - Multiservice Data Manager Performance Data Reference

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 - MDM MDP Data Formats Reference Guide

XML

The following is an example of Performance data for MDM in XML format:

```
PMFile=Begin
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonPerfRecord_V2.0.xsd,2005-03-17T13:00:02EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId
47.142.128.115

Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
fiveMinCollectionJobTable,Snapshot,5,2005-03-17T13:00:02EST
Label,Label,Label,Label
fiveMinCollectionJobID,fiveMinCollectionJobName,fiveMinCollectionJobStartTime,fiveMinCollectionJobExecutionTime
Value,Value,Value,Value
1,IEMS5minCollection,1111082100898,2233
Table=End

Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
tableSpaceTable,Snapshot,5,2005-03-17T13:00:01EST
Label,Label,Label
tableSpaceName,usedTableSpaceInBytes,usedTableSpaceInPercent
Value,Value,Value
IEMS_TS,45875200,44
IEMS_EVENT_TS,134610944,16
IEMS_PERF_TS,13238272,2
Table=End

Table=Begin
```

```
TableId,MeasurementKind,IntervalDuration,CaptureTime
fiveMinTransferJobTable,Snapshot,5,2005-03-17T13:00:02EST
Label,Label,Label,Label
fiveMinTransferJobID,fiveMinTransferJobName,fiveMinTransferJobStartTime,fiveMinTransferJobExecutionTime
Value,Value,Value,Value
1,IEMS5minTransfer,1111082103882,453
Table=End
```

```
Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
deviceEventRateTable,Snapshot,5,2005-03-17T13:00:01EST
Label,Label,Label,Label
deviceID,deviceName,eventRate,eventRateDetails
Value,Value,Value,Value
3,rtpo-mg9kem.us.nortel.com-MG9K-Mgr_7.0,0,106 events received in 298170 milliseconds.
2,wnc0s0pe.us.nortel.com-MG9K-Mgr_9.0,0,14 events received in 298170 milliseconds.
1,SYSLOG,0,6 events received in 298170 milliseconds.
Table=End
```

```
Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
fiveMinReportJobTable,Snapshot,5,2005-03-17T13:00:02EST
Label,Label,Label,Label
fiveMinReportJobID,fiveMinReportJobName,fiveMinReportJobStartTime,fiveMinReportJobExecutionTime
Value,Value,Value,Value
1,IEMS5minReport,1111082100898,733
Table=End
```

```
SingleValues=Begin
MeasurementKind,IntervalDuration
Snapshot,5
MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability
```

```
systemRestartCount,2005-03-
17T13:00:00EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.system,2,Valid

numOfActiveClients,2005-03-
17T13:00:00EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.client,6,Valid

numOfEventsFromUnknownCustlogDevices,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,6,Valid

eventQueueSize,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,0,Valid

numOfEventsFromUnknownSNMPDevices,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,0,Valid

avgEventThroughputRate,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,0,Valid

numOfEventsFromUnknownDevices,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,6,Valid

maxEventThroughputRate,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,2,Valid

numOfDiscardedEvents,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,0,Valid

numOfEvents,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,150735,Valid

numOfEventsAdded,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,137,Valid

numOfAlarmsCleared,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,73,Valid

numOfMajorAlarms,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,263,Valid

numOfWarningAlarms,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,75,Valid

numOfCriticalAlarms,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,36,Valid

numOfAlarmsAdded,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,47,Valid

numOfMinorAlarms,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,74,Valid
```

```
numOfActiveAlarms,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,448,Valid

numOfDBCleanUpPolicyExecutions,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.database,1,Valid

applicationHeapSize,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.memory,101923064,Valid

maxApplicationHeapSize,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.memory,139169296,Valid

numOfAttributesCollected,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,19411,Valid

numOfReportsJobsProvisioned,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,0,Valid

numOfTransferJobsProvisioned,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,0,Valid

numOfCollectionJobsProvisioned,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,0,Valid

numOfAttributesCollectedOverThisInterval,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,176,Valid

numOfFailedReportJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,0,Valid

numOf24HrSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,0,Valid

numOf30MinSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,0,Valid

numOf12HrSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,0,Valid

numOf15MinSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,0,Valid

numOf60MinSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,0,Valid

numOf5MinSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
```

```
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCollectionJobs,1,Valid

numOf15MinPartialSuccessfulJobs,2005-03-17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSuccessfulCollectionJobs,0,Valid

numOf60MinPartialSuccessfulJobs,2005-03-17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSuccessfulCollectionJobs,0,Valid

numOf5MinPartialSuccessfulJobs,2005-03-17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSuccessfulCollectionJobs,0,Valid

numOf24HrPartialSuccessfulJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSuccessfulCollectionJobs,0,Valid

numOf30MinPartialSuccessfulJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSuccessfulCollectionJobs,0,Valid

numOf12HrPartialSuccessfulJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSuccessfulCollectionJobs,0,Valid

numOf24HrFailedCollectionJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollectionJobs,0,Valid

numOf30MinFailedCollectionJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollectionJobs,0,Valid

numOf12HrFailedCollectionJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollectionJobs,0,Valid

numOf15MinFailedCollectionJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollectionJobs,0,Valid

numOf60MinFailedCollectionJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollectionJobs,0,Valid

numOf5MinFailedCollectionJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollectionJobs,0,Valid

numOf24HrFailedTransferJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
```

```
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransferJobs,0,Valid

numOf30MinFailedTransferJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransferJobs,0,Valid

numOf12HrFailedTransferJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransferJobs,0,Valid

numOf15MinFailedTransferJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransferJobs,0,Valid

numOf60MinFailedTransferJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransferJobs,0,Valid

numOf5MinFailedTransferJobs,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransferJobs,0,Valid

numOfManagedObjects,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,345,Valid

numOfDevicesInUnManagedState,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,4,Valid

numOfAddedManagedObjects,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfDevicesInUnknownState,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,9,Valid

numOfUnknownDeviceStateTransitions,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfDeletedManagedObjects,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfThrottledDeviceStateTransitions,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfDevicesInThrottledState,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfSystemUnManagedDeviceStateTransitions,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfDevicesInSystemUnManagedState,2005-03-17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid
```


[illegible]

[illegible]

BDF

The MDM provides a Bulk Data Format option for PM data as well as the CSV file format. The BDF format and reference information can be found in the [Preside MDM MDP Data Formats Reference Guide](#).

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 - MDM Overview
- 241-6001-011 - MDM Fault Management Tools
- 241-6001-013 - MDM Remote Network Communication System User Guide
- 241-6001-015 - MDM Network Model Administration

- 241-6001-022 - MDM Network Reporting System
- 241-6001-023 - MDM Configuration Management Tools
- 241-6001-031 - MDM Performance Management

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 - MSS 15000, MG 15000 & MDM - Basics (PT-AAL1/UA-AAL1/UA-IP)
- NN10070-461 - Upgrading Multiservice Switch 15000 (PT-AAL1/UA-AAL1)
- NN10092-911 - MSS 15000, MG 15000 & MDM Fault Overview (PT-AAL1/UA-AAL1/UA-IP)
- NN10114-511 - MSS 15000, MG 15000 & MDM Configuration Overview (PT-AAL1/UA-AAL1/UA-IP/PT-AAL2)
- NN10158-711 - MSS 15000, MG 15000 & MDM Performance (PT-AAL1/UA-AAL1/UA-IP)
- NN10180-611 - MSS 15000, MG 15000 & MDM Security and Administration (PT-AAL1/UA-AAL1/UA-IP)
- NN10185-461 - Upgrading MDM
- NN10198-912 - MSS 15000, MG 15000 & MDM Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
- NN10225-512 - MSS 15000, MG 15000 & MDM Configuration Attribute Summary (PT-AAL1/UA-AAL1/UA-IP/PT-AAL2)

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:

PMFile=Begin

MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime

PM,commonPerfRecord_V2.0.xsd,2005-03-16T10:55:01EST

System=Begin

SystemId

NortelNetworks/IEMS

Entity=Begin

EntityId

172.16.144.134

SingleValues=Begin

MeasurementKind,IntervalDuration

Snapshot,5

MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability

totalBytesRxd,2005-03-

16T10:55:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceControl.scu.scuMessaging.ipoaMIB,14792,Valid

rxedTimeoutCount,2005-03-

16T10:55:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceControl.scu.scuMessaging.ipoaMIB,0,Valid

bytesSentPerSec,2005-03-

16T10:55:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceControl.scu.scuMessaging.ipoaMIB,24,Valid

cellDropCount,2005-03-

16T10:55:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceControl.scu.scuMessaging.ipoaMIB,0,Valid

oversizedPDUCount,2005-03-

16T10:55:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceControl.scu.scuMessaging.ipoaMIB,0,Valid

bytesRxdPerSec,2005-03-

16T10:55:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceControl.scu.scuMessaging.ipoaMIB,24,Valid

totalBytesSent,2005-03-

16T10:55:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceControl.scu.scuMessaging.ipoaMIB,16765,Valid

SingleValues=End

Entity=End

System=End

PMFile=End

GUI/CLUI Documentation for SAM21 EM

GUI Launching and User procedures

- NN10409-500 - ATM/IP Solution-level Configuration Management
- NN10402-600 - ATM/IP Solution-level Administration and Security
- NN10111-511 - SAM21 Shelf Controller Configuration Management

Related documents

- NN10025-111 - SAM21 Shelf Controller Basics
- NN10408-900 - ATM/IP Solution-level Fault Management
- NN10155-711 - SAM21 Shelf Controller Performance Management
- NN10177-611 - SAM21 Shelf Controller Administration and Security

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 Management

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:

```
PMFile=Begin
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonPerfRecord_V2.0.xsd,2005-03-24T14:55:02EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId
172.17.40.230

SingleValues=Begin
MeasurementKind,IntervalDuration
Snapshot,5
MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability
sysDescr,2005-03-24T14:55:01EST,.iso.org.dod.internet.mgmt.mib-2.system,Product:
IPmedia 2000;SW Version: 4.60B.003,Valid
snmpOutPkts,2005-03-24T14:55:01EST,.iso.org.dod.internet.mgmt.mib-2.snmp,159,Valid
snmpInBadVersions,2005-03-24T14:55:01EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid
snmpInBadCommunityNames,2005-03-24T14:55:01EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid
snmpInTotalReqVars,2005-03-24T14:55:01EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,323,Valid
snmpOutTraps,2005-03-24T14:55:01EST,.iso.org.dod.internet.mgmt.mib-2.snmp,6,Valid
snmpInBadCommunityUses,2005-03-24T14:55:01EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid
snmpInPkts,2005-03-24T14:55:01EST,.iso.org.dod.internet.mgmt.mib-2.snmp,154,Valid
snmpInTotalSetVars,2005-03-24T14:55:01EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid
```

snmpInASNParseErrs, 2005-03-24T14:55:01EST, .iso.org.dod.internet.mgmt.mib-2.snmp, 0, Valid

tcpOutSegs, 2005-03-24T14:55:01EST, .iso.org.dod.internet.mgmt.mib-2.tcp, 42, Valid

tcpInSegs, 2005-03-24T14:55:01EST, .iso.org.dod.internet.mgmt.mib-2.tcp, 7148, Valid

udpOutDatagrams, 2005-03-24T14:55:02EST, .iso.org.dod.internet.mgmt.mib-2.udp, 3974, Valid

udpInDatagrams, 2005-03-24T14:55:02EST, .iso.org.dod.internet.mgmt.mib-2.udp, 238, Valid

snmpSilentDrops, 2005-03-24T14:55:02EST, .iso.org.dod.internet.mgmt.mib-2.snmp, 0, Valid

acPerfCpMessageSendErrors, 2005-03-24T14:55:02EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp, 0, Valid

acPerfCpNumDupsForCompletedTransactions, 2005-03-24T14:55:02EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp, 0, Valid

acPerfCpMessageMaxRetransmissionsExceeded, 2005-03-24T14:55:02EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp, 421, Valid

acPerfCpMessageReceiveErrors, 2005-03-24T14:55:02EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp, 0, Valid

acPerfCpMessageRetransmissions, 2005-03-24T14:55:02EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp, 2954, Valid

acPerfCpNumDupsForOutstandingTransactions, 2005-03-24T14:55:02EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp, 0, Valid

acPerfCpMessagesFromUntrustedSources, 2005-03-24T14:55:02EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp, 0, Valid

acPerfCpProtocolSyntaxErrors, 2005-03-24T14:55:02EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfCp, 0, Valid

acPerfRtpRcvrLostPackets, 2005-03-24T14:55:02EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfRtp, 0, Valid

acPerfRtpFailedDueToLackOfResources, 2005-03-24T14:55:02EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaGateway.acPerfRtp, 0, Valid

acPerfIvrPlayCollectRequests, 2005-03-24T14:55:02EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaServices.acPerfIvr, 0, Valid

acPerfIvrPlayRequests, 2005-03-24T14:55:02EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaServices.acPerfIvr, 0, Valid

acPerfIvrPlayCollectFailedDueToLackOfResources, 2005-03-24T14:55:02EST, .iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.acPerfMediaServices.acPerfIvr, 0, Valid

```
acPerfIvrPlayFailedDueToProvMismatch,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrContDigitCollectRequests,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrPlayFailedDueToLackOfResources,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrPlayCollectFailedDueToProvMismatch,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrContDigitCollectFailedDueToLackOfResources,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfBctFailedDueToLackOfResources,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfBct,0,Valid

acPerfBctRequests,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfBct,0,Valid

acPerfConfRequests,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfConf,0,Valid

acPerfConfPortsUsed,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfConf,0,Valid

acPerfConfAddFailedDueToLackOfResources,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfConf,0,Valid

acPerfConfFailedDueToLackOfResources,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfConf,0,Valid

acPerfTtFailedDueToLackOfResources,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfTt,0,Valid

acPerfTtRequests,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfTt,0,Valid

acPerfSystemPacketEndpointsInUse,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfSystem,0,Valid

SingleValues=End

Entity=End

System=End

PMFile=End
```

GUI/CLUI Documentation for APS

GUI Launching and User procedures

- NN10340-511 - MS 2000 Series Configuration Management

Related documents

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

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 :

- NN10408-900 - ATM/IP Solution-level 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	NN10408- 900 - ATM/IP Solution-level 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

- NN10409-500 - ATM/IP Solution-level Configuration Management

Related documents

- NN10402-600 - ATM/IP Solution-level Administration and Security
- NN10440-450 - Upgrading the Carrier VoIP 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 for a raise alarm:

```
system.sysUpTime.0 => 0:28:36
snmpTrapOID.0 => nnExtAlarmCritical
alarmActiveResourceId =>
1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.2
8.50.48.48.53.45.48.57.45.48.55.44.49.57.58.53.55.58.51.56.46.48.44.45.48.52
.58.48.48.140819
alarmActiveDateAndTime => 2004-1-22,4:34:20.0,
alarmActiveDescription => If 10 (or more) records with unsupported version are
received consecutively, Major fault log is generated and the connection is
closed
nnExtAlarmActiveEventType => 1
nnExtAlarmActiveProbableCause => 166
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => QCA 301
nnExtAlarmActiveResourceDescription => IEMS=rtp4cmt-QOS
nnExtAlarmActiveManualClear => 4
nnExtAlarmActiveSequenceNumber => 3
```

The following is an example of a QCA log in SNMP format for a clear alarm:

```
system.sysUpTime.0 => 0:28:36
snmpTrapOID.0 =>
alarmActiveResourceId =>
1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.2
8.50.48.48.53.45.48.57.45.48.55.44.49.57.58.53.55.58.51.56.46.48.44.45.48.52
.58.48.48.140819
alarmActiveDateAndTime => 2004-1-22,4:34:20.0,
alarmActiveDescription => If 10 (or more) records with unsupported version are
received consecutively, Major fault log is generated and the connection is
closed
nnExtAlarmActiveEventType => 1
nnExtAlarmActiveProbableCause => 1024
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => QCA 399
nnExtAlarmActiveResourceDescription => IEMS=rtp4cmt-QOS
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

- NN10409-500 - ATM/IP Solution-level 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 OMs or PMs associated with this application.

GUI/CLUI Documentation for TMM

GUI Launching and User procedures

- NN10409-500 - ATM/IP Solution-level Configuration Management

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 :

- NN10408-900 - ATM/IP Solution-level 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	NN10408- 900 - ATM/IP Solution-level 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 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.
```

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
e 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 - Carrier VoIP 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
- NN10408-900 ATM/IP Solution-level Fault Management
- NN10275-909 Carrier VoIP 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

- NN10048-461 Upgrading the MG9000
- NN10409-500 ATM/IP Solution-level Configuration Management
- NN10408-900 ATM/IP Solution-level 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

- NN10409-500 ATM/IP Solution-level 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 - Carrier VoIP Fault Management Logs Reference
- NN10408-900 - ATM/IP Solution-level 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 Carrier VoIP 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 repo
rt 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

Related documents

- NN10083-911 - CS2000 Fault Management
- NN10402-600 - ATM/IP Solution-level Administration and Security
- NN10409-500 - ATM/IP Solution-level Configuration Management
- NIS V208-1 - V5.2 Interface Specification for CS2000

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] NN10402-600 - ATM/IP Solution-level Administration and Security

Network Engineering

- [5] <SN08 SEB number> - IAC Engineering Guidelines
- [6] <SN08 SEB number> - IAW Engineering Guidelines
- [7] <SN08 SEB number> - UAIP Engineering Guidelines
- [8] <SN08 SEB number> - PT-IP Engineering Guidelines
- [9] <SN08 SEB number> - VoATM Engineering Guidelines
- [10] <SN08 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>

IEMS Appendix 1: Northbound OSS Configurations

Depending on customer requirements, a single-source OSS interface can be provided from the IEMS server. As an alternate configuration, to support customer transition, some NE specific OSS interfaces can be provided via SDM in parallel with the interfaces provided by IEMS.

For some existing Nortel Networks ATM customers with no new equipment (such as VTOA-AAL1 solutions with only MG4K, PP15K-MSS and XA-Core), the SDM can provide the complete set external interface to third party OSSs. This configuration is only supported for solutions frozen in the SN06 hardware configuration.

In normal configuration, the IEMS is configured to forward all of its collected faults to the OSS through its aggregated interface. The aggregated interface can supply the feed in NTSTD, SCC2, Syslog or SNMP (v2 or v3) format.

The alternate SDM feed can optionally, in addition to the IEMS feed, provide fault streams equivalent to the SN06 streams for the following devices. Use of the optional SDM feed is not required:

- GWC - via GWC Mgr (SESM) on SSPFS via custlog to SDM
- SAM21 - via SAM21 Mgr on SSFPS via custlog to SDM
- UAS - via UAS Mgr (SESM) on SSPFS via custlog to SDM
- PVG (MG7K, MG15K) - via MDM to passport log streamer to SDM
- Passport 15K MSS - via MDM to passport log streamer to SDM

Note: All of the streams above also go into IEMS for proper IEMS GUI and security operation. OSSs will still connect to IEMS for any of the other equipment in the portfolio. IEMS can block OSS delivery of the alternate feeds northbound if the same OSS is also connected to the SDM to prevent duplication.

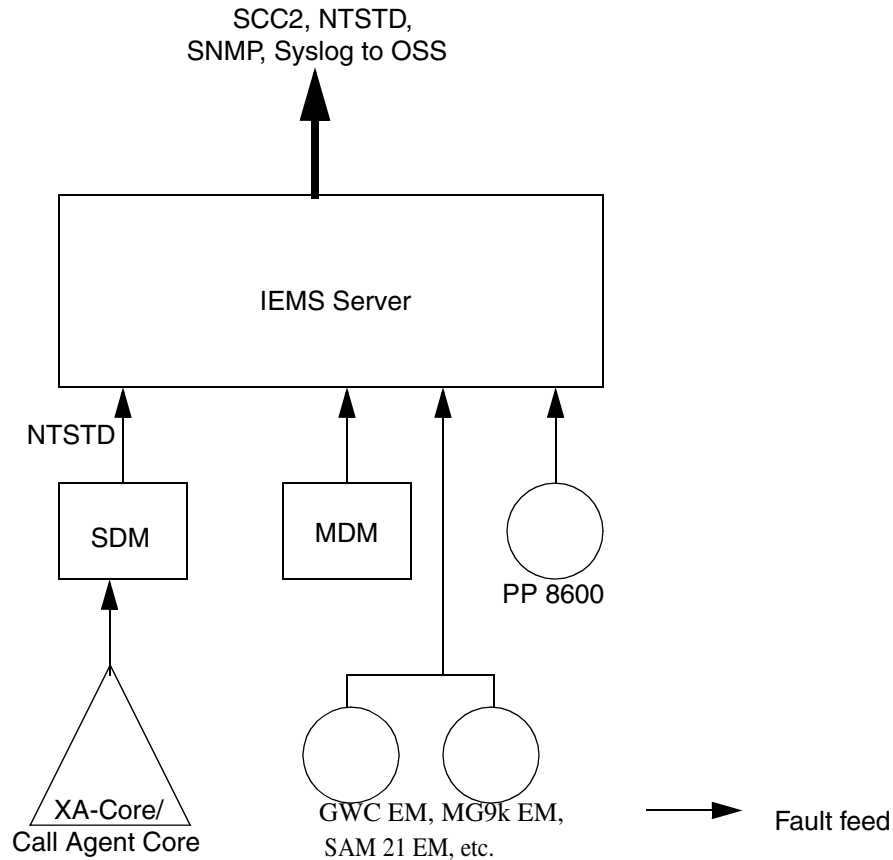
These are in addition to fault streams which can originate from SDM and are supported in all configurations, including TDM only and VTOA-AAL1 solutions:

- CM (XA-Core or Compact) - via SDM
- SDM platform and applications - via SDM

All other fault streams are only supported via IEMS as of SN07. (including but not limited to STORM, CICM, SSPFS Platforms, MS20x0, NGSS)

(SSTrunks), SSLines, RTP MP (BCP 7100), MAS, PP8600, MCS System Manager).

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. 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.

IEMS 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
nlmLogName, nlmLogIndex        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:

```
Ntype=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:

```
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 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 corresponding
    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
```




Chapter 3: (I)SN09FF Features

Product = CS 2000

A00009026--RMGC Security

Functional Description

1: Applicable Solution(s)

IAC, Int'l IAC

1.1 Description

The RMGC Security feature for the SN09 release will enable secure communications between the RMGC (or RMGC/Audio Controller) and the Multimedia Terminal Adapter (MTA).

Background

Small line gateways need to be provisioned with the address of their call processing (CallP) gateway controller (GWC) before they can provide service. Without an RMGC this must be done manually either in a configuration file downloaded to the gateway or directly on the gateway itself. This manual provisioning is difficult to manage and time consuming.

The RMGC serves as a registration agent that provides the gateways with a single location to obtain the fully qualified domain name (FQDN) (e.g., cms/gwc-08.iplab.gwsite-3.ny.net) of their associated CallP GWC. This simplifies the gateway provisioning. All gateways are provided with the RMGC FQDN. Each gateway will contact the RMGC before coming into service and the RMGC will redirect them to their controlling GWC.

Security

Many network deployments require the confidentiality, integrity, and authentication that is provided by Kerberos and IPSec services. When a Call Server 2000 (CS2K) network is deployed with security enabled, the components must all be secured. Prior to SN09 the RMGC (and Audio Controller (AC)/RMGC) combination were not secured.

In order to deploy an RMGC (or AC/RMGC) into a secure network it must be able to respond to requests from the MTA for secure associations (SAs). The method of establishing a SA is to use Kerberos for key management and Internet Protocol Security (IPSec) for secure connections.

The interaction between the MTA and the RMGC is straight-forward. Before coming into service the MTA will send an RSIP message to the RMGC. This RSIP message will initiate a SA negotiation with the RMGC. Kerberos will be used to negotiate an IPSec SA over which the RSIP is sent. The RMGC will respond with an RSIP redirect (over the SA) that contains the FQDN of it's associated CallP GWC. After this exchange the RMGC and MTA have no interaction until the next time that the MTA restarts.

Main Feature Items

The items that are addressed by this feature are:

- IPSec SA Management: The SAs that are used for the RSIP exchange between the RMGC and the MTA must have a short lifetime and must not be renewed. There are a large number of MTAs (maximum of 115,000) and the RMGC cannot maintain an SA database of that size.
- Memory Recovery: Even with the short lived SAs and no SA renewal enabled by this feature, there is still a need to economize the memory usage since the high water mark for the SA storage is higher than that supported by the small lines profile.
- MTA Recovery: In order to maintain quick recovery times for the MTAs, the CallP GWC must be modified slightly. In the case of a large restart event (like a power failure) the CallP GWC and restarting MTA must be able to re-establish contact without waiting for service from the RMGC, when possible.

The RMGC is modified to support multiple pools of SAs specifically to support the AC/RMGC combination profile. This ensures that the AC is able to set up secure connections when the RMGC is under heavy load.

To Provision an RMGC

The provisioning of the RMGC is very similar to that of a CallP GWC in that Kerberos and Connection Policies must be created. The only change is when a connection policy is created there is a limitation for the IPSec SA lifetime. This value must be between an upper and lower limit (10 seconds to 20 seconds). Any other value will not be accepted, the user will only be successful with the provisioning when this rule is conformed to.

1.2 Hardware Requirements or Dependencies

This feature can be deployed on the CEM-750 based GWC card in the SAM21 shelf.

This feature will function correctly on the CEM-905 GWC card as well. This configuration has not been tested but no issues are anticipated.

1.3 Software Requirements or Dependencies

This feature can be deployed in a dedicated (RMGC only) or combination (RMGC and Audio Controller) profile.

1.4 Limitations and restrictions

The user may only provision Kerberos-managed connection policies with a strict limit on the IPSec SA lifetime. If the user tries to create a connection policy with IPSec SA lifetimes that are outside of the range, the connection policy will not be created and the user will be instructed to enter an acceptable lifetime.

1.5 Interactions

The behavior of the SA between the CallP GWC and its associated MTAs will be different as a result of this feature. In a power failure or restart scenario, the SA will be deleted from the CallP GWC in order to accelerate the recovery process. The user may detect this behavior if the number of SAs is being observed regularly.

1.6 Glossary

ACK	Acknowledgement
CallP	Call Processing
CS2K	Call Server 2000 (packet switching fabric)
FQDN	Fully Qualified Domain Name
GW	Gateway
GWC	Gateway Controller
IPSec	Internet Protocol Security
KDC	Key Distribution Center
KMP	Key Management Protocol
KRB	Kerberos
MTA	Multimedia Terminal Adapter
RMGC	Redirecting Media Gateway Controller
RSIP	Restart In Progress (NCS protocol message)
SA	Secure Association
DNS	Domain Name Server

ESP	Encryption Security Payload
SADB	Security Association Database

Product = CS 2000

A00010880--ABI SMU Support

Functional Description

1: Applicable Solution(s)

UA-AAL1

1.1 Description

This activity adds support for the SMU (Subscriber Module Urban) and its subtending RCU (Remote Concentrator Urban) 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 only the IP version MG9K.

The main customer viable changes for this activity will be the ability to provision the EXTDS512 optional field as part of the tuple in table LTCINV for the SMU 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 (part of the Configuration chapter).

No RMM functionality will be supported off an ABI SMU. To support line test on the RCUs, the test configuration will be via an RMM off an ABI LTC/LGC or off an ABI SMA2.

This feature also allows the ABI SMU to be supported in MG9K ESA.

1.2 Hardware Requirements or Dependencies

There are no hardware requirements for this project.

1.3 Software Requirements or Dependencies

The CM changes will be in SN10. Some core software will be submitted in the SN09 time frame to make patchback to SN09 easier. The GWC changes will

be in GC100. The SMU load is currently frozen. The last load was built in the XPM13 time frame out of the XPM13BC context. The XPM portion for the SMU loads will be patched back to XPM13.

1.4 Limitations and restrictions

- LDT PSAP (Line Digit Trunk Public Safety Answering Point) will not be supported off an ABI SMU.
- RMMs will not be supported off an ABI SMU.
- ABI SMU is supported in MG9K ESA but ISDN functionality will not be supported while in ESA. Currently, ISDN is not supported on any ABI XPM while in ESA.
- The SMU supports PPhones by using the D-channels provides by the ISP (ISDN Signalling Processor) and DCH (D-Channel Handler) cards. Because ISDN is not supported in MG9K ESA, the SMU will not support PPhones in MG9K ESA.
- Only the IP version of the MG9K is supported. The ATM version is not supported.

1.5 Interactions

This new code will need to interact with the existing ABI framework for link maintenance, packet connection setup, and MG9K ESA.

1.6 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
ABI	Access Bridging Interface
LDT PSAP	Line Digit Trunk Public Safety Answering Point
RCU	Remote Concentrator Urban
RMM	Remote Maintenance Module
SMU	Subscriber Module Urban

2: Configuration Management for A00010880

2.1 Hardware and Software Requirements

N/A

2.2 Initial Configuration

N/A

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

N/A

2.4 Upgrade Considerations

N/A

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

New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
LTCINV	CHANGED	UNCHANGED

2.5.1 Name: LTCINV

Line Trunk Controller Inventory Table

2.5.1.1 Functional description

Existing Table.

2.5.1.1.1 Usage sequence and implications (CM Only)

Current datafill order remains unchanged.

2.5.1.1.2 Size

Table Size remains unchanged.

2.5.1.1.3 Fields/OIDs

Table LTCINV is changed such that an SMU XPM can now add the optional field, EXTDS512. This optional field was already valid for XPMs which were supported in an ABI configuration (e.g. LTC, LGC, PLGC, SMA2, etc.). This field is used to identify the host gateway, as defined in table GATWYINV.

This change should have no impact on documentation, other than allowing an SMU entry to have field EXTDS512 as was previously allowed for LTC, LGC, PLGC, SMA2 and SMS.

Table 2 Table LTCINV, field OPTATTR description

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTATTR	changed	n/a	EXTDS512	Now valid to enter EXTDS512 as an value in the OPTATTR field for SMU XPM.

2.5.1.1.4 Datafill example

The following example shows sample datafill for table LTCINV with SMU datafilled as an ABI XPM.

```
SMU 0 186 SME 1 18 2 E 26 6X02EE ESU13BB (POTS POTSEX) $ (4 30)
(4 31)(4 32) (4 33) $ (UTR15 ) (MSG6X69 ) (CMR13 CMR10A) $
NORTHAM MX77AA MX77AA 0 UPFWNR04 (EXTDS512 HOST ABI
10) $ 6X40AC N
```

2.5.1.1.5 Table release history update

n/a

2.5.1.1.6 Supplementary information

The changes made to table LTCINV allowing SMU XPMs OPTATTR field to contain the EXTDS512 value are analogous to previous features allowing other XPMs to be supported in an ABI configuration.

2.5.1.1.7 Translation verification and other tools

N/A

2.6 Service Orders (SO) (CM & SESM)

N/A

2.7 Software optionality control (SOC)

N/A

2.8 Element Management

N/A

2.9 User interface changes

N/A

2.10 OSSGate Interface Changes

N/A

2.11 Security

N/A

2.12 Configuration Walkthrough

N/A

Product = CS 2000

A00012109--Session Server¹ Shared Library Replacement (SLR) Patching

Functional Description

1: Applicable Solution(s)

PT-IP

1.1 Description

This activity enables Shared Library Replacement (SLR) patching for the SIP Trunking application on the NGSS.

The Unified Software Management (USM²) Patch manager application running on the Session Server will be used to download and apply/remove/query patches on the Session Server. USM is also responsible

1. Session Server is also referred to as the NGSS in some documentation.

2. The USM functionality is part of the Siren program. USM provides a number of capability; however, the Session Server is only making use of the patch management functionality. Detailed information on USM patch management capabilities can be found in A00009264 - SIREN Installation and Patching.

for pushing Inform Lists from the Session Server to an appropriately configured location.

Figure 1 provides a broad overview of the general patching process for Session Server.

Figure 2 provides a more detailed illustration of the steps involved in the Patch Creation process.

Note: This feature is only responsible for the SLR patching functionality on the SessionServer. Other information provided here related to patch creation, downloading, and general patching, etc...on the Session Server is provided here for informational purposes only and is not a function of this specific feature.

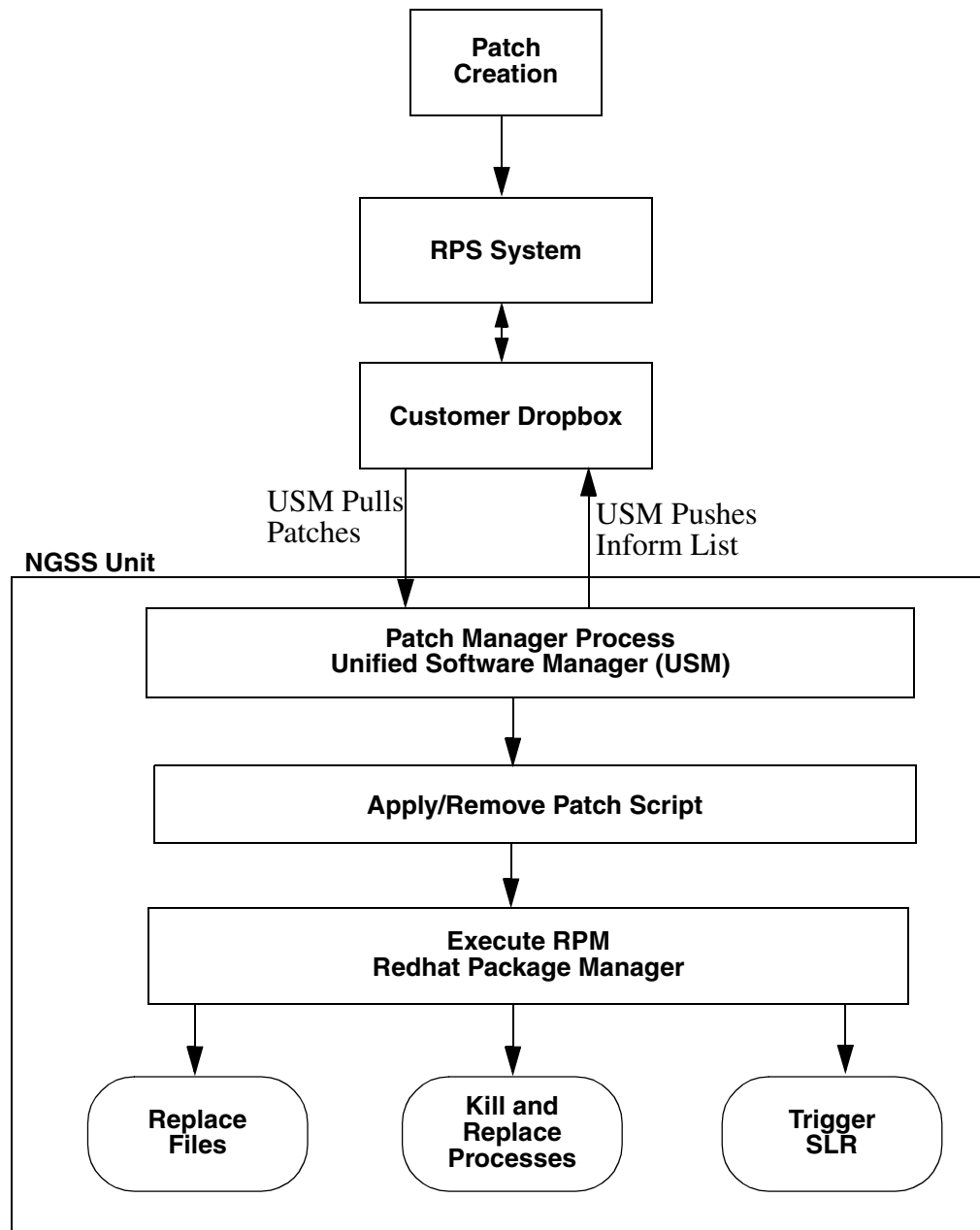
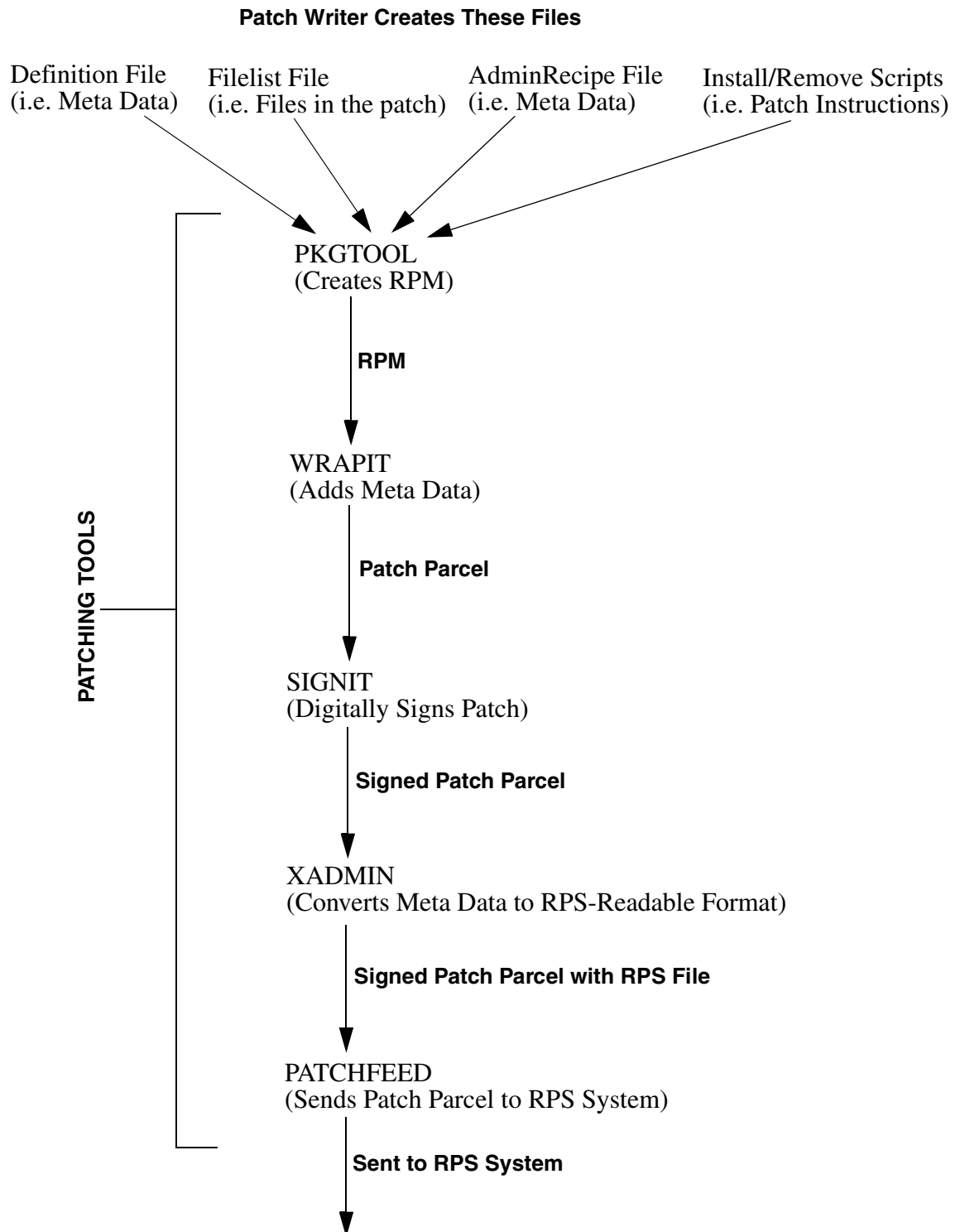
Figure 1 Session Server Patching Process

Figure 2 Session Server Patch Creation Process

During patch creation a few files are called by the patching tool (*pkgtool*) to perform the actual tasks required to apply the patch and to include necessary patch administration information as part of the patch. These files are discussed here briefly.

- Filelist.pkg

The filelist file defines which elements should be included with your software package. For example, this is where the patch writer defines which files are to be replaced on the Session Server, and the directory path of those files in both the Clearcase view and within the Session Server.

- Definition.pkg

The definition file defines information describing the package such as name, version, prerequisites, description. These items are defined via XML Tags. There are over 40 possible tags - although only those designated as pertinent to the particular application need to be filled in. The only tags currently being used out of the Definition.pkg at the time of this writing are the pkg_summary and pkg_description. Output from this file is used to populate fields in the RPM.

- AdminRecipeFile

This file, similar to the definition.pkg file, consists of tags. These tags are used to populate the adminfile that results from a patch build. All of the documented tags can be used in this file and will result in adminfile entries. Again, only those deemed applicable need to be populated.

The pkgtool builds RPM packages based on filelist.pkg and definition.pkg files. The wraptit tool metadata wraps the RPM packages produced by pkgtool. Wraptit will default the metadata fields unless there is an admindata recipe file that overrides the defaults.

- Install, Remove scripts

Next come the install and remove scripts. These files define the action that will occur when the patch is applied or removed.

1.1 Hardware Requirements or Dependencies

Not applicable.

1.2 Software Requirements or Dependencies

Session Sever SLR patching is available in SN09 drop 2.

1.3 Limitations and restrictions

Please note the following:

- The SLR capability provided by this feature only addresses the Session Server Trunk (SST) application.
- This feature does not address SLR patching for NCGL

- This feature does not address SLR patching for SPC.
- Figure 1 on page 771 lists the Session Server components that are SLR patchable (i.e., hitless).

Table 1 Session Server Software Component Patchability

Component	Patching Method	SLR/ Hitless	Comments
HTML files and scripts (e.g. database upgrade scripts)	Simple file replacement	Yes	None.
JSP files used in OAMP interface	File replacement, followed by stopping and restarting Tomcat servlet container	Yes	Web access for the OAMP interface is temporarily inaccessible during the patch application. Users will get an error when trying to access a web page during this window. Call processing is not affected.
Solid database	Kill and replace	Yes	In this case, the version of the Solid database is being changed on the Session Server. The previous version of the database is killed and the new version supplied in the patch is started. During this kill and replace window, web access to the provisioning pages is temporarily unavailable and users will receive an error message if they attempt to access those pages while the patch is being applied. Call processing is not affected since all provisioning data is cached in the application at startup and the database does not need to be accessed during call processing. Note the database watchdog process must be stopped before replacing the Solid database to prevent a swact.
Web Server	Kill and replace	Yes	In this case, the version of the onboard web server is being changed on the Session Server. Access to the OAMP interface through the web is temporarily unavailable during the patch. Call processing is not affected.
Miscellaneous auxiliary processes (e.g. database watchdog process, SCP NCAS server process, SCPLite process, app mtc)	Kill and replace	Yes	Any process that can be stopped, replaced, and restarted in a patch without affecting call processing or causing a swact falls in this category. Currently this category includes the process that monitors the health of the Solid database and the process used for Non-Call Associated Signalling (NCAS) between the DMS core and the Session Server.
SPC Application (Session Policy Controller)	Kill and replace on inactive unit, swact, and then kill and replace on newly inactive unit	No	Patching any part of the SPC application currently requires the entire executable to be replaced. This means that the executable must be stopped before it can be replaced and thus these patches cannot be done in a hitless manner.

Table 1 Session Server Software Component Patchability

Component	Patching Method	SLR/ Hitless	Comments
3rd Party RadVision software used in SIP application	Kill and replace on inactive unit, swact, and then kill and replace on newly inactive unit	No	If a new version of the RadVision stack must be patched in or if specific bug fixes are required in the Radvision code for the SIP application, the patch cannot be done in a hitless manner.
Adding new OM (Operational Measurements) registers or groups to the SIP application	Kill and replace on inactive unit, swact, and then kill and replace on newly inactive unit	No	Note that existing OM registers can be pegged in new places in the SIP application in a hitless patch, but new registers or groups cannot be added without requiring a swact. To lessen the impact of this restriction, this activity will add placeholders for new OM groups and new registers within existing OM groups so that these “spare” OM structures could be used in a hitless patch.
SIP application process (except for RadVision code and new OMs)	SIP shared library replacement (SLR)	Yes	The vast majority of patches fall in this category since it covers all call processing fixes for the SIP application, except for the RadVision code and new OMs. Global data structures within the SIP application cannot be changed with an Session Server SLR patch, but this activity will add placeholders for new data that could be used in a patch. If these placeholders are not sufficient for a particular patch, then a kill and replace with swact patch is required or the functionality could be delivered in an MR.

1.4 Interactions

None known at this time.

1.5 Operational Measurements

This activity adds spare OM registers and spare OM groups for use by the SIPGW application. Refer to the Performance section for details.

1.6 Glossary

Term	Description
NCGL	Nortel Carrier Grade Linux
RPM	Redhat Package Manager
SLR	Shared Library Replacement
SPC	Session Policy Control.
USM	Unified Software Management

2: Performance Management for A00012109

2.1 Performance management strategy

Unchanged

2.2 Performance management tools and utilities

Unchanged

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

This activity adds five spare registers to each of the NGSS SIPGW OM groups listed below:

- SIPGW_CALLP
- SIPGW_SERVICES
- SIPGW_MISC
- SIPGW_TLS
- SIPGW_OVERLOAD
- SIPGW_OOB
- SIPGW_NCAS

In addition, the following three spare OM groups are added by this feature:

- SIPGW_SPARE1
- SIPGW_SPARE2
- SIPGW_SPARE3

The spare OM registers and spare OM groups introduced by this activity are reserved for future use.

2.3.1 PM, OM, and stats format

2.3.1.1 SIPGW_CALLP spare OMs

The following table lists the spare registers added to the SIPGW_CALLP OM group.

Table 1 OM Group: SIPGW_CALLP

Register Name	Description
SIPGW_CALLP_SPARE_1	reserved for future use
SIPGW_CALLP_SPARE_2	reserved for future use
SIPGW_CALLP_SPARE_3	reserved for future use

Register Name	Description
SIPGW_CALLP_SPARE_4	reserved for future use
SIPGW_CALLP_SPARE_5	reserved for future use

2.3.1.2 SIPGW_SERVICES spare OMs

The following table lists the spare registers added to the SIPGW_SERVICES OM group.

Table 2 OM Group: SIPGW_SERVICES

Register Name	Description
SIPGW_SERVICES_SPARE_1	reserved for future use
SIPGW_SERVICES_SPARE_2	reserved for future use
SIPGW_SERVICES_SPARE_3	reserved for future use
SIPGW_SERVICES_SPARE_4	reserved for future use
SIPGW_SERVICES_SPARE_5	reserved for future use

2.3.1.3 SIPGW_MISC spare OMs

The following table lists the spare registers added to the SIPGW_MISC OM group.

Table 3 OM Group: SIPGW_MISC

Register Name	Description
SIPGW_MISC_SPARE_1	reserved for future use
SIPGW_MISC_SPARE_2	reserved for future use
SIPGW_MISC_SPARE_3	reserved for future use
SIPGW_MISC_SPARE_4	reserved for future use
SIPGW_MISC_SPARE_5	reserved for future use

2.3.1.4 SIPGW_TLS spare OMs

The following table lists the spare registers added to the SIPGW_TLS OM group.

Table 4 OM Group: SIPGW_TLS

Register Name	Description
SIPGW_TLS_SPARE_1	reserved for future use
SIPGW_TLS_SPARE_2	reserved for future use
SIPGW_TLS_SPARE_3	reserved for future use
SIPGW_TLS_SPARE_4	reserved for future use
SIPGW_TLS_SPARE_5	reserved for future use

2.3.1.5 SIPGW_OVERLOAD spare OMs

The following table lists the spare registers added to the SIPGW_OVERLOAD OM group.

Table 5 OM Group: SIPGW_OVERLOAD

Register Name	Description
SIPGW_OVERLOAD_SPARE_1	reserved for future use
SIPGW_OVERLOAD_SPARE_2	reserved for future use
SIPGW_OVERLOAD_SPARE_3	reserved for future use
SIPGW_OVERLOAD_SPARE_4	reserved for future use
SIPGW_OVERLOAD_SPARE_5	reserved for future use

2.3.1.6 SIPGW_OOB spare OMs

The following table lists the spare registers added to the SIPGW_OOB OM group.

Table 6 OM Group: SIPGW_OOB

Register Name	Description
SIPGW_OOB_SPARE_1	reserved for future use
SIPGW_OOB_SPARE_2	reserved for future use
SIPGW_OOB_SPARE_3	reserved for future use
SIPGW_OOB_SPARE_4	reserved for future use
SIPGW_OOB_SPARE_5	reserved for future use

2.3.1.7 SIPGW_NCAS spare OMs

The following table lists the spare registers added to the SIPGW_NCAS OM group.

Table 7 OM Group: SIPGW_NCAS

Register Name	Description
SIPGW_NCAS_SPARE_1	reserved for future use
SIPGW_NCAS_SPARE_2	reserved for future use
SIPGW_NCAS_SPARE_3	reserved for future use
SIPGW_NCAS_SPARE_4	reserved for future use
SIPGW_NCAS_SPARE_5	reserved for future use

2.3.1.8 SIPGW_SPARE1 spare OMs

The following table lists the registers added to the new SIPGW_SPARE1 OM group.

Table 8 OM Group: SIPGW_SPARE1

Register Name	Description
SIPGW_SPARE1_REG_1	reserved for future use
SIPGW_SPARE1_REG_2	reserved for future use
SIPGW_SPARE1_REG_3	reserved for future use
SIPGW_SPARE1_REG_4	reserved for future use
SIPGW_SPARE1_REG_5	reserved for future use
SIPGW_SPARE1_REG_6	reserved for future use
SIPGW_SPARE1_REG_7	reserved for future use
SIPGW_SPARE1_REG_8	reserved for future use
SIPGW_SPARE1_REG_9	reserved for future use
SIPGW_SPARE1_REG_10	reserved for future use

2.3.1.9 SIPGW_SPARE2 spare OMs

The following table lists the registers added to the new SIPGW_SPARE2 OM group.

Table 9 OM Group: SIPGW_SPARE2

Register Name	Description
SIPGW_SPARE2_REG_1	reserved for future use
SIPGW_SPARE2_REG_2	reserved for future use
SIPGW_SPARE2_REG_3	reserved for future use
SIPGW_SPARE2_REG_4	reserved for future use
SIPGW_SPARE2_REG_5	reserved for future use
SIPGW_SPARE2_REG_6	reserved for future use
SIPGW_SPARE2_REG_7	reserved for future use
SIPGW_SPARE2_REG_8	reserved for future use
SIPGW_SPARE2_REG_9	reserved for future use
SIPGW_SPARE2_REG_10	reserved for future use

2.3.1.10 SIPGW_SPARE3 spare OMs

The following table lists the registers added to the new SIPGW_SPARE3 OM group.

Table 10 OM Group: SIPGW_SPARE3

Register Name	Description
SIPGW_SPARE3_REG_1	reserved for future use
SIPGW_SPARE3_REG_2	reserved for future use

Register Name	Description
SIPGW_SPARE3_REG_3	reserved for future use
SIPGW_SPARE3_REG_4	reserved for future use
SIPGW_SPARE3_REG_5	reserved for future use
SIPGW_SPARE3_REG_6	reserved for future use
SIPGW_SPARE3_REG_7	reserved for future use
SIPGW_SPARE3_REG_8	reserved for future use
SIPGW_SPARE3_REG_9	reserved for future use
SIPGW_SPARE3_REG_10	reserved for future use

2.3.2 Performance File (CSV, SSV, XML) Format

Unchanged

2.3.3 OM Group template (applies only to DMS)

N/A

Product = CS 2000

A00012349 -- U3WC Support for SIP Lines

1: Applicable solution(s)

CHS

1.1 Description

This feature expands the existing Three Way Call (3WC) and Usage Sensitive Three Way Call (U3WC) services to IBN and RES type SIP Lines.

The 3WC/U3WC service provides the activation/deactivation of the Three Way Calling on the line. In SIP Lines case, actual conferencing service is provided by edge device like Optical Network Terminator (ONT) or by the CS2K Session Server, on an ad-hoc basis, as in the case of a PC Client. To the CS2K Core, the calls appear as separate ones.

This feature supports both possible methods to invoke U3WC from a UA (User Agent), that is, via the access code or via flash access (same as normal 3WC, no access code).

When a UA, in a stable call state, invokes this feature, it triggers the core to first check for the 3WC or U3WC option provisioning, for that SIP line. If any of these options are provisioned correctly, the second (consultation) leg

origination attempt is allowed to proceed. Otherwise, the origination attempt is denied and the caller is sent to treatment for the add-on leg. If the second leg call is successful, the UA can flash again to conference the three parties involved. This activity will not pre-empt the other features from allowing the second leg call origination.

1.1.1 Billing

Each time DPL U3WC is invoked, a billing record based on Structure Code 00001 with Call Type of 048 and Service Feature of 018 is created. For DPL, the conferencing is done at the client or on ad-hoc basis at the CS2K SS and hence no conference resources are used in the core. Also, the conference notification from User Agent is not being implemented as part of this activity. Because of this, the DPL U3WC billing record will be made always consistent with the TOTAL_DURATION setting of the U3WC_ELAPSED_TIME, irrespective of this parm being set to any other values. Also the billing record will be generated for every successful U3WC consult call termination, regardless of whether a conference is ever established.

The module code 260 will be appended to the DPL U3WC billing records to indicate that they pertain to SIP lines, when the RECORD_MC260 tuple is set to ON in table AMAOPTS. An example DPL U3WC billing record is shown below.

Figure 1 Example call code 048 for U3WC billing

```
*HEX ID:AA STRUCTURE CODE:40001C CALL CODE:048C SENSOR TYPE:036C
SENSOR ID:0619351C REC OFFICE TYPE:036C REC OFFICE ID:0619351C
DATE:50929C TIMING IND:00000C STUDY IND:0000000C CLD PTY OFF-HK:0C
SERVICE OBSERVED:0C OPER ACTION:0C SERVICE FEATURE:018C ORIG
NPA:613C ORIG NUMBER:6215674C OVERSEAS IND:0C TERM NPA:00613C TERM
NUMBER:6216004C CONNECT TIME:1408247C ELAPSED TIME:000000467C
MODULE CODE:260C COMPONENT ROLE:101C IP SERVICE PROTOCOL:001C
MODULE CODE:260C COMPONENT ROLE:201C IP SERVICE PROTOCOL:001C
MODULE CODE:000C
```

1.1.2 Operational Measurements (OMs)

Currently in the CS2K core, for non-DPL case, the U3WC OM registers are being pegged for the User Three Way Call service. This OM has the U3WCATT (U3WC Attempts), U3WCCONS (U3WC consultations) and the U3WCCONF (U3WC conferencing) registers that are pegged.

For DPL case, the conferencing service is provided by the UA or the CS2K SS and the conference notification from User Agent or CS2K SS is not available to the core. Hence for DPL, it is not possible to peg the U3WCCONF register. If the other two registers are pegged, it could lead to an imbalance over time.

For this reason, none of the U3WC OM registers will be pegged for the DPL case.

1.2 Hardware Requirements or Dependencies

Not Applicable

1.3 Software Requirements or Dependencies

Not Applicable

1.4 Limitations and restrictions

The following are the restrictions and limitations of this service:

- The conferencing capability shall be enabled in the clients (for UAs like ONTs) or ad-hoc conferencing shall be provided by the CS2K SS (for UAs like PC clients).
- For DPL case, none of the U3WC OM registers will be pegged. Please refer to the [“Operational Measurements \(OMs\)”](#) section above.
- This activity supports consult leg originations with or without the VSCs. However, for originations with only the U3WC VSCs, then followed by CDN digits after second dial tone, the PMA/AMS setup needs to be configured, so that digit collection can take place.
- Client based refer or redirect requests will not be screened or blocked by 3WC/U3WC options.
- The 3WC option must be explicitly datafilled for SIP lines, for IBN type and when U3WC is not applicable, for the RES type also, in order to establish additional sessions, once the first session has been answered.
- Conference Notification from User Agent (ONT or PC Client or a SIP Phone) is not planned to be implemented as part of this activity. Hence the DPL U3WC billing record will be always consistent with the TOTAL_DURATION setting of the U3WC_ELAPSED_TIME, irrespective of this parm being set to any other values. Also the billing record will be generated for every successful U3WC consult call termination, regardless of whether a conference is ever established. Module code 260 will be appended to the DPL U3WC billing records to indicate that they pertain to SIP lines, when the RECORD_MC260 tuple is set to ON in table AMAOPTS.

1.5 Interactions

- U3WC option is not compatible with the CXR (Call Transfer) option (refer to the U3WC related FN sections of actids AQ1302). U3WC if active on a RES line, will disappear (become inactive), once the CXR option is assigned to that line.

- For 3WC option, if the client needs to transfer the call, will have to invoke REFER before exiting. While 3WC is active, call transfer screening will occur when the controller gets out of the conference. At that point, the CXR option provisioning will determine if the call between the remaining 2 parties will survive or not.
- 911 calls on consult leg are treated the same way as any other calls and don't have any preferential processing.

1.6 Glossary

Term	Description
3WC	Three Way Call
CS2K	Communication Server 2000
CS2K SS	Communication Server 2000 - Session Server
DPL	Direct Packet Lines
ONT	Optical Network Terminator
PC	Personal Computer
SIP	Session Initiation Protocol
U3WC	Usage Sensitive Three Way Call
UA	User Agent

Product = CS 2000

A00012478--Compact Call Agent: Geo Support for GigE ***Functional Description***

1: Applicable Solution(s) (see note below)

1.1 Description

Note: The GigE link is applicable only to the CS2100 for the enterprise market.

This feature supports GigE interface for sparing or synchronizing data between the two MCG905-270 CCAs for both Geo and non-Geo configurations.

This feature enables synchronization of data between two Compact Call Agent (CCA) blades over a Gigabit Ethernet link. The current design uses Fiber Channel (FC) for keeping data synchronized. This feature will provide an additional option of synchronization over Gigabit Ethernet (GigE) depending on the customers' needs.

GigE is an ethernet technology that provides an alternative for high-speed data transmission (1 gigabit per second) to achieve memory synchronization between active and inactive CCA. The principal benefits of GigE are:

- It provides a low cost, reliable and fast data transmission solution. GigE is based on the Ethernet protocol and Ethernet standards are the most deployed network backbone solution.
- It is scalable and upgradable. It may be possible to upgrade data synchronization over GigE to 10 GigE in the future.

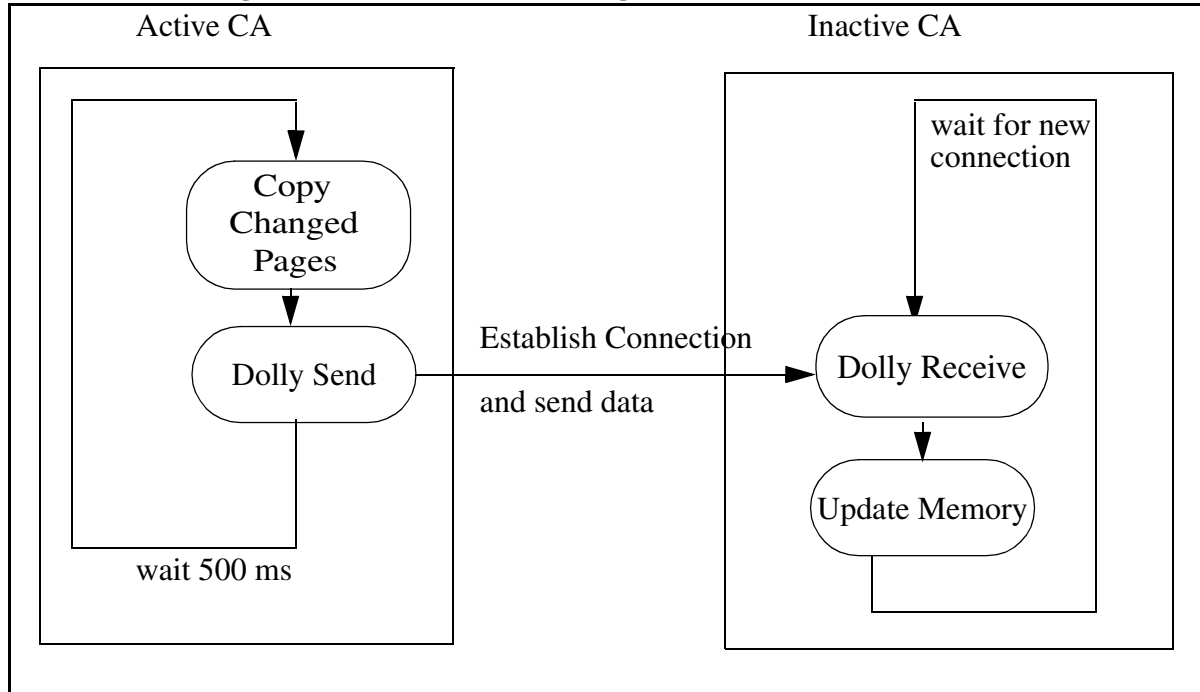
Other benefits include:

- A GigE link has a lower cost to provision and maintain than a Fiber Channel link for Geo applications. For customers who do not own optical transport between geo sites, GigE has a lower lease cost than Fiber Channel.
- It is expected that a GigE link for Geo applications will allow greater distances between sites to be supported.

The desired behavior of this feature is to provide an ethernet transport option between two MCPN905-based CCA cards. The MCPN765-based CCA cards do not support the GigE ports and hence will continue to use Fiber Channel.

This feature will provide high synchronization bandwidth for the Dolly process. Dolly is a linux process running on both the active and inactive CCA. The instance of Dolly running on the active CCA is responsible for sending the "dirty" or "changed" memory pages to the inactive CCA. The instance of Dolly running on the inactive CCA is responsible for receiving those changed pages and passing them to PEEL to update memory [Figure 1].

All changed pages are collected and copied into a buffer on the active CCA every 500 milliseconds. The Dolly process running on the active CCA will establish connection over the GigE link with the Dolly process running on the inactive CCA. Once the connection is established, data transmission will start. Any packet loss will be retransmitted to ensure that the inactive does not have a corrupt image due to loss of information. Upon completion of data transmission, the inactive CCA will copy the received data into memory and wait for the next new connection.

Figure 1 Functional Behavior Diagram

- This feature will provide an in-service method to change the FC connection to GigE (and vice-versa) for both Geo and non-Geo configurations with MCPN905-based CCA.
- Support to select either FC or GigE will be provided by the SAM21 Element Manager GUI. The work is documented in feat.A00012581.
 - The EM GUI will have a separate Sparing Link Type tab to allow selection of either Fiber Channel or Gigabit Ethernet link for sparing or data synchronization between the CCA cards.
 - Once the link selection has been made through the EM GUI, that information will be written in the “*extrainfo*” file on the configured Bootp server.
- The MCPN905-based software load will have support for both FC and GigE links between the CCA cards and it will be up to the customer to choose either of the two links (FC, only if they have FC PMC) but not both at the same time.
- This feature shall continue to support the FC links for MCPN765-based Compact Call Agent cards for both Geo and non-Geo configurations.
- For both Geo and non-Geo configurations, a new configuration path supported for upgrade will be

- from MCPN905-based CCA with FiberChannel set up as synchronization link to MCPN905-based CCA with GigE set up as synchronization link; and vice-versa

1.1.1 Reference Configuration

The Gigabit Ethernet port of the PIM11 on the PrPMC815 card will be used for synchronizing data between the Call Agent cards.

The Fiber Channel connection will remain configurable as it is today, whenever the Fiber Channel hardware and driver are present.

1.1.1.1 Non-Geographic Survivability Mode Configuration

On a standard CS2000-Compact with MCPN905 (NTRX51HZ) CCA cards synchronization of data between the CCA units will be done over a direct and dedicated Gigabit Ethernet link (1000BaseT connection). This will be a point-to-point connection. An example is shown in Figure 2.

1.1.1.2 Geographic Survivability Mode Configuration

- On a Geographically Survivable CS2000-Compact with MCPN905 (NTRX51HZ) CCA cards synchronization of data between the two CCA units will be done via the CS-LAN router. An example is shown in Figure 2, using ERS 8600.
- Configuration of CCA interactions with the local CS-LAN router in each site will be configured on each CCA blade using the setgeoconfig script tool as it is done today. No changes are being made to that procedure.
- The internal architecture of the CS-LAN router should enable building secure VLANs. When port-based VLANs are configured, each VLAN is completely separated from another (broadcast domain). Its unique hardware architecture allows each packet to be analyzed independently of the preceding one. This mode guarantees complete traffic isolation by allowing discarding of untagged traffic on tagged port or tagged traffic on untagged ports. Even if a tagged port receives traffic with a VLAN Id which identifies a VLAN from another customer configured on the switch, this traffic is completely discarded.

In other words - any traffic within this type of VLAN cannot exit the VLAN, nor can traffic from another VLAN be sent to a port within this VLAN when the IP default gateway is not set. This enables us to use an IP address for the sparing or synchronization of data on the MCPN905-based CCA GigE card without having to advertise it. Traffic will be confined between both CCA cards whether connected directly via a point-to-point fibre or via the CS-LAN router.

- The CS-LAN router must also support JUMBO frames. For example, the 8608SX(E), 8608GT(E), 8608GB(E), 10GE I/O modules and the 2 Gig ports of the 8632TXE board have the ability to forward 9600 (MTU) jumbo frames.

- The CS-LAN router may require an additional module (if it is not already equipped) with 1000BaseT GBIC support for Gigabit Ethernet transmission. For example, the ERS 8600 CS-LAN will require an additional 8608 module equipped with a 1000BaseT GBIC to support GigE. An example of the configuration procedure is shown in Figure 3.
- For configuring the GigE link on any CS-LAN router the engineering guidelines must be followed.
- Please refer to Appendix A for a step by step example in OTT3 about how to configure ERS 8600 to enable sparing over GigE in Geographic Survivable lab.

Figure 2 An example of data synchronization or sparing over GigE on MCPN905 CCA

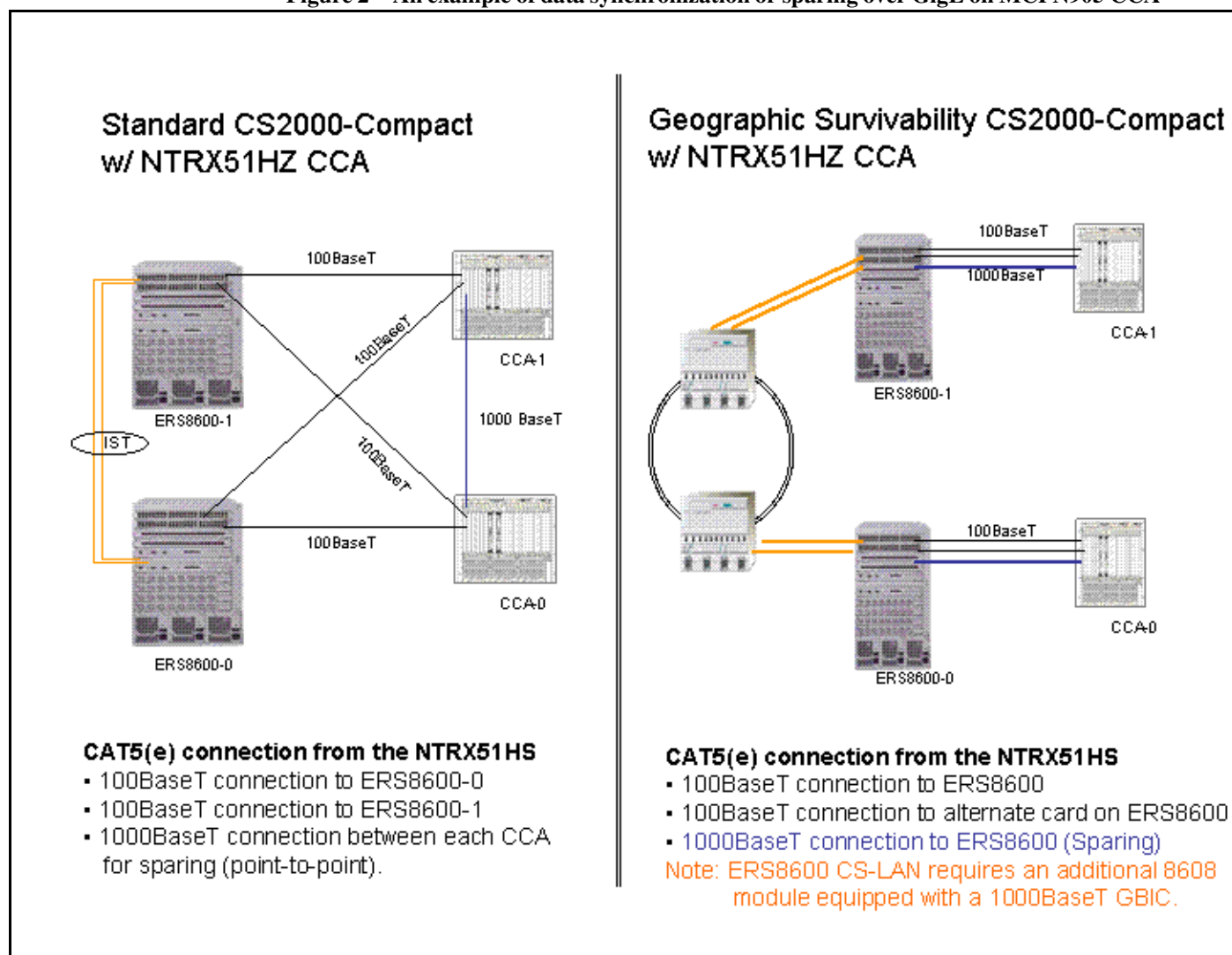


Figure 3 An Example of CSLAN configuration for sparing over GigE on MCPN905 CCA using ERS 8600 router

ERS 8600 CS-LAN configuration for GigE sparing on MCPN905 CCA NTRX51HZ

EXAMPLE

vlan 905 create byport 1 name "CCA-Sparing"

vlan 905 add-mlt 3

← This is the MLT ID for the IST across both CS-LAN ERS8600.

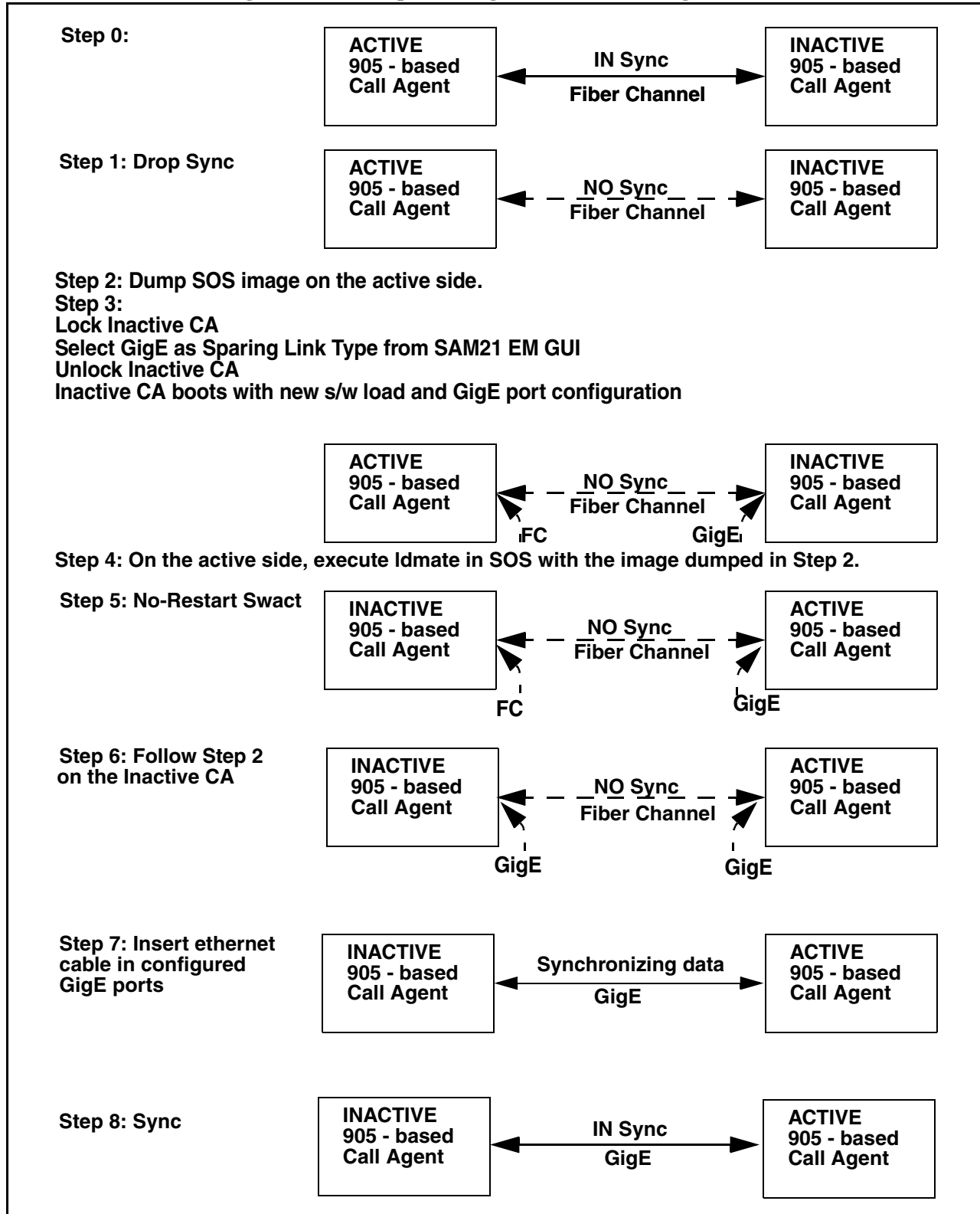
vlan 905 ports remove x/y member portmember

← Remove any ports in this subnet.

vlan 905 ports add 1/1,2/1, a/b member portmember

← Add the two ports from MLT 3, and add the port a/b where the sparing link is connected.

Figure 4 An example of a migration from FC to GigE

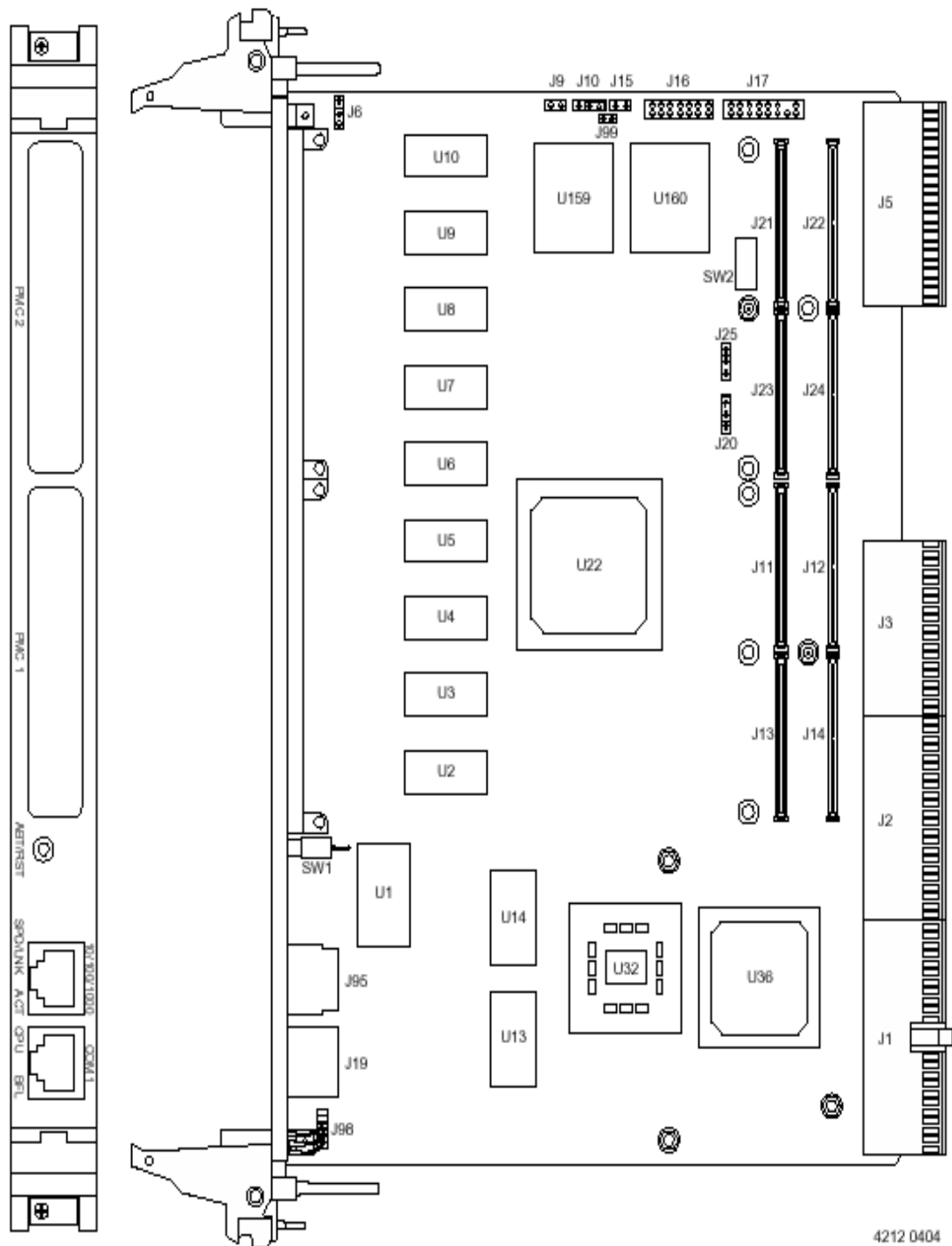


1.1.2 Upgrade scenario

The following upgrade scenarios are for both non-Geo and Geo survivable CS2000-CCA.

1.1.2.1 Hardware and Software upgrade

- In order to use Gigabit Ethernet for data synchronization or sparing, the two CCA blades must be MCPN905-based.
- The two MCPN905-based CCA blades must be equipped with a software load that supports data synchronization over Gigabit Ethernet link.
- The 1000BaseT cable must be inserted in the configured GigE ports on the PrPMC815 before attempting to bring the blades in synchronization.
- For geo configurations, a CS-LAN router is required that supports Gigabit Ethernet.
- It requires specific hardware configuration in order to enable the GigE port on the PrPMC815. On the 905 itself, PMC1 is at the middle of the board (connectors J11 to J14). PMC2 at the top (connectors J21 to J24). On the transition module the PIM for PMC1 is in the middle of the transition module J11. PIM2 is at the top J24.
For 3pc-905 blade, if both PrPMC815 and FC PMC are present, PrPMC815 must be installed in PMC2 which is at the top of the board and FC PMC must be installed in PMC1 which is in the middle of the board. The rear transition module should be aligned with the position of PrPMC815 so it must be installed in PIM2 which is at the top of the board. If only PrPMC815 is present, PrPMC815 and rear transition module must be installed at the same position as described above.



1.1.2.2 System Impact of Failure Scenarios

In case, there is a fault in the 1000BaseT cable, there will no sparing of data over GigE link. This can cause a potential outage since the switch will be in simplex.

1.1.2.3 Recovery Behavior

If there a problem in the upgrade scenario above, the upgrade can be aborted and the system reverted back to the original configuration.

For example, if a failure happens during an upgrade from a MCPN905-based CCA with synchronization over Fiber Channel to an MCPN905-based CCA with synchronization over GigE, the failure can be corrected by reverting back to using Fiber Channel for synchronization on the MCPN905-based CCA by selecting Fiber Channel as the Sparing Link Type from the SAM21 EM GUI, since the new software load will support FC as well.

1.2 Hardware Requirements or Dependencies

1. For both Geo and non-Geo configurations, a 1000BaseT Gigabit Ethernet cable is required.
2. For Geo-Survivable configurations, the CS-LAN router must be equipped to support Gigabit Ethernet transmissions. For example, the ERS8600 CS-LAN will require an additional 8608 module equipped with a 1000BaseT GBIC.

1.3 Software Requirements or Dependencies

1. SN09FF load (or higher) for Call Agent
2. SN09FF load (or higher) for SAM21 Element Manager GUI

1.4 Limitations and restrictions

- To minimize loss of calls during a migration from FC to GigE, a no-restart swact may be used only
 - when the CPU utilization is less than 40% and the number of changed pages count is less than 2200,
 - on the same CCA software load on both CCA blades.

The CPU Utilization can be seen from the tool CAPCI. The number of changed pages can be calculated by checking the SLUTIL field in CAPCI. SLUTIL represents the number of changed pages divided by the maximum sparing link (or synchronization) bandwidth. The maximum sparing link bandwidth is usually set to 6000 pages unless specified otherwise.

$$\text{SLUTIL} = \frac{\text{number of changed pages}}{6000} \times 100$$

1.5 Interactions

Feature A00012581 is directly related to this feature. The SAM21 EM GUI which provides the customer to input the Sparing Link Type is covered under feature A00012581.

1.6 Customer documentation impacts

This feature affects some logs, alarms, and element management as follows:

1. For the custom log changes all the appearances of "FC" are renamed to "SL", i.e.

```
Dec 5 15:35:17 172.16.16.70 logman: CCA335 MAJOR FLT Link
Connectivity ^M Unit Number : 1, ACTIVE ^M Description : Link0:
SYSB, mateCon: BAD, netCon: BAD; Link0 Mode: FULL_DUPLEX;
Link1: INSV, mateCon: OK, netCon: OK; Link1 Mode: FULL_DUPLEX;
BLink: INSV, mateCon: OK; SL: INSV;
```

2. Same for the alarm changes, all the appearances of "FC" are renamed to "SL", i.e.

```
Alarm Severity Description
2 CAMtc LnkCon major Link0: INSV, mateCon: OK, netCon: OK;
3 Sys Link0 Mode: FULL_DUPLEX;
4 Con Link1: INSV, mateCon: OK, netCon: OK;
5 Appl Link1 Mode: FULL_DUPLEX;
6 BLink: SYSB, mateCon: BAD;
7 SL: SYSB;
```

3. In CCAMTC, the "FC" for the carrier sparing state is replaced by "SL", i.e.

```
CallAgent SYS CON APPL Unit: 1
C MisM NTP . simplx
M
CoreMtc Jam: Link0: Link1: BLnk: SL: Appl:
0 Quit Unit0 Inact no . Act . Inact . . nosync /waiting
2 CAMtc Unit1 Act no . Act . Inact . . nosync .
```

4. There is a new query util "QuerySL" in CCAMTC slot 16 all mtc levels to query the type is sparing link, i.e.

```
CallAgent SYS CON APPL Unit: 1
C MisM NTP . simplx
M
CoreMtc Jam: Link0: Link1: BLnk: SL: Appl:
0 Quit Unit0 Inact no . Act . Inact . . nosync /waiting
2 CAMtc Unit1 Act no . Act . Inact . . nosync .
3 Sys
4 Con
5 Appl
```

```
6
7
8
9
10
11
12
13 LogQuery
14 Alarm
15 QueryIP
16 QuerySL
17 Help
18 Refresh Sparing Link (SL) Type: Gigabit Ethernet
root
```

In SAM21 EM, there is a new tab window for the 905 card for the customer to choose which sparing link to use, "Fiber Channel" or "Gigabit Ethernet".

1.7 Appendix A

ERS 8600 Configure Example in OTT3 to Enable Sparing Over GigE in Geographic Survivable Lab

```
OTT3 CSLAN P8600-1-B0:5# config vlan 12
OTT3 CSLAN P8600-1-B0:5/config/vlan/12# info
```

```
Sub-Context: create fdb-entry fdb-filter fdb-static ip ports srcmac
static-mcast
```

```
mac
```

```
Current Context:
```

```
Vlan 12 is not created
```

```
OTT3 CSLAN P8600-1-B0:5/config/vlan/12# create byport 1 name "CA_GigE"
OTT3 CSLAN P8600-1-B0:5/config/vlan/12# info
```

```
Sub-Context: create fdb-entry fdb-filter fdb-static ip ports srcmac
static-mcast
```

```
mac
```

```
Current Context:
```

```
        action : N/A
        add-mlt :
        addDsapSsap :
        removedSsapSsap : N/A
        agetime : N/A
        delete : N/A
        qoslevel : 1
        name : CA_GigE
```

```
OTT3 CSLAN P8600-1-B0:5/config/vlan/12# ports
OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ports# info
```

Sub-Context:

Current Context:

```
add:
    portnumber -
    active member -
    staticmember -
    notallowtojoin -
remove: N/A
```

```
OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ports# config ethernet 4/1
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1# info
```

Sub-Context: eapol ip lacp limit-fdb-learning mroute-limit multimedia
pcap remote

e-mirroring smlt stg unknown-mac-discard vlacp

Current Context:

Port 4/1 :

```
        lock : false
        block-traffic : false
        name :
        auto-negotiate : false
```

```
        duplex : full
    enable-diffserv : false
    access-diffserv : false
        qos-level : 1
        routing : enable
    unknown-mac-discard : disable
        high-secure : false
        default-vlan-id : 0
    untag-port-default-vlan : disable
    tagged-frames-discard : disable
        perform-tagging : disable
        svlan-porttype : normal
    untagged-frames-discard : disable
        loop-detect : disable        action port-down
            state : up
            linktrap : enable
    multicast rate-limit : disabled
    broadcast rate-limit : disabled
        sffd : disabled
        cp-limit : enabled multicast-limit 15000
broadcast-limit 10000
```

```
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1# name "CA_Cu_GigE"
```

```
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1# config vlan 12 ports
```

```
OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ports# add 4/1 member
portmember
```

```
OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ports# info
```

Sub-Context:

Current Context:

add :

portmember - 4/1

activemember - 4/1

```
staticmember -
notallowtojoin -
remove : N/A
```

```
OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ports# config ethernet 4/6
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/6# info
```

Sub-Context:

Current Context:

Port 4/6 :

```
lock : false
block-traffic : false
name :
auto-negotiate : false
duplex : full
enable-diffserv : false
access-diffserv : false
qos-level : 1
routing : enable
unknown-mac-discard : disable
high-secure : false
default-vlan-id : 12
untag-port-default-vlan : disable
tagged-frames-discard : disable
perform-tagging : disable
svlan-porttype : normal
untagged-frames-discard : disable
loop-detect : disable      action port-down
state : up
linktrap : enable
multicast rate-limit : disabled
broadcast rate-limit : disabled

sffd : disabled
```

```
cp-limit : enabled multicast-limit 15000
broadcast-limit 10000
```

```
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/6# name "CA_Sx_GigE"
OTT3 CSLAN P8600-0-B0:5/config/ethernet/4/6# auto-negotiate enable
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/6# config vlan 12 ports
OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ports# add 4/6 member
portmember
OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ports# info
```

Sub-Context:

Current Context:

```
add :
    portmember - 4/1,4/6
    activemember - 4/1,4/6
    staticmember -
    notallowtojoin -
remove : N/A
```

```
OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ports# .
OTT3 CSLAN P8600-1-B0:5/config/vlan/12# ip
OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ip# rip
OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ip/rip# info
```

Sub-Context:

Current Context:

```
rip : disable
advertise-when-down : disable
auto-aggregation : disable
cost : 1
default-listen : disable
default-supply : disable
holddown : 120
```



```
in-policy : N/A
out-policy : N/A
timeout : 180
triggered-update : disable
listen : enable
manualtrigger : N/A
poison : disable
supply : enable
```

```
OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ip/rip# .
OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ip# ospf
OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ip/ospf# info
```

Sub-Context:

Current Context:

```
advertise-when-down : disable
ospf : disable
interface-type : broadcast
hello-interval : 10
dead-interval : 40
poll-interval : 120
priority : 1
metric : 0
authentication-type : none
authentication-key :
area : 0.0.0.0
```

```
OTT3 CSLAN P8600-1-B0:5/config/vlan/12/ip/ospf# config ethernet 4/1 ip
rip
```

```
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1/ip/rip# info
```

Sub-Context:

Current Context:

Port 4/1 :

```
rip : disable
advertise-when-down : disable
auto-aggregation : disable
cost : 1
default-listen : disable
default-supply : disable
holddown : 120
in-policy : N/A
out-policy : N/A
timeout : 180
triggered-update : disable
listen : enable
manualtrigger : N/A
poison : disable
supply : enable
```

OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1/ip/rip# .

OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1/ip# ospf

OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1/ip/ospf# info

Sub-Context:

Current Context:

Port 4/1 :

```
advertise-when-down : disable
ospf : disable
interface-type : broadcast
hello-interval : 10
dead-interval : 40
poll-interval : 120
priority : 1
metric : 0
authentication-type : none
```

```
authentication-key :  
    area : 0.0.0.0
```

```
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1/ip/ospf# .  
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1# stg 1  
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1/stg/1# info
```

Sub-Context:

Current Context:

Port 4/1 :

```
change-detection : enable  
faststart : disable  
pathcost : 100  
priority : 128  
stp : disable
```

```
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1/stg/1# .  
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1/ip# arp  
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1/ip/arp-response# info
```

Sub-Context:

Current Context:

Port 4/6 :

```
arp-response : enable
```

```
OTT3 CSLAN P8600-1-B0:5/config/ethernet/4/1/ip/arp-response# top  
OTT3 CSLAN P8600-0-A0:5# config sys  
OTT3 CSLAN P8600-0-A0:5/config/sys# set ?
```

Sub-Context: action eapol flags msg-control record-reservation snmp
ssh

Current Context:

```
clock-sync-time <minutes>
contact <contact>
ecn-compatibility <enable|disable>
global-filter <enable|disable>
info
location <location>
mgmt-virtual-ip <ipaddr/mask>
mroute-stream-limit <enable|disable>
mtu <bytes>
name <prompt>
portlock <on|off>
sendAuthenticationTrap <true|false>
smlt-on-single-cp <enable|disable> [timer <value>]
topology <on|off>
udp-checksum <enable|disable>
udpsrc-by-vip <enable|disable>
vlan-bysrcmac <enable|disable>
wsm-direct-mode <enable|disable>
```

OTT3 CSLAN P8600-0-A0:5/config/sys# set mtu?

set MTU (with CRC) to one of three values: 1522, 1950 and 9600 bytes

Required parameters:

<bytes> = MTU value {1522..9600}

Command syntax:

mtu <bytes>

OTT3 CSLAN P8600-0-A0:5/config/sys# set

OTT3 CSLAN P8600-0-A0:5/config/sys/set# mtu 9600

OTT3 CSLAN P8600-0-A0:5/config/sys/set# info

Sub-Context: action eapol flags msg-control record-reservation snmp
ssh

Current Context:

mgmt-virtual-ip : 0.0.0.0/0.0.0.0

udp-checksum : enable

```

                                udp-source : disable
                                clock-sync-time : 60
                                mroute-stream-limit : disable
                                contact : support@nortelnetworks.com
                                location : 4655 Great America Parkway, Santa
Clara, CA 950
54
                                name : OTT3 CSLAN P8600-0-A0
                                portlock : off
                                sendAuthenticationTrap : false
                                topology : on
                                globalFilter : enable
                                vlanBySrcMac : disable
                                ecn-compatibility : enable
                                wsm-direct-mode : disable
                                smlt-on-single-cp : disable timer 3
                                System MTU : 9600

OTT3 CSLAN P8600-0-A0:5/config/sys/set# .
OTT3 CSLAN P8600-0-A0:5/config/sys# top
OTT3 CSLAN P8600-0-A0:5# save config
Save config to file /flash/config.cfg successful.
```

Product = CS 2000

A00012526--TDM Call Recording Feature

Functional Description

1: Applicable Solution(s)

PT-IP, UA-IP, Int'l UA-IP

1.1 Description

This feature provides trunk information in the ICM (Intelligent Call Management) protocol to facilitate call recording functionality in a TDM environment. It supports trunk on a PVG, DTC, SPM or LTC. PVG trunks also

require datafill defined by feature A00012527: 'Provisioning of CS2K trunks on GW and Carrier basis' to access the correct information.

1.1.1 Background

ICM is a SCAI (Switch-Computer Applications Interface) protocol.

SCAI specifies an architecture and an Open Systems Interconnection (OSI) application layer protocol suite for peer-to-peer data communication between host computer applications and switch applications, thereby enabling the functional integration of computer systems and telephony switching systems.³

Remote Operation Service Element (ROSE) is used to support the interactive communication between the switch and host application.

Currently, ICM services exist for the use of four types of customers.

- Automatic Call Distribution (ACD) customers
- Meridian Digital Centrex (MDC) customers
- Residential (RES) customers
- SL-100 Private Branch Exchange (PBX) customers

ICM uses the following Operation Classes.

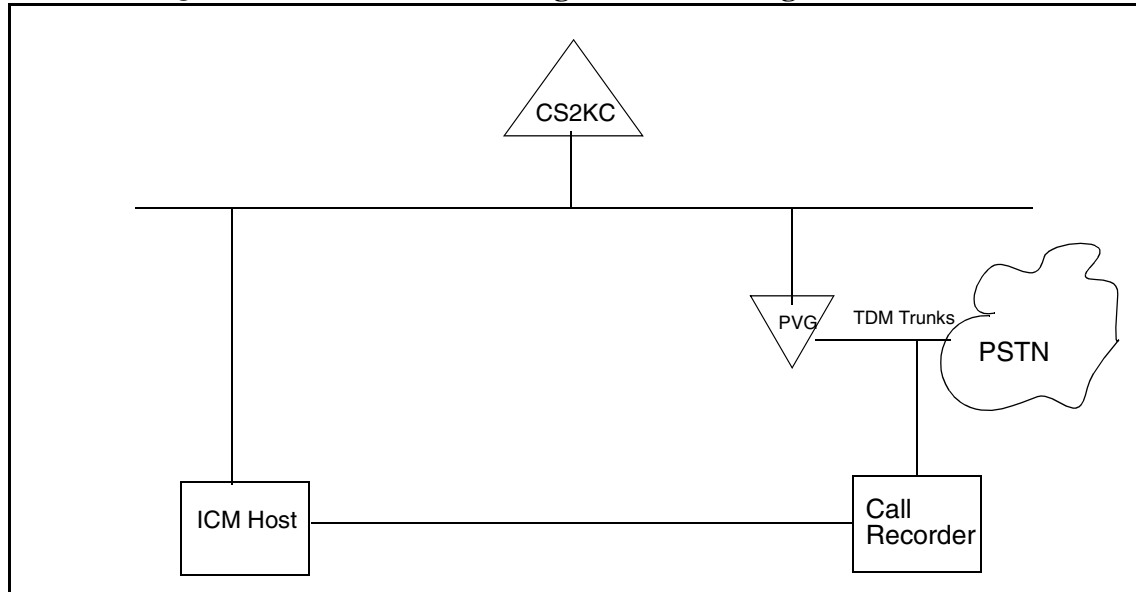
- Class 1: Synchronous, reporting success or failure
- Class 2: Asynchronous, reporting success or failure
- Class 5: Asynchronous, outcome not reported

1.1.2 Functionality Overview

Call recording functionality for TDM trunks utilizes the ICM protocol and a call recording device which taps into the TDM trunk involved in the call. A high-level diagram is shown below.

The CS2KC switch sends the ICM messages to the ICM Host (which is a Genesys CTI server for this case). The ICM Host will then relay required information to the Call Recorder, which will then start recording on the trunk.

3. Taken from the ANSI SCAI Standard document: ANSI TI.626-1993

Figure 1 TDM Call Recording Functional Diagram

To properly record calls and retrieve recorded calls, the system needs the following trunk information:

- PM Type
- PM Number
- Carrier Number
- Channel Number

This feature will provide this additional trunk information in the following ICM messages:

- dv_call_offered_U
- dv_call_queued_U

1.1.3 Feature Overview

To provide the trunk information in ICM messages, the following is required:

- SOC to control functionality
- SCAISSRV Table Control to subscribe for the trunk information
- ICM Enhancements including new SCAI protocol version SCAI19
- Call Processing and Error Handling
- New Log SCAI600

1.1.4 SOC

This feature will have a state controlled SOC, ICM00085.

- With the SOC turned on, the switch will attempt to send trunk information in the appropriate ICM messages. Reference the call processing section of this document for a complete description of the requirements to send trunk information.
- With the SOC turned off, the switch does not attempt to send trunk information in ICM.

Please reference the Configuration section of this feature for more information.

1.1.5 Table SCAISSRV Subscription Changes

The following changes in the table SCAISSRV are required to provide subscription to the changed SCA/ICM messages.

1.1.5.1 Subscription for ACD

A new default tuple ACDEVENT19\$ will be created with the new parameter TRNKINFO in functions CALLQUED and CALLOFFR.

1.1.5.2 Subscription for Residential and Centrex lines

- A new default tuple RESEVENT19\$ will be created with the new parameter TRNKINFO in function CALLOFFR.
- A new default tuple CTXEVENT19\$ will be created with the new parameter TRNKINFO in function CALLOFFR.

Please reference the Configuration section of this feature for more information on table SCAISSRV.

1.1.6 ICM Message Enhancements

This feature introduces a new parameter, **TRNKINFO**, in the following ICM call related messages.

- DV_Call_Queued_U
- DV_Call_Offered_U

The ASN.1 notations for these messages are shown in the Appendix of this document.

The new parameter, TRNKINFO, is added with the following information:

- PM Type: string {PVG, GW, DTC, SPM, LTC}
- PM Number: integer {0-1023}
- Carrier Number: integer {1-168}
- Channel Number: integer {1-31}

The changes are included in a new SCAI protocol version, SCAI19, as described in the next section.

1.1.6.1 Application Logon SCAI Service Version

The dv-Appl-Logon message contains a parameter, Service Version, which uniquely identifies the version of messages which will be sent during the session. A new Service Version value will be created to uniquely identify the stream of messages which are new or changed during this software release. The new Service Version will be SCAI19.

This new Service Version (SCAI19) must be specified in the dv-Appl-Logon message for the host application to receive the enhanced messages. If a Service Version lower than SCAI19 is specified, the TRNKINFO parameter will not be contained in the above three SCAI messages sent to the Host.

The Service Version is upward compatible. This means all of the functionality enabled and provided with any of the previous Service Versions will be provided in SCAI19. Future DMS/CS2K/Cs2Kc software releases will provide additional ICM functionality but will continue to allow the specification of the SCAI19 Service Version. Therefore, applications written to use SCAI19 will not require rewriting to continue to work properly.

1.1.7 Call Processing and Error Handling

Throughout call processing, anytime one of the three modified ICM messages is to be sent out, the switch will attempt to include the new TRNKINFO parameter. The following conditions must be met in order for this to occur:

1. SOC ICM00085 must be set to ON.
2. The SCAI Service Version is at least SCAI19.
3. An ICM switch-host session is established. A successful dv-Appl-Logon request was sent by the host computer.
4. The line which the host application is monitoring must be associated to the session via dv-DN-Associate.
5. For Centrex/Res lines the line option ECM with suboption CALL_EVENTS and SCAIRDIR must be set to 'Y'.
6. The switch-host session is subscribed to the new default tuples, ACDEVENT19\$, CTXEVENT19\$ or RESEVENT19\$.

For call which meet all of the above criteria, the trunk information will be sent if available. If the PVG trunk information is not available then it cannot be sent and a new SCAI600 log is generated.

Note: Nodal calls do not have a trunk involved in the call and therefore, have no trunk information. No log is generated for these calls.

For calls which do not meet the above criteria, the TRNKINFO parameter will not be sent. No log is generated.

PVG trunk information is obtained from tables created and altered by feature A00012527: Provisioning of CS2K trunks on GW and Carrier basis. The tables include GATWYINV and GWEPCARR. Please reference feature documentation for A00012527 for more information on these tables.

DTC, SPM and LTC trunks obtain the information from table TRKMEM.

1.1.8 Log SCAI600

A new SCAI log, SCAI600, is created to indicate when a call should have sent the trunk information parameter, TRNKINFO, in the ICM message but was not able to because it was not available for a PVG trunk. The trunk information may not be available for a number of reasons including incorrect or missing datafill. The action is to check the datafill in tables TRKMEM, GATWYINV and GWEPCARR.

Please reference the Fault Management section of this feature for more information on this log.

1.2 Hardware Requirements or Dependencies

N/A

1.3 Software Requirements or Dependencies

If PVG trunk information is not available to the SCAI environment due to no manual entry of the SESM datafill in appropriate tables (look at activity A00012527: Provisioning of CS2K trunks on GW and carrier basis) the TRNKINFO parameter cannot be sent in the SCAI messages and log SCAI600 is generated.

1.4 Limitations and restrictions

New option TRNKINFO cannot be sent in ICM messages if no trunk information is available for the call. PVG trunks will log the missing datafill.

After an ONP from a patched load with this functionality, it is possible when the version is increased for services below 19 to 19 or above, that the TRNKINFO parameter may be set to Y via tables SCAIPROF/SCAISSRV and begin being sent. If PVG trunks are being used but are not datafilled in GATWYINV/GWEPCARR then log SCAI 600 will be generated for each message sent with missing datafill.

1.5 Interactions

None of the existing interactions will be affected or changed by this activity. No new interactions will be introduced by this activity

1.6 Glossary

Term	Description
ACD	Automatic Call Distribution
ASN	Abstract Syntax Notation
CTI	Computer Telephone Integration
DN	Directory Number
ICM	Intelligent Call Management
MDC	Meridian Digital Centrex
RES	Residential Enhanced Services
SCAISSRV	Switch Computer Application Interface SCAI Service

1.7 Appendix: ASN.1 Notations for Modified ICM Messages

This sections shows the ASN.1 notations for the following modified ICM messages in SCAI19:

- DV_Call_Queued_U
- DV_Call_Offered_U

The new parameter, TRNKINFO, is added with the following information:

- PM Type: string {PVG, GW}
- PM Number: integer {0-1023}
- Carrier Number: integer {1-168}
- Channel Number: integer {1-31}

The parameters below which are ***italicized and bold*** are new to these messages. The letter 'U' in the message name indicates that the message is unconfirmed, i.e., this operation requires no outcome to be reported by the host. The letter 'C' at the end of the message's name indicates that the message requires confirmation from the host.

1.7.1 DV_Call_Queued_U message

The switch sends this RO of Operation Class 5 to the host when a call to an ACD DN associated with the current session is received by the switch and placed in the Incoming Call Queue.

1.7.1.1 Changed DV_Call_Queued_U ASN.1 definition.

ASN.1 Encoding

dv-CALL-QUEUED-U ARGUMENT OPERATION

ARGUMENT CallQueuedArgument ::= 6

```

CallQueuedArgument ::= SEQUENCE
{
    networkCallID [0] IMPLICIT SEQUENCE
        {
            networkNodeID [0] IMPLICIT INTEGER OPTIONAL,
            localCallID [1] IMPLICIT INTEGER OPTIONAL
        } OPTIONAL,

    acdDN [1] IMPLICIT OCTET STRING OPTIONAL,
    origCallingNumber [2] IMPLICIT OCTET STRING OPTIONAL,
    origChargeNumber [3] IMPLICIT OCTET STRING OPTIONAL,
    callHistoryInfo [4] IMPLICIT SEQUENCE
        {
            callType [0] IMPLICIT ENUMERATED
                {
                    callTransferred (1),
                    callOverflowed (2),
                    callRedirected (3),
                    callForwarded (4),
                    callConsult (5),
                    callConference (6),
                    callReturnedToQueue (7),
                    callRouted (8)
                } OPTIONAL,

            origInboundDN [1] IMPLICIT OCTET STRING OPTIONAL,
            prevApplicationID [2] IMPLICIT INTEGER OPTIONAL,
            hostCallData [3] IMPLICIT OCTET STRING OPTIONAL
        } OPTIONAL,

    acdGroup [5] AddressType OPTIONAL,
    forwardingParty [6] ForwardingPartyType OPTIONAL,
    cpadigs [7] IMPLICIT OCTET STRING OPTIONAL,
    uuiParameter [8] IMPLICIT OCTET STRING OPTIONAL,

    trnkInfo [9] IMPLICIT SEQUENCE
        {
            {PM Type [0] IMPLICIT OCTET STRING OPTIONAL,

            PM Number [1] IMPLICIT INTEGER OPTIONAL,

            Carrier Number [2] IMPLICIT INTEGER OPTIONAL,

            Channel Number [3] IMPLICIT INTEGER OPTIONAL
        }
        OPTIONAL
    }

```

AddressType ::= CHOICE

```

{ positionID           [0] IMPLICIT INTEGER,
  dialedDigits         [1] IMPLICIT IA5STRING,
  stationNumber        [2] IMPLICIT OCTET STRING,
  q931Address          [3] Q931AddressType }

Q931 AddressType      ::= SEQUENCE
{ numberTypeNumberPlan [0] OCTET STRING OPTIONAL,
  presentationScreeningIndicator [1] OCTET STRING OPTIONAL,
  digits               [2] IA5 STRING OPTIONAL }

ForwardingPartyType    ::= IMPLICIT SEQUENCE
{ firstFwdNumber       [0] AddressType OPTIONAL,
  firstFwdReason       [1] IMPLICIT ENUMERATED
    { unknown          (0),
      userBusy         (1),
      noReply          (2),
      unconditional    (3) } OPTIONAL,
  lastFwdNumber        [2] AddressType OPTIONAL,
  lastFwdReason        [3] IMPLICIT ENUMERATED
    { unknown          (0),
      userBusy         (1),
      noReply          (2),
      unconditional    (3) } OPTIONAL },

```

1.7.1.2 DV_Call_Queued_U:Coded example.

An ACD call has been initiated from the OrigCallingNumber 6136217703 6134444444 and offered over a trunk to an ACD group with Primary DN 6136212111, for which no agent is available, the call is placed in the Incoming Call Queue and the switch sends DV-CALL-QUEUED-U to the host. No Return Result is required or received by the switch from the host.

INVOKE

CS2K =====> HOST

Hex Dump			Information Element	Comments
Tag	Length	Content		
a1	54		INVOKE	Message length is 84 bytes decimal
02	02	03 ff	InvokeID	The InvokeID is 1023
02	01	06	Operation	Operation value for DV-CALL-QUEUED-U is decimal 6
30	4b		Argument	CallQueued argument is of Sequence type and is 75 bytes long decimal

Hex Dump			Information Element	Comments
Tag	Length	Content		
a0	09		NetworkCallId	The NetworkCallId is a constructor of 9 bytes long
80	04	03 38 d0 90	NetworkNodeId	The NetworkNodeId is 54055056
81	01	0d	LocalCallId	The LocalCallId is 13
81	0a	36 31 33 36 32 31 32 31 31 31	ACDDN	The called ACDDN of the Group is 6136212111
82	0c	00 83 36 31 33 36 32 31 37 37 30 33	Original Calling Number	The first 2 bytes are fixed and must not be read at present. The original calling number is 6136217703
A5	0c		Acd group	The ACDGroup is of type Constructor and is 12 bytes long
82	0a	36 31 33 36 32 31 32 31 31 31	Station number	The station number of the ACDGroup is 6136212111
87	0a	36 31 33 34 34 34 34 34 34 34	CPADIGS	The CPA value is 6134444444
A9	0E		trnkInfo	is a constructor of 14 bytes long.
80	03	50 56 47	PM Type	PVG
81	01	39	PM Number	decimal 57
82	01	54	Carrier Number	decimal 84
83	01	10	Channel Number	decimal 16
Hex Dump= a1 54 02 02 03 ff 02 01 06 30 4b a0 09 80 04 03 38 d0 90 81 01 0d 81 0a 36 31 33 36 32 31 32 31 31 31 82 0c 00 83 36 31 33 36 32 31 37 37 30 33 a5 0c 82 0a 36 31 33 36 32 31 32 31 31 31 87 0a 36 31 33 34 34 34 34 34 34 34 a9 0E 80 03 50 56 47 81 01 39 82 01 54 83 01 10				

1.7.2 DV_Call_Offered_U message

This section describes the DV-CALL-OFFERED-U message the switch uses to notify the host that a ICM Party has been selected for ACD. The party has been selected to handle an incoming call to one of the DN's belonging to the associated environment of the current switch-host session when the call is about to be offered to the ICM Party. This call comes in over a trunk.

1.7.2.1 Changed DV_Call_Offered_U ASN.1 definition.

ASN.1 Encoding

dv-CALL-OFFERED-U	OPERATION
	ARGUMENT CallOfferedArgument ::= 5
CallOfferedArgument	::= SEQUENCE
{ networkCallID	[0] IMPLICIT SEQUENCE
{ networkNodeID	[0] IMPLICIT INTEGER OPTIONAL,
localCallID	[1] IMPLICIT INTEGER OPTIONAL }
	OPTIONAL,
acdDN	[2] IMPLICIT OCTET STRING OPTIONAL,
origCallingNumber	[3] IMPLICIT OCTET STRING OPTIONAL,
origChargeNumber	[4] IMPLICIT OCTET STRING OPTIONAL,
callHistoryInfo	[5] IMPLICIT SEQUENCE
{ callType	[0] IMPLICIT ENUMERATED
{ callTransferred	(1),
callOverflowed	(2),
callRedirected	(3),
callForwarded	(4)
callConsult	(5),
callConference	(6),
callReturnedToQueue	(7),
callRouted	(8) } OPTIONAL,
origInboundDN	[1] IMPLICIT DeviceAddressType OPTIONAL,
prevApplicationID	[2] IMPLICIT INTEGER OPTIONAL,
hostCallData	[3] IMPLICIT OCTET STRING OPTIONAL }
	OPTIONAL,
acdGroup	[6] AddressType OPTIONAL,
callMode	[7] IMPLICIT ENUMERATED
{ callWaited	(1) } OPTIONAL,
destDeviceID	[8] AddressType OPTIONAL,
forwardingParty	[9] ForwardingPartyType OPTIONAL,
cpadigs	[10] IMPLICIT OCTET STRING OPTIONAL,

```

    uuiParameter      [11]IMPLICIT OCTET STRING OPTIONAL,

    trnkInfo          [12] IMPLICIT SEQUENCE

    {PM Type           [0] IMPLICIT OCTET STRING OPTIONAL,
    PM Number          [1] IMPLICIT INTEGER OPTIONAL,
    Carrier Number     [2] IMPLICIT INTEGER OPTIONAL,
    Channel Number     [3] IMPLICIT INTEGER OPTIONAL}
    OPTIONAL

}

AddressType ::= CHOICE
{ positionID      [0] IMPLICIT INTEGER,
  dialedDigits    [1] IMPLICIT IA5STRING,
  stationNumber   [2] IMPLICIT OCTET STRING,
  q931Address     [3] Q931AddressType }

Q931AddressType ::= SEQUENCE
{ numberTypeNumberPlan [0] OCTET STRINGOPTIONAL,
  presentationScreeningIndicator [1] OCTET STRINGOPTIONAL,
  digits              [2] IA5 STRING OPTIONAL }

ForwardingPartyType ::= IMPLICIT SEQUENCE
{ firstFwdNumber      [0] AddressTypeOPTIONAL,
  firstFwdReason      [1] IMPLICIT ENUMERATED
    { unknown         (0),
      userBusy        (1),
      noReply         (2),
      unconditional   (3) } OPTIONAL,

  lastFwdNumber       [2] AddressType OPTIONAL,
  lastFwdReason       [3] IMPLICIT ENUMERATED
    { unknown         (0),
      userBusy        (1),
      noReply         (2),
      unconditional   (3) } OPTIONAL }

```

1.7.2.2 DV_Call_Offered_U: Coded example.

An ACD call is initiated from the OrigCallingNumber 6136217703 by dialing 6134444444 and is assigned a LocalCallID = 9. The call is offered over a trunk to an acd agent with posid 7707 of the acd group with primary DN 613621111.

The switch sends DV-CALL-OFFERED-U to the host. No Return Result is required or received by the switch from the host.

INVOKE**CS2K ===== > HOST**

Hex Dump			Information Element	Comments
Tag	Length	Content		
a1	5a		INVOKE	this message is 90 bytes decimal
02	02	03 f9	InvokeID	the InvokeID is 1017
02	01	05	Operation	the operation is DV-CALL-OFFERED-U [5]
30	51		Argument	CallOffered argument is of Sequence type and is 81 bytes long decimal
a0	09		NetworkCallId	The NetworkCallId is a constructor 9 bytes
80	04	03 38 d0 90	NetworkNodeId	The NetworkNodeId is 54055056
81	01	09	LocalCallId	The LocalCallId is 9 decimal
82	0a	36 31 33 36 32 31 32 31 31 31	acd_dn	6136212111
83	0c	00 83 36 31 33 36 32 31 37 37 30 33	OrigCallingNumber	The first two bytes are fixed and presently must not be read. The customer's OrigCallingNumber is 6136217703
a6	0c		acd_grp	
82	0a	36 31 33 36 32 31 32 31 31 31	StationNumber	The called DN is 6136212111
a8	04		DeviceID	The DeviceID is of type Constructor and is 4 bytes long
80	02	1e 1b	pos_id_2	7707
8a	0a	36 31 33 34 34 34 34 34 34 34	CPADIGS	The CPA value is 6134444444
Ac	0E		trnkInfo	is a constructor of 14 bytes long.

Table 1: Field descriptions

Field	Value	Description
SCAI GROUP		Identifies the scai group as datafilled in SCAIGRP Table with which the ECM session is established.
REF TAB	TRKMEM	Reference table TRKMEM to find trunk information missing from other tables.

2.1.4 Action

Check the datafill in tables TRKMEM, GATWYINV and GWEPCARR. Use the information from TRKMEM and determine the correct setting from SESM for the other tables.

Another option is to set the TRNKINFO parameter to N via tables SCAIPROF/SCAISSRV.

3: Configuration Management for A00012526

3.1 Hardware and Software Requirements

There is no specific hardware requirement for this feature. The basic ICM software package as well as the software for the SN10 feature A00012527 are needed to use this feature.

3.2 Initial Configuration

The subscription to this feature has to be done according to the DS section below.

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

N/A

3.4 Upgrade Considerations

3.4.1 Dump and Restore (CM)

No new tables are being added for this feature.

3.4.2 Element Management Upgrade

N/A

3.4.3 Downgrade impact

None.

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

3.5.1 New/modified tables, MIBs, or Database Schema

The following table describes changed table information.

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
SCAISSRV	Changed	Unchanged

3.5.2 Table/MIB/Remote Database Schema information

3.5.2.1 Name: SCAISSRV

Switch Computer Application Interface Subservices table.

3.5.2.1.1 Functional description

Table SCAISSRV is used to enter default tuples for each SCAI message category as well as to add customizable category. This allows the customer to subscribe to these categories using Table SCAIPROF.

3.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

3.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SCAISSRV	0	511	Protected

3.5.2.1.4 Fields/OIDs

The following table lists fields for table SCAISSRV.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
TRNKINFO	New	Subfield	Y/N	trunk information

A new default tuple CTXEVENT19\$ under category CTXEVENT will be created with the optional parameter TRNKINFO of the function CALLOFFR set to Y.

A new default tuple RESEVENT19\$ under category RESEVENT will be created with the optional parameter TRNKINFO of the function CALLOFFR set to Y.

A new default tuple ACDEVENT19\$ under category ACDEVENT will be created with the optional parameter TRNKINFO of the function CALLQUED and CALLOFFR set to Y.

TABLE SCAISSRV
SUBSERV SPROFILE

```
-----
CTXEVENT19$ CTXEVENT (SETOFFHK Y Y Y)
(CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y)
(CALLANSWR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y) (CALLREL Y Y Y Y)
(CALLNAME Y Y Y Y Y) $
```

```
RESEVENT19$ RESEVENT (SETOFFHK Y Y)
(CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y)
(CALLANSWR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y) (CALLREL Y Y Y)
(CALLNAME Y Y Y Y Y) $
```

```
ACDEVENT19$ ACDEVENT (CALLQUED Y Y Y Y Y Y Y Y Y Y Y Y Y)
(CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y)
(CALLANSWR Y Y Y Y Y Y Y Y Y Y Y Y Y Y)
(CALLREL Y Y Y Y Y Y Y) (AGTLGDIN Y Y Y) (AGTLGDOUT Y Y)
(AGTREADY Y Y)
(AGTNREADY Y Y N) (LOBEVENT Y Y Y) (EMKEVENT Y Y Y Y Y Y)
(AGT SETACT Y Y N)
$
```

3.5.2.1.5 Datafill example

The following example shows sample datafill for table SCAISSRV.

1. EXAMPLE

TABLE: SCAISSRV

>add TRKTUP1

MACHINES NOT IN SYNC - DMOS NOT ALLOWED

JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED

ENTER Y TO CONTINUE PROCESSING OR N TO QUIT

>y

CATEGORY:

>CTXEVENT

FUNCTION:

>CALLOFFR

> NCALLID: Y

> CALLLNGNO:Y

> CALLNGNAME: Y

CHARGENO: Y

CALLTYPE: Y

ORIGDN: Y

ORIGNAME: Y

PREVAPPL:Y

HOSTCALD: Y

DEVICEID: Y

FWDPARTY: Y

TRNKINFO: Y

FUNCTION:

>\$

>\$

TUPLE TO BE ADDED:

TRKTUP1

>TRNKINFO: Y

FUNCTION:

>CALLQUED

>NCALLID: Y

>ACDDN: Y

>CALLNGNO: Y

>CHARGENO: Y

>CALLTYPE: Y

>ORIGDN: Y

>PREVAPPL: Y

>HOSTCALD: Y

>ACDGROUP: Y

>FWDPARTY: Y

>CPADIGS: Y

> TRNKINFO: Y

>FUNCTION:

>\$

TUPLE TO BE ADDED:

TRKTUP2

ACDEVENT (CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y Y) (CALLQUED

Y Y Y Y Y Y Y Y Y Y Y Y Y) \$

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

>y

3.5.2.1.6 Table release history update

A new field TRNKINFO is added under function CALLOFFR for categories RESEVENT, CTXEVENT and ACDEVENT, under function CALLQUED for category ACDEVENT.

This feature will be released in SN10. An activatable patch will also be available in SN09.

3.5.2.1.7 Supplementary information

N/A

3.5.2.1.8 Translation verification and other tools.

SCAISSRV does not use translation verification tools.

3.6 Service Orders (SO) (CM & SESM)

N/A

3.7 Software optionality control (SOC)

This feature will have a state controlled SOC. With the SOC turned on, the new parameter added to indicate the trunk information will be sent in the two existing messages, dv_call_queued_U and dv_call_offered_U messages, provided the new parameter is subscribed for these messages and the call is coming in from a trunk. For nodal calls, no trunk information will be provided, the new parameter will not show in the message.

With the SOC turned off, even if the new parameter for the three messages have been subscribed to, the new parameter will not be sent along with the messages.

Table 4 SOC

SOC option name:	ICM Call Recording
SOC option title:	Call Recording
SOC option control type:	State
New SOC option?	Yes
SOC option order code	ICM00085
Option defined in DRU:	CCM
Affected products:	LEC00023, LET 00023, LLT00023, SN10, ISN10, SE09, SE10

Product = CS 2000

A00012527--Provisioning of CS2K trunks on GW and Carrier basis

Functional Description

1: Applicable Solution(s)

PT-IP

1.1 Description

This activity allows mapping of trunk TID's on CS2K core based on GW and carrier, using CM tables GATWYINV and GWEPCARR.

Currently, provisioning of GWs and carriers for CS2000 trunking is done in the CS2K EM (SESM). Provisioning of trunk groups and individual trunk members is done in the CS2K CM. A trunk member in the CM is mapped to a channel on a carrier in SESM using a node and terminal number (TID). No GW or carrier information is currently available on the CM for trunks configured on gateways. Because of this data split, existing OA&M on the CM can only identify the TID of a trunk to the craftsperson by giving the physical circuit location. This has resulted in

1. a multi-step process for the craftsperson to locate a physical GW and pack (CM -> SESM -> GW element manager or physical hardware).
2. the inability to provide maintenance services on GW or carrier from the CM.
 - post by GW or carrier in TTP
 - OMs on a GW basis
 - GW alarm

As part of this activity, changes will be made in the following areas:

- Support for PVG and GW profiles for table GATWYINV
- Introduction of new table GWEPCARR
- Modification of CktLoc command in MAPCI, TTP level to display Gateway and Carrier information.

This activity will support both North American and International loads.

Figure 1 Trunk Carrier / GW data in core

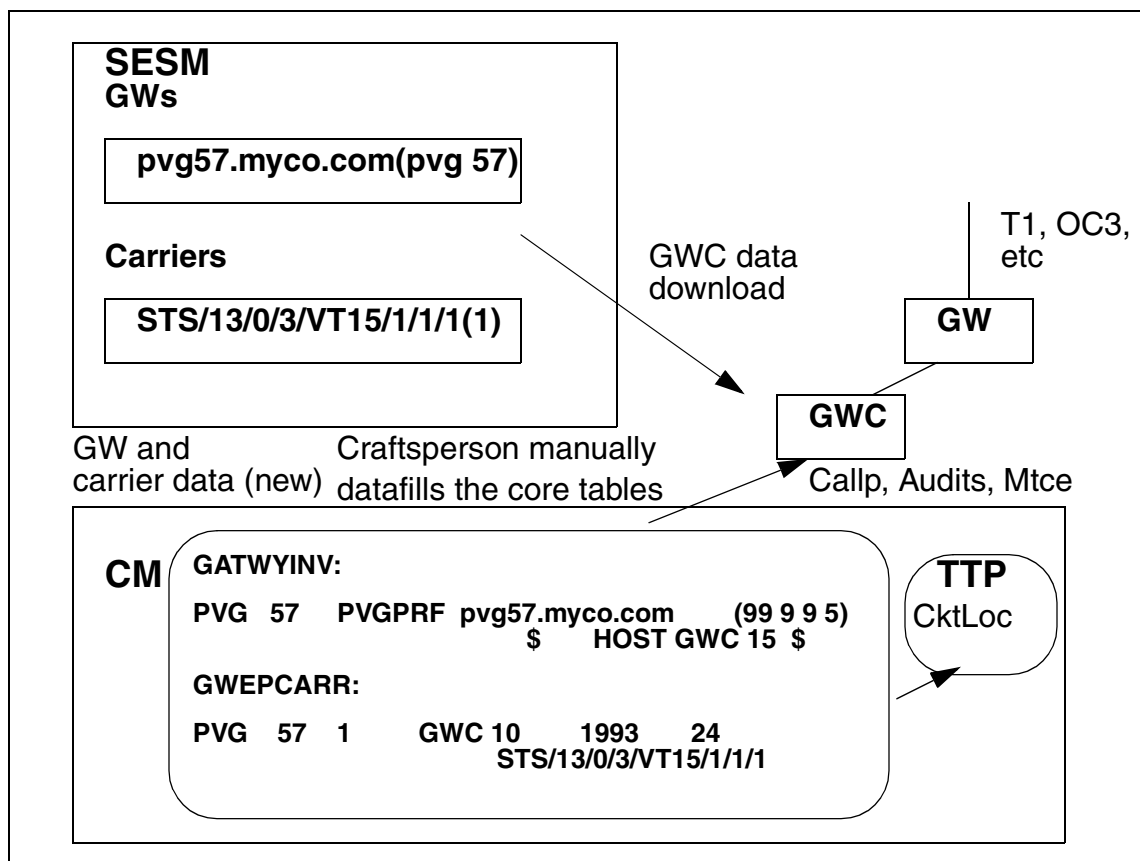


Figure 2 TTP Display with Modified CktLoc Command

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
AMDI	.	DLOG E	.	1 SPM	.	SYSB	57C..	.	SDM
M				*C*		CR C	*C*		M
TTP									
0 QUIT	POST	1	DELQ		BSYQ		DIG		
2 Post_	TTP	6-0000							
3 SEIZE	CKT TYPE	PM NO.			COM LANG	STA S R	DOT TE	RESULT	
4	2W S7 S7	GWC 15	12		TEST	0 INB			
5 BSY								R	
6 RTS									
7 TST									
8									
9 CktInfo									
10 CktLoc									
11 Hold	CktLoc								
12 NEXT	GW	Ckt	Chnl						
13 RLS	PVG 57	1	1						
14 Ckt_									
15 Trnslvf_	GW Name								
16 StkSdr_	PVG RTP1023								
17 Pads	Endpoint Name								
18 Level_	STS/13/0/3/VT15/1/1/1/1								
ADMIN									
Time 15:59	>								

Note 1: Automatic upload from SESM to GATWYINV and GWEPCARR tables in core is not supported as part of this activity. The craftsperson has to manually datafill the tables by looking into the SESM details.

1.1.1 GW Data - Table GATWYINV

Table GATWYINV is an existing table that houses the gateway related information. It currently allows only ABI GWs which are provisioned in parallel in the CM and SESM. This activity shall allow support for PVG and GW profiles in table GATWYINV.

Datafill each gateway in table GATWYINV prior to datafill in table GWEPCARR. Deleting of tuple in GATWYINV is not allowed if the Gateway type and number are being referenced in table GWEPCARR.

For details on what/how this is provisioned, refer to the Configuration section of this feature.

1.1.2 Carrier Data - Table GWEPCARR

Table GWEPCARR is a new table that shall hold the mapping from GW and carrier number to the TID range used by trunks on the carrier. The key to table GWEPCARR is the GW type and number and the carrier number. The number of channels on a carrier is restricted to 24 for North America and 31 for International. The table will also hold the carrier name information.

The internal representation of GWEPCARR shall be used to map GW and carrier group number to the TIDs used for that carrier. There shall also be a mapping from TID to GW and carrier .

Datafilling table GWEPCARR with a gateway, that does not exist in table GATWYINV, is not allowed.

For details on what/how this is provisioned, refer to “ 12.5.3 Table GWEPCARR Database Schema information” in the CN chapter of this book.

1.1.3 Trunk Test Position (TTP - CM)

At MAPCI, TTP level, the CktLoc command is not currently supported for GWC trunks. This component shall support GWC for CktLoc and shall display the gateway and carrier information for the trunk member currently being posted, if the TID to Carrier mapping exists in Table GWEPCARR.

If the posted trunk does not have TID to Carrier mapping in table GWEPCARR, then a message “CARRIER INFO NOT PRESENT IN TABLE GWEPCARR” would be displayed.

The CktLoc will not be supported for GWC audio nodes as part of this activity.

For details on what/how this is done, refer to the Configuration section of this feature.

1.2 Hardware Requirements or Dependencies

N/A

1.3 Software Requirements or Dependencies

This feature requires the Core load to be a succession load.

1.4 Limitations and restrictions

Craftsperson should provision the Gateway and carrier information in SESM. The same information must be manually datafilled in core as well.

1.5 Interactions

N/A

1.6 Glossary

Term	Description
CM	Computing Module (also known as "Core")
CS2K	Call Server 2000
EM	Element Manager
GATWYINV	Gateway Inventory Table
GW	Gateway
GWC	Gateway Controller
GWEPCARR	Gateway Endpoint Carrier Table
PM	Peripheral Module
PVG	Packet Voice Gateway
SESM	Succession Element Sub-element Manager
TID	Terminal Identifier
TRKMEM	Trunk Member Table
TTP	Trunk Test Position
CktLoc	Circuit Location
MAPCI	Maintenance and Administration Position Command Interpreter

2: Configuration for A00012527

2.1 Hardware and Software Requirements

Software Requirements:

- SN09 drop 2 Succession Core load or later

2.2 Initial Configuration

N/A

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

N/A

2.4 Upgrade Considerations

2.4.1 Dump and Restore (CM)

Table GATWYINV and GWEPCARR will use the existing data transfer "TabXfr" mechanism available to all Table Control tables to preserve their data during an upgrade.

2.4.2 Element Management Upgrade

N/A

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

2.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
GATWYINV	CHANGED	UNCHANGED
GWEPCARR	NEW	NEW

2.5.2 Table GATWYINV Database Schema information

2.5.2.1 Name: GATWYINV

Long Table Name: GATeWaY INventory

2.5.2.1.1 Functional description

Table GATWYINV holds the gateway related information. It currently allows only ABI GWs which are provisioned in parallel in the CM and SESM. The modification shall allow support for PVG and GW gateways.

As the gateway physical location and element manager information is not significant for GW and PVG gateway types, the tuple options ELMGR and GTWYLOC are not allowed for these gateway types.

GATWYINV Table needs to be datafilled prior to datafilling table GWPCARR.

2.5.2.1.2 Usage sequence and implications (CM Only)

No change to datafill order. The sequence is as follows:

1. Table SERVINV - GWC datafill
2. Table GATWYINV - GW datafill

2.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
GATWYINV	0	32767	Memory is automatically allocated in increments with block size of 2K.

2.5.2.1.4 Fields/OIDs

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GTWYPRFL	Changed	Refined to support for 2 new profiles	PVGPRF GWPRF	PVG gateway profile Generic Gateway (GW) profile

2.5.2.1.5 Datafill example

Figure 1 Sample GATWYINV Tuples with PVG and GW profiles

GTWY	PMNO	GTWYPRFL	GTWYNAME	GTWYADDR	GTWYCSPM	GTWYOPTS
PVG	5	PVGPRF	pvg5.myco.com	(99 9 9 5) \$	HOST GWC 15	\$
GW	1	GWPRF	gw1.myco.com	(99 9 9 6) \$	HOST GWC 15	\$

Figure 2 Prompting sequence and Range values for GATWYINV

```

TABLE GATWYINV
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
GTWYPMNO:
TYPE OF GTWYPMNO IS GTWY_TC_KEY_T
TYPE IS GTWY_TC_KEY_T MULTIPLE WITH
      GTWY_TYPE   {NLGW,ABI,CICM,GW,MG9K,PVG,MS,SESS}
      GTWY_NO     {0 TO 1023}
GTWYPMNO:
>PVG 5
GTWYPRFL:
TYPE OF GTWYPRFL IS GTWY_PROFILE_TYPE
TYPE IS GTWY_PROFILE_TYPE {NILPROFILE,GWPRF,MG9KITP,MG9KABI,
                           CICMPRF,MSUAS,PVGPRF,ST3PPRF,
                           LT3PPRF,SL3PPRF,LL3PPRF,CALIXC7,
                           SSL1PRF}
GTWYPRFL:
PVGPRF
GTWYNAME:
TYPE IS GTWY_NAME_VECTOR VECTOR OF UP TO 32 CHAR'S
>PVG5.myco.com'
GTWYADDR:
192 21 165 70
GTWYCSPM:
HOST GWC 3
GTWYOPTN:
>$
TUPLE TO BE ADDED:
PVG 5 PVGPRF PVG5.myco.com (192 21 165 70) $ HOST GWC 3 $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
.>y
TUPLE ADDED

```

Deletion of Tuple from table GATWYINV is not allowed, if that tuple is referenced in Table GWEPCARR.

Figure 3 GATWYINV Tuple deletion**TABLE GATWYINV:**

>pos GW 1

GW 1 GWPRF gw1.myco.com (99 9 9 6) \$ HOST GWC 3 \$

>del

MACHINES NOT IN SYNC - DMOS NOT ALLOWED

JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED

ENTER Y TO CONTINUE PROCESSING OR N TO QUIT

>y

Error: Table GWEPCARR still references this Gateway.!**Action: Remove all references to this Gateway before deleting.**

TUPLE TO BE DELETED:GW 1 GWPRF gw1.myco.com (99 9 9 6) \$ HOST GWC 3 \$

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

>n

DMO REJECTEDWARNING: CURRENTLY NOT POSITIONED

2.5.2.1.6 Table release history update

SN09 drop 2 Feature A00012527: Available in the Core with the SN09 drop 2 or later release.

Modified field: GTWYPRFL to support for PVG and GW profiles.

2.5.2.1.7 Supplementary information

N/A

2.5.2.1.8 Translation verification and other tools

Table GATWYINV does not impact translations. Therefore TABAUDIT is the tool used to verify the contents of table GATWYINV.

Figure 4 Sample tabaudit output for Verifying Table GATWYINV datafill

```

>tabaudit
TABAUDIT:
>include gatwyinv
>execute
-----
|                                     |
|          TABAUDIT STATUS          |
|                                     |
|-----|
The following tables are included:    table GATWYINV (95)

The following tables are excluded:
From table VERSIONS (0)              to table SERVRINV (94).
From table LTCINV (96)               to table INWATNPA (1449).
Please confirm ("YES", "Y", "NO", or "N"):
>y
Creating TABAUDIT summaryfile: SUMMARY$TTY0 on SFDEV.
Starting DMS data verification ...
Table GATWYINV: New table control.
Completed tuple checking.
SUMMARY: Tbl GATWYINV: tuples checked 0, passed 0, failed 0.
Data verification is completed.

```

2.5.3 Table GWEPCARR Database Schema information

2.5.3.1 Name: GWEPCARR

Long Table Name: GateWay End Point CARRIER

2.5.3.1.1 Functional description

New table GWEPCARR shall hold the mapping from GW and carrier number to the TID range used by trunks on the carrier. The key to table GWEPCARR is the GW type and number and the carrier number. The number of channels on a carrier is restricted to 24 for North America and 31 for International. The table will also hold the carrier name information.

Only Add and Delete operations will be supported on table GWEPCARR.

Datafilling table GWEPCARR with a gateway, that does not exist in table GATWYINV, is not allowed.

2.5.3.1.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

1. Table GATWYINV - Gateway datafill.
2. Table GWEPCARR - New Table, Gateway and carrier datafill.

2.5.3.1.3 Fields/OIDs

Table 4 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Valid entries	Explanation and action
GWCARR	New	GW_TYPE	{NLGW,ABI,CICM,GW,M G9K,PVG,M S,SESS}	{GW, PVG}	This is the type of the gateway as defined on the Core. The valid values are PVG and GW.
		GW_NUM	{0 - 1023}	{0-1023}	This is the unique external number of the gateway.
		CARRIER_NUM	{0 - 168}	{1-168}	This is the carrier over which the trunk is configured. Valid Values are in the range {1 - 168}
HOST	New	HOST_TYPE	{GWC}	{GWC}	This is a valid pm type of the cside host xpm.
		HOST_NO	{0 - 255}	{0 - 255}	The unique external number of the cside host Gateway Controller.
START	New	GW_CARR_TERM_NUM_TC	{1 - 4094}	{1 - 4094}	This gives the starting terminal number on a particular carrier.
CARRSIZE	New	GTWY_CARRIER_SIZE_TC	{0 - 31}	{24, 31}	This is 24 for North America and 31 for International loads.
CARRNAME	New	CARR_NAME_VECTOR	Up to 32 Char's	Up to 32 Char's	Carrier Name as given in the SESM

2.5.3.1.4 Datafill example

Figure 5 Sample GWEPCARR tuples

TABLE GWEPCARR:					
GWCARR	HOST	START	CARRSIZE	CARRNAME	

PVG 1 2	GWC 3	25	24	sts/13/0/3/vt15/1/1/1	
GW 1 1	GWC 3	1	24	sts/13/0/3/vt15/1/1/1	

Figure 6 Prompting sequence and Range values for GWEPCARR

```

>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
GWCARR:
TYPE OF GWCARR IS GWEPCARR_KEY_T

TYPE IS GWEPCARR_KEY_T MULTIPLE WITH
    GW_TYPE      {NLGW,ABI,CICM,GW,MG9K,PVG,MS,SESS}
    GW_NUM       {0 TO 1023}
    CARRIER_NUM {0 TO 168}
GWCARR:
GWCARR:
>ms 0 0
HOST:
TYPE OF HOST IS GW_CARR_HOST_NODE
TYPE IS GW_CARR_HOST_NODE MULTIPLE WITH
    HOST_TYPE     {GWC}
    HOST_NO       {0 TO 255}
HOST:
>gwc 0
START:
TYPE OF START IS GW_CARR_TERM_NUM_TC
TYPE IS GW_CARR_TERM_NUM_TC {1 TO 4094}
START:
>1
CARRSIZE:
TYPE OF CARRSIZE IS GTWY_CARRIER_SIZE_TC
TYPE IS GTWY_CARRIER_SIZE_TC {0 TO 31}
CARRSIZE:
>32
CARRNAME:
TYPE OF CARRNAME IS CARR_NAME_VECTOR
TYPE IS CARR_NAME_VECTOR VECTOR OF UP TO 32 CHAR'S
CARRNAME:
>'sts/13/0/3/vt15/1/1/1'
TUPLE TO BE ADDED:
MS 0 0 GWC 0 1 32 sts/13/0/3/vt15/1/1/1(2)

Gateway type must be either PVG or GW
Carrier Number must be in the range 1 to 168
Carrier size must be 24 or 31 channels

Gateway does not exist in table GATWYINV
PVG 5 1 GWC 3 1 24 sts/13/0/3/vt15/1/1/1
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
.>y
TUPLE ADDED

```

2.5.3.1.5 Table release history update

Release SN09 drop 2, feature A00012527: Initial release of this new table GWEPCARR.

2.5.3.1.6 Supplementary information

N/A

2.5.3.1.7 Translation verification and other tools

Table GWEPCARR does not impact translations. TABAUDIT tool is not supported as Update operation is not allowed for GWEPCARR table.

2.6 Software optionality control (SOC)

N/A

2.7 Element Management

Telco should continue to provision SESM as before.

2.8 User interface changes

The most basic improvement to OA&M made possible using carrier information in the CM is in the TTP. The CktLoc command is not currently supported for GWC trunks. This component shall support GWC for CktLoc and shall allow display of carrier information for the trunk member currently being posted.

2.8.1 MAPCI, TTP Level, CktLoc Command changes

Figure 7 Existing TTP Display with Modified CktLoc Command

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
AMDI	.	DLOG E	.	1 SPM	.	SYSB	57C..	.	SDM
M				*C*		CR C	*C*		M
TTP									
0 QUIT		POST	1 DELQ		BSYQ		DIG		
2 Post_		TTP 6-0000							
3 SEIZE		CKT TYPE	PM NO.		COM LANG	STA S R	DOT TE	RESULT	
4		2W S7 S7 GWC	15 12		TEST	0 INB			
5 BSY							R		
6 RTS									
7 TST									
8									
9 CktInfo									
10 CktLoc									
11 Hold		CktLoc							
12 NEXT		GW	Ckt Chnl						
13 RLS		PVG 57	1 1						
14 Ckt_									
15 Trnslvf_		GW Name							
16 StkSdr_		PVGRTP1023							
17 Pads		Endpoint Name							
18 Level_		STS/13/0/3/VT15/1/1/1/1							
ADMIN									
Time 15:59		>							

To access the CktLoc from the CI environment, enter:

```
>MAPCI;MTC;TRKS;TTP;
```

```
>Post g <Trunk>
```

```
>CktLoc
```

If the TID to carrier mapping is not present (Gateway and carrier entry not in GWEPCCARR Table), then the following error message will be displayed.

Figure 8 Error Message for CktLoc if gw and carrier Info not present in GWEPCCARR

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
AMDI	.	DLOG	E	1 SPM	.	SYSB	57C..	.	SDM
M				*C*		CR C	*C*		M
TTP									
0 QUIT		POST	1	DELQ		BSYQ	DIG		
2 Post_		TTP	6-0000						
3 SEIZE		CKT TYPE		PM NO.		COM LANG	STA S R	DOT TE	RESULT
4		2W S7 S7 GWC	7	12		TEST	0 INB		
5 BSY								R	
6 RTS									
7 TST									
8									
9 CktInfo									
10 CktLoc									
11 Hold		CktLoc							
12 NEXT		CARRIER INFO NOT PRESENT IN TABLE GWEPCCARR							
13 RLS									
14 Ckt_									
15 Trnslvf_									
16 StkSdr_									
17 Pads									
18 Level_									
ADMIN									
Time 15:59									>

2.9 OSSGate Interface Changes

N/A

2.10 Security

N/A

2.11 Configuration Walkthrough

The craftsperson has to manually look into the SESM datafill and then provision tables GATWYINV and GWEPCCARR in core.

Given below are the SESM data and the corresponding core datafills that needs to be done.

Figure 9 Gateway information in SESM

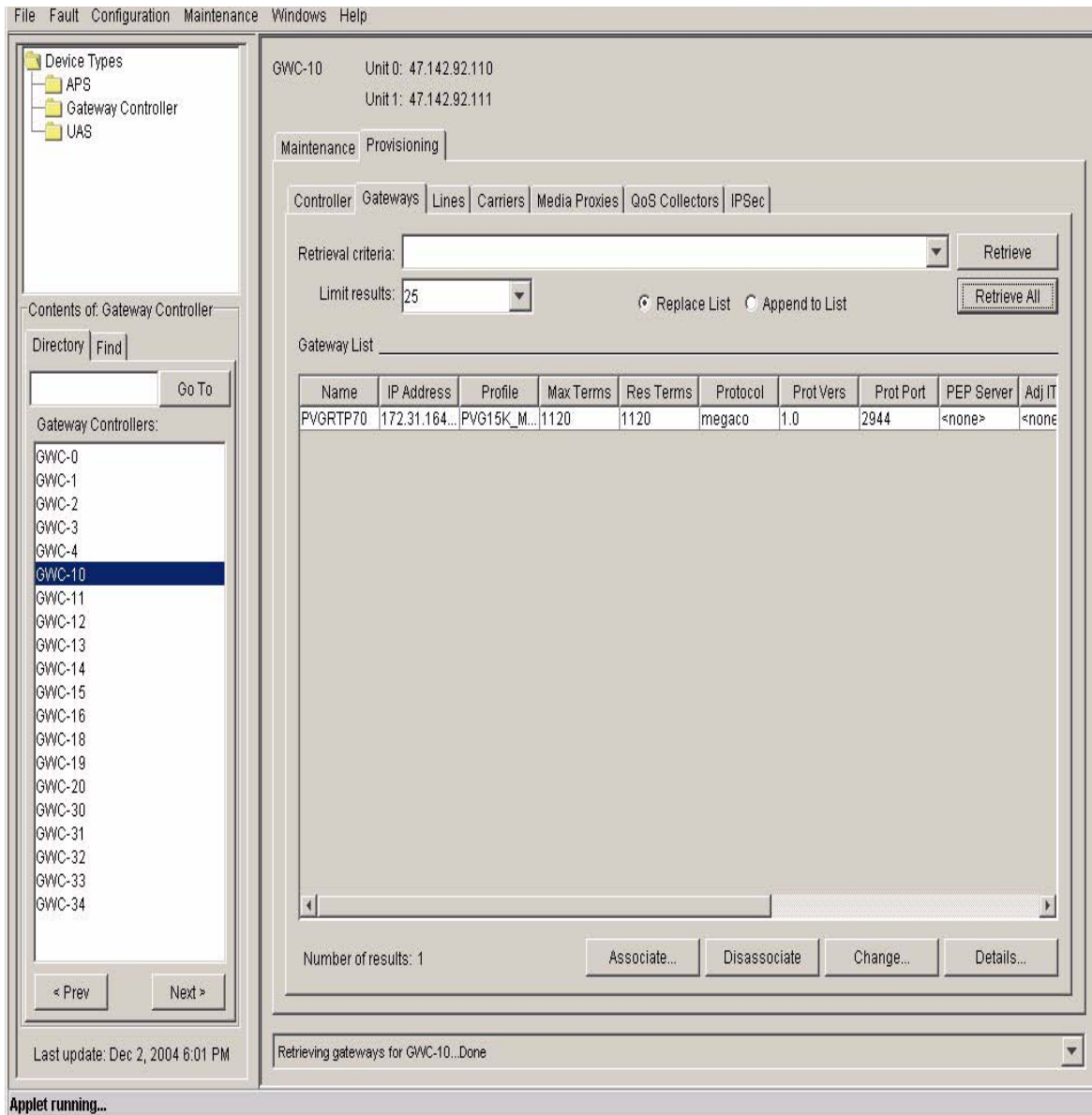


Figure 10 Table GATWYINV - Sample tuple

GTWY	PMNO	GTWYPRFL	GTWYNAME	GTWYADDR	GTWYCSPM	GTWYOPTS
PVG	5	PVGPRF	PVGRTP70	(172 31 164 1) \$	HOST GWC 10	\$

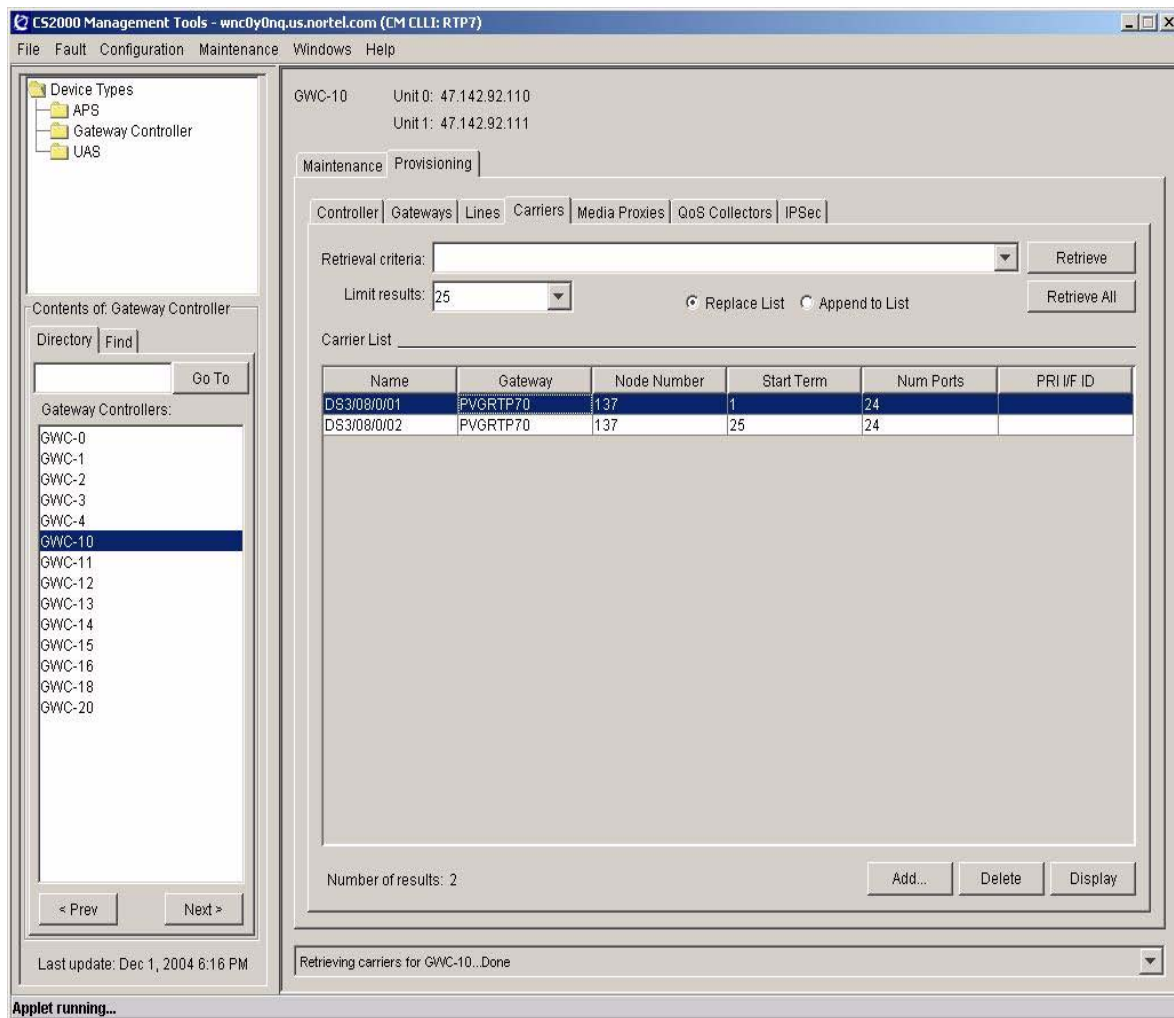
Figure 11 Carrier information in SESM**Figure 12 Table GWEPCCARR - sample tuples**

TABLE GWEPCCARR:					
GWCARR		HOST	START	CARRSIZE	CARRNAME
PVG 1 1		GWC 10	1	24	DS3/08/0/02

Product = CS 2000

A00012569--NI2 PRI/ ISUP UUI over SCAI

Functional Description

1: Applicable Solution(s)

PT-IP, SE10

1.1 Description

1.1.1 User-to-User Service (UUI) Information Element (IE)

The PRI User-to-User Signalling (UUS) supplementary service enables a user to send/receive a limited amount of information to/from another user. This information is passed transparently without modification of content through the network over the signalling channel in association with the call.

UUS allows communication of ISDN users by transferring user-to-user information (UUI) during call establishment, call confirmation and/or call clearing phases of a call, within call control messages. Maximum 128 octets of user-to-user information can be transferred in each message. The UUI is already supported in Setup message for PRI NI2 GWC trunks.

This feature will support UUI for Setup Q931 messages i.e call establishment phase for

- DTCI and SPM peripherals for NI2 PRI trunk
 - GWC, SPM and DTCI peripherals for NTNA PRI Trunks
- UUS option will be enabled by datafilling in table LTDATA.

The UUI data from the setup will be tandemmed to ISUP IAM (Initial address message) without any modification to the UUI data field. Similarly, UUI data from the ISUP IAM will be tandemmed to PRI setup message without any modification to the UUI field.

1.1.2 UUI over SCAI

SCAI (Switch Computer Application Interface) is a messaging link provided by the CS2K to a host computer. The information carried across the X.25/TCP-IP link allows applications running on the CS2K to communicate with applications running on the host computer.

This feature will support delivery of UUI in the following SCAI messages:

- DV_Call_Received_C
- DV_Call_Queued_U

- DV_Call_Offered_U

In order to support UUI, the size of outgoing ICM messages will be increased from 256 bytes to 512 bytes. The support of UUI over the SCAI link will be supported only for SCAI19 and later service versions.

1.2 User-to-User Service (UUI) Information Element (IE)

1.2.1 Functional overview

In order to provide the User to User service on an NI2 PRI / NTNA PRI variant, two levels of requirements need to be met.

- There are 2 possibilities of UUS subscription, “Required” or “Preferred”. This feature will support only “Preferred” subscription.
- The second level is the request for a call. This is accomplished by the presence of a UUI IE in a received SETUP message.

The user to user data in any subsequent messages (Alert, Connect & Disconnect) is discarded.

This feature supports only the “Preferred UUS” option. The UUS is an existing option in table LTDATA.

User-to-User Service (UUS) starts with UUS option datafilled against a given LTID in table LTDATA. The UUS option is already available for tuples in table LTDATA. At present, it is enabled for NI-2 LTIDS on GWC. This feature enables UUS as an option for NI-2 LTIDs on SPM and XPM(DTCI). The Feature also supports UUS as an option for NTNA PRI LTIDs on SPM, XPM(DTCI) and GWC.

A call initiated with a Q.931 SETUP message having no UUI IE proceeds as non-UUS call.

This feature also supports mapping of UUI and UUS related messages for the following interworking:

- NI-2 PRI to/from NI-2 PRI
- NI-2 PRI to/from ANSI ISUP
- NTNA PRI to/from NTNA PRI
- NI-2 PRI to NTNA PRI

This feature will support UUS for NI-2 variant PRI and NTNA PRI100 variant on the following peripherals:

- A legacy XPM (DTCI)
- A SPM (DMSCP/MG4K)

- A GWC that hosts an H.248 trunk GW (PVG)

1.2.2 Delivery of UUS:

The Subscription of UUS has the following two possibilities:

- Preferred UUS
- Required UUS

1.2.2.1 Preferred UUS

Preferred UUS indicates that originating ISDN user can send a UUI IE in the Q.931 SETUP message to activate the service. If the UUI IE cannot be delivered to the far end user, due to a failure scenario the call continues without UUS active.

Preferred UUS subscription is obtained by datafilling table LTDATA with service option 'UUS' as shown in example below.

Preferred UUS will be supported by this feature.

Figure 1 External view of tuple in Table LTDATA with Preferred option

TABLE LTDATA

LTDKEY LTDRSLT

ISDN 641 SERV SERV N N ALWAYS ALWAYS (UUS) \$

1.2.2.2 Required UUS

REQUIRED UUS indicates that the originating ISDN user can send an UUI IE in the Q.931 SETUP message to activate the service. If the UUI IE cannot be delivered to the far end user due to a failure scenario, the call is cleared at the originating switch.

REQUIRED UUS will not be supported as part of this feature.

1.2.3 Message Protocols

1.2.3.1 ISDN UUI IE

The ISDN User to User Information Element structure is based upon the CCITT Recommendation Q.931 ISDN user-network interface layer 3 specification. The ISDN User to User Information Element structure will be as follows:

Table 1 User-user information element, coded #7E

Byte	8	7	6	5	4	3	2	1
1	0	1	1	1	1	1	1	0
User-User Information Element Identifier								
2	Length of user-user contents							
3	Protocol Discriminator							
4	User Information							
:	:							
n	:							

- “n” can be a maximum of 131 bytes, which means up to 128 bytes of user information may be included.
- Protocol Discriminator is coded as 0 0 0 0 0 0 0 0 to indicate User Specific protocol.
- The User to User Information Element must be at least 3 bytes long in order for the UUS functionality to be invoked.
- The length of the UUI IE information is not regarded in the above 3 bytes limit check. Thus the presence of the first three bytes is mandatory for the UUI IE to be accepted.

1.2.3.2 User-to-User information parameter (UUI) on ISUP

The purpose of the User-to-user information parameter is to convey information between ISDN users. This information is not interpreted by the network, but rather is carried transparently and delivered to the remote user(s).

The format of the user-to-user information parameter is shown in the table below:

Table 2 User-user information parameter, coded #20

	8	7	6	5	4	3	2	1
1	User-user							
	0	0	1	0	0	0	0	0
	Information Parameter Identifier							
2	Length of user-user contents							
3	Protocol discriminator							
4etc	User information							

1.2.4 PRI to PRI/ISUP messaging

The UUS functionality is requested by including UUI IE in the SETUP message. When the originating CS2K receives the UUI IE in the SETUP message, table LTDATA static data will be checked. If Table LTDATA is NOT datafilled to support Preferred UUS, then the UUI IE will be stripped from the SETUP message and a STATUS message with Cause value of 50 “Requested Facility Not Subscribed” will be sent to the originator and the call will continue. If table LTDATA is datafilled to support Preferred UUS, then the ISDN UUI IE in the SETUP message will be carried across the network, the UUI IE will be mapped to the SETUP message for PRI to PRI calls and delivered to the ISDN end user.

The UUI data from the setup will be tandemed to ISUP IAM (Initial address message) without any modification to the UUI data field. Similarly, UUI data from the ISUP IAM will be tandemed to PRI setup message without any modification to the UUI field.

1.2.5 Preferred UUS Behavior

The Preferred UUS functionality will be requested by including UUI IE in the Q.931 SETUP message. When the Originator receives the UUI IE in the Q.931 SETUP message, Table LTDATA static data will be checked for subscription.

- **Preferred UUS Provisioning Phase:**

If table LTDATA is datafilled to support Preferred UUS, then the UUI IE in the Q.931 SETUP message will be carried across the network. The UUI IE will be mapped to the Q.931 SETUP message for PRI to PRI calls and/or PRI to ISUP calls, delivered to the end user.

- **Preferred UUS Call Request Phase:**

A call with specific parameters is requested by the calling party. If the (calling party) Originator sending the Q.931 setup message containing the UUI parameter, and if the Originator subscribes to the UUS service, then the UUI is mapped to SCP_X_Originate message. Otherwise the PM (DTCI, XPM, SPM) will send a Q.931 STATUS message to the Originator to indicate that the UUS facility was NOT subscribed. The Q.931 STATUS message with Cause value of 50 “Requested Facility Not Subscribed” will be sent to the originator and the call will continue without the UUI information.

Table 3 Error Scenario Handling

EVENT	ACTION BY SPCS/CS2K
UUS in Setup, but calling party has not subscribed to UUS option in LTDATA table.	Discard UUS; return STATUS (cause #50) to calling party; continue call processing
UUS in SETUP cannot be further conveyed due to unsupported signaling. (Delivery of UUS is "Preferred")	Discard UUS; continue call processing; return STATUS (cause #69) to calling party.
User-User Information Element too long (excessive of 131 octets)	Discard UUS; continue call processing; Return STATUS (cause #43) to sending party
UUS in CONNect,	Discard UUS; continue call processing;
UUS in DISConnect,	Discard UUS
UUS is present in an inappropriate clearing message (RELease)	Discard UUS; return RELease COMplete (cause #43) to sending party; continue call clearing
SETUP message length exceeds maximum supported number of octets	Discard UUS; continue call processing; return STATUS (cause #43) to sending party

1.2.6 Information Element and Parameter Summary

A 'X' in Table 4 indicates that the IE, or parameter, can be included in the message identified in the column on the left. A blank entry indicates inclusion of the IE, or parameter, is invalid or not applicable.

Table 4 Information Element and Parameter Summary

Message	UII IE	UII Parm	Notes	UII Supported
Setup (SETUP)	X		Call Request message	Yes
Alerting (ALERT)	X			No
Connect (CONNECT)	X		Call Confirmation message	No
Disconnect (DISC)	X		Call clearing message	No
Initial Address Message (IAM)		X	Call Request message	Yes
Address Complete Message (ACM)		X		Yes
Answer Message (ANM)		X	Call Confirmation message	Yes
Release (ISUP REL)		X	Call Clearing message	Yes

1.2.7 Hardware Requirements or Dependencies

None.

1.2.8 Limitations and restrictions

- The maximum length supported for the ISDN UII IE is 131 bytes.
- The maximum length supported for the ISUP UII Parameter is 131 bytes.
- The scope of this feature is limited to UUS enhancement for NI-2 PRI variant and NTNA PRI variant only.
- Only “Preferred” UUS option is supported by this feature.
- The protocol specifics outlined in this document reflect UUS for the Nortel North American PRI variant (NI-2 PRI and NTNA DMS PRI) only.
- The CS2K validates UUS subscription for ISDN PRI call originations only.
- When the CS2K receives a UII IE in a message that does not support UII, the CS2K sends a Q.931 STATUS message response.
- When the CS2K discards the UII IE from a Q.931 message, indication of this is only communicated to the far end (FE) of the PRI. Indication that the UII IE was discarded (a Q.931 STATUS message) is not propagated along adjacent PRI trunk connections.

1.3 UII over SCAI

1.3.1 Description

The first PRI SETUP message (Initial Address message; IAM in the case of ISUP) sent from the originating switch can contain UII (User to User Information) parameter. The UII is used by the terminating switch as call related data.

This feature ensures that UII arriving over the following trunks is delivered to the ICM environment.

1. NI2 PRI
2. NTNA PRI
3. ANSI ISUP

This activity will provide the UII in ICM messages for the following agent types:

1. ACD agents
2. MDC agents
3. RES agents.

UUI IE from CS2K to the SCAI host will only be reflected in all the will be in every DV_Call_Queued_U, DV_Call_Offered_U and DV_Call_Received_C message.

1.3.2 Modified ICM Messages

This feature introduces a new parameter, namely **UIIPARM** in the following ICM call related messages.

- DV_Call_Queued_U
- DV_Call_Offered_U
- DV_Call_Received_C

The ASN.1 notations for the above mentioned three messages for ACD customer provided by this activity are shown in this section. The length fields are variable because the length depends on the variable contents. The tag values are taken from the Remote Operation Service Element (ROSE) protocol.

The maximum length of UUI supported by the new parameter is 128 bytes. The new parameter will show up in the above said messages on the basis of the appropriate subscription which will be discussed later.

The UUI is supported in the above-mentioned four messages for a SCAI-monitored terminator only.

- **SCAI19 Service Version**

- The ICM application Logon message contains a parameter; service Version, which is used to identify the stream of messages which will be allowed across the link. This service version is used as a method of protecting the integrity of host applications which choose not to upgrade their software to accept new message types after a switch has been upgraded to a new service version.
- The new service version SCAI19 needs to be added to the current list of SCAI service versions to receive modified messages with new parameter. The new service version is accepted at application logon processing time. The processing of individual messages which are introducing new encoding / decoding, adheres to the Service Version of ICM.

***Note:** The parameters which are **italicized and bold** are new to these messages. The letter 'U' in the message name indicates that the message is unconfirmed, i.e., this operation requires no outcome to be reported by the host. The letter 'C' at the end of the message's name indicates that the message requires confirmation from the host.*

1.3.2.1 DV_Call_Queued_U message

The switch sends this Remote Operation of Class 5 to the host when a call to an ACD DN associated with the current session is received by the switch and placed in the Incoming Call Queue.

1.3.2.1.1 Changed DV_Call_Queued_U ASN.1 definition.**ASN.1 Encoding**

```

dv-CALL-QUEUED-U ARGUMENT      OPERATION

                                ARGUMENT CallQueuedArgument ::=
6
                                SEQUENCE
                                {
                                networkCallID      [0] IMPLICIT SEQUENCE
                                {
                                networkNodeID      [0] IMPLICIT INTEGER OPTIONAL,
                                localCallID        [1] IMPLICIT INTEGER OPTIONAL}
                                OPTIONAL,

                                acdDN              [1] IMPLICIT OCTET STRING OPTIONAL,
                                origCallingNumber  [2] IMPLICIT OCTET STRING OPTIONAL,
                                origChargeNumber  [3] IMPLICIT OCTET STRING OPTIONAL,
                                callHistoryInfo    [4] IMPLICIT SEQUENCE

                                { callType          [0] IMPLICIT ENUMERATED
                                {
                                callTransferred    (1),
                                callOverflowed      (2),
                                callRedirected      (3),
                                callForwarded      (4),
                                callConsult        (5),
                                callConference      (6),
                                callReturnedToQueue (7),
                                callRouted          (8)} OPTIONAL,

                                origInboundDN      [1] IMPLICIT OCTET STRING OPTIONAL,
                                prevApplicationID  [2] IMPLICIT INTEGER OPTIONAL,
                                hostCallData       [3] IMPLICIT OCTET STRING OPTIONAL}
                                OPTIONAL,

                                acdGroup           [5] AddressType OPTIONAL,
                                forwardingParty    [6] ForwardingPartyType OPTIONAL,
                                cpadigs           [7] IMPLICIT OCTET STRING OPTIONAL
                                uuiParameter      [8] IMPLICIT OCTET STRING OPTIONAL

                                AddressType:: = CHOICE
                                {
                                positionID        [0] IMPLICIT INTEGER,

```

dialedDigits [1] IMPLICIT IA5STRING,
stationNumber [2] IMPLICIT OCTET STRING,
q931Address [3] Q931AddressType}

Q931 AddressType ::= SEQUENCE
{ numberTypeNumberPlan [0] OCTET STRING OPTIONAL,
presentationScreeningIndicator [1] OCTET STRING OPTIONAL,
digits [2] IA5 STRING OPTIONAL }

ForwardingPartyType ::= IMPLICIT SEQUENCE
{ firstFwdNumber [0] AddressType OPTIONAL,
firstFwdReason [1] IMPLICIT ENUMERATED
{ unknown (0),
userBusy (1),
noReply (2),
unconditional (3) } OPTIONAL,
lastFwdNumber [2] AddressType OPTIONAL,
lastFwdReason [3] IMPLICIT ENUMERATED
{ unknown (0),
userBusy (1),
noReply (2),
unconditional (3) } OPTIONAL },

1.3.2.1.2 DV_Call_Queued_U:Coded example.

An ACD call has been initiated from the OrigCallingNumber 6136217703 with UI '01 02 03 04 05 06 07 08 09 0a', by dialing 6134444444 and assigned a LocalCallID = 13, and offered it to an ACD group with Primary DN 6136212111, for which no agent is available, the call is placed in the Incoming Call Queue and the switch sends DV-CALL-QUEUED-U to the host. No Return Result is required or received by the switch from the host.

INVOKE

CS2K =====> HOST

Hex Dump			Information Element	Comments
Tag	Length	Content		
a1	54		INVOKE	Message length is 84 bytes decimal
02	02	03 ff	InvokeID	The InvokeID is 1023
02	01	06	Operation	Operation value for DV-CALL-QUEUED-U is decimal 6
30	4b		Argument	CallQueued argument is of Sequence type and is 75 bytes long decimal

Hex Dump			Information Element	Comments
Tag	Length	Content		
a0	09		NetworkCallId	The NetworkCallId is a constructor of 9 bytes long
80	04	03 38 d0 90	NetworkNodeId	The NetworkNodeId is 54055056
81	01	0d	LocalCallId	The LocalCallId is 13
81	0a	36 31 33 36 32 31 32 31 31 31	ACDDN	The called ACDDN of the Group is 6136212111
82	0c	00 83 36 31 33 36 32 31 37 37 30 33	Original Calling Number	The first 2 bytes are fixed and must not be read at present. The original calling number is 6136217703
A5	0c		Acd group	The ACDGroup is of type Constructor and is 12 bytes long
82	0a	36 31 33 36 32 31 32 31 31 31	Station number	The station number of the ACDGroup is 6136212111
87	0a	36 31 33 34 34 34 34 34 34 34	CPADIGS	The CPA value is 6134444444
88	0a	01 02 03 04 05 06 07 08 09 0a	UII	The UII IE data is '01 02 03 04 05 06 07 08 09 0a'.
Hex Dump= a1 54 02 02 03 ff 02 01 06 30 4b a0 09 80 04 03 38 d0 90 81 01 0d 81 0a 36 31 33 36 32 31 32 31 31 31 82 0c 00 83 36 31 33 36 32 31 37 37 30 33 a5 0c 82 0a 36 31 33 36 32 31 32 31 31 31 87 0a 36 31 33 34 34 34 34 34 34 34 34 88 0a 01 02 03 04 05 06 07 08 09 0a				

1.3.2.2 DV_Call_Offered_U message

This section describes the DV-CALL-OFFERED-U message the switch uses to notify the host that a ICM Party has been selected for ACD. The party has been selected to handle an incoming call to one of the DNs belonging to the associated environment of the current switch-host session when the call is about to be offered to the ICM Party.

1.3.2.2.1 Changed DV_Call_Offered_U ASN.1 definition.

ASN.1 Encoding

dv-CALL-OFFERED-U	OPERATION
	ARGUMENT CallOfferedArgument ::= 5
CallOfferedArgument	::= SEQUENCE
{ networkCallID	[0] IMPLICIT SEQUENCE
{ networkNodeID	[0] IMPLICIT INTEGER OPTIONAL,
localCallID	[1] IMPLICIT INTEGER OPTIONAL}
	OPTIONAL,
acdDN	[2] IMPLICIT OCTET STRING OPTIONAL,
origCallingNumber	[3] IMPLICIT OCTET STRING OPTIONAL,
origChargeNumber	[4] IMPLICIT OCTET STRING OPTIONAL,
callHistoryInfo	[5] IMPLICIT SEQUENCE
{ callType	[0] IMPLICIT ENUMERATED
{ callTransferred	(1),
callOverflowed	(2),
callRedirected	(3),
callForwarded	(4)
callConsult	(5),
callConference	(6),
callReturnedToQueue	(7),
callRouted	(8)} OPTIONAL,
origInboundDN	[1] IMPLICIT DeviceAddressType OPTIONAL,
prevApplicationID	[2] IMPLICIT INTEGER OPTIONAL,
hostCallData	[3] IMPLICIT OCTET STRING OPTIONAL}
	OPTIONAL,
acdGroup	[6] AddressType OPTIONAL,
callMode	[7] IMPLICIT ENUMERATED
{ callWaited	(1)} OPTIONAL,
destDeviceID	[8] AddressType OPTIONAL,
forwardingParty	[9] ForwardingPartyType OPTIONAL,
cpadigs	[10] IMPLICIT OCTET STRING OPTIONAL
uuiParameter	[11]IMPLICIT OCTET STRING OPTIONAL}
AddressType	::= CHOICE
{ positionID	[0] IMPLICIT INTEGER,
dialedDigits	[1] IMPLICIT IA5STRING,
stationNumber	[2] IMPLICIT OCTET STRING,

q931Address [3] Q931AddressType}

Q931AddressType ::= SEQUENCE
 { numberTypeNumberPlan [0] OCTET STRING OPTIONAL,
 presentationScreeningIndicator [1] OCTET STRING OPTIONAL,
 digits [2] IA5 STRING OPTIONAL }

ForwardingPartyType ::= IMPLICIT SEQUENCE
 { firstFwdNumber [0] AddressType OPTIONAL,
 firstFwdReason [1] IMPLICIT ENUMERATED
 { unknown (0),
 userBusy (1),
 noReply (2),
 unconditional (3) } OPTIONAL,

lastFwdNumber [2] AddressType OPTIONAL,
 lastFwdReason [3] IMPLICIT ENUMERATED
 { unknown (0),
 userBusy (1),
 noReply (2),
 unconditional (3) } OPTIONAL }

1.3.2.2.2 DV_Call_Offered_U: Coded example.

An ACD call is initiated from the OrigCallingNumber 6136217703 with UUI '01 02 03 04 05 06 07 08 09 0a' in setup message by dialing 6134444444 and is assigned a LocalCallID = 9. The call is offered to an acd agent with posid 7707 of the acd group with primary DN 613621111. The switch sends DV-CALL-OFFERED-U to the host. No Return Result is required or received by the switch from the host.

INVOKE

CS2K =====> HOST

Hex Dump			Information Element	Comments
Tag	Length	Content		
a1	5a		INVOKE	this message is 90 bytes decimal
02	02	03 f9	InvokeID	the InvokeID is 1017
02	01	05	Operation	the operation is DV-CALL-OFFERED-U [5]
30	51		Argument	CallOffered argument is of Sequence type and is 81 bytes long decimal
a0	09		NetworkCallId	The NetworkCallId is a constructor 9 bytes

Hex Dump			Information Element	Comments
Tag	Length	Content		
80	04	03 38 d0 90	NetworkNodeId	The NetworkNodeId is 54055056
81	01	09	LocalCallId	The LocalCallId is 9 decimal
82	0a	36 31 33 36 32 31 32 31 31 31	acd_dn	6136212111
83	0c	00 83 36 31 33 36 32 31 37 37 30 33	OrigCallingNumber	The first two bytes are fixed and presently must not be read. The customer's OrigCallingNumber is 6136217703
a6	0c		acd_grp	
82	0a	36 31 33 36 32 31 32 31 31 31	StationNumber	The called DN is 6136212111
a8	04		DeviceID	The DeviceID is of type Constructor and is 4 bytes long
80	02	1e 1b	pos_id_2	7707
8a	0a	36 31 33 34 34 34 34 34 34 34	CPADIGS	The CPA value is 6134444444
8b	0a	01 02 03 04 05 06 07 08 09 0a	UUI	The UUI IE data is '01 02 03 04 05 06 07 08 09 0a'.
Hex Dump = a1 5a 02 02 03 f9 02 01 05 30 51 a0 09 80 04 03 38 d0 90 81 01 09 82 0a 36 31 33 36 32 31 32 31 31 31 83 0c 00 83 36 31 33 36 32 31 37 37 30 33 a6 0c 82 0a 36 31 33 36 32 31 32 31 31 31 a8 04 80 02 1e 1b 8a 0a 36 31 33 34 34 34 34 34 34 34 34 8b 0a 01 02 03 04 05 06 07 08 09 0a				

1.3.2.3 DV_Call_Received_C message

The switch uses the DV-CALL-RECEIVED-C message to notify the host that a call to an ACD group belonging to an Associated environment with which the host has an established session has been received. This allows the host to "redirect" the call.

1.3.2.3.1 Changed DV_CALL_Received_C ASN.1 definition.

ASN.1 Encoding

dv-CALL-RECEIVED-C	OPERATION
	ARGUMENT CallReceivedArgument
	RESULT
	ERRORS {call-Received-Error}
	LINKED {dv-CALL-REDIRECT} ::=
10	
CallReceivedArgument	::= SEQUENCE
{networkCallID	[0] IMPLICIT SEQUENCE
{networkNodeID	[0] IMPLICIT INTEGER OPTIONAL,
localCallID	[1] IMPLICIT INTEGER OPTIONAL}
	OPTIONAL,
acdDN	[1] IMPLICIT OCTET STRING OPTIONAL,
origCallingNumber	[2] IMPLICIT OCTET STRING OPTIONAL,
origChargeNumber	[3] IMPLICIT OCTET STRING OPTIONAL,
callHistoryInfo	[4] IMPLICIT SEQUENCE
{callType	[0] IMPLICIT ENUMERATED
{callTransferred	(1),
callOverflowed	(2),
callRedirected	(3),
callForwarded	(4)
callConsult	(5),
callConference	(6),
callReturnedToQueue	(7),
callRouted	(8)} OPTIONAL,
origInboundDN	[1]
IMPLICIT OCTET STRING	
OPTIONAL,	
prevApplicationID	[2] IMPLICIT INTEGER OPTIONAL,
hostCallData	[3] IMPLICIT OCTET STRING
	OPTIONAL}
	OPTIONAL,
acdGroup	[5] AddressType OPTIONAL,
forwardingParty	[6] ForwardingPartyType OPTIONAL,
cpadigs	[7]IMPLICIT OCTET STRING OPTIONAL
<i>uuiParameter</i>	<i>[8]IMPLICIT OCTET STRING</i>
<i>OPTIONAL}</i>	
AddressType	::= CHOICE
{positionID	[0] IMPLICIT INTEGER,
dialedDigits	[1] IMPLICIT IA5STRING,
stationNumber	[2] IMPLICIT OCTET STRING,
q931Address	[3] Q931AddressType}
Q931AddressType	::= SEQUENCE

```

{ numberTypeNumberPlan      [0] OCTET STRING OPTIONAL,
  presentationScreeningIndicator [1] OCTET STRING OPTIONAL,
  digits                     [2] IA5 STRING OPTIONAL }

```

```

ForwardingPartyType      ::= IMPLICIT SEQUENCE
{ firstFwdNumber          [0] AddressType OPTIONAL,
  firstFwdReason          [1] IMPLICIT ENUMERATED
    { unknown             (0),
      userBusy            (1),
      noReply             (2),
      unconditional       (3) } OPTIONAL,
  lastFwdNumber           [2] AddressType OPTIONAL,
  lastFwdReason           [3] IMPLICIT ENUMERATED
    { unknown             (0),
      userBusy            (1),
      noReply             (2),
      unconditional       (3) } OPTIONAL }

```

call-Received-ErrorERROR ::= 0

1.3.2.3.2 DV_Call_Received_C: Coded example.

An ACD call has been initiated from the OrigCallingNumber 9192466001, with UII in setup by dialing 9197224444 and assigns a LocalCallID = 4 to the call meant for ACD group with Primary DN of the ACD group =9194815200. The switch sends DV-CALL-RECEIVED-C message to the host which responds with either Return Result message or Return Error message.

INVOKE CS2K =====> HOST

Hex Dump			Information Element	Comments
Tag	Length	Content		
a1	51		INVOKE	this message is 81 bytes decimal
02	02	03 f9	InvokeID	the InvokeID is 1017 decimal
02	01	0a	Operation	the operation is DV-CALL-RECIEVED-C[10] decimal
30	48		Argument	CallReceived argument is of Sequence type and is 72 bytes long decimal
a0	06		NetworkCallId	the NetworkCallId is a constructor 6 bytes
80	01	00	NetworkNodeId	the NetworkNodeid is 0
81	01	04	LocalCallId	the LocalCallId is 4

Hex Dump			Information Element	Comments
Tag	Length	Content		
81	0a	39 31 39 34 38 31 35 32 30 30	ACDDN	the called ACDDN is 9194815200
82	0c	00 83 39 31 39 32 34 36 36 30 30 31	OrigCallNumber	the first two bytes are fixed and presently unused. The customer's OrigCallNumber is 9192466001
a5	0c		ACDGroup	the ACDGroup is a type constructor 12 bytes
82	0a	39 31 39 34 38 31 35 32 30 30	StationNumber	the customer group's Primary ACDDN is 9194815200
87	0a	39 31 39 37 32 32 34 34 34 34	CPADIGS	The CPA value is 9197224444
88	0a	01 02 03 04 05 06 07 08 09 0a	UII	The UII IE data is '01 02 03 04 05 06 07 08 09 0a'
Hex Dump= a1 51 02 02 03 f9 02 01 0a 30 48 a0 06 80 01 00 81 01 04 81 0a 39 31 39 34 38 31 35 32 30 30 82 0c 00 83 39 31 39 32 34 36 36 30 30 31 a5 0c 82 0a 39 31 39 34 38 31 35 32 30 30 87 0a 36 31 33 37 32 32 34 34 34 34 88 0a 01 02 03 04 05 06 07 08 09 0a				

1.3.3 Size expansion of ICM messages

The size of outgoing ICM messages will be increased from the existing 256 bytes to 512 bytes. The increased size will be available for TCP/IP link set only. For X.25 link sets, the maximum available size will be 241 bytes.

If the size of a message with UII parameter becomes greater than 241 bytes in X.25 link set, then the UII will be discarded from the message and the message will be sent with the remaining parameters. In such scenarios, a SCAI LOG 304 will be generated indicating the removal of UII.

Note: It is recommended to upgrade from X.25 to TCP/IP to get the full use of UII over the SCAI link.

1.3.4 Subscription

The following changes in table SCAISSRV are required to provide subscription to receive ICM messages with the new parameter. Preconditions to be satisfied by a party in order to receive all the messages with new parameter are also given in this section.

1.3.4.1 Changes in table SCAISSRV

The changes in table SCAISSRV are made for the following SCAI messages:

- DV_Call_Received_C
- DV_Call_Queued_U
- DV_Call_Offered_U

An optional parameter UIIPARM is added to the existing parameters in the function CALLQUED, CALLOFFR and CALLRE CDC which are present in the following categories: CTXEVENT, RESEVENT, ROUTING and ACDEVENT messages in table SCAISSRV.

During the software upgrade, the existing tuples of table SCAISSRV which are present in loads prior to the introduction of the aforementioned four tuples, would be modified by reformat procs during table transfer to reflect UIIPARM parameter in the functions CALLQUED, CALLOFFR and CALLRE CDC as 'N'.

Following are the sample tuples shown:

TABLE SCAISSRV SUBSERV SPROFILE

```
-----
ACDEVENT15$ ACDEVENT (CALLQUED Y Y Y Y Y Y Y Y Y Y Y Y N)
(CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y Y N)
(CALLANSWR Y Y Y Y Y Y Y Y Y Y Y Y Y)
(CALLREL Y Y Y Y Y Y Y) (AGTLGDIN Y Y Y) (AGTLGDOUT Y Y)
(AGTREADY Y Y)
(AGTNREADY Y Y N) (LOBEVENT Y Y Y) (EMKEVENT Y Y Y Y Y Y Y)
```

TABLE SCAISSRV
SUBSERV SPROFILE

ROUTING15\$ ROUTING (CALLRECD C Y Y Y Y Y Y Y Y Y Y Y Y **N**)
 (CALLREDIR Y Y Y) \$

A new default tuple CTXEVENT19\$ under category CTXEVENT will be created with the optional parameter UUIPARM of the function CALLOFFR set to Y. Prior to this, the latest default tuple in the category CTXEVENT is CTXEVENT13\$.

A new default tuple RESEVENT19\$ under category RESEVENT will be created with the optional parameter UUI of the function CALLOFFR set to Y. Prior to this, the latest default tuple in the category RESEVENT is RESEVENT13\$.

A new default tuple ROUTING19\$ under category ROUTING will be created with the optional parameter UUI of the function CALLRECD C set to Y. Prior to this, the latest default tuple in the category ROUTING is ROUTING15\$.

A new default tuple ACDEVENT19\$ under category ACDEVENT will be created with the optional parameter UUIPARM of the function CALLQUED, and CALLOFFR set to Y. Prior to this, the latest default tuple in the category ACDEVENT is ACDEVENT15\$.

Table 5 SCAISSRV table changes

Category	Function	Added Parameters	New/Same
CTXEVENT	CALLOFFR / CALLANSWR	UUIPARM	Old function and new parameter
RESEVENT	CALLOFFR / CALLANSWR	UUIPARM	Old function and new parameter
ROUTING	CALLRECD C	UUIPARM	Old function and new parameter
ACDEVENT	CALLQUED / CALLOFFR / CALLANSWR	UUIPARM	Old function and new parameter

TABLE SCAISSRV**SUBSERV SPROFILE**

```

-----
CTXEVENT19$ CTXEVENT (SETOFFHK Y Y Y)
(CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y)
(CALLANSWR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y) (CALLREL Y Y Y Y)
(CALLNAME Y Y Y Y Y) $

```

TABLE SCAISSRV**SUBSERV SPROFILE**

```

-----
RESEVENT19$ RESEVENT (SETOFFHK Y Y)
(CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y)
(CALLANSWR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y) (CALLREL Y Y Y)
(CALLNAME Y Y Y Y Y) $

```

TABLE SCAISSRV**SUBSERV SPROFILE**

```

-----
ROUTING19$ ROUTING (CALLRECDC Y Y Y Y Y Y Y Y Y Y Y Y Y Y)
(CALLREDIR Y Y Y) $

```

TABLE SCAISSRV**SUBSERV SPROFILE**

```

-----
ACDEVENT19$ ACDEVENT (CALLQUED Y Y Y Y Y Y Y Y Y Y Y Y Y Y)
(CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y)
(CALLANSWR Y Y Y Y Y Y Y Y Y Y Y Y Y Y)
(CALLREL Y Y Y Y Y Y Y) (AGTLGDIN Y Y Y) (AGTLGDOUT Y Y)
(AGTREADY Y Y)
(AGTNREADY Y Y N) (LOBEVENT Y Y Y) (EMKEVENT Y Y Y Y Y Y Y)

```

1.3.4.2 Preconditions to receive the modified ICM messages.

- The state SOC ICM00083 should be ON.
- A party must be a ACD DN or ECM associated in order to get the modified messages.
- The Service Version should at least be SCAI19.
- The ICM session on which the DV_Call_Queued_U message is to be sent with the new parameter must subscribe to the ACDEVENT category and CALLQUED function. Also the parameter **UIIPARM** in the function CALLQUED must be set to *Y*.
- The ICM session on which the DV_Call_Offered_U message is to be sent with the new parameter must subscribe to either ACDEVENT, CTXEVENT or RESEVENT category and CALLOFFR function. Also the parameter **UIIPARM** in the function CALLOFFR must be set to *Y* and **UIIPARM** in function CALLQUED and CALLRE CDC must be set to *N*.
- The ICM session on which the DV_Call_Received_C message are to be sent with the new parameter must subscribe to the ROUTING category and CALLRE CDC function. Also the parameter **UIIPARM** in the function CALLRE CDC must be set to *Y*.

1.3.5 Message Flow Scenarios

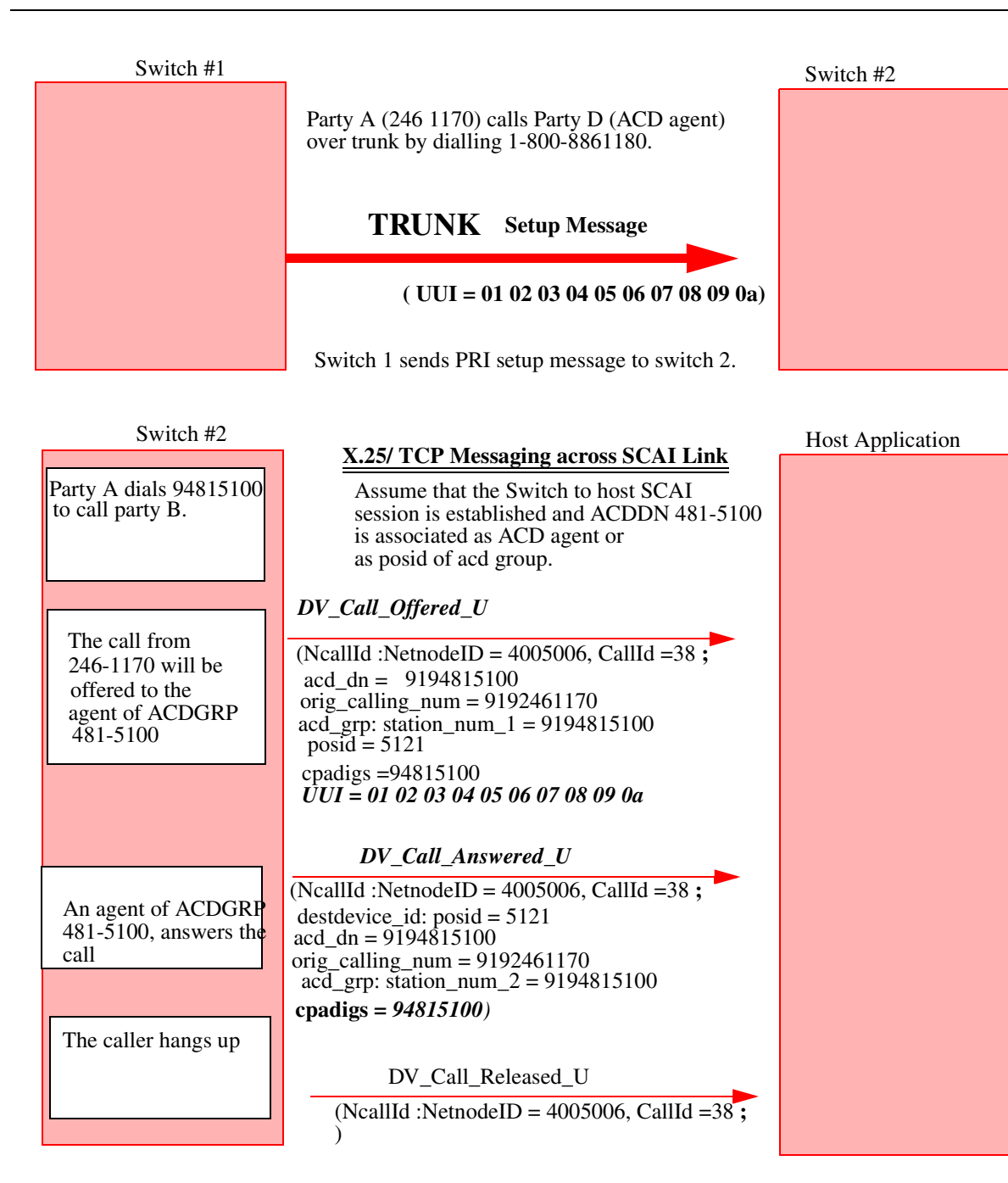
Consider some message flow scenarios to get better understanding of the feature. In all the scenarios mentioned below, assume the following, unless stated otherwise:

1. *Parties B, C and D are always ECM associated ACD/MDC/RES agents.*
2. *Parties B and C belong to same switch.*
3. *Party A is any agent that requires service from a call centre and may be on the same network or a different network.*
4. *All the preconditions mentioned in section Please refer to “1.3.4.2 Preconditions to receive the modified ICM messages.” on page 856. are satisfied by all the parties.*
5. *The modified messages are shown in bold and italics.*
6. *The messaging that remains the same may not been shown explicitly.*
7. *The term trunks mean any of the trunks mentioned in section Please refer to “1.3.1 Description” on page 842..*
8. *In all the scenarios, the statement ‘party A calls party B/D’ is to be interpreted as ‘party A dials to reach a call centre and the call terminates to agents B/D within that call centre’.*

1.3.5.1 Example 1: UII IE in DV_Call_Offered_U

Party A (2461170) calls party B (ACD agent of ACDGRP 4815100, posid: 5121) over PRI/ISUP trunk and party B answers.

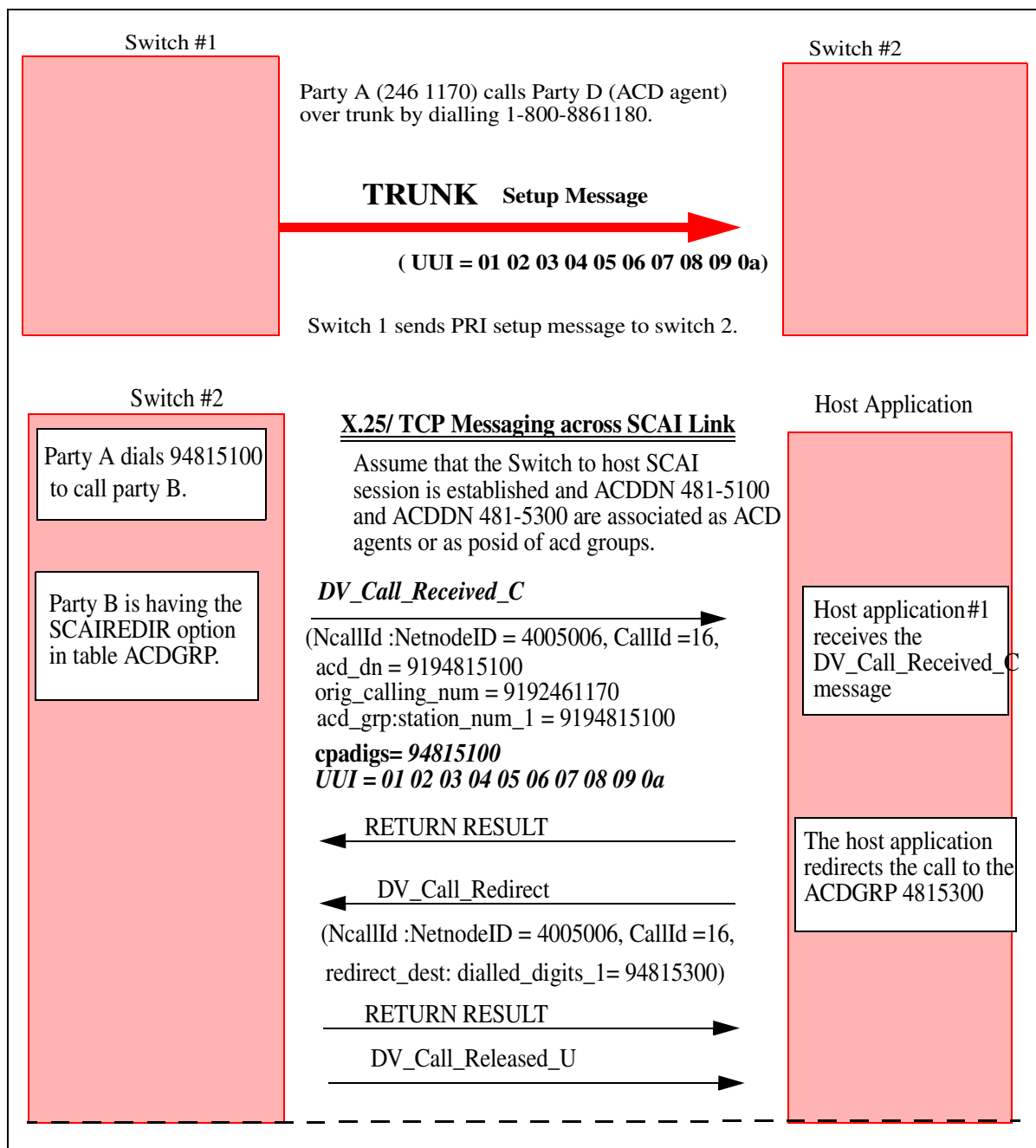
Figure 2 UII in DV_Call_Offered_U



1.3.5.2 Example 2: UII IE in DV_Call_Received_C message

Party A (2461170) calls party B (ACD agent of ACDGRP 4815100, posid: 5121) over PRI/ISUP trunk and party B answers.

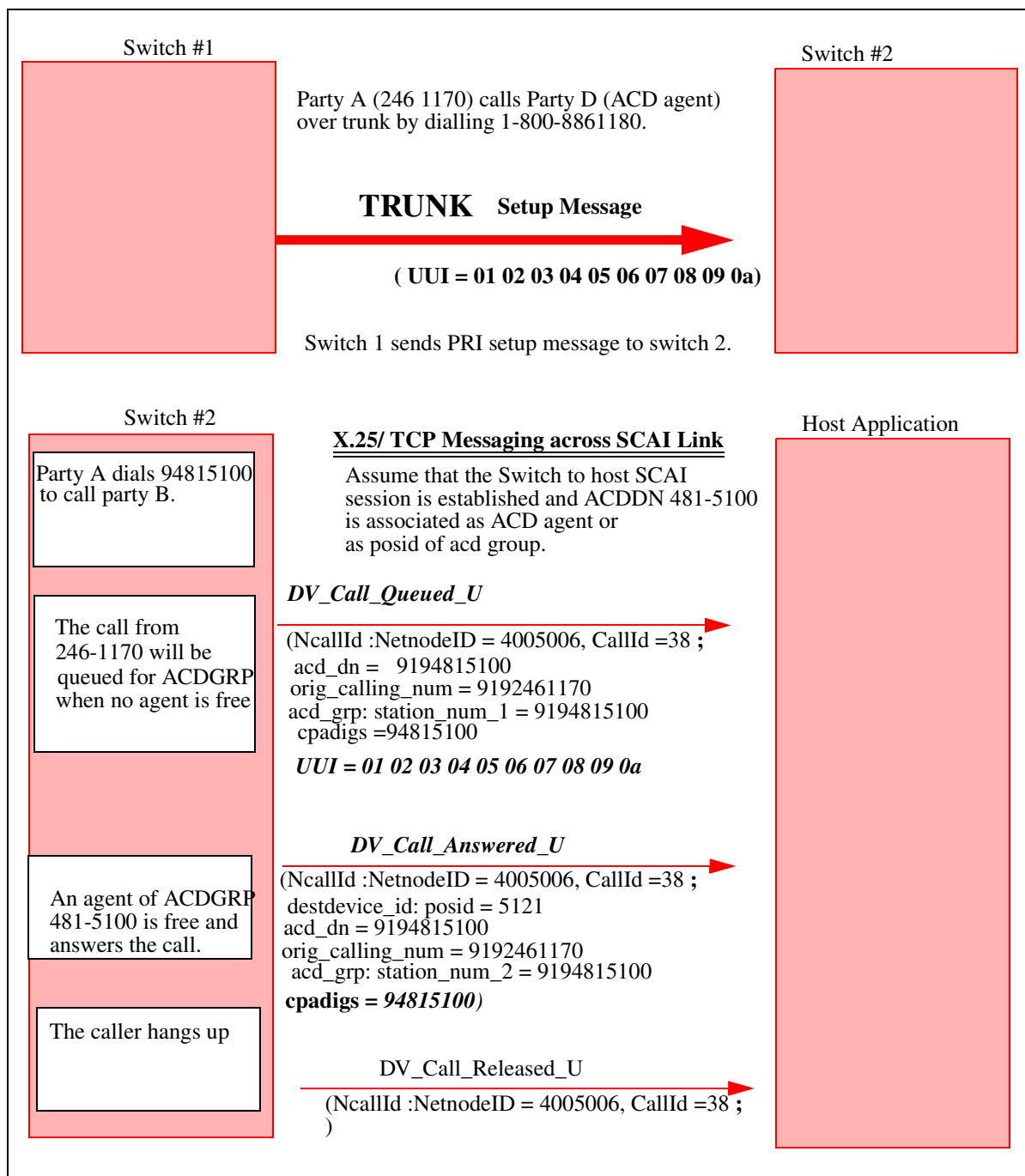
Figure 3 UII in DV_Call_Received_C message



1.3.5.3 Example 3: UII IE in DV_Call_Queued_U

Party A (2461170) calls party B (ACD agent of ACDGRP 4815100, posid: 5121) over ISUP/PRI and party B answers.

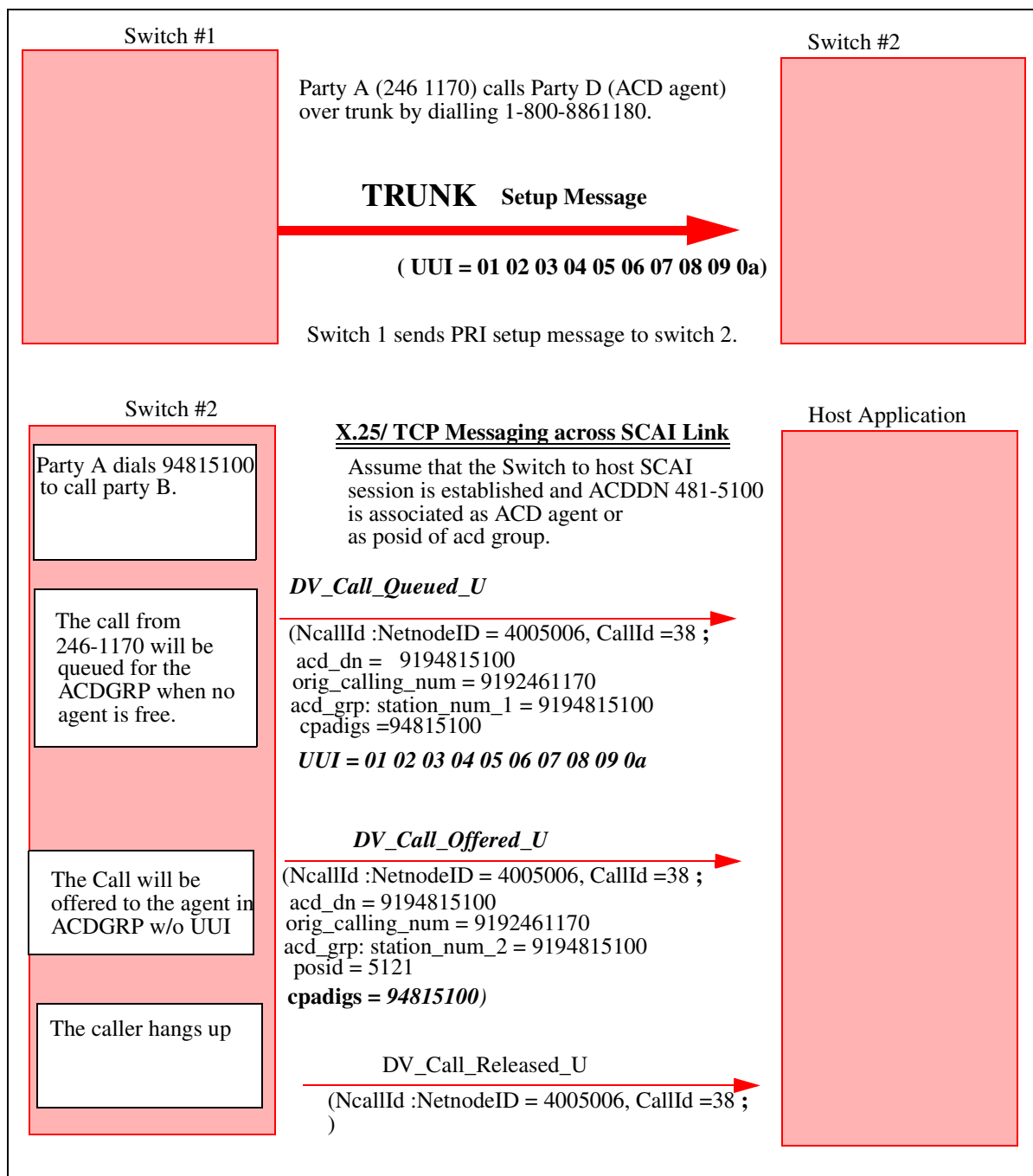
Figure 4 UII in DV_Call_Queued_U



1.3.5.4 Example 4: UII IE not in DV_Call_Offered_U

Party A (2461170) calls party B (ACD agent of ACDGRP 4815100, posid: 5121) over ISUP/PRI and party B answers.

Figure 5 UII in DV_Call_Queued_U



1.3.6 SOC

The UII IE data delivery to SCAI is controlled by state SOC ICM00083. The UII IE data is delivered to the SCAI host only if the SOC is turned on and the sub service supporting UII is subscribed.

In case a call over a ISUP/NI2 PRI trunk with UII IE terminates on a SCAI monitored agent and the SOC ICM00083 is IDLE, the UII shall not be delivered to the SCAI host even if the profile in SCAIPROF is subscribed to the subservice with support for UII.

The SOC functionality shall be available in SN10 and SN09 Drop II shall have the functionality as an activatable patch. When CS2K with patch CFZ40 activated on SN09 upgrades to SN10 or higher release, the SOC Option ICM00083 will be automatically turned ON during ONP.

Note: The delivery of UII IE over incoming NI-2 PRI or ANSI ISUP messages will not be SOC controlled.

1.3.7 Logs

If the total size of the outgoing ICM message with UII exceeds the maximum supported size of outgoing ICM message then the UII IE will be discarded and LOG SCAI 304 will be generated.

1.4 Hardware Requirements or Dependencies

Not Applicable

1.5 Software Requirements or Dependencies

Not Applicable

1.6 Limitations and restrictions

This feature does not ensure the correct UII IE population for the protocol variants other than those specified

1.7 Interactions

Not Applicable

1.8 Applicable customer facing sections

1.8.1 Fault Management

1.8.1.1 Logs (LG)

SCAI 304: The snapshot of the log is given below:

```
RSNN10AG  SCAI304 JAN14 22:30:56 5348 INFO UIIPARM  
DISCARDED  
MESSAGE : DV-CALL-QUEUED-U
```

LINK ID : DNA: 0000000000000000 PROTOCOL: 1 1 1 1
DEVICE : MPC: 0 LINK: 3
SCAI GROUP: SCAI_GRP1
LINKSET NAME: X25_LNK1

SCAI304 log limitation: There are certain scenarios in which the SCAI304 log will be generated with LINK ID, DEVICE ID and LINKSET NAME set as unavailable. This happens when the queue used to transmit the message to the SCAI host is decided at a later stage. That is, the queue information is available only at a later stage after the UUI parameter is discarded. The queue information is needed to get the LINK ID, DEVICE ID and LINKSET NAME details.

1.8.2 Configuration

1.8.2.1 Data schema (DS)

Figure 6 Data Schema changes in Tables LTDATA and SCAISSRV

TABLE LTDATA
LTDKEY LTDRSLT

 ISDN 641 SERV SERV N N ALWAYS ALWAYS (UUS) \$

TABLE SCAISSRV
SUBSERV SPROFILE

 CTXEVENT19\$ CTXEVENT (SETOFFHK Y Y Y)
 (CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y Y Y **Y**)
 (CALLANSWR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y) (CALLREL Y Y Y Y)
 (CALLNAME Y Y Y Y Y) \$

TABLE SCAISSRV
SUBSERV SPROFILE

 RESEVENT19\$ RESEVENT (SETOFFHK Y Y)
 (CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y Y Y **Y**)
 (CALLANSWR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y) (CALLREL Y Y Y)
 (CALLNAME Y Y Y Y Y) \$

TABLE SCAISSRV
SUBSERV SPROFILE

 ROUTING19\$ ROUTING (CALLRECDC Y Y Y Y Y Y Y Y Y Y Y Y **Y**)
 (CALLREDIR Y Y Y) \$

TABLE SCAISSRV
SUBSERV SPROFILE

 ACDEVENT19\$ ACDEVENT (CALLQUED Y Y Y Y Y Y Y Y Y Y Y Y **Y**)
 (CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y Y **Y**)
 (CALLANSWR Y Y Y Y Y Y Y Y Y Y Y Y)
 (CALLREL Y Y Y Y Y Y) (AGTLGDIN Y Y Y) (AGTLGDOUT Y Y)
 (AGTREADY Y Y)

1.8.2.2 User Interface

Not applicable

1.8.2.3 Element Management

Not applicable

1.8.2.4 Alarms

Not applicable

1.8.2.5 Security

Not applicable

1.8.2.6 Office Parameters

Not applicable

1.8.2.7 Service orders (SO)

Not applicable.

1.8.3 Man machine interface (MM)

Not applicable.

1.8.4 Operational measurements (OM)

Not Applicable.

1.8.5 AMA/Billing information (AM)

Not Applicable.

1.8.6 Real-time

Not Applicable.

1.8.7 Engineering Information

Not Applicable

1.9 Glossary

Term	Description
UUI	User to User Information
UUS	User to User signalling
ACD	Automatic Call Distribution
SCAI	Switch-Computer Applications Interface
ICM	Intelligent Call Management
PRI	Primary Rate Interface
NI-2	National ISDN 2

Term	Description
XPM	eXtended Peripheral Module
GWC	GateWay Controller
SPM	Service Peripheral Module
SPCS	Stored Program Controlled switching System
IAM	Initial Address Message
ACM	Address Complete Message
ANM	ANswer Message
IAM	Initial Address Message
REL	RELease message
REL COM	RELease COMplete message
RO	Remote Operation
RES	Residential Enhanced Services
MDC	Meridian Digital Centrex
LCS	Local Concrete Syntax.
ISUP	ISDN User Part

Product = CS 2000

A00012570-- Disabling Non-secure Network Services in SSPFS

Functional Description

1: Applicable Solution(s)

DMS, MCS

1.1 Description

When non-secure services within the operating system are not used, they should be disabled to close down any port(s) used by these services and reduce the exposures to security threats. Non-secure services such as ftp, tftp, telnet, SNMP and NFS may have secure equivalents. Therefore the use of the non-

secure services can be disabled altogether when not in use. A configuration tool is required to selectively disable the non-secure services.

This activity provides some configuration tools to assist customers in configuring the server based on their security policy. Upon completion of the fresh system installation or upgrade, the customer (security administrator) has the possibility to apply the security policy on the server via a command line interface.

As part of this feature, non-secure network services not required by our product offerings (such as rpc in inetd.conf) will be disabled by default during initial system installation and upgrades.

This feature is targeted for all SSPFS platforms and profiles.

1.2 Hardware Requirements or Dependencies

Not applicable.

1.3 Software Requirements or Dependencies

Not applicable

1.4 Limitations and Restrictions

The following operating system services will be configurable/disabled by default on fresh install:

- List the RPC post IT.

This feature only provides configuration tools for services registered in the inetd.conf and the proftpd.conf files.

The configuration tools are only available to the root user.

Any services started under inittab, initd or the rpcd daemons are not affected.

1.5 Interactions

This feature interacts with any applications already deployed that makes use of the services listed above in section 2.5.

1.6 Glossary

2: Configuration Management for A00012570

2.1 Hardware and Software Requirements

Any SSPFS supported platform running SN09.1+ release.

2.2 Initial Configuration

The initial configuration is done via SSPFS CDs. Upon completion of the SSPFS fresh install, this feature will disable: ftp, tftp, telnet, snmp and nfs.

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

No new office parameters introduced by this feature.

2.3.1 New/modified office/subnet parameters

Not applicable.

2.3.2 Parameter information

Not applicable.

2.4 Upgrade Impact

Upon system upgrade from one release to the other, the state of non-secure services is preserved. The disabling of such services has to be performed via cli after the upgrade.

2.4.1 Dump and Restore (CM)

Not applicable.

2.4.2 Element Management Upgrade

Not applicable.

2.4.3 Downgrade impact

Since the non-secure service state are not altered on upgrade, there is no impact on downgrade.

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

2.5.1 New/modified tables MIBs or Database Schema

Not applicable.

2.5.2 Table/MIB/Remote Database Schema information

Not applicable.

2.6 Service Orders (SO) (CM & SESM)

Not applicable.

2.7 Software optionality control (SOC)

Not applicable.

2.8 Element Management

Not applicable.

2.8.1 New/modified GUIs

Not applicable.

2.8.2 GUI information

Not applicable.

2.8.3 CLUI Interface

As identified before, new sub-menu items will be introduced into the “**Security Services Configuration**” layer within the configuration panel for SSPFS cli configuration tool.

2.9 User interface changes

2.9.1 Directory: <directory name/MAP level>

For pictorial representation of the menu level, please refer to the diagram in figure 2.

The top level CLUI is invoked via the command cli. The result is listed below:

```
# cli
Command Line Interface
1 - View
2 - Configuration
3 - Other

X - exit

select -
```

To get to the configuration level, the operator is requested to enter 2. The resulting menu is prompted to the operator:

```
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 - Remote Backup Configuration
10 - Database Configuration
11 - NFS Configuration
12 - Bootp Configuration
13 - Restricted Shell Configuration
14 - Security Services Configuration
15 - Login Session
16 - Location Configuration
```

```
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - exit
```

select –

Option 14 above will be extended. Here is the new menu generated when the operator selects option 14:

```
Security Services Configuration
1 - Socks Configuration
2 - IEMS Server Location Configuration
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet, snmp and nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - query_registry (Query Network Services Package Registration)
X - exit
```

select -

Upon selection of any of the new sub-menus 4-6, the operator will get the following commands menu:

```
Common Services Configuration (ftp, tftp, telnet, snmp and nfs)
1 - query_common_inetd (Services State Query )
2 - enable_common_inetd (Enable a service registered in inetd.conf)
3 - disable_common_inetd (Disable a service registered in inetd.conf)

X - exit
```

select -

Here is an example of the result of a query state for the Common Network Services:

```
Common Services State
0. telnet    Enabled
1.  ftp      Disabled
2.  tftp      Enabled
3.  snmp      Disabled
4.  nfs       Disabled
```

Here is an example of the disable Service command:

```
Enable Common Service
1. tftp /usr/sbin/in.tftpd
2. telnet /usr/sbin/in.telnetd
Select service number to disable: 1
The selected services was tftp /usr/sbin/in.tftpd
Configuration file updated.
Operating system deamon refreshed.
OpARATION completed.
```

Upon the selection of proftpd User Configuration, the operator will receive the following options:

- 1 - query_proftpd_users (Query users defined in proftpd)
- 2 - add_proftpd_user (Add a user to proftpd)
- 3 - add_dflit_GWC_anonymous_user (Restore the GWC anonymous user)
- 4 - del_proftpd_user (Delete a given user from proftpd)
- 5 - query_user_registry (Query the packages registered for ftp users)

2.9.2 Command: <command command name>

Not applicable.

2.9.2.1 Qualifications and warnings

Not applicable.

2.9.2.2 Responses

Not applicable.

2.9.2.3 Example

Not applicable.

2.10 Security

The security implications of this feature are that on a fresh install of the SSPFS software, the default state of the non-secure services such as ftp, tftp, snmp, telnet and nfs will be preserved. A configuration tool is provide to root user group to be able to manually disable these services to increase the security profile of the target platform.

2.10.1 Network Configuration

Not applicable.

2.10.2 Key Management

Not applicable.

2.10.3 Protocol

Not applicable.

2.10.4 Authentication

Not applicable.

2.11 Configuration Walkthrough

The section walks through minor changes in the platform initial installation, upgrade, patching and power cycle/failover.

On system installation, a minor change is performed to the sspfs post-install script resulting into the disabling non-necessary services such as RPC not used in any sspfs product offering.

On system upgrade, the setting of non-secure services is maintained throughout the upgrade. Once the system is re-clone/back in sync, then the non-secure services can be disabled manually via cli.

For system patching via NPM, the preferred option is to use sftp. Therefore the deactivation of non-secure services should have no impact to the patchability of the platform.

For power-cycle or failover of a node in the cluster, there is a small window of time when the control files are being synchronized and the inetd services is being re-initialized. Since this script functionality is typically done once after upgrade, it is acceptable to re-run the configuration if a power-cycle or failover occurred during the configuration changes.

Product = CS 2000

A00012735 -- Session Server Fault Handling Enhancements ***Functional Description***

1: Applicable Solution(s)

PT-IP

1.1 Description

This activity extends the coverage of hardware faults handled by the Session Server NCGL Platform Manager software and thus increases the reliability of the Session Server platform. This activity involves the detection and reporting of hardware faults in the following areas:

- Power Supplies
- Fan Speeds
- System Temperature
- System Voltage
- Miscellaneous Hardware Elements

1.2 Hardware Requirements or Dependencies

The software of activity interacts with functions of the existing SAM XTS (HP CC3310) hardware of the Session Server platform. No new hardware is required.

1.3 Software Requirements or Dependencies

No new software or firmware dependencies are introduced by this activity.

1.4 NCGL Platform Web Pages

An Element Management web based interface is provided to perform the platform or application maintenance and monitoring of logs and alarms. The platform web interface resides under the Communication Server 2000 NCGL Platform Manager link on the Session Server EM web login page. This web interface can be accessed from either the Succession IEMS or a general web browser running on a client machine.

This activity introduces enhancements to the fault handling of the NCGL software within the NGSS platform. These enhancements include the monitoring and alarming of the various hardware resident sensors. These sensor monitors are displayed in a new Sensors page of the Succession Communication Server 2000 NCGL Platform Manager web pages. When mate connectivity exists, data for both units are shown on the Sensors page.

The sensors are categorized as either primary or secondary sensors. The primary sensors are always reported on the Sensors page while the value of a secondary sensor is only reported when the sensor is reporting a failure. In terms of alarms and customer logs, no such distinction between primary and secondary sensors applies - all sensors are treated the same.

The sensors are also categorized into the following sensor groups for purposes of sensor display, logging and alarming:

1. Power Supplies:

There are two power supply modules, labelled “A” and “B”, per unit. Sensors report module presence and operational status. There is one primary and 2 secondary sensors per power supply module.

2. Fan Speed:

There are 4 internal fan speed sensors and no secondary sensors per unit.

3. System Temperature:

There are 4 primary temperature sensors plus 1 secondary sensor per unit.

4. System Voltage:

There are 3 primary power line sensors plus 9 secondary sensors per unit.

5. Miscellaneous Hardware Elements:

There are no primary sensors reported but up to 39 secondary sensors might be reported per unit.

The format of sensor information for a single unit of the new Sensors web page appears below in Table 1 on page 874. Where applicable the units of the sensor

readings appear in the Sensor Status column. In the cases of sensors with thresholds, the current value of the sensor plus associated thresholds are provided. Note that these thresholds are established in the hardware and this activity does not provide a method to change the threshold values. Where applicable the severity of the threshold (minor or major) is shown indicating that the exceeding the threshold will result in the assignment of the respective severity or higher.

The alarm severity column allows easier identification of the failed sensors and correlation with alarm indicators and customer log reports. A higher severity may appear in the alarm severity column in comparison to the minor threshold. This might happen if multiple sensors with the same replaceable component (FRU) are reporting failures. Please see the alarm subsection for more information.

If the secondary sensors report a failure indication, then the sensors records will appear in the “<any other sensor failure reports>” fields. Reports for one or more failed secondary sensors could appear on the Sensor page. If no secondary sensors report failures, then no additional records appear.

Table 1: Unit Sensor Format

Sensor Group		Sensor Status
Unit 0 Chassis Sensors		Alarm: <chassis alarm severity>
Fan Speed	80mm, Left	<current RPM plus thresholds>
	80mm, Right	<current RPM plus thresholds>
	40mm, Left:	<current RPM plus thresholds>
	40mm, Right	<current RPM plus thresholds>
System Temp	Baseboard	<status plus current degrees C>
	Processor 1	<status plus current degrees C>
	Processor 2	<status plus current degrees C>
	Front Panel	<status plus current degrees C>
	Other	<any other sensor failure reports>
System Voltage	3.3V	<current Volts plus hi/low thresholds>
	5V	<current Volts plus hi/low thresholds>
	12V	<current Volts plus hi/low thresholds>
	Other	<any other sensor failure reports>
Miscellaneous H/W Elements		<any other sensor failure reports>
Unit 0 Power Supply Module A		Alarm: <power supply A alarm severity>
Power Supply	A	<PS present and status> <any other sensor failure reports>
	Other	<any other sensor failure reports>
Unit 0 Power Supply Module B		Alarm: <power supply B alarm severity>
Power Supply	B	<PS present and status> <any other sensor failure reports>
	Other	<any other sensor failure reports>

The Sensors page provides the latest values of the last sensor sample. No history of sensor readings or failures is provided. The customer logs may be used to identify such a history. Here is an example Sensor page display for a single unit.

Sensor Group		Sensor Status
Unit 0 Chassis Sensors		MAJOR
Fan Speed	80mm,Left	Current = 4029.00 RPM Low Minor/Major = 1989.00/1836.00 RPM
	80mm,Right	Current = 3315.00 RPM Low Minor/Major = 1989.00/1836.00 RPM
	40mm,Left	Current = 9537.00 RPM Low Minor/Major = 3774.00/3264.00 RPM
	40mm,Right	Current = 8925.00 RPM Low Minor/Major = 3774.00/3264.00 RPM
System Temp	Baseboard	Current = 87.00 C Low Minor/Major = 10.00/5.00 C High Minor/Major = 60.00/65.00 C
	Processor1	Current = 33.00 C Low Minor/Major = 0.00/- 10.00 C High Minor/Major = 75.00/80.00 C
	Processor2	Current = 32.00 C Low Minor/Major = 0.00/- 10.00 C High Minor/Major = 75.00/80.00 C
	Front Panel	Current = 25.00 C Low Minor/Major = 10.00/5.00 C High Minor/Major = 40.00/45.00 C
	Other	OK
System Voltage	3.3V	Current = 3.41 volts Low Minor/Major = 3.08/2.99 volts High Minor/Major = 3.54/3.64 volts
	5V	Current = 5.01 volts Low Minor/Major = 4.68/4.52 volts High Minor/Major = 5.33/5.49 volts
	12V	Current = 16.03 volts Low Minor/Major = 11.16/10.79 volts High Minor/Major = 12.71/13.08 volts
	Other	OK
Miscellaneous H/W Elements		OK
Unit 0 Power Supply Module A		MAJOR
Power supply	A	presence detected
	Other	minor 22 performance lags; minor 23 performance lags;
Unit 0 Power Supply Module B		minor
Power supply	B	presence detected
	Other	minor 26 performance lags;

1.5 Alarms

This activity introduces new alarms for reporting faults due to:

1. Power Supply related failure
2. Fan Speed threshold exceeded
3. System Temperature threshold exceeded
4. System Voltage threshold exceeded
5. Miscellaneous hardware sensors reporting failure

The new alarms are associated with an field replaceable unit (FRU). There are two FRU types involved with the sensor monitoring:

1. the server chassis and contained baseboard
2. the power supply module

There are two power supply FRUs, A (left when viewed from rear) and B (right), per session server module.

For the new alarms:

1. An XTS382 alarm and log signifies the occurrence of a server chassis/baseboard sensor alarm condition.
2. An XTS383 alarm and log signifies the occurrence of a power supply module alarm condition

For each unit, at any time at most one alarm should be raised for each FRU. Once raised, the severity of an alarm might escalate if:

- the number of failed primary or secondary sensors in the group detecting failure increases or
- the nature of the sensor failure changes (e.g. both minor and major thresholds are crossed)

When raised these alarms may be viewed on the Alarms page of the NCGL Platform Manager web pages. Note that the Alarms page is refreshed approximately every 45 seconds.

The NCGL platform also supports the reporting of alarm events to an SNMP host target. These SNMP traps are typically configured to route to the Succession IEMS. Traps for the new alarms follow the same format, fields values and behavior as existing platform alarm traps. When raising an alarm, the SNMP traps are associated with the XTS382 and XTS383 identifiers. Once all sensor conditions associated with an FRU are cleared, the alarm is cleared and an XTS682 or XTS683 SNMP trap and customer log are generated.

Alarms are formatted and displayed as follows:

<Type> <ID> <Timestamp> <Host> <Severity> <Description>

1.5.1 Alarm Type

The alarm type specifies the alarm category for the given alarm. Each of the new alarms are associated with the Equipment Alarm type.

Table 2: Alarm Type Selection

Log Number	Elements	Type
XTS382/XTS682	Chassis/Baseboard Sensor	Equipment alarm
XTS383/XTS683	Power Supply Sensor	Equipment alarm

1.5.2 Alarm ID

The alarm ID specifies, in general terms, why the given alarm was raised. The alarm ID choices for the new alarms are:

1. Cooling system problem:
2. Processor Problem:
3. Threshold Crossed
4. Power Problem
5. Equipment Malfunction

For cases of multiple, diverse alarm conditions against the same FRU, the equipment malfunction identifier is used.

1.5.3 Alarm Timestamp

The alarm timestamp specifies the date and time when the given alarm was raised.

1.5.4 Alarm Host

The host field contains the Session Server host name from where alarm was raised.

1.5.5 Alarm Severity

The alarm severity specifies the seriousness of the given alarm. The following alarm severities apply to the alarms introduced by this activity:

- 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 a service affecting condition has developed and a timely corrective action is required.
- Cleared - Note that 'cleared' will not be seen on the Alarms Panel, since the Alarms Panel only shows alarms that are currently raised.

For severity selections of the new alarms of this activity please refer table 1.

1.5.6 Alarm Description

The alarm description provides specific details about the given alarm. For the alarms introduced by this activity, the description field includes:

- location:
For the power supply module alarms, this indicates either "A" (left when viewed from rear) or "B" (right when viewed from rear) for the applicable FRU.

- sensor counts:
The number of sensor reporting failure for the FRU is also given.

Here are example fields from the Alarms Panel on the platform web pages:

Type: Equipment

ID: Threshold Crossed

Date: Monday December 12th 2005 04:17:46 AM

Host: NGSS0

Severity: Minor

Description: Chassis sensor alarm raised. 1 sensor is reporting a failure.

1.6 Customer Logs

The Session Server Element Manager provides a web page for viewing of customer logs. The customers log panel displays a historical view of customer logs that have been generated on the Session Server unit.

This activity adds new customer logs to the existing platform (XTS) logs. The new customer logs are associated with the types of field replaceable units where the hardware sensors reside.

The Session Server customer logs are generated using syslog. Here is the format for the new logs.

<time stamp> <host name> <process name> <Name> <Number> <Severity> <Event type> <Label> <Description>

The log description field follows the same format as the alarm description field described in “Alarm Description” on page 878.

Here are the field values for these new customer logs.

Table 3: Fields of the New Logs

Name	Number	severity	Event Type	Label	Description
XTS	382	MINOR	FLT	Chassis Sensor Fault	Chassis sensor alarm raised. <#> sensor <is/are> reporting a failure.
XTS	382	MAJOR	FLT	Chassis Sensor Fault	Chassis sensor alarm raised. <#> sensor <is/are> reporting a failure.
XTS	682	CLEARED	INFO	Chassis Sensor Condition Cleared	Chassis sensor condition cleared.
XTS	383	MINOR	FLT	Power Supply Sensor Fault	Power supply alarm raised in module <A/B>. <#> sensor <is/are> reporting a failure.
XTS	383	MAJOR	FLT	Power Supply Sensor Fault	Power supply alarm raised in module <A/B>. <#> sensor <is/are> reporting a failure.
XTS	683	CLEARED	INFO	Power Supply Sensor Condition Cleared	Power supply condition cleared in module <A/B>.

1.7 Limitations and restrictions

This activity does not introduce further limitations or restrictions to the NGSS platform. Please note that this activity addresses the failure monitoring

documented in the FN section of A00004005. Please refer to A00004005 for other limitations and restrictions of the NGSS platform.

1.8 Interactions

Not applicable.

1.9 Glossary

Term	Description
New term	Definition

2: Fault Management for A00012735

2.1 Fault management strategy

This activity builds upon the fault management services and software of NCGL Platform Manager in A00004005 introducing support for managing some new fault conditions.

2.2 Fault management tools and utilities

No new tools and utilities are introduced by this activity. The current approach to fault management applies.

2.3 Session Server Fault Handling Logs and Alarms.

This section describes the logs and alarms introduced by this activity.

The logs and alarms can be viewed via the web browser interface on the Succession Communication Server 2000 NCGL Platform Manager - via Alarms panel and Customer Logs panel.

This activity introduces the following logs:

2.3.1 Fault Handling Alarms/Logs

- XTS382, XTS682: Chassis Sensor Fault
- XTS383, XTS683: Power Supply Sensor Fault

2.3.2 Field Description

The new logs follow the existing XTS log format and are composed of the fields shown in the table given below.

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log.
Process Name	Alphanumeric	Identifies the NCGL or application process that generated the report.
Log Number	Alphanumeric	The component prefix and number of the log
Severity	Alphanumeric	The log severity (may be related to alarm severity)
Event Type	Alphanumeric	The type of trouble recorded
Label	Alphanumeric	Title label for the log.
Component Id	Alphanumeric	The component id is the unit hostname.
Description	Alphanumeric	Description of the log including location information when applicable and sensor details.

Here is an example platform /var/log/custlog entry:

Dec 9 06:22:41 NGSS0 alarmd: XTS382 MAJOR FLT Chassis Fault Detected
NGSS0 Chassis sensor alarm raised. 2 sensors are reporting failures.

Here is an example alarm entry from the platform web pages:

Type: Equipment

ID: Threshold Crossed

Date: Friday December 8, 2005 02:39:06 PM

Host: NGSS1

Description: Chassis sensor alarm raised. 1 sensor is reporting a failure.

Here is a sample from an IEMS resident log file.

Dec 9 15:00:35 rtpo-cmt IEMS: _V2_~I=~H=rtpo-cmt~A=IEMS~S=1017~~
XTS383 MAJOR FLT XTS Fault Location: RTPOSST0-Unit-
1;172.18.164.14 Notification Id: 17^M State: Raised^M Category:
equipment Cause: thresholdCrossed(51) Time: Dec 09 15:00:19 2005
Component Id: RTPOSST0_1 Specific Problem: Description: Power
supply alarm raised in module A. 1 sensor is reporting a failure.

Dec 9 15:07:00 rtpo-cmt IEMS: _V2_~I=~H=rtpo-cmt~A=IEMS~S=2218~~
IEMS607 NONE INFO IEMS Autogenerated Clear^M Location:
RTPOSST0-Unit-1;172.18.164.14^M NotificationID: 17^M State:
Clear^M Time: Dec 09 15:07:00 2005^M Specific Problem: ^M
Category: equipment^M Component Id: RTPOSST0_1^M Description:
Raised log: XTS383; Power supply alarm raised in module A. ^M 1 sensor
is reporting a failure.

2.3.3 Fault Handling Alarms/Logs

The fault handling elements produces the following alarm and logs.

2.3.3.1 XTS382

2.3.3.1.1 Explanation When a sensor reports a failure condition, an XTS382 alarm is raised on the Alarms panel of the NCGL Session Server unit. An XTS382 log is generated.

2.3.3.1.2 Format Alarm/Log: Power Supply Failure Alarms/Logs

Type: Equipment

ID: equipmentMalfunction

Event: FLT

Label: Chassis Sensor Fault

Severity:

- Minor: a single, minor sensor fault has been detected by the hardware sensors for the unit's power supplies
- Major: either multiple, minor or at least one major sensor fault has been detected
- Critical: not currently generated

2.3.3.1.3 Field descriptions Refer to [“Field Description” on page 881](#).

2.3.3.1.4 Action On the NCGL Platform Manager web pages view the Sensor Information, System Information panels. Examine existing alarms and associated logs.

Inspect the environmental conditions of the unit.

If the Sensor Status field of the Sensor Information page indicates that presence is not detected, confirm that all drives and FRUs are correctly seated and latched into the chassis.

Consider chassis replacement or contact technical support if the condition continues.

2.3.3.1.5 Associated Operational Measurements or Performance Measurements

None.

2.3.3.1.6 Additional information None.

2.3.3.2 XTS682

2.3.3.2.1 Explanation When XTS382 Chassis Sensor fault condition and alarm is cleared. An alarm trap and INFO log XTS682 are generated.

2.3.3.2.2 Format Alarm/Log: Power Supply Alarm Cleared

Type: Equipment

ID: equipmentMalfunction

Event: INFO

Label: Power Supply Alarm Cleared

Severity: None

2.3.3.2.3 Field descriptions See Section 11.3.

2.3.3.2.4 Action None.

2.3.3.2.5 Associated Operational Measurements or Performance Measurements None.

2.3.3.2.6 Additional information None.

2.3.3.3 XTS383

2.3.3.3.1 Explanation When there is one or more sensors report failure conditions with either power supply module A or B, an XTS383 alarm is raised on the Alarms panel of the NCGL Session Server unit.

2.3.3.3.2 Format >> Alarm/Log: Fans Failure Alarms/Logs

----> Type: Equipment

---->ID: equipmentMalfunction

---->Event: FLT

---->Label: Fans Problem

---->Severity: Minor, Major

2.3.3.3.3 Field descriptions See [“Field Description” on page 881](#).

2.3.3.3.4 Action On the NCGL Platform Manager web pages view the Sensor Information, System Information panels. Examine existing alarms and associated logs.

Inspect the environmental conditions of the affected power supplies in the unit.

If the Sensor Status field of the Sensor Information page indicates that presence is not detected, confirm that the power supply module is correctly seated and latched into the chassis.

Consider chassis replacement or contact technical support if the condition continues.

If the alarm is critical, contact Nortel Networks support personnel for assistance.

2.3.3.3.5 Associated Operational Measurements or Performance Measurements None

2.3.3.3.6 Additional information None

2.3.3.4 XTS683

2.3.3.4.1 Explanation When XTS383 Minor/Major Power Supply Sensor Fault alarm condition is cleared, an INFO alarm/log XTS683 is generated.

2.3.3.4.2 Format

>>Alarm/Log: Fans Problem Alarm Cleared

---->Type: Equipment

---->ID: EquipmentMalfunction

---->Event: INFO

---->Label: Power Supply Condition Cleared

---->Severity:None

2.3.3.4.3 Field descriptions See Section [“Field Description”](#) on page 881.

2.3.3.4.4 Action None

2.3.3.4.5 Associated Operational Measurements or Performance Measurements None

2.3.3.4.6 Additional information None

Product = CS 2000

A00012889 -- Passphrase Protected Keys for SSH

Functional Description

1: Applicable Solution(s)

DMS

1.1 Description

The applications (SBA and OMDD) on the SDM/CBM, use either standard FTP (insecure) or OpenSSH SFTP (secure) to perform outbound file transfers to the downstream machine.

Currently, for secure outbound file transfer, only password-based authentication is supported.

This feature enhances the existing secure outbound file transfer functionality by introducing the key-based (public key) authentication.

The key-based authentication mechanism is provided as an additional option for the user. Hence, the user can select to use either the password-based or the key-based authentication while adding and changing the secure file transfer schedules in the SBA (billmtc) or OMDD (omui) user interface programs. The actual configuration details are documented in the configuration section.

When the user configures secure file transfer schedule with key-based authentication, the keypair (public/private key files) will be automatically generated with a random passphrase. The keypair will be stored under ~maint/.ssh/ directory and the passphrase will be stored in the Private Data Manager in an encrypted format.

If there is a failure in generating the cryptographic keys, an info log SDM666 will be generated.

Ex:

```
SDM666 Oct 12 04:33:59 1234 NONE INFO Failed to generate  
cryptographic keys for user=maint, app_name=OMDD, index=ftd1
```

1.2 Hardware Requirements or Dependencies

No new hardware requirements or dependencies are introduced by this feature.

1.3 Software Requirements or Dependencies

The customer's downstream machine (OSS) should be running a SSH-2 server compatible with SFTP client of OpenSSH. The OpenSSH software should be installed on the SDM/CBM too.

1.4 Limitations and restrictions

- The initial host key acceptance of the downstream processor should be done manually before it can use the SSH protocol to transfer the files from SDM/CBM. Figure 1 shows an example of how to accept a host key manually. The .ssh/known_hosts file in maint user's home directory will be edited by SSH software to include the host key. After that, the applications (SBA/OMDD) can use SSH to send files to the downstream OSS as maint/root. This procedure must be performed for each downstream destination.
- Automatic dumping of the public key file on the remote system is NOT supported by this feature. All users have to manually dump the contents of the public key file into the user's authorization file on the remote system.

Note: If the remote system is running OpenSSH server, the public key should be appended to .ssh/authorized_keys or .ssh/authorized_keys2 file of the user. Figure 2 shows an example of how to append the public key to .ssh/authorized_keys file of the user.

- The SSH-2 server running on the downstream OSS must be compatible with OpenSSH sftp client.
- The data transfers of AFT, RTB and sendtape applications are not secured.

Figure 1 Host key acceptance

```

On SDM/CBM
> login: root
> root's Password: xxxx
> su 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.

```

Figure 2 Appending public key to authorized_keys file of the user on the downstream machine

```

On SDM/CBM
> login: root
> root's Password: xxxx
> cd ~maint/.ssh
> ssh root@47.135.214.66 'cat >> .ssh/authorized_keys' < sba:occ:dirp:oss_rsa.pub
> Password:
>

```

1.5 Interactions

No

1.6 Applicable customer facing sections

Fault Management

Logs __X__

Alarms __X__

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_

1.7 Glossary

Term	Description
SDM	Supernode Data Manager
CBM	Core Billing Manager
SBA	SDM/CBM Billing Application
OMDD	Operational Measurements Data Delivery
OMUI	OMDD User Interface
SSH	Secure Shell
FTP	File Transfer Protocol
SFTP	Secure File Transfer Protocol (SSH internal protocol)
OSS	Operations Support System

2: Configuration Management for A00012889

2.1 Hardware and Software Requirements

- OpenSSH installed on SDM/CBM.
- SBA and OMDD applications are installed and InSv.

2.2 Initial Configuration

- Configure and activate a SBA stream.
- No initial configuration of OMDD is required.

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

N/A

2.4 Upgrade Impact

N/A

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

N/A

2.6 Service Orders (SO) (CM & SESM)

N/A

2.7 Element Management

N/A

2.8 Command interface changes

N/A

2.9 Security

2.9.1 Secure Data Transfer to OSS with Public Key Authentication

This feature enhances the existing secure outbound file transfer functionality by introducing the key-based (public key) authentication.

The key-based authentication mechanism is provided as an additional option for the user. Hence, the user can select to use either the password-based or the key-based authentication while adding and changing the secure file transfer schedules in the SBA (billmtc) or OMDD (omui) user interface programs.

2.9.2 Passphrase protection.

The passphrase is stored in the Private Data Manager in an encrypted format.

2.10 Configuration Walkthrough

2.10.1 Host key acceptance for 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 1 shows an example how to accept a host key manually.

Figure 1 Host key acceptance

2.10.2 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 “sendfile” command can be used to validate if OSS is ready for key-based authentication. Text in bold indicates changes in SBA UI.

Figure 2 shows an example on how a user can configure secure outbound file transfer using password-based authentication.

Figure 3 shows an example on how a user can configure secure outbound file transfer using key-based authentication.

Figure 4 shows an example of how to append the public key to .ssh/authorized_keys file of the user on the remote system running with OpenSSH server.

Figure 5 and Figure 6 shows an example of how a user can modify the existing schedule tuple configuration.

Figure 7 and Figure 8 shows an example of how a user can delete the schedule tuple.

Figure 2 Prompts for schedule add (*Password based authentication*).

Valid streams are {'OCC'}.
Press Enter to accept 'OCC'.
Enter Stream:

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: OSS

Valid protocols are {'FTPW', 'RFTPW', 'SFTPW', 'KSFTPW'}.
Press Enter to accept 'FTPW'.
Enter Protocol: SFTPW

WARNING: File Transfer to this destination will fail if OpenSSH is not installed
Please install OpenSSH if it is not already installed.

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:

... (con't on next figure)

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:

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:

... (con't on next figure)

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

```
Stream           : 'OCC'
File_Format_Type : 'DIRP'
Destination      : 'OSS'
Protocol         : 'SFTPW'
Primary_Destination : '47.135.213.53'
Primary_Port     : '22'
Alternate_Destination : '47.135.213.53'
Alternate_Port    : '22'
Start_Time       : '00:00'
Stop_Time        : '23:00'
Interval         : '120'
Remote_Storage_Directory: '/billing'
Remote_Login      : 'test'
Remote_Password   : '*****'
Maximum_Retries   : '3'
Retry_Wait_Time   : '1'
File_Extension    : ''
Field_Separator   : '.'
Active           : 'Yes'
```

Valid actions are {'Save', 'Edit', 'Abort'}.

Press Enter to accept 'Edit'.

Enter Action: save

Schedule tuple added.

Figure 3 Prompts for schedule add (Key based).

Valid streams are {'OCC'}.
Press Enter to accept 'OCC'.
Enter Stream:

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: OSS

Valid protocols are {'FTPW', 'RFTPW', 'SFTPW', '**KSFTPW**'}.
Press Enter to accept 'FTPW'.
Enter Protocol: **KSFTPW**

WARNING: File Transfer to this destination will fail if OpenSSH is not installed
Please install OpenSSH if it is not already installed.

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:

... (con't on next figure)

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'.

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:

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

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:

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

Stream : 'OCC'
File_Format_Type : 'DIRP'
Destination : 'OSS'
Protocol : 'KSFTPW'
Primary_Destination : '47.135.213.53'
Primary_Port : '22'
Alternate_Destination : '47.135.213.53'
Alternate_Port : '22'
Start_Time : '00:00'
Stop_Time : '23:00'
Interval : '120'
Remote_Storage_Directory: '/billing'
Remote_Login : 'test'
Maximum_Retries : '3'
Retry_Wait_Time : '1'
File_Extension : ''
Field_Separator : '.'
Active : 'Yes'

Valid actions are { 'Save', 'Edit', 'Abort' }.

Press Enter to accept 'Edit'.

Enter Action: save

Schedule tuple added.

The public key on the CBM is stored at :

/cbmdata/users/maint/.ssh/sba:occ:dirp:oss_rsa.pub

Please append this public key to the user's authorization file on the destination machine.

Press Return to Continue...

Figure 4 Appending public key to authorized_keys file of the user on the downstream machineOn SDM/CBM

```
> login: root
> root's Password: xxxx
> cd ~maint/.ssh
> ssh root@47.135.214.66 'cat >> .ssh/authorized_keys' < id_rsa.pub
> Password:
>
```

Figure 5 Prompts for schedule change (From password to key-based).

```
Valid streams are {'AMA', 'OCC'}.
Press Enter to accept 'AMA'.
Enter Stream: OCC

Valid file format types are {'DIRP'}.
Press Enter to accept 'DIRP'.
Enter File_Format_Type:

Valid destinations are {'OSS', }.
Press Enter to accept 'OSS'.
Enter Destination:

Stream          : 'OCC'
File_Format_Type : 'DIRP'
Destination     : 'OSS'
Protocol        : 'SFTPW'
Primary_Destination : '47.135.213.53'
Primary_Port     : '22'
Alternate_Destination : '47.135.213.53'
Alternate_Port   : '22'
Start_Time      : '00:00'
Stop_Time       : '23:00'
Interval        : '120'
Remote_Storage_Directory: '/billing'
Remote_Login     : 'test'
Remote_Password  : '*****'
Maximum_Retries  : '3'
Retry_Wait_Time  : '1'
File_Extension   : ''
Field_Separator  : '.'
Active           : 'Yes'

Enter the field name to be changed. Stream, File_Format_Type
and Destination cannot be changed.
Enter 'All' to be prompted for all field names.
Press Enter to accept 'All'.
Enter Field_Name: Protocol

Valid protocols are {'FTPW', 'RFTPW', 'SFTPW', 'KSFTPW'}.
Press Enter to accept 'SFTPW'.
Enter Protocol: KSFTPW
```

WARNING: File Transfer to this destination will fail if OpenSSH is not installed
Please install OpenSSH if it is not already installed.

Primary port can be 22 or between 1025 and 65535.

Press Enter to accept '22'.

Enter Primary_Port:

Alternate port can be 22 or between 1025 and 65535.

Press Enter to accept '22'.

Enter Alternate_Port:

Stream : 'OCC'
File_Format_Type : 'DIRP'
Destination : 'OSS'
Protocol : 'KSFTPW'
Primary_Destination : '47.135.213.53'
Primary_Port : '22'
Alternate_Destination : '47.135.213.53'
Alternate_Port : '22'
Start_Time : '00:00'
Stop_Time : '23:00'
Interval : '120'
Remote_Storage_Directory: '/billing'
Remote_Login : 'test'
Maximum_Retries : '3'
Retry_Wait_Time : '1'
File_Extension : ''
Field_Separator : '.'
Active : 'Yes'

Valid actions are { 'Save', 'Edit', 'Abort' }.

Press Enter to accept 'Edit'.

Enter Action: Save

Schedule tuple changed.

The public key on the CBM is stored at :
/cbmdata/users/maint/.ssh/sba:occ:dirp:oss_rsa.pub

Please append this public key to the user's authorization file on the destination machine.

Press Return to Continue...

Figure 6 Prompts for schedule change (From Key-based to Password).

Valid streams are {'AMA', 'OCC'}.

Press Enter to accept 'AMA'.

Enter Stream: OCC

Valid file format types are {'DIRP'}.

Press Enter to accept 'DIRP'.

Enter File_Format_Type:

Valid destinations are {'OSS', }.

Press Enter to accept 'OSS'.

Enter Destination:

Stream : 'OCC'

File_Format_Type : 'DIRP'

Destination : 'OSS'

Protocol : 'KSFTPW'

Primary_Destination : '47.135.213.53'

Primary_Port : '22'

Alternate_Destination : '47.135.213.53'

Alternate_Port : '22'

Start_Time : '00:00'

Stop_Time : '23:00'

Interval : '120'

Remote_Storage_Directory: '/billing'

Remote_Login : 'test'

Maximum_Retries : '3'

Retry_Wait_Time : '1'

File_Extension : ''

Field_Separator : '.'

Active : 'Yes'

Enter the field name to be changed. Stream, File_Format_Type
and Destination cannot be changed.

Enter 'All' to be prompted for all field names.

Press Enter to accept 'All'.

Enter Field_Name: Protocol

Valid protocols are {'FTPW', 'RFTPW', 'SFTPW', 'KSFTPW'}.

Press Enter to accept 'KFTPW'.

Enter Protocol: SFTPW

WARNING: File Transfer to this destination will fail if OpenSSH is not installed
Please install OpenSSH if it is not already installed.

Primary port can be 22 or between 1025 and 65535.

Press Enter to accept '22'.

Enter Primary_Port:

Alternate port can be 22 or between 1025 and 65535.

Press Enter to accept '22'.

Enter Alternate_Port:

Remote password can have between 1 and 20 characters.

Enter Remote_Password: *****

Re-enter Remote_Password: *****

Stream : 'OCC'
File_Format_Type : 'DIRP'
Destination : 'OSS'
Protocol : 'SFTPW'
Primary_Destination : '47.135.213.53'
Primary_Port : '22'
Alternate_Destination : '47.135.213.53'
Alternate_Port : '22'
Start_Time : '00:00'
Stop_Time : '23:00'
Interval : '120'
Remote_Storage_Directory: '/billing'
Remote_Login : 'test'
Remote_Password : '*****'
Maximum_Retries : '3'
Retry_Wait_Time : '1'
File_Extension : ''
Field_Separator : '.'
Active : 'Yes'

Valid actions are { 'Save', 'Edit', 'Abort' }.

Press Enter to accept 'Edit'.

Enter Action: Save

Schedule tuple changed.

Press Return to Continue...

Figure 7 Prompts for schedule delete (password-based).

```
Stream          : 'OCC'
File_Format_Type : 'DIRP'
Destination      : 'OSS'
Protocol         : 'SFTPW'
Primary_Destination : '47.135.213.53'
Primary_Port     : '22'
Alternate_Destination : '47.135.213.53'
Alternate_Port    : '22'
Start_Time       : '00:00'
Stop_Time        : '23:00'
Interval         : '120'
Remote_Storage_Directory: '/billing'
Remote_Login      : 'test'
Remote_Password   : '*****'
Maximum_Retries   : '3'
Retry_Wait_Time   : '1'
File_Extension    : ''
Field_Separator   : '.'
Active           : 'Yes'

Valid responses are { 'Yes', 'No', 'Abort' }.
Press Enter to accept 'No'.
Delete this tuple? yes

1 schedule tuple(s) deleted.

Press Return to Continue...
```

Figure 8 Prompts for schedule delete (key-based)

```
Stream          : 'OCC'
File_Format_Type : 'DIRP'
Destination      : 'OSS'
Protocol         : 'KSFTPW'
Primary_Destination : '47.135.213.53'
Primary_Port     : '22'
Alternate_Destination : '47.135.213.53'
Alternate_Port    : '22'
Start_Time       : '00:00'
Stop_Time        : '23:00'
Interval         : '120'
Remote_Storage_Directory: '/billing'
Remote_Login      : 'test'
Maximum_Retries   : '3'
Retry_Wait_Time   : '1'
File_Extension    : ''
Field_Separator   : '.'
Active           : 'Yes'

Valid responses are { 'Yes', 'No', 'Abort' }.
Press Enter to accept 'No'.
Delete this tuple? yes

1 schedule tuple(s) deleted.

Press Return to Continue...
```

2.10.3 OMDD specific configuration

This activity modifies the Add, List and Modify File Transfer Destination menus of OMUI. 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.

When the file transfer destination is added or modified, user will be asked to select the type of user authentication, in addition to the already existing parameters. The choices for the type of user authentication will be “Password” and “Key”.

If the user chooses “Key”, a message will be displayed informing the user to dump the contents of the public key file into the authorization file of the destination machine.

Figure 9 shows an example configuration of file transfer destination using Password-based authentication.

Figure 10 shows an example configuration of file transfer destination using Key-based authentication.

The same changes are made in the “Modify File Transfer Destination” menu also.

Figure 11 shows the list of names of the file transfer destinations that are currently configured.

The text in bold indicate the changes to the OMDD UI.

Figure 9 OMUI File Transfer Destination menu (password-based)

Add File Transfer Destination
File Transfer Destination name > ftd1
Destination IP Address > 47.135.214.61
Type of File Transfer: Standard/Secure > Secure
Type of Autentication: Password/Key > Password
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)? Y

Please wait....
ftd1: the request was successful.

Press Enter for File Transfer Destination menu.

Figure 10 OMUI File Transfer Destination menu (key-based)

Add File Transfer Destination

File Transfer Destination name > ftd1
 Destination IP Address > 47.135.214.61
 Type of File Transfer: Standard/Secure > Secure
Type of Authentication: Password/Key > Key
 Destination Port [22] >
 Destination Login > user1
 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)? Y

Please wait....

ftd1: the request was successful.

The public key on the CBM is stored at :
/cbmdata/users/maint/.ssh/OMDD:ftd1_rsa.pub

Please append this public key to the user's authorization file on the destination machine.

Press Enter for File Transfer Destination menu.

Figure 11 List File Transfer Destination

List of File Transfer Destinations

FTD name	IP Address	Transfer type	Port	Login name
ftd1	47.135.214.6	Secure-Password	22	User1
ftd2	47.135.214.6	Secure-Key	22	User2

1. List File Transfer Destination Usage.
 2. Return to File Transfer Destination menu.

Select Option >

Product = CS 2000

CR Q01333369 -- Triggering gateway capabilities audit while changing T.38 network option on CS2K with TGCP gateways

Functional Description

1: Applicable Solution(s)

This applies to a CS2K running SN09FF having GWCs with one or more TGCP gateways provisioned.

1.1 Description

Toggling of T.38 from “OFF” to “ON / LOOSE”, OR from “ON/LOOSE” to “OFF” in the “Network Codec Profile” using CMT, will trigger a GW capabilities audit on all ENABLED TGCP gateways.

The gateways’ response to the GW capabilities audit will be used to update a GWC’s knowledge of gateways’ capabilities (including the TGCP packages supported on the gateways). The GWC will not include T.38 codec-options nor monitor for T.38 events in further TGCP messages if the gateways’ response doesn’t include the FXR package.

1.2 Limitations and restrictions

Craftspersons need to take specific care while deactivating T.38 in the “Network Codec Profile”. They must ensure that T.38 has been deactivated on all provisioned TGCP gateways before deactivating it on CS2K. An outage could be caused if this order of deactivating T.38 is not followed.

Note that the outage caused by the deactivation procedure is due to limitations set by T.38 specifications; that is:

- the dynamic nature in which the GW can alter its capabilities (i.e., in-service upgrades, toggling of T.38 support within the gateway EM)
- it is necessary for the GWC to discover the capabilities of the GW.
- if the GW receives a request for T.38 and it is not enabled on the GW, that request must be NACKed.

Product = CS2K Management Tools

A00009576--RASless Provisioning

Functional Description

1: Applicable Solution(s)

CHS

1.1 Description

This feature delivers the ability for a craftperson to explicitly provision the CS2K with the optional “RAS-less” functionality on a H.323 gateway/gatekeeper basis. The RAS-less capability is configured during gateway association via the CS2K Management Tools server.

H.225 defines RAS (Registration, Admission and Status) messages and procedures for controlling access to the network. These messages allow H.323 endpoints to discover and register with a H.323 gatekeeper, to provide information about their capabilities and to request the allocation of appropriate amounts of bandwidth. For some applications, H225/H245 signaling should be used between the CS2K and another entity (e.g. softswitch, gatekeeper, or gateway) for setting up calls, but with no RAS messages. This mode of operation is deemed “RAS-less”.

The optional RAS-less capability can be provisioned via the GUI or OSSGate XML interface of the CS2K Management Tools server during gateway association. Only H.323 gateways/gatekeepers can be configured with the RAS-less option.

1.1.1 CS2K Management Tools GUI changes

The associate gateway operation has been updated with the ability to configure the optional RAS-less capability. The RASLess option is displayed as part of the GWC Provisioning Panel of the CMT (CS2K Management Tools) GUI. The “Details” button of the Gateway tab has been updated to display the RASLess option configuration setting.

Once the associate media gateway operation is invoked, the corresponding associate media gateway dialog is launched. To configure the RAS-less functionality, a craftperson must choose a H.323 gateway profile from the “Gateway profile name” pull down menu of the associate media gateway dialog box.

If a H.323 gateway profile is chosen, specific H.323 configuration data options are presented. A new optional gateway data application panel has been added to the associate gateway dialog box. The optional “RAS-less” data is presented

as part of the new optional gateway data choices. A craftperson can enable the RAS-less capability by setting the option to “true”. The default value is “false”.

Once all the required data is entered, the “OK” button of the associate media gateway dialog box will be enabled. By clicking on the “OK” button, the GWC EM will process the operation and generate the required SNMP messages. The SNMP messages are sent to the respective GWC. The craftperson will receive a successful or failure response from the GWC EM upon completion of the operation.

The “Details” button of the Gateway tab of the GUI will display the new optional data if supported by the specific gateway profile. A craftperson can click on the Details button to launch a gateway’s Details dialog box. The optional gateway data will be displayed for the respective gateway. The RASLess option is listed in the dialog box if the selected gateway is H.323. If there isn’t any gateway application data defined for the selected gateway, a dialog box will be launched indicating the respective gateway profile does not have any optional data defined.

The Details button is also used to display the associated “root middleboxes” of a respective gateway. Currently, H.323 gateways do not support root middleboxes.

Note: All current H.323 gateway profiles support the new optional RASLess configuration except for the H323_PROXY gateway profile.

1.1.2 OSSGate XML interface changes

The assocMG and queryMG operations of the OSSGate interface have been modified to support the optional RAS-less configuration data. The optional RAS-less data is only applicable to H.323 gateways/gatekeepers.

XML Associate MG changes

The optional RAS-less data has been added to the assocMG operation and can be configured against a H.323 gateway/gatekeeper.

To configure a “RASLess” H.323 gateway/gatekeeper, a valid assocMG XML command must include the optional RAS-less data.

assocMG - specifies the provisioning method. It has two attributes: USN (Unique Sequence Number) and version. The USN is used by an OSS to map requests with responses. The USN value specified in the request is returned in the response. The version attribute specifies the version of the method being used.

Parameters - specifies that the following elements are parameters for the method. Included in the parameters are:

- **mgUIName** - delimits MG name value.
- **mgProfileName** - delimits the MG profile name value to be applied to the MG.
- **mgIpAddr** - delimits the MG IP address value.

The new parameter is:

- *gwAppDataList* - *delimits the new optional data which includes RASLess.*

XML Query MG changes

The optional RAS-less data has been added to the queryMG operation *response* and will only be returned when a H.323 gateway/gatekeeper is queried. The queryMG XML command has not been modified.

queryMG - specifies the provisioning method. It has two attributes: USN and version. The USN is used by an OSS to map requests with responses. The USN value specified in the request is returned in the response. The version attribute specifies the version of the method being used.

Parameters - specifies that the following elements are parameters for the method.

mgUIName - delimits MG name value. When this parameter element is specified the attributes of the MG specified are returned.

If a H.323 gateway/gatekeeper is queried, the RAS-less configuration will be returned via the optional device data parameter.

The optcn component of the A00009576 book contains GUI and XML examples detailing the new RASLess option for H.323 gateways/gatekeepers. The OSS User's Guide details the OSSGate interface.

1.2 Hardware Requirements or Dependencies

There are no hardware requirements or dependencies for the CS2K H.323 RAS-less optional capability.

1.3 Software Requirements or Dependencies

This feature is being delivered as part of the Succession release SN09FF.

1.4 Limitations and Restrictions

- The optional RAS-less feature can only be provisioned against H.323 gateways/gatekeepers on the CS2K.
- The gateway profile “H323_PROXY” does not support the RAS-less functionality.
- The optional RAS-less feature is not supported with a NAT configuration of N:1. The N:1 NAT configuration is when multiple gateways behind a NAT share the same “NAT’d” IP address and the gateways are uniquely identified by the port value.
- The provisioned protocol port value of the H.323 gateway/gatekeeper on the H.323 GWC (via the CMT GUI or XML interface) must be set to the CS (call signaling) port value of the gateway for RAS-less mode. (i.e. If the H.323 gateway is not behind a NAT and the call signaling port value is set to 1720 on the gateway, the gateway’s provisioned protocol port value on the GWC must be set to 1720).
- A RAS-less H.323 gateway that is behind a NAT with a 1:1 configuration (one private IP mapped to one public IP to the H.323 GWC), must have the provisioned protocol port value on the GWC set to a non-zero port value. The non-zero port value on the GWC must be mapped via the NAT to the gateway’s call signaling port value.

1.5 Interactions

This activity enables a craftperson to explicitly provision the RAS-less functionality against a H.323 gateway/gatekeeper on the CS2K. The associate gateway operation processed on the CS2K Management Tools server is updated with the ability accept the optional data via the GUI or XML interface.

1.6 Glossary

Acronym	Definition
CLLI	Common Language Location Identifier
CM	Computing Module
CMT	Call Server 2000 Management Tools
CORBA	Common Object Request Broker Architecture
CPE	Customer Premises Equipment
CS2K	Call Server 2000
DMS	Digital Multiplex System

ETSI	European Telecommunications Standards Institute
GW	Gateway
GWC	Gateway Controller
GWC EM	Gateway Controller Element Manager
H.323	Industry protocol for GW/GK<->GW/GK communication (not an acronym).
IDL	Interface Definition Language
IP	Internet Protocol
ITA	Internet Transparency Agent
LAN	Local Area Network
MIB	Management Information Block
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
PSTN	Public Switched Telephone Network
RAS	Registration, Admission and Status
SDP	Session Description Protocol
SESM	Succession Element and Sub-Element Manager [system]
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSPFS	Succession Solaris Platform Foundation Software

SS7	Signaling System 7
TCP	Transmission Control Protocol
TID	Terminal Identifier
TMM	Trunk Maintenance Manager
TN	Terminal Number
USN	Unique Sequence Number
XML	Extensible Markup Language

2: Configuration Management for A00009576

2.1 Hardware and Software Requirements

This feature is being delivered as part of the Succession release SN09FF.

2.2 Initial Configuration

This activity enables a craftperson to explicitly provision the RAS-less functionality against a H.323 gateway/gatekeeper on the CS2K. The associate media gateway operation processed on the CS2K Management Tools server has been updated with the ability to accept optional device data via the GUI or OSSGate XML interface. The RASLess option is part of the new optional application data. The new optional data, including RASLess, can be queried and viewed via the GUI or XML interface of the CMT (CS2K Management Tools) server.

The CS2K Management Tools server and GWC(s) (Gateway Controllers) must be configured with the SN09FF software.

2.3 Subnet parameters (SESM)

The RAS-less capability is configured during gateway association via the CS2K Management Tools server.

H.225 defines RAS (Registration, Admission and Status) messages and procedures for controlling access to the network. These messages allow H.323 endpoints to discover and register with a H.323 gatekeeper, to provide information about their capabilities and to request the allocation of appropriate amounts of bandwidth. For some applications, H225/H245 signaling should be used between the CS2K and another entity (e.g. softswitch, gatekeeper, or gateway) for setting up calls, but with no RAS messages. This mode of operation is deemed "RAS-less".

2.3.1 New/modified subnet parameters

Table 1 New RAS-less parameter

Parameter name	NEW/ CHANGED/ DELETED/ RELOCATED	Domain (CM or Subnet Management
RASLess	New	associate media gateway, query media gateway

2.3.2 Parameter information

The optional RASLess boolean configures a H.323 gateway/gatekeeper on the CS2K with the RAS-less capability.

2.3.2.1 RASLess

RASLess

2.3.2.1.1 Functional description

The optional RASLess boolean configuration signifies to the CS2K H.323 Gatekeeper application that the respective gateway/gatekeeper will function in a “RAS-less” mode.

2.3.2.1.2 Provisioning rules Range information

Only H.323 gateways/gatekeepers can be configured with the RASLess option.

2.3.2.1.3 Range information

Table 2 Range Information

Minimum	Maximum	Default
boolean option (True or False)	boolean option (True or False)	False

2.3.2.1.4 Activation

The parameter is activated once a H.323 gateway/gatekeeper with the RASLess option set to “True” is provisioned.

2.3.2.1.5 Dependencies

There are no table dependencies.

2.3.2.1.6 Consequences

The RASLess option is a boolean.

2.3.2.1.7 Verification

A craftperson can verify that the RASLess option is working if a H.323 gateway/gatekeeper can successfully register without sending RAS messages to a CS2K H.323 gatekeeper.

2.4 Upgrade Considerations

The RASLess functionality was added to the H.323 GWC in the SN08 release. The functionality was configured by setting the gateway's protocol port value to "1720". During an upgrade from SN08/SN09 to SN09FF, all H.323 gateways/gatekeepers with a provisioned port value of "1720" will have the RASLess boolean set to "True".

2.4.1 Element Management Upgrade

If an attempt is made to provision a H.323 gateway/gatekeeper with the RASLess functionality on a pre-SN09FF H.323 GWC, an error message will be generated and presented to the craftperson via the CS2K Management Tools GUI or XML interface.

2.4.2 Downgrade impact

If a downgrade is executed the RASLess option will be deleted from the respective H.323 gateways/gatekeepers.

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

2.5.1 New GWC-APP-DATA-MIB

Table 3 New or modified tables

MIB name	NEW/CHANGED/ or DELETED
GWC-APP-DATA-MIB	New

2.5.2 Table/MIB/Remote Database Schema information

A new optional GWC-APP-DATA-MIB has been created to convey optional application specific data to the GWC.

2.5.2.1 Name: GWC-APP-DATA-MIB

2.5.2.1.1 Functional description

The new GWC-APP-DATA-MIB is a generic structure to provide the ability of the GWC EM to convey optional application data to the GWC.

2.5.2.1.2 OIDs

The following table lists OIDs for the new GWC-APP-DATA-MIB.

Table 4 OID descriptions

OID	New or Changed	Subfield or refinement	Entry	Explanation and action
appDataGlobalId	New	N/A	GWCDeviceGID	global identifier
appDataTag	New	N/A	Integer	name
appDataValue	New	N/A	String	value

Table 4 OID descriptions

OID	New or Changed	Subfield or refinement	Entry	Explanation and action
appDataEntryStatus	New	N/A	RowStatus	status column for row entry

2.5.2.1.3 Datafill example

The following example shows sample datafill for table Optional Device Data.

globalID, RASLESS, true

2.6 Element Management

2.6.1 New/modified GUIs and Functionality

This section describes the changes to GUI of the CS2K Management Tools server affected as a result of this activity.

Table 5 Modified GUI

GUI name	NEW, CHANGED, or DELETED
Associate Media Gateway	Changed by adding optional application data in SN09FF
Details dialog box of the Gateway tab component	Changed by adding optional application data in SN09FF

2.6.2 GUI information

2.6.2.1 GUI name: Associate Media Gateway

Associate Media Gateway

Gateway name: MY_RASLESS_BCM

Gateway IP address: 10.10.10.10

Gateway controller name: GWC-18

Gateway profile name: NORTEL_BCM

Reserved terminations: 24

Gateway Application Data

Gateway Attributes	Attribute Data
Rasless	true

Internet Transparency

☐ MG outside CS2K VPN, not behind NAT

IP-VPN / LBL Selection

☒ IP-VPN(NATs) ☐ LBLs ☐ IP-VPN(NAT)-LBLs

Adj Network Zone: <none>

Signal Protocol

Protocol type: H.323 (6)

Protocol port: 0

Protocol version: 4.0

OK Cancel

Please note that GUI snapshot above displays the RASLess option for a H.323 gateway during an associate gateway operation.

2.6.2.1.1 Functional description

The Associate Media GW dialog box is displayed by using the configuration menu from the main CMT (CS2K Management Tools) GUI or by selecting the “Associate” button from the Gateway panel of a GWC. This dialog box is used to add gateways to the CMT, which in turn populates the respective GWC

device. The fields that are available with this dialog have not been updated. An optional data component has been added.

2.6.2.1.2 GUI usage and implications

The associate gateway operation has been updated with the ability to configure the optional RAS-less capability. The RASLess option is displayed as part of the GWC Provisioning Panel of the CMT GUI. The Gateway Tab of the GWC Provisioning Panel has been updated to display the RASLess option.

Once the associate media gateway operation is invoked, the corresponding associate media gateway dialog is launched. To configure the RAS-less functionality, a craftperson must choose a H.323 gateway profile from the “Gateway profile name” pull down menu of the associate media gateway dialog box.

If a H.323 gateway profile is chosen, specific H.323 configuration data options are presented. The new optional data panel has been added to the associate gateway dialog box. The optional “RAS-less” data is presented as part of the new optional data choices. A craftperson can enable the RAS-less capability by setting the option to “true”. The default value is “false”.

Once all the required data is entered, the “OK” button of the associate media gateway dialog box will be enabled. By clicking on the “OK” button, the GWC EM will process the operation and generate the required SNMP messages. The SNMP messages are sent to the respective GWC. The craftperson will receive a successful or failure response from the GWC EM upon completion of the operation.

The “Details” button of the Gateway tab of the GUI will display the new optional data if supported by the specific gateway profile. A craftperson can click on the Details button to launch a gateway’s Details dialog box. The optional gateway data will be displayed for the respective gateway. The RASLess option is listed in the dialog box if the selected gateway is H.323. If there isn’t any gateway application data defined for the selected gateway, a dialog box will be launched indicating the respective gateway profile does not have any optional data defined.

The Details button is also used to display the associated “root middleboxes” of a respective gateway. Currently, H.323 gateways do not support root middleboxes.

Note: All current H.323 gateway profiles support the new optional RASLess configuration except for the H323_PROXY gateway profile.

2.6.2.2 GUI name: Gateway tab of the GWC Provisioning Panel

CS2000 Management Tools - rtpgsesm.us.nortel.com (CM CLI: RTPG)

File Fault Configuration Maintenance Windows Help

Device Types
 APS
 Gateway Controller
 UAS

Contents of: Gateway Controller
 Directory Find
 Go To

Gateway Controllers:
 GWC-0
 GWC-1
 GWC-2
 GWC-3
 GWC-4
 GWC-5
 GWC-6
 GWC-7
 GWC-8
 GWC-9
 GWC-10
 GWC-11
 GWC-12
 GWC-13
 GWC-14
 GWC-16
 GWC-18
 GWC-19

GWC-4 Unit 0: 172.16.96.114
 Unit 1: 172.16.96.115

Maintenance Provisioning

Controller Gateways Lines Carriers Media Proxies QoS Collectors IPsec

Retrieval criteria: Retrieve
 Limit results: 25 Replace List Append to List Retrieve All

Gateway List

Name	IP Address	Profile	Max Terms	Re...	Protocol	Prot ...	Prot Port	Adj ITRANS M...
ACME_CAR_GWC4	10.19.199.22	CISCO_2600	4094	24	H.323	4.0	0	NATZ
ACME_EXT_C36_GWC4	10.19.199.22	CISCO_2600	4094	24	H.323	4.0	0	NATZ
ACME_EXT_C72_GWC4	10.19.199.22	CISCO_2600	4094	24	H.323	4.0	0	NATZ
ACME_EXT_S1K_GWC4	10.19.199.22	CISCO_2600	4094	24	H.323	4.0	0	NATZ
BCMX1	10.19.199.135	NORTEL_BCM	4094	24	H.323	4.0	7000	NATA
BCMY2	10.19.199.195	NORTEL_BCM	4094	24	H.323	4.0	6100	NATB
M1Y1	10.19.199.195	SUCCESSION_1000	4094	24	H.323	4.0	7000	NATB
S1000_X1	10.19.199.135	SUCCESSION_1000	4094	24	H.323	4.0	5000	NATA
rtp_lab_cse1k_1	10.19.199.135	SUCCESSION_1000	4094	24	H.323	4.0	8000	NATA
verf_node_1	47.11.197.40	SUCCESSION_1000	4094	24	H.323	4.0	1719	outtsp
verf_node_3	47.11.197.110	SUCCESSION_1000	4094	24	H.323	4.0	1719	outtsp

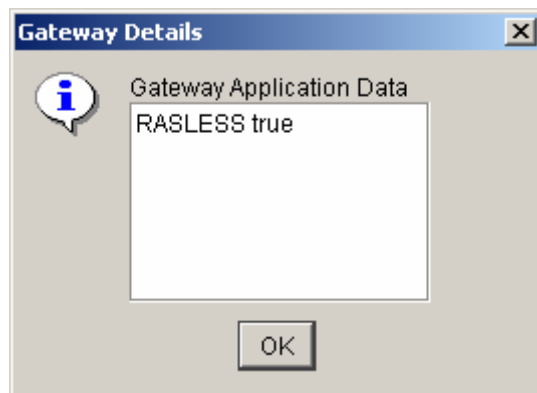
Number of results: 11 Associate... Disassociate Change... Details...

Last update: Jan 20, 2005 3:09 PM Retrieving gateways for GWC-4...Done

Applet running...

To display the gateway optional data, a craftperson must click on the “Details” button in the lower right corner of the Gateway tab. The Gateway tab is a component of the GWC Provisioning Panel.

The GUI snapshot below displays the details of a H.323 RAS-less configured gateway.



2.6.2.2.1 Functional description

The “Details” button of the Gateway tab of the GUI will display the new optional data if supported by the specific gateway profile. A craftperson can click on the Details button to launch a gateway’s Details dialog box. The optional gateway data will be displayed for the respective gateway. The RASLess option is listed in the dialog box if the selected gateway is H.323. If there isn’t any gateway application data defined for the selected gateway, a dialog box will be launched indicating the respective gateway profile does not have any optional data defined.

2.7 User interface changes

2.7.1 OSSGate User Interface

This activity modifies support for the operations listed below:

- **associateMG (updated functionality for H.323)**
- **queryMG response (updated functionality for H.323)**

2.7.2 Terminology & Description of New Method Parameters

2.7.2.1 assocMG

The Associate MG command is the OSSGate XML interface used to datafill media gateways. This interface has been modified by adding the optional device data, which includes the RASLess option.

2.7.2.2 queryMG

The Query MG command is the OSSGate XML interface used to retrieve media gateways provisioned on the CS2K. The query interface will return the new RASLess boolean if the query MG operation was invoked against a RAS-less H.323 gateway/gatekeeper.

2.7.3 H.323 Gateway Certificate Changes

H.323 Nortel BCM Certificate changes example

```
<?xml version="1.0" encoding="UTF-8" ?>
<certificate>

  <MaxEndpoints>4094</MaxEndpoints>
  <Category>LARGE</Category>
  <EndpointType>nocarrierTrkGwcNN</EndpointType>
  <GenerateLGRP>true</GenerateLGRP>
  <ResvTermMandatory>true</ResvTermMandatory>
  <ChangeIPAvailable>true</ChangeIPAvailable>
  <DispPhyLocation>false</DispPhyLocation>
  <InventoryType>H.323 Gateway</InventoryType>
  <InventoryRole>Media Gateway</InventoryRole>
  <SupportedProtocol>
    <protocolName>h323</protocolName>
    <version>4.0</version>
  </SupportedProtocol>
  <GWCPProfileNumber>61</GWCPProfileNumber>
  <EPIDGenDesc>auto1</EPIDGenDesc>
  <ServiceTypeList>H323</ServiceTypeList>
  <ServiceTypeList>ITRANS</ServiceTypeList>
  <CompatibleGWProfileList>NORTEL_BCM</CompatibleGWProfileList>
  <GwAppData name="Rasless" values="false,true" pattern="truefalse"/>

  <GatewayNameFormatList>
    <nameFormat formatKey="GATEWAY.H323" enabled="true">
      <delimiters>`</delimiters>
      <maxTokens>1</maxTokens>
      <name>H323 Gateway</name>
      <tokenFormats>
        <tokenFormat tokenKey="GW">
          <pattern><![CDATA[["'<=>]]></pattern>
          <name>Name</name>
        </tokenFormat>
      </tokenFormats>
    </nameFormat>
    <nameFormat formatKey="GATEWAY.ALL" enabled="true">
      <template>gatewayName</template>
      <delimiters>none</delimiters>
      <minLength>1</minLength>
      <maxLength>32</maxLength>
      <name>Generic For All Gateways</name>
      <tokenFormats>
```

Please note that all the existing H.323 certificates except "H323_PROXY" were updated to include the new RASLess option.

2.7.4 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.

2.7.4.1 Command Examples for Associate MG command

The command syntax for assocMG command has changed from prior releases in reference to adding optional data for H.323 gateways. The syntax is listed here as a convenience.

Example format of an **assocMG** command with RASLess

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <assocMG usn="1" version="1.0">
        <Parameters>
          <mgUIName>MY_RASLESS_BCM</mgUIName>
          <mgProfileName>NORTEL_BCM</mgProfileName>
          <mgIpAddr>47.142.10.10</mgIpAddr>
          <mgProtocolType>6</mgProtocolType>
          <mgProtocolVersion>4.0</mgProtocolVersion>
          <mgProtocolPort>1720</mgProtocolPort>
          <gwcUIName>GWC-18</gwcUIName>
          <reservedTerminations>24</reservedTerminations>
          <gwAppDataList>
            <gwAppData>
              <gwAppTag>Rasless</gwAppTag>
              <gwAppValue>true</gwAppValue>
            </gwAppData>
          </gwAppDataList>
        </Parameters>
      </assocMG>
    </Methods>
  </Command>
</CommandList>
```

2.7.4.2 Command Examples for queryMG command

The command syntax for queryMG command has not changed from prior releases in reference to querying H.323 gateways. The response has changed and now includes the optional data RASLess for H.323 gateways. The syntax is listed here as a convenience.

Example format of a **queryMG** command

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <queryMG usn="1" version="1.0">
        <Parameters>
          <mgUIName>MY_RASLESS_BCM</mgUIName>
        </Parameters>
      </queryMG>
    </Methods>
  </Command>
</CommandList>
```

Example format of a queryMG response with the RASLess option

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
<Response><Interface>cs2kCfgMgrIf</Interface>
<Methods><queryMG usn="1" version="1.0">
<ReturnData>
<Row>
<mgUIList>MY_RASLESS_BCM</mgUIList>
<mgIpList>47.142.10.10</mgIpList>
<callServerId>MY_CS2K</callServerId>
<gwcUIName>GWC-18</gwcUIName>
<svcTypeList>6</svcTypeList>
<svcTypeList>5</svcTypeList>
<nodeName>GWC 18</nodeName>
<itransMiddleboxName>NOT_SET</itransMiddleboxName>
<algName>NOT_SET</algName>
<engrEndPoints>24</engrEndPoints>
<protType>h323</protType>
<protVersion>4.0</protVersion>
<protPort>1720</protPort>
<profileName>NORTEL_BCM</profileName>
<maxEngrEndPoints>4094</maxEngrEndPoints>
<frameNumber>not_set</frameNumber>
<unitNumber>not_set</unitNumber>
<frameType>not_set</frameType>
<floorPos>not_set</floorPos>
<rowPos>not_set</rowPos>
<framePos>not_set</framePos>
<unitPos>not_set</unitPos>
<gwAppDataList>
<gwAppData>
<gwAppTag>RASLESS</gwAppTag>
<gwAppValue>true</gwAppValue>
</gwAppData>
</gwAppDataList>
</Row><RC>0</RC>
<MsgTxt>Query of a Single MG was successful</MsgTxt>
</ReturnData>
</queryMG>
</Methods>
</Response>
</CommandList>
```

2.7.5 XML Schema Listings for affected RASLess H.323 commands

2.7.5.1 Assoc MG

The AssocMG schema has been updated to include the optional application data.

```
<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:element name="frameNumber" type="FrameNumberType" minOccurs="0" />
    <xsd:element name="unitNumber" type="UnitNumberType" minOccurs="0" />
    <xsd:element name="frameType" type="xsd:string" minOccurs="0" />
    <xsd:element name="floorPosition" type="xsd:unsignedShort" minOccurs="0" />
    <xsd:element name="rowPosition" type="xsd:string" minOccurs="0" />
    <xsd:element name="framePosition" type="xsd:unsignedShort" minOccurs="0" />
    <xsd:element name="unitPosition" type="xsd:unsignedShort" minOccurs="0" />
    <xsd:element name="slotPosition" type="xsd:unsignedShort" minOccurs="0" />
    <xsd:choice minOccurs="0">
      <xsd:element name="pepServerName" type="xsd:token" />
      <xsd:element name="algName" type="xsd:token" />
      <xsd:element name="itransMiddleboxName" type="xsd:token" />
      <xsd:element name="rootMiddleboxName1" type="NoSpaceNameType" />
    </xsd:choice>
    <xsd:element name="rootMiddleboxName2" type="NoSpaceNameType" minOccurs="0" />
    <xsd:element name="rootMiddleboxName3" type="NoSpaceNameType" minOccurs="0" />
    <xsd:element name="rootMiddleboxName4" type="NoSpaceNameType" minOccurs="0" />
    <xsd:element name="rootMiddleboxName5" type="NoSpaceNameType" minOccurs="0" />
    <xsd:element name="gwAppDataList" type="GwAppDataListType" minOccurs="0" />
  </xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

The snbase.xsd was updated with the new GwAppDataListType:

```

<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>
<!-- *****
-->
<!-- * Define GwAppDataType -->
<!-- *****
-->
<xsd:complexType name="GwAppDataType">
  <xsd:sequence>
    <xsd:element name="gwAppTag" type="xsd:string"/>
    <xsd:element name="gwAppValue" type="xsd:string"/>
  </xsd:sequence>
</xsd:complexType>
<!-- *****
-->
<!-- * Define GwAppDataListType -->
<!-- *****
-->
<xsd:complexType name="GwAppDataListType">
  <xsd:sequence>
    <xsd:element name="gwAppData" type="GwAppDataType" minOccurs="0"
maxOccurs="20"/>
  </xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

2.7.5.2 Query MG

No changes have been made to the QueryMG schema. The response for H.323 gateways will include the gateway optional data.

2.8 Limitations and Restrictions

- The optional RAS-less feature can only be provisioned against H.323 gateways/gatekeepers on the CS2K.
- The optional RAS-less feature is not supported with a NAT configuration of N:1. The N:1 NAT configuration is when multiple gateways behind a NAT share the same “NAT’d” IP address and the gateways are uniquely identified by the port value.
- The gateway profile “H323_PROXY” does not support the RAS-less functionality.
- The provisioned protocol port value of the H.323 gateway/gatekeeper on the H.323 GWC (via the CMT GUI or XML interface) must be set to the CS (call signaling) port value of the gateway for RAS-less mode. (i.e. If the H.323 gateway is not behind a NAT and the call signaling port value is set to 1720 on the gateway, the gateway’s provisioned protocol port value on the GWC must be set to 1720).
- A RAS-less H.323 gateway that is behind a NAT with a 1:1 configuration (one private IP mapped to one public IP to the H.323 GWC), must have the provisioned protocol port value on the GWC set to a non-zero port value. The non-zero port value on the GWC must be mapped via the NAT to the gateway’s call signaling port value.

2.9 Configuration Walkthrough

2.9.1 Adding a H.323 GW with RASLess option

- SN09FF
 - Add a H.323 GWC to the system
 - Associate GW with the GWC including the RASLess option set to “true”
 - Adds GW to GWC
 - Add a H.323 Carrier
 - Adds EPG to GW

Product = CS 2000

A00010742--GWC EM Enhancements to support SIREN

Functional Description

1: Applicable Solution(s)

PT-IP, UA-IP, IAW, IAC, MCS, Int'l IAW, Int'l IAC, Int'l PT-IP, Int'l UA-IP

1.1 Description

In Succession, the provisioning of a Gateway Controller Card (GWC) is performed by the GWCEM/SESM and the SAM21 software components.

The SAM21 component is responsible for provisioning sufficient card data to identify the card (e.g., the IP addresses and the software load file location), and to initiate the booting of the GWC application.

The GWCEM/SESM component is responsible for provisioning all other data required for the GWC to operate as a switch (e.g., gateway data, endpoint data, alarm processing, trap processing, IPSEC data, middle boxes, timing parameters, sizing limitations, capabilities, etc.). Also included is an array of activities which include, for example, the ability to audit, monitor, patch, alarm, initiate card imaging, core provisioning and synchronization, and general health and maintenance of the GWC devices and their application processing.

For Siren, the SAM21 component is being replaced by various Siren subsystems (e.g., Config, AMF, and MTCE). In addition, the GWC application itself is being moved onto new Siren blades, and may be modified to use new interfaces within the Siren platform.

The GWCEM/SESM software will still reside on the Sun N240 SSPFS platform. The items implemented by this feature are the design changes required for the GWCEM and the SESM software to function correctly with the removal of the SAM21 component, and to address any changes required in the GWCEM to GWC interfaces made as a result of the GWC incorporation into the new Siren architecture.

This feature implements the changes required to allow the GWCEM/SESM to provide the same provisioning functionality with the newly based GWC on the Siren ATCA platform.

1.1.1 User Interface Changes

There are two user interface changes made by this activity in the GWC EM GUI.

1. In Siren configuration, the ability to bring up the SAM21 card view of the GWC card is removed, and the warm and cold swact buttons are replaced with a single 'swact' button. There is no change for Carrier VoIP installations.

2. In both Siren and Succession configurations, the 'Add GWC' dialog box will now prompt only for GWC name and not the IP address. The IP addresses will be determined internally by the hardware management software. The GWC names are listed in a pulldown menu for selection. This list contains GWCs that are provisioned in the hardware manager (SAM21EM for Succession, CLI on Typhoon for Siren), but not yet provisioned in the EM.

There is also one change made to the OSSGate XML schema. For the add GWC (addGWCtoCS) operation, the GWC IP address will now be looked up using the GWC name (gwcUIName). Therefore, the active IP address (gwcActvIp) is no longer required by the EM software and is being made optional. Note that this parameter may still be specified, but it will be ignored.

1.2 Hardware Requirements or Dependencies

For customers continuing with the Succession product line, there are no new hardware requirements.

For customers choosing the Siren product line, there are no new hardware requirements specifically for this activity, but changes are made to the current GWC EM software to work with the new Siren product line.

1.3 Software Requirements or Dependencies

For customers continuing with the Succession product line, there are no new software requirements or dependencies.

For customers choosing the Siren product line, there are no new software requirements specifically for this activity, but changes are made to the current GWC EM software to work with the new Siren product line.

1.4 Limitations and restrictions

This feature does not address Succession to Siren migration for SESM/GWC EM.

1.5 Interactions

Not Applicable

1.6 Glossary

Term	Description
GWC	Gateway Controller
EM	Element Manager

2: Configuration Management for A00010742

2.1 Hardware and Software Requirements

The components modified by this feature, GWC EM and SESM, will be delivered as part of the CS2M load (CS2K Management Tools). CS2M requires the SSPFS (Solaris Software Platform Foundation Software) load as its platform software. The software will interact with GWCs and other necessary components within the Succession and Siren environments.

2.2 Initial Configuration

The CS2M install scripts will be changed to prompt the user if running in Succession or Siren environment. If running in Siren environment, then the SAM21EM software will not be installed. Also, the configure script will prompt the user for the Siren shelf's IP address and port and a userid and password to enable communication from the EM to the Siren shelf.

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

Not applicable

2.4 Upgrade Considerations

2.4.1 Dump and Restore (CM)

None

2.4.2 Element Management Upgrade

The SESM configuration information as to whether it is configured as Siren or Succession should be saved over an upgrade. Upgrade procedures will be the same as the Succession CS2M upgrade procedures.

It should be noted that this feature does not address Succession to Siren migration for SESM/GWC EM.

2.4.3 Downgrade impact

Downgrades are not applicable for the first release.

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

Not applicable

2.6 Service Orders (SO) (CM & SESM)

Not applicable

2.7 Software optionality control (SOC)

Not applicable

2.8 Element Management

The GWCEM/SESM component of the CS2K Management Tools is used to perform configuration and provisioning of GWCs.

2.8.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
GWC EM	Changed

2.8.2 GUI information

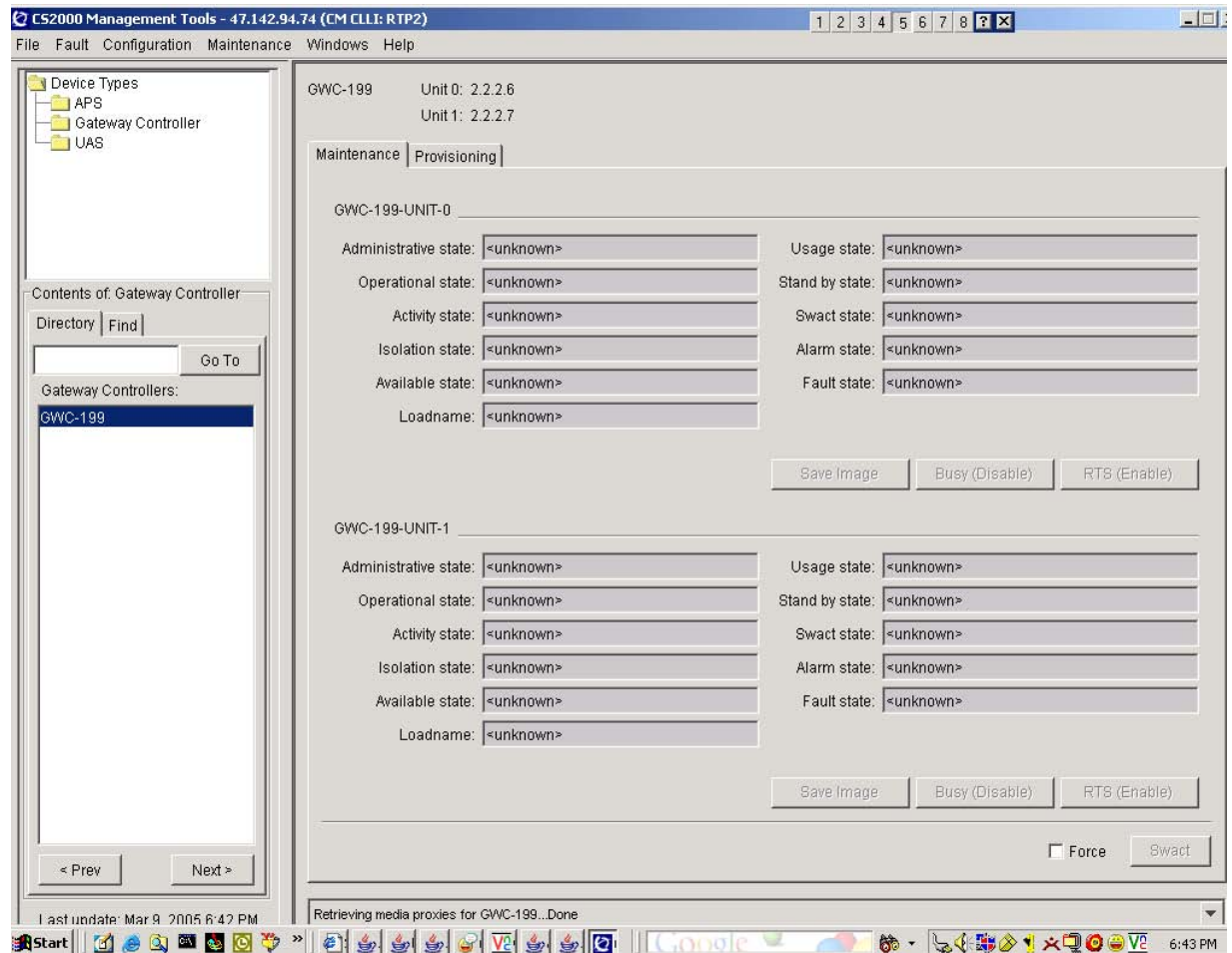
2.8.2.1 GUI name: GWC EM

Gateway Controller Element Manager

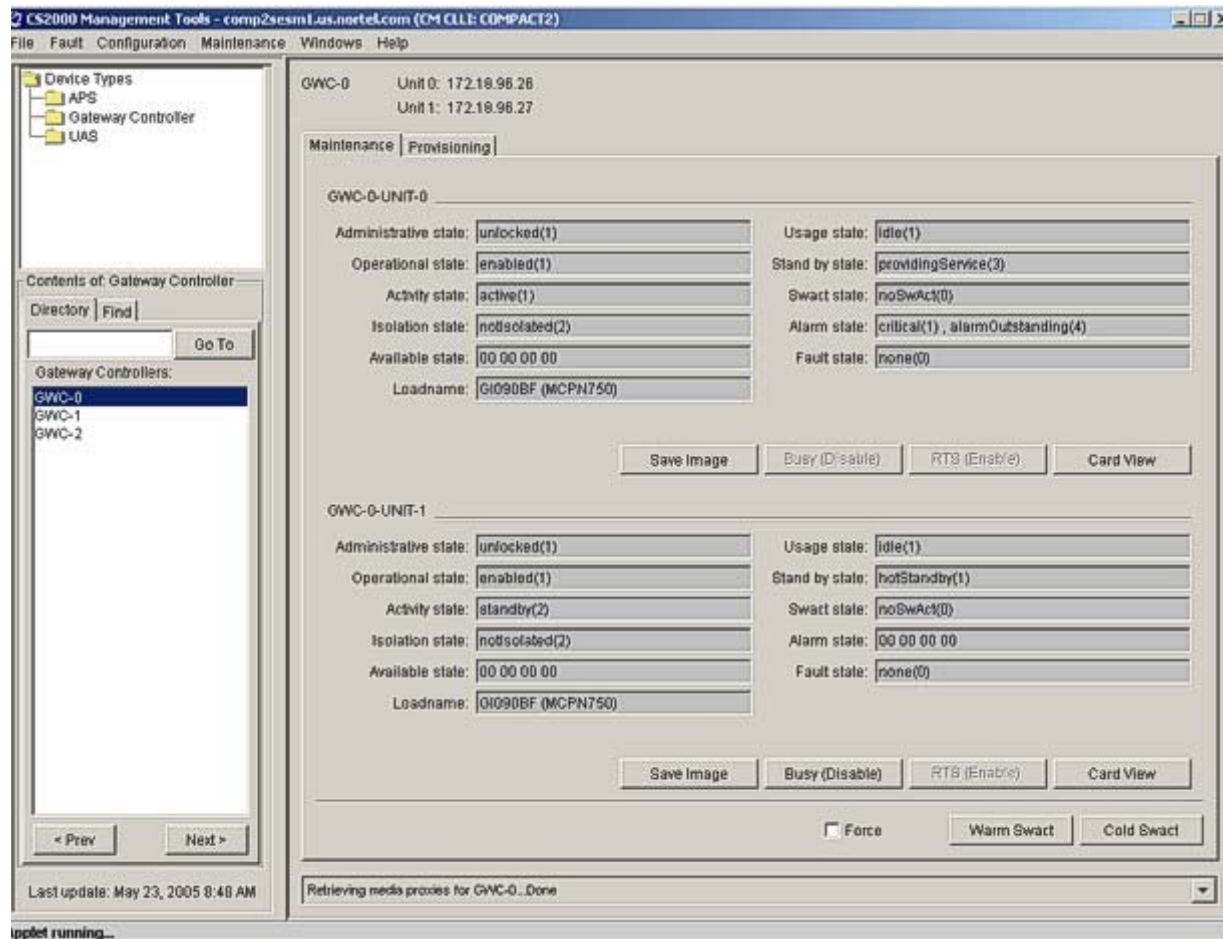
2.8.2.1.1 Functional description

There are two modifications necessary in the GWC EM GUI.

1. In Siren configuration, the ability to bring up the SAM21 card view of the GWC card is removed, and the warm and cold swact buttons are replaced with a single 'swact' button. The following picture shows the changes necessary for the Siren platform.



For clarity, it should be noted that for Carrier VoIP installations, the card view button will still be present, and the warm and cold swact buttons are not changed. This is shown below.



- In both Siren and Succession configurations, the 'Add GWC' dialog box will now prompt only for GWC name and not the IP address. The IP addresses will be determined internally by the hardware management software. This picture shows the list of GWC's displayed to the user. These GWC's are the Gateway Controllers already provisioned in the Siren Shelf (in case of Siren) or SAM21 (in case of Succession).

Add Gateway Controller

Gateway controller name: GWC-0

Gateway default domain name: GWC-0
GWC-1
GWC-2

GWC Profile Information

Gateway controller profiles: APG

Tone data: NORTHAM

Term Type	Exec Data
ABTRK	GWCEX

Capability	Capacity
APG	6048
APG GWs	3
IPSEC	

GWC Bearer Networks and Codec Profile Information

Bearer networks: NET_IP(IP)

GWC codec profile: MadMax

OK Cancel

2.8.2.1.2 GUI usage and implications

Current datafill order unchanged.

2.8.2.1.3 GUI size

No changes

2.8.2.1.4 GUI fields

Not applicable

2.8.2.1.5 Usage example

See screen examples in section <cross-ref>“Functional description” .

2.8.2.1.6 GUI release history update

The IP address field is removed from the ‘Add GWC’ dialog.

The ‘Card View’ button is removed in the Siren environment, and the ‘Warm Swact’ and ‘Cold Swact’ buttons are combined into a single ‘Swact’ button.

2.8.2.1.7 Context sensitive launching information

No changes

2.8.2.1.8 Supplementary information

Not applicable

2.9 User interface changes

Not applicable

2.10 OSSGate Interface Changes

2.10.1 XML Command Changes

The Add GWC (addGWctoCS) operation is modified to make parameter gwcActvIp optional. The IP address will be looked up using the GWC name (gwcUIName). The tag is made optional because we do not want to change the current external OSS interface. If gwcActvIp is provided, it will not be used.

2.10.1.1 Command XML

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <addGWctoCS usn="1" version="1.0">
        <Parameters>
          <csUIName>COMPACT6</csUIName>
          <gwcUIName>GWC-12</gwcUIName>
          <profileName>LARGE_LINENA</profileName>
          <gwcSnmpPort>161</gwcSnmpPort>
          <msgRouterIp>47.142.128.144</msgRouterIp>
          <msgRouterIpPort>4684</msgRouterIpPort>
          <bearerNetworkName>NET_IP</bearerNetworkName>
          <bearerFabricType>IP</bearerFabricType>
          <codecProfileName>Test</codecProfileName>
          <termType>POTS</termType>
          <termType>KEYSET</termType>
          <execLineup>POTSEX</execLineup>
          <execLineup>KSETEX</execLineup>
        </Parameters>
      </addGWctoCS>
    </Methods>
  </Command>
</CommandList>
```

2.10.1.2 Response XML

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Response>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <addGWCtoCS usn="1" version="1.0">
        <RC>0</RC>
        <MsgTxt>Add GWC operation was successful</MsgTxt>
      </addGWCtoCS>
    </Methods>
  </Response>
</CommandList>
```

2.10.2 Additional OSSGate Changes

None

2.11 Security

Not applicable

2.12 Configuration Walkthrough

Not applicable

Product = CS 2000

A00011827--GWC Autonomous SWACT

Functional Description

1: Applicable Solution(s)

UA-IP

1.1 Description

The objective of this feature is to provide an optional capability for Gateway Controllers (GWCs) to autonomously switch activity (SWACT) when communication has been lost with all associated media gateways. This functionality adds an additional layer of redundancy to the network in an attempt to reduce Call Processing outages during partial network failures.

1.1.1 Overview

The autonomous SWACT is an additional option provided to the customer for utilizing redundant network components. The autonomous SWACT functionality is on a GWC node basis and is only supported on GWCs supporting trunk and/or large line gateways. This option is provided as an attempt to automatically recover lost communication between the GWC and its associated media gateways. An autonomous SWACT of the GWC is by no means guaranteed to recover communication between the network components; however, it provides an additional mechanism for the customer to reduce outages and minimize the need for manual intervention.

An autonomous SWACT of a GWC is only performed after the provisioned timer expires, given that the timer is started after all associated media gateways, for that GWC, have been taken out of service by the GWC, and the messaging queues that notify the Core of the state transitions have been processed. The time period to wait before performing a SWACT is a provisionable value on a per GWC basis through the CMT GUI. The delay period helps to ensure the GWCs will not autonomously SWACT during brief network interruptions.

Prior to an autonomous SWACT, the GWC will verify that the inactive unit is in-service and capable of accepting activity. The GWC cannot guarantee connectivity to the gateways will be restored after the SWACT is performed. Depending on the location of the outage in the network, the SWACT may, or may not, restore connectivity.

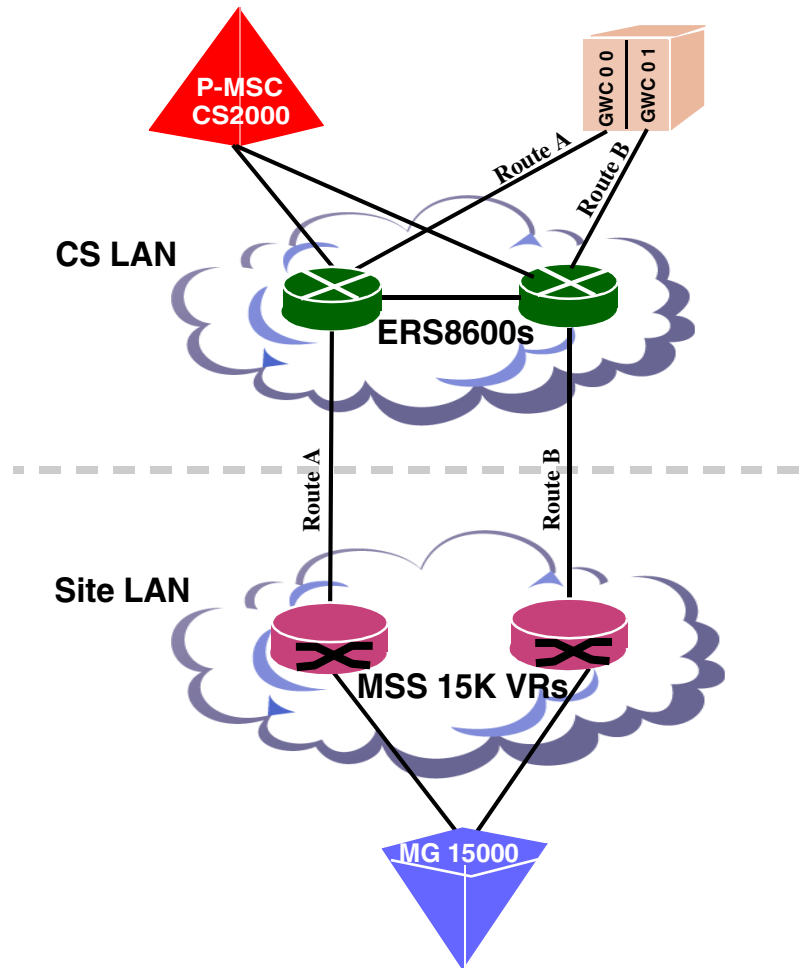
After an autonomous SWACT, the newly active unit will not attempt another autonomous SWACT until communication has been restored to at least one gateway. Until communication can be verified between the GWC and at least one gateway, additional SWACTs will provide no appreciable benefit in recovering communication with the gateways.

To assist the customer with identifying network failures, a critical alarm is raised in CMT when communication is lost with the GWC's associated gateways. A second critical alarm is raised when the autonomous SWACT has been initiated.

1.1.2 Network Topology

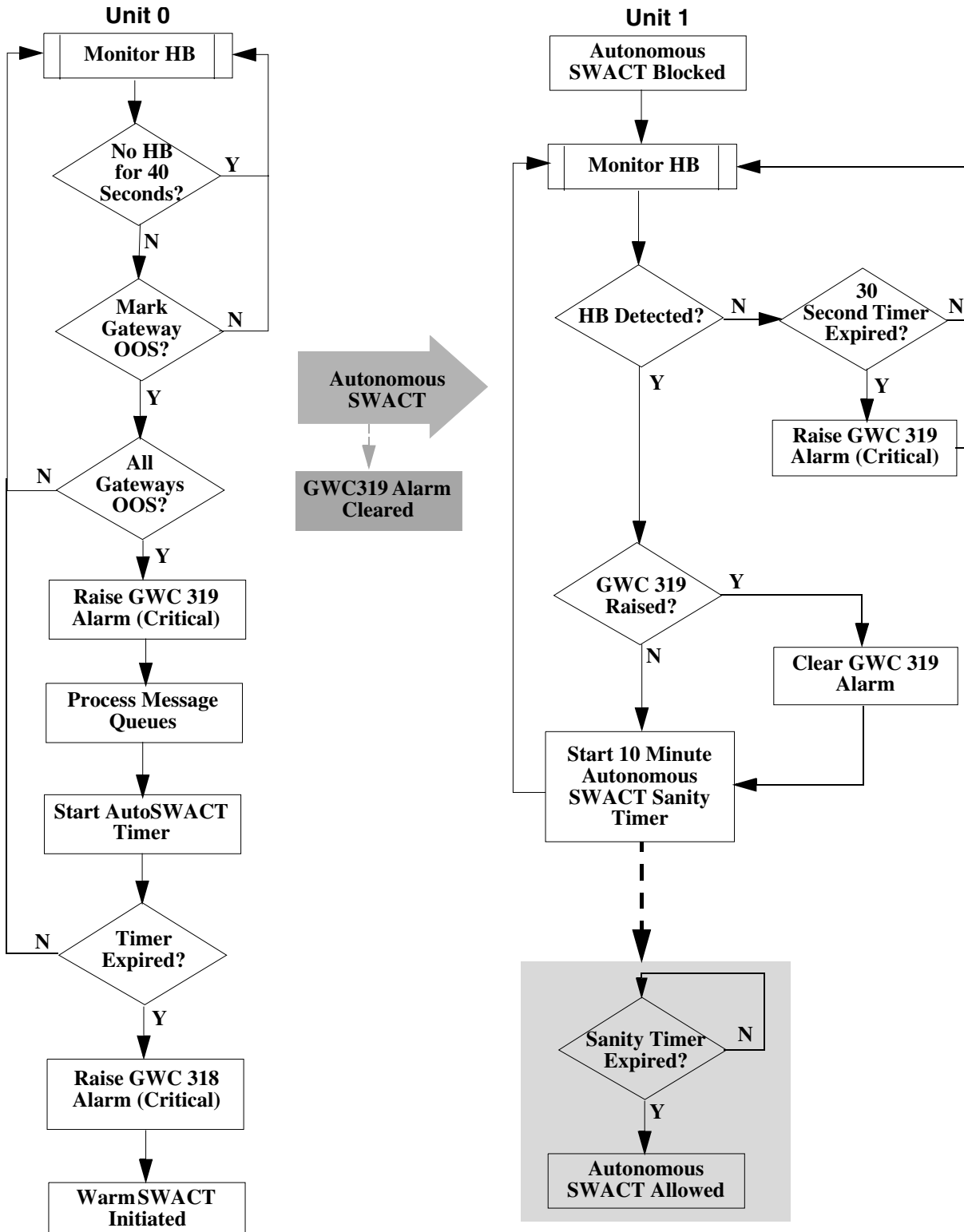
In certain network configurations, an autonomous SWACT may recover lost communication between the GWC and its associated media gateways.

In the following network diagram, each GWC unit is associated with a different MSS 15000 Virtual Router (MSS 15000 VR). In the event the MSS 15000 VR associated with the active unit encounters a network fault, a SWACT to the mate GWC unit will utilize the redundant path restoring communication between the GWC and the media gateway.

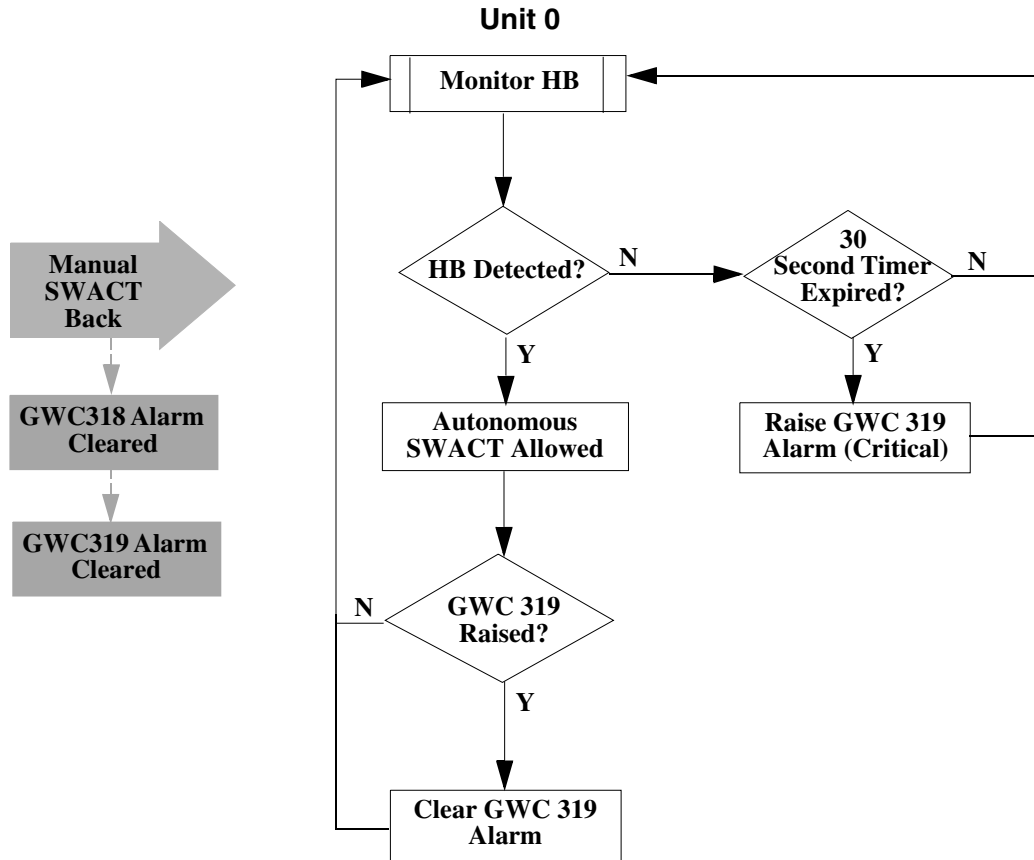
Figure 1 Network Configuration

1.1.3 Flow Diagram

The following diagram details the flow of control for the GWC autonomous SWACT functionality. In the flow diagram that follows, HB refers to heartbeat.



The following diagram shows the logic flow following a manual Warm SWACT back to the original active unit following an autonomous SWACT.



1.2 Autonomous SWACT Controls

1.2.1 GWC Safeguards

Safeguards have been added in the GWC to prevent

- an autonomous SWACT from occurring prior to an outage condition being cleared, and,
- to prevent an autonomous SWACT from being performed too soon after the system has recovered.

After the autonomous SWACT has completed, the newly active unit prevents a second autonomous SWACT from occurring until the previous condition has been cleared.

Once the condition is cleared, a ten (10) minute sanity timer is started. During this ten minute period autonomous SWACT requests are queued. When the sanity timer expires, the request is processed as normal.

Should the condition clear, either while the request is queued, or while the time delay is being processed, the request will be canceled and no SWACT will occur.

1.2.2 Manual SWACT Interactions

At no time are manual SWACT requests from the GWC element manager blocked due to the autonomous SWACT functionality. Manual SWACTs are processed regardless of the state of the autonomous SWACT functionality. Any pending autonomous SWACT requests are canceled when a manual SWACT is processed.

1.3 Call Management

The autonomous SWACT application performs a Warm SWACT to switch activity to the mate unit. The Warm SWACT permits stable calls to remain active over the SWACT for certain gateway and call types. The handling of calls over the SWACT is described in the following sections.

1.3.1 H.248 Trunk Gateways

1.3.1.1 ISUP and PRI Trunk Calls

Calls on ISUP and PRI trunks remain active on the Call Server when heartbeat is lost with the gateway. When the gateway is determined to be unresponsive, the gateway is taken out-of-service and trunks with stable calls are transitioned from the Call Processing Busy (CPB) state to the Call Processing Deload (CPD) state. Once communication is restored, trunks in the CPD state are transitioned back to the CPB state.

1.3.1.2 PTS Trunk Calls

PTS trunk calls do not survive when the gateway is taken out-of-service. When the gateway is determined to be unresponsive, and subsequently taken out-of-service, all calls are immediately released.

1.3.2 TGCP Trunk Gateways

TGCP trunk calls do not survive when the gateway is taken out-of-service. All calls on TGCP gateways are immediately released when the gateway is determined to be unresponsive and taken out-of-service.

1.3.3 Line Gateways

1.3.3.1 Large Line Gateways

Large line gateways may provide Emergency Standalone (ESA) capabilities. For such gateways, intra-switched calls survive when the gateway is taken

out-of-service; however, all other calls are released when the gateway is taken out-of-service.

1.3.3.2 Small Line Gateways

The autonomous SWACT functionality is not supported for GWCs supporting small line gateways.

1.4 Provisioning

The autonomous SWACT functionality is provisionable on a per GWC node basis. When a GWC is added the functionality is disabled, which is the default state. The CMT GUI is used to enable, or disable, the functionality. The GUI also provides the ability to set the timer value. The timer value identifies the time to wait before performing the autonomous SWACT after the loss of communication has been identified.

Please refer to the Configuration section of this document for provisioning details.

1.5 Logs and Alarms

New CMT alarms and logs are generated to indicate actions taken by the autonomous SWACT activity. This section provides a brief description of the alarms and logs. Please refer to the Fault Management section of this document for complete details.

1.5.1 Alarms

Two new critical CMT alarms are created to supplement existing major alarms which are raised when communication is lost to a gateway. The new alarms identify these conditions:

- Communication with the GWC's associated gateways is down
- Autonomous SWACT initiated

The first alarm is raised if communication to the GWC's associated gateways is lost. This alarm is cleared when communication is detected with at least one associated gateway. It is also cleared when the GWC is manually or automatically SWACT and is raised again on the newly active unit if communication is still lost with all the associated gateways.

The second alarm is raised when an autonomous SWACT is initiated from the unit detecting the communication outage. This alarm indicates that the system has taken action to correct the problem. The alarm is cleared

- manually from the CMT interface, or
- when activity is switched back to the original unit.

Additional information on clearing this alarm manually may be found in the Configuration (CN) section of this document.

These alarms are raised in addition to the existing major alarms raised against each gateway that loses communication with the GWC. Individual gateway alarms are raised prior to the SWACT and cleared as communication is restored to the gateways.

1.5.2 Customer Logs

Customer logs are generated for the raising and clearing of alarms. Please refer to the Fault Management section for a list of the supported logs.

1.6 Hardware Requirements or Dependencies

The autonomous SWACT activity does not require special hardware. The autonomous SWACT functionality is supported on the MCPN750, MCPN905, and ATCA platforms.

1.7 Software Requirements or Dependencies

The autonomous SWACT functionality is available for packetized voice solutions that utilize IP solutions (IP over GigE and AAL5) and ATM solutions (Voice over AAL2) with these products:

- MSC Server 1000
- MSC Server 2000
- CS 2000 (North American and International software loads)
- CS 2000 - Compact (North American and International software loads)

1.8 Limitations and restrictions

1. The capability to enable GWC autonomous SWACT is available on CMT for all GWCs, but the GWC autonomous SWACT action can only occur on GWCs hosting trunk and/or large line gateways. This action can not occur on GWCs hosting audio servers or small line gateways.
2. The GWC cannot verify the autonomous SWACT will restore lost communication to the associated gateways prior to attempting the SWACT.

1.9 Interactions

None.

1.10 Use Cases

1.10.1 Network Outage, GWC SWACT Recovers Gateways

1. The loss of communication with a gateway is detected.
2. The gateway is taken out-of-service.

3. It is confirmed that all associated media gateways have lost communication with this GWC.
4. The critical alarm (GWC 319) is raised indicating communication with all associated media gateways has been lost.
5. It is confirmed that all messaging queues have completed processing.
6. The SWACT is delayed for the duration of the timer value provisioned in the CMT.
7. A critical alarm (GWC 318) is sent to CMT indicating a autonomous SWACT is being initiated.
8. A Warm SWACT is performed, clearing the GWC 319 alarm.
9. The newly active unit monitors for communication with the associated media gateways.
10. Communication with at least one gateway is detected.
11. A ten (10) minute sanity timer is started to prevent further autonomous SWACTs until the timer expires.
12. After the sanity timer expires, autonomous SWACTs are again permitted.

Note: If communication with all associated media gateways is lost while the sanity timer is running, a SWACT event is queued and processed upon expiration of the sanity timer. Should communication be restored while the event is still queued, the event is cancelled and no SWACT is performed.

1.10.2 Network Outage, GWC SWACT Delayed Recovery

1. The loss of communication with a gateway is detected.
2. The gateway is taken out-of-service.
3. It is confirmed that all associated media gateways have lost communication with this GWC.
4. The critical alarm (GWC 319) is raised indicating communication with all associated media gateways has been lost.
5. It is confirmed that all messaging queues have completed processing.
6. The SWACT is delayed for the duration of the timer value provisioned in the CMT.

7. A critical alarm (GWC 318) is sent to CMT indicating a autonomous SWACT is being initiated.
8. A Warm SWACT is performed, clearing the GWC 319 alarm.
9. The newly active unit monitors for communication with the associated media gateways.
10. No communication is detected after thirty (30) seconds.
11. The critical alarm, GWC 319, is raised indicating communication with all associated media gateways has not been recovered.
12. The GWC continues to monitor for heartbeat from associated media gateways.
13. Communication with at least one media gateway is detected.
14. The GWC 319 alarm is cleared.
15. A ten (10) minute sanity timer is started to prevent further autonomous SWACTs until the timer expires.
16. After the sanity timer expires, autonomous SWACTs are again permitted.

Note: If communication with all associated media gateways is lost while the sanity timer is running, a SWACT event is queued and processed upon expiration of the sanity timer. Should communication be restored while the event is still queued, the event is cancelled and no SWACT is performed.

1.10.3 Manual Warm SWACT back to the original GWC unit when Communication has not been restored with an Autonomous SWACT

1. The loss of communication with a gateway is detected.
2. The gateway is taken out-of-service.
3. It is confirmed that all associated media gateways have lost communication with this GWC.
4. The critical alarm (GWC 319) is raised indicating communication with all associated media gateways has been lost.
5. It is confirmed that all messaging queues have completed processing.
6. The SWACT is delayed for the duration of the timer value provisioned in the CMT.

7. A critical alarm (GWC 318) is sent to CMT indicating a autonomous SWACT is being initiated.
8. A Warm SWACT is performed, clearing the GWC 319 alarm.
9. The newly active unit monitors for communication with the associated media gateways.
10. No communication is detected after thirty (30) seconds.
11. The critical alarm, GWC 319, is raised indicating communication with all associated media gateways has not been recovered.
12. A manual Warm SWACT is performed from the CMT
13. Both the GWC 318 and GWC 319 alarms are cleared
14. The newly active unit monitors for communication with the associated media gateways.
15. No communication is detected after thirty (30) seconds.
16. The critical alarm, GWC 319, is raised indicating communication with all associated media gateways has not been recovered.
17. The GWC continues to monitor for heartbeat from associated media gateways.
18. Communication with at least one media gateway is detected.
19. The GWC 319 alarm is cleared.

1.11 Glossary

Term	Description
ATCA	Advanced Telecom Computing Architecture
CS2000	Call Server 2000
CDMA	Code Division Multiple Access
CMT	CS2000 Management Tools
ERS8600	Ethernet Routing Switch 8600
ESA	Emergency Standalone
GWC	Gateway Controller
ISUP	ISDN User Part
MSC	Mobile Switching Center

Term	Description
P-MSC	Packet Mobile Switching Center
PRI	Primary Rate Interface
PTS	Per Trunk Signaling
SWACT	Switch of Activity
TGCP	Trunking Gateway Control Protocol
VR	Virtual Router

2: Fault Management for A00011827

2.1 Fault management strategy

Two new critical CMT alarms are introduced by this activity. The new alarms identify the following conditions:

- Communication with the GWC's associated gateways is down
- Autonomous SWACT initiated

The first alarm is raised if communication to the GWC's associated gateways is lost. This alarm is cleared when communication is detected with at least one associated gateway. It is also cleared when the GWC is manually or automatically SWACT and is raised again on the newly active unit if communication is still lost with all the associated gateways.

The second alarm is raised when an autonomous SWACT is initiated due to a loss of communication to all the associated media gateways. This alarm indicates that the system has taken action in an attempt to restore communication. This alarm remains active until manually cleared or gets automatically cleared when the GWC is SWACT back to the original active unit.

These alarms are raised in addition to the existing major alarms raised against each gateway that loses communication with the GWC. These alarms are raised prior to the SWACT and cleared as communication is restored to each individual gateway after the SWACT.

2.2 Fault management tools and utilities

2.2.1 Faults, Alarms and Logs

New logs and alarms are generated as tools to identify a potential network outage. The new alarms are:

- GWC 318 - Indicates that an autonomous SWACT has been initiated

- GWC 319 - Indicates that communication with the GWC's associated gateways is down

Along with the alarms the following logs are generated.

- PM181 - GWC SWACT indication with reason

2.3 Logs

2.3.1 Log Title/Log ID: PM181

2.3.1.1 Formats

2.3.1.1.1 NTSTD

Row 1: <Log Header>

Row 2: <Event>

Row 3: <Reason>

2.3.1.2 Example

```
RTPY09AW          PM181 APR27 08:13:20 2502 INFO GWC 7
                   GWC activity dropped.
                   Reason: no GW communication
```

2.3.1.3 Explanation

The existing PM181 is used to report a GWC SWACT has occurred. The format of this log is unchanged.

The Autonomous SWACT activity adds a new reason to the PM181 log to indicate the cause of the autonomous SWACT. In this case, the reason indicates that a SWACT has occurred due to loss of communication with all associated media gateways.

2.3.1.4 Field descriptions

Table 1: Field descriptions

Field	Value	Description
Reason	no GW communication	Communication with all associated media gateways has been lost.

2.3.1.5 Action

This log indicates a problem in the network exists. The Element Managers for related network components should be used to identify the root cause.

2.3.1.6 Associated Operational Measurements or Performance Measurements

N/A

2.3.1.7 Additional information

None

2.4 Alarms

2.4.1 GWC 318

2.4.1.1 Integrated Element Manager GUI Fields

Table 2: IEMS/SESM Alarm GUI Field descriptions: GWC 318

Field	Value
Severity	Critical
Category	Communications
LogName	GWC
LogNumber	318
ProbableCause	Underlying resource unavailable
SpecificProblem	<Element Name>: No communication with associated media gateway(s)
BodyText	Autonomous SWACT initiated

2.4.1.2 Example of Alarm in CMT Alarm Manager

Log Name:GWC 318

NE Name:GWC-9-UNIT-0

Alarm Level:Critical

Category:Communications

Alarm Time:15:17:33 16-Nov-2005 EST

Probable Cause:Underlying resource unavailable

SystemUptime:23 hours, 10 minutes, 4 seconds.

Component ID: GWC=GWC-9-UNIT-0;Version=GN91AWJK; Unit=unit_0;Software=AUTOSWACT

Alarm Description: Autonomous SWACT initiated

Specific Problem: GWC-9-UNIT-0: No communication with associated media gateway(s)

2.4.1.3 Explanation

Description: This log indicates that the autonomous SWACT has been initiated to restore communication with the GWC's associated media gateways.

Severity: Critical

2.4.1.4 Action

The Element Managers for related network components should be consulted to identify failures within the network. This alarm can be manually cleared or gets automatically cleared when the GWC is swact back to the original active unit.

2.4.1.5 Corresponding Clear Log

GWC 399

2.4.1.6 Syslog Format of Alarm Clear

```
Nov 17 01:48:39 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=1510~~ GWC399 NONE INFO GWC
Fault^M Location: GWC-9-UNIT-0^M NotificationID: 5^M State: Clear^M Time: Nov 16 15:17:54
2005^M Component Id: GWC=GWC-9-UNIT-0;Version=GN91AWJK;Unit=unit_0;
Software=AUTOSWACT^M Description: Autonomous SWACT initiated
```

2.4.1.7 NTSTD

```
znc0s0jh *** GWC 318 NOV16 15:17:33 0126 TBL GWC Fault
Location: GWC-9-UNIT-0
NotificationID: 5
State: Raise
Category: communications
Cause: underlyingResourceUnavailable
Time: Nov 16 15:17:33 2005
Component Id: GWC=GWC-9-UNIT-0;Version=GN91AWJK; Unit=unit_0;Software=AUTOSWACT
Specific Problem: GWC-9-UNIT-0: No communication with associated media gateway(s)
Description: Autonomous SWACT initiated
```

2.4.1.8 SCC2

```
*C17 GWC 318 0115 TBL GWC Fault
Location: GWC-9-UNIT-0
NotificationID: 5
State: Raise
Category: communications
Cause: underlyingResourceUnavailable
Time: Nov 16 15:17:33 2005
Component Id: GWC=GWC-9-UNIT-0;Version=GN91AWJK; Unit=unit_0;Software=AUTOSWACT
Specific Problem: GWC-9-UNIT-0: No communication with associated media gateway(s)
```

Description: Autonomous SWACT initiated

2.4.1.9 Syslog

Nov 17 01:48:18 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=1500~~ GWC318 CRIT TBL GWC Fault^M Location: GWC-9-UNIT-0^M NotificationID: 5^M State: Raise^M Category: communications^M Cause: underlyingResourceUnavailable^M Time: Nov 16 15:17:33 2005^M Component Id: GWC=GWC-9-UNIT-0;Version=GN91AWJK;Unit=unit_0;Software=AUT^M OSWACT^M Specific Problem: GWC-9-UNIT-0: No communication with associated media gateway(s)^M Description: Autonomous SWACT initiated

2.4.1.10 SNMP

sysUpTime. => 12:46:43
 snmpTrapOID. => nnExtAlarmCritical
 mib-2. =>
 1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.28.50.48.48.53.45.49.49.45.49.54.44.49.53.58.51.48.58.52.53.46.48.44.45.48.53.58.48.48.5565
 mib-2. => <bel>i<vt><dle><si><rs>-<nul>-<enq><nul>
 mib-2. => Autonomous SWACT initiated
 nnExtAlarmActiveEventType => 2
 nnExtAlarmActiveProbableCause => 554
 nnExtAlarmActiveAdditionalText => GWC-9-UNIT-0: No communication with associated media gateway(s)
 nnExtAlarmActiveDocumentationPointer => GWC318
 nnExtAlarmActiveResourceDescription =>
 IEMS=0x00000063000000a12f8e809a-GWC-9-UNIT-0;GWC=GWC-9-UNIT-0;Version=GN91AWJK;Unit=unit_0;Software=AUTOSWACT
 nnExtAlarmActiveManualClear => 1
 nnExtAlarmActiveSequenceNumber => 1208

2.4.2 GWC 319

2.4.2.1 Integrated Element Manager GUI Fields

Table 3: IEMS/SESM Alarm GUI Field descriptions: GWC 319

Field	Value
Severity	Critical
Category	Communications
LogName	GWC
LogNumber	319
ProbableCause	Underlying resource unavailable

Table 3: IEMS/SESM Alarm GUI Field descriptions: GWC 319

Field	Value
SpecificProblem	<Element Name>: No communication with associated media gateway(s)
BodyText	GWC communication loss with associated media gateway(s)

2.4.2.2 Example of Alarm in CMT Alarm Manager

Log Name:GWC 319
 NE Name:GWC-9-UNIT-0
 Alarm Level:Critical
 Category:Communications
 Alarm Time: 15:17:23 16-Nov-2005 EDT
 Probable Cause:Underlying resource unavailable
 SystemUptime:22 hours, 38 minutes, 51 seconds.
 Component ID: GWC=GWC-9-UNIT-0;Version=GN91AWJK; Unit=unit_0;Software=SSC
 Alarm Description: GWC communication loss with associated media gateway(s)
 Specific Problem: GWC-9-UNIT-0: No communication with associated media gateway(s)

2.4.2.3 Explanation

Description: This log indicates that communication to the GWC's associated media gateways is down.

Severity: Critical

2.4.2.4 Action

The Element Managers for related network components should be consulted to identify failures within the network. This log will be cleared after a swact but is raised again on the newly active unit if communication is still lost with all the associated gateways. This log will be cleared when communication to at least one gateway is restored.

2.4.2.5 Corresponding Clear Log

GWC 399

2.4.2.6 Syslog Format of Alarm Clear

```

Nov 17 01:48:39 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=1510~~ GWC399 NONE INFO GWC
Fault^M Location: GWC-9-UNIT-0^M NotificationID: 4^M State: Clear^M Time: Nov 16 15:17:54
2005^M Component Id: GWC=GWC-9-UNIT-0;Version=GN91AWJK;Unit=unit_0;Software=SSC^M
Description: GWC communication loss with associated media gateway(s)
  
```

2.4.2.7 NTSTD

znc0s0jh *** GWC319 NOV16 15:17:23 0125 TBL GWC Fault

Location: GWC-9-UNIT-0

NotificationID: 4

State: Raise

Category: communications

Cause: underlyingResourceUnavailable

Time: Nov 16 15:17:23 2005

Component Id: GWC=GWC-9-UNIT-0;Version=GN91AWJK; Unit=unit_0;Software=SSC

Specific Problem: GWC-9-UNIT-0: No communication with associated media gateway(s)

Description: GWC communication loss with associated media gateway(s)

2.4.2.8 SCC2

*C17 GWC 319 0114 TBL GWC Fault

Location: GWC-9-UNIT-0

NotificationID: 4

State: Raise

Category: communications

Cause: underlyingResourceUnavailable

Time: Nov 16 15:17:23 2005

Component Id: GWC=GWC-9-UNIT-0;Version=GN91AWJK; Unit=unit_0;Software=SSC

Specific Problem: GWC-9-UNIT-0: No communication with associated media gateway(s)

Description: GWC communication loss with associated media gateway(s)

2.4.2.9 Syslog

Nov 17 01:48:09 znc0s0jh IEMS: _V2_~I~H=znc0s0jh~A=IEMS~S=1499~~ GWC319 CRIT TBL GWC Fault^M Location: GWC-9-UNIT-0^M NotificationID: 4^M State: Raise^M Category: communications^M Cause: underlyingResourceUnavailable^M Time: Nov 16 15:17:23 2005^M Component Id: GWC=GWC-9-UNIT-0;Version=GN91AWJK;Unit=unit_0;Software=SSC^M Specific Problem: GWC-9-UNIT-0: No communication with associated media g^M ateway(s)^M Description: GWC communication loss with associated media gateway(s)

2.4.2.10 SNMP

sysUpTime. => 12:46:33

snmpTrapOID. => nnExtAlarmCritical

mib-2. =>

1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.28.50.48.48.53.45.49.49.45.49.54.44.49.53.58.51.48.58.51.53.46.48.44.45.48.53.58.48.48.5563

mib-2. => <bel>i<vt><dle><si><rs>#-<nul>-<enq><nul>

mib-2. => GWC communication loss with associated media gateway(s)

nnExtAlarmActiveEventType => 2

nnExtAlarmActiveProbableCause => 554

nnExtAlarmActiveAdditionalText => GWC-9-UNIT-0: No communication with associated media gateway(s)

nnExtAlarmActiveDocumentationPointer => GWC319

```
nnExtAlarmActiveResourceDescription =>  
IEMS=0x00000063000000a12f8e809a-GWC-9-UNIT-0;GWC=GWC-9-UNIT-0;Ver-  
sion=GN91AWJK;Unit=unit_0;Software=SSC  
nnExtAlarmActiveManualClear => 1  
nnExtAlarmActiveSequenceNumber => 1206
```

3: Configuration Management for A00011827

3.1 Hardware and Software Requirements

The autonomous SWACT activity does not require special hardware.

The autonomous SWACT functionality is available for packetized voice solutions that utilize IP solutions (IP over GigE and AAL5) and ATM solutions (Voice over AAL2) with these products:

- MSC Server 1000
- MSC Server 2000
- CS 2000 (North American and International software loads)
- CS 2000 - Compact (North American and International software loads)

3.2 Initial Configuration

- The initial configuration for GWC autonomous SWACT is disabled for each GWC.

3.3 Upgrade Considerations

3.3.1 Element Management Upgrade

The following upgrades are supported:

- SN07 -> SN09.1
- SN08 -> SN09.1
- SN09 -> SN09.1

3.3.2 Downgrade impact

If a downgrade is needed, then the GWCs go back to the initial GWC autonomous SWACT state of disabled.

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

3.4.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
GWC Maintenance Controls MIB	NEW	N/A
GWC.GWCMTCCONTROLS	NEW	N/A

3.4.2 Table/MIB/Remote Database Schema information

3.4.2.1 Name: GWC-Maintenance-Controls-MIB

3.4.2.1.1 Functional description

The GWC-Maintenance-Controls-MIB contains timers and other maintenance-related controls that are provisioned in CMT and are needed in the GWC.

3.4.2.1.2 Fields/OIDs

The following table lists fields/OIDs for GWC-Maintenance-Controls-MIB:

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
gwcAutoSwactTimer	New		1	The timer represents the time to wait before doing a SWACT, given that the time starts after the following conditions have been met: -All gateways have been taken out-of-service by the GWC due to lost communication. The GWC determines communication has been lost with a gateway after approximately 40 seconds without receiving a message. -The messaging queues have been processed to notify the Core of the state transitions.

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
gwcAutoSwactAlarmFlag	New		2	This flag is sent down to the GWC to request the clearing of the alarm when the GWC does an autonomous SWACT.

3.4.2.1.3 Table release history update

SN09.1: Initial version of the GWC-Maintenance-Controls-MIB.

3.4.2.1.4 Translation verification and other tools

GWC-Maintenance-Controls-MIB does not use translation verification tools.

3.4.2.2 Name: GWC.GWCMTCCONTROLS**3.4.2.2.1 Functional description**

The GWC.GWCMTCCONTROLS table contains timers and other maintenance-related controls that are provisioned in CMT.

3.4.2.2.2 Fields/OIDs

The following table lists fields/OIDs for GWC.GWCMTCCONTROLS

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GWCID	New		VARCHAR 2 (32) NOT NULL	The ID of the GWC.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
AUTOSWACTTIMER	New		NUMBER	The timer represents the time to wait before doing a SWACT, given that the time starts after the following conditions have been met: -All gateways have been taken out-of-service by the GWC due to lost communication. The GWC determines communication has been lost with a gateway after approximately 40 seconds without receiving a message. -The messaging queues have been processed to notify the Core of the state transitions.

3.4.2.2.3 Datafill example

The following example shows sample datafill for table GWCMTCCONTROLS:

GWCID AUTOSWACTTIMER

GWC-2 40

3.4.2.2.4 Table release history update

SN09.1: Initial version of the GWCMTCCONTROLS table.

3.4.2.2.5 Translation verification and other tools

GWCMTCCONTROLS does not use translation verification tools.

3.5 Element Management

3.5.1 New/modified GUIs

Table 4 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Controller Panel	Changed
Change GWC Auto Swact Dialog	NEW

3.5.2 GUI information

3.5.2.1 GUI name: ControllerPanel

The Controller Panel is within the Provisioning Panel.

3.5.2.1.1 Functional description

The Controller Panel contains IP address information, the GWC profile, Bearer Network and Codec Profile information, and other general information for the selected GWC. This GUI is modified to also contain GWC Autonomous SWACT information, as well as an additional Change button to change the state of the control and/or timer and to make a request to the GWC to do a clear of the Swact Alarm.

3.5.2.1.2 GUI usage and implications

The Controller Panel displays and modifies information concerning the GWC. The state of the GWC Autonomous SWACT control and timer (if control is enabled) is displayed on the Controller Panel. The GWC Autonomous SWACT state is initially disabled for all GWCs. If the Change button is selected, the state and/or timer can be changed for the specified GWC.

3.5.2.1.3 GUI size

Table 5 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Controller Panel	No change.	No change.	N/A

3.5.2.1.4 GUI fields

The following table lists new fields for the Controller Panel GUI:

Table 6 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
GWC Auto SWACT	New			A new label, field and button is added to the Controller Panel.	GWC-Maintenance-Controls-MIB

3.5.2.1.5 Usage example

The following example shows a sample GUI for the Controller Panel where GWC Autonomous SWACT is disabled:

CS2000 Management Tools - 47.142.94.59 (CM CLI: COMPACT6)

File Fault Configuration Maintenance Windows Help

Device Types
 APS
 Gateway Controller
 UAS

Contents of Gateway Controller
Directory Find
Go To

Gateway Controllers:
GWC-9

< Prev Next >

Last update: Sep 21, 2005 1:09 PM

GWC-9 Unit 0: 47.142.128.154
Unit 1: 47.142.128.155

Maintenance Provisioning

Controller Gateways Lines Carriers Media Proxies QoS Collectors IPsec

IP Addresses _____ Element Manager _____
Active: 47.142.128.152 IP address: 47.142.94.59
Inactive: 47.142.128.153 SNMP port: 161
Unit 0: 47.142.128.154 Trap port: 162
Unit 1: 47.142.128.155

Profile _____ Call Agent _____
Current: TRUNKNA Change... Node number: 37

Capability	Capacity	Units
Trunks	4094	ports
Large Gateways	24	gateways
IP Security		

Exec Lineup	Term Type
UTR250	PRAB
GWCEX	ABTRK
GWC250	AB250

General

Bearer Network and Codec Profile _____
 ☐ Enable Location Identification reporting
 Bearer network: NET_IP
 Bearer fabric type: IP
 Codec Profile: profile1 Change...

GWC Statistics Data: Statistics
GWC default gateway domain name: <None>
GWC Autonomous Swact: disabled Change...

Retrieving media proxies for GWC-9...Done

3.5.2.1.6 GUI release history update

SN09.1: Modification of Controller Panel for GWC Autonomous SWACT.

3.5.2.1.7 Context sensitive launching information

N/A

3.5.2.1.8 Supplementary information

N/A

3.5.2.2 GUI name: ChangeGWCAutoSwact**3.5.2.2.1 Functional description**

The new dialog contains a check box for enabling the control and a timer where the user can enter an integer between 0 and 300 seconds. The timer cannot be filled in if GWC Autonomous SWACT is not enabled.

Three buttons exist on the dialog. The OK button is to process the changes. The Cancel button is to close the dialog without processing changes. After the autonomous SWACT occurs and the customer has identified and fixed the problem on the inactive unit, the Clr Alarm button can be used to make a request to the GWC to clear the alarm that gets generated when the GWC does an autonomous SWACT.

3.5.2.2.2 GUI usage and implications

This dialog appears whenever the GWC Autonomous SWACT button is selected on the Controller Panel. The current status of the control and timer for the selected GWC is displayed.

3.5.2.2.3 GUI size

Table 7 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
ChangeGWC AutoSwact	0	N/A	N/A

3.5.2.2.4 GUI fields

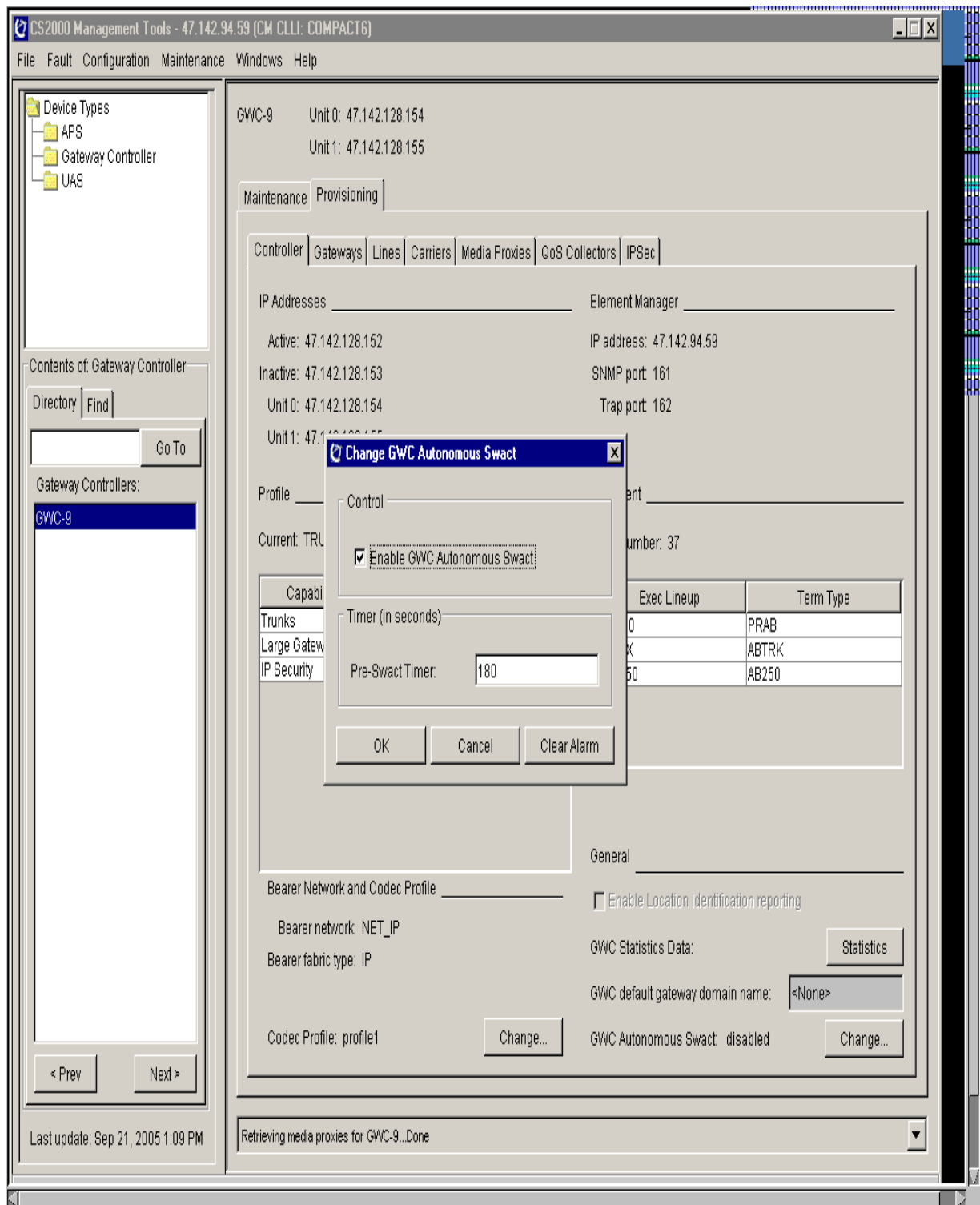
The following table lists fields for GUI:

Table 8 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Control	New		1	A check box, allowing the user to enable or disable GWC Autonomous SWACT.	GWC-Maintenance-Controls-MIB
Timer	New		2	A label and text box where the user can fill in the pre-Swact timer. The timer is only valid if the control is in the enabled state. The default value for the timer is 180 seconds.	GWC-Maintenance-Controls-MIB

3.5.2.2.5 Usage example

The following example shows a sample dialog for the ChangeGWCAutoSwact GUI:



3.5.2.2.6 GUI release history update

SN09.1: Creation of Change GWC Autonomous Swact dialog.

3.5.2.2.7 Context sensitive launching information

N/A

3.5.2.2.8 Supplementary information

N/A

3.5.3 CLUI Interface

N/A

3.6 Configuration Walkthrough

A change of the GWC Autonomous SWACT information can be made anytime after the GWC has been added.

Product = CS2K Management Tools

A00012183--Public Key Manager

Functional Description

1: Applicable Solution(s)

UA-AAL1, UA-IP

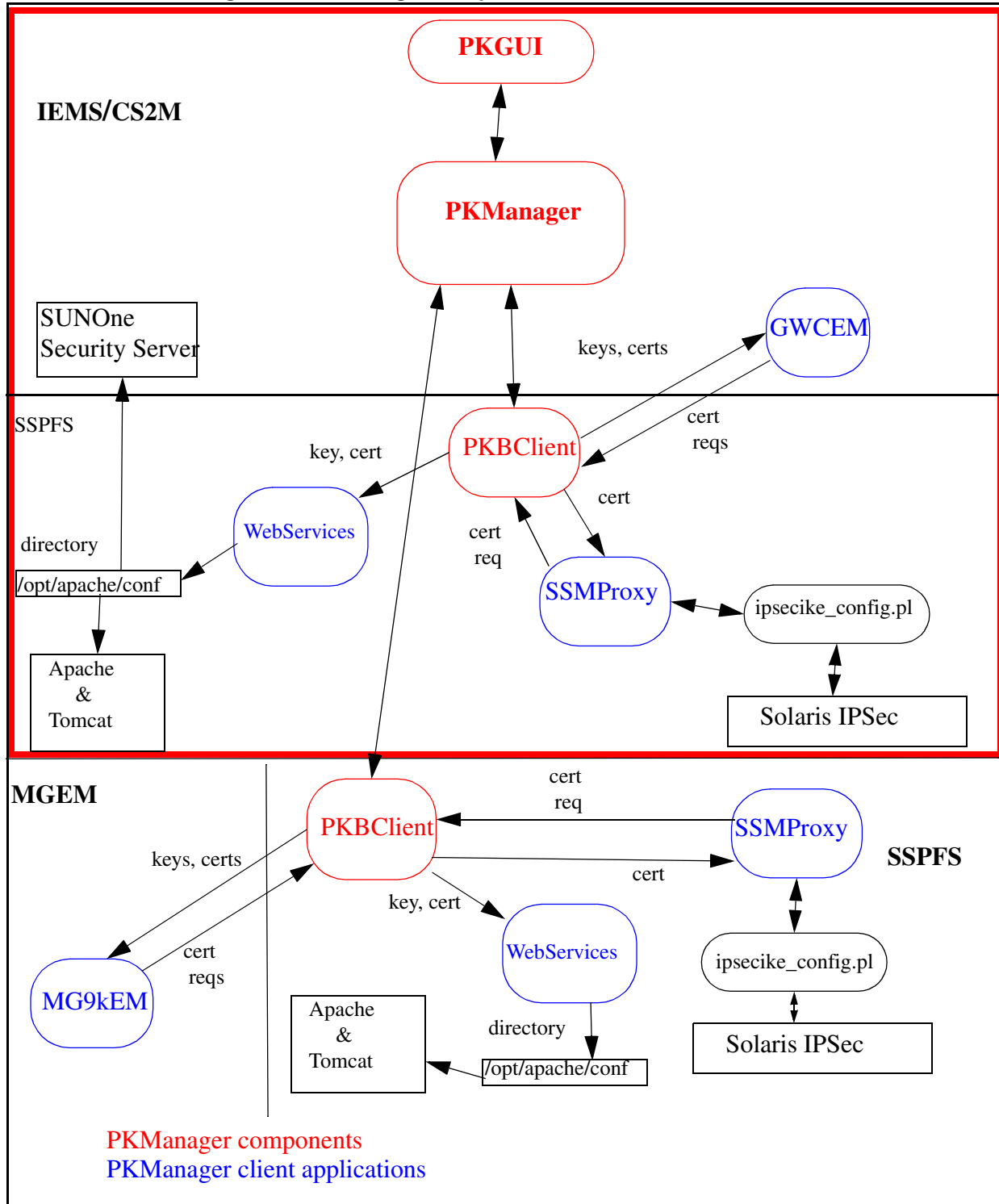
1.1 Description

The PKManager provides the user with the ability to automate the tracking and management of certificate replacement for the following supported devices:

- MG9KEM
- MG9K
- GWCEM
- GWC
- SSM
- WebServices

The following figure shows the PKManager relationships with its client components.

Figure 1 PKManager components and clients



Note: Certificates are always delivered directly to the active unit of an HA cluster and then mirrored using filesystem synchronization services.

The Certificate Manager automates the management and replacement of device certificates for supported devices. In addition to this, a Web interface (PKGUI) is available to authorized users to perform a variety of manual actions. This GUI can be launched independently from a web browser or from within the IEMS client window. A new application managed object is added to IEMS to allow single sign-on launching and alarm integration for the Certificate Manager with IEMS.

Note: This tool restricts access to users belonging to the authorization groups “*secadm*” and “*secro*”. All operations in the GUI will check for group membership before allowing access to a given operation. The group “*secadm*” is used to permit all operations in this tool; while “*secro*” is used to permit viewing and browsing only. See the Configuration section of this feature for further operation mapping details.

The section following summarizes the operations available to the user through the PKGUI interface. **Further details on the PKGUI can be found in the Configuration section of this feature.**

1.2 PKGUI User Operations

- 1 **Generate CSR for Export** - this request is used to initiate the process of importing certificates that are generated by a commercial or external certificate authority. This request will cause the PKBroker to generate a file that contains an openssl PKCS#10 certificate signing request.
- 2 **Import Certificate for Integrated Client** - this request is used to import a certificate generated by a commercial or external certificate authority. By doing so the certificate management and monitoring services of the PKManager for a device whose certificate management is integrated with that supported by the PKManager are obtained. The matching CSR must be present to successfully import the associated certificate.
- 3 **Import Certificate for Non-Integrated Client** - this request is used to obtain the expiration monitoring services of PKManager for a certificate that authenticates a device whose certificate management is not integrated with that supported by the PKManager.
- 4 **Create Non-Integrated Certificate for Export** - this request is used to have the PKBroker generate a file that contains a private key, a second file that contains a compatible X509 v3 certificate for a non-integrated device whose certificate management is not integrated with that supported by the PKManager. PKBCA signing and root certificate files are also provided for export. The expiration monitoring services of PKManager are activated on the certificate.

- 5 **Create Integrated Certificate for Export** - this request is used to have the PKBroker generate a file that contains a private key, a second file that contains a compatible X509 v3 certificate for a device whose certificate management is integrated with that supported by the PKManager. PKBCA signing and root certificate files are also provided for export. The expiration monitoring services of PKManager are activated on the certificate. Integrated applications that require manual installation of initial certificates are handled through this request.
- 6 **Revoke Certificate** - this request is used to immediately revoke any certificate that is monitored by the PKManager. Integrated device certificates that are revoked result in creation and delivery of replacement certificates using the appropriate process (notify of replacement or notify request CSR).
- 7 **Revoke CA Certificate** - this request is used to initiate the CA certificate replacement procedures for a certificates generated by the PKManager. This is potentially a highly processing intensive procedure that can take several hours to complete depending on the device types and number of certificates that must be replaced.
- 8 **Inherit Certificate** - this request is used to import a WebServices certificate generated by a commercial or external certificate authority. By doing so the certificate management and monitoring services of the PKManager are obtained. This enables a purchased and the valid certificate to continue to be used.
- 9 **Browse certificates** - The PKGUI provides the user with the ability to list managed certificates and their states.
- 10 **Alarm Browser** - PKGUI provides access to view all outstanding alarms generated by the PKManager. PKManager logs and alarms can be found in the Fault Management section of this feature.

See the Configuration section of this feature for further user interface details.

1.2.1 MG9K-EM

MG9kEM is enhanced to support the use of public key certificates for securing the MG9k's OAM&P link and the VMG call control links. MG9kEM will be used to provision, distribute and manage the public key certificates for the MG9k gateways.

See the Configuration section of this feature for further user interface details.

1.2.2 GWC-EM

The intent of this development is to address the need to support large scale IP telephony deployments which require digital certificates for authentication. Digital certificates are used mainly to support IPSEC which is used by NEs (for example GWCs, MG9000) to insure secure call control message

communications. They are also used on a smaller scale for secure communication between element managers and network elements.

The GWCEM will retrieve the certificates and private key from IEMS and provision, distribute and manage them for the GWCs.

The GWCEM GUI is changed to allow customers to enable IKE authentication in communication between Gateway Controller and Media Gateway.

- Create/Change IKE authentication item.
- Apply IKE authentication to Connection Policy.
- View/Replace PKI certificate chain.

See the Configuration section of this features for further user interface details.

1.3 Hardware Requirements or Dependencies

There are no hardware dependencies imposed by this feature.

1.4 Software Requirements or Dependencies

1.4.1 PKManager

The PKManager will initially be bundled and installed as part of IEMS installation on SSPFS. The application itself depends on certain common functions provided by SSPFS to provide consistency with other solution components. These include logging, security, and database services.

1.4.2 MG9KEM

The Mg9kEM PKI support is dependent on the PKBroker software running on SN09.x IEMS and PKBClient software running on SN09.x SSPFS.

The new Mg9kEM PKI capabilities are only supported for Mg9k gateways running SN09.x and newer software loads.

1.4.3 GWCEM

N/A

1.5 Limitations and restrictions

1.5.1 PKManager

1.5.2 MG9KEM

1.5.3 GWCEM

In order to provide backwards compatibility, for pre-SN09.1 GWC loads, only one authentication method can be selected. Refer to the Configuration section of this feature for details.

1.6 Interactions

1.6.1 PKManager

The PKManager interacts with its clients through the PKBClient interface introduced into all SSPFS installations. Each supported client application communicates with the Certificate Manager through this interface.

1.6.2 MG9KEM

The IPsec and IKE provisioning is controlled at the SSM and not the Mg9kEM. Adding/deleting policies may result in communication loss between the EM and Mg9k.

Enabling security for the Mg9k is done from the LCI; not from the EM.

Mg9kEM PKI support does not change the existing IPsec preshared key procedures.

1.6.3 GWCEM

N/A

1.7 Glossary

Term	Description
PKManager (PKBroker)	Public Key Manager
PKBClient	Public Key Broker Client
PKGUI	Public Key GUI
IEMS	Integrated Element Management System
GWCEM	Gateway Controller Element Manager
MG9KEM	Media Gateway9000 Element Manager
CA	Certificate Authority
CA Certificate	Certificate issued to a certificate authority, used to sign digital signature certificates that the CA issues
CSR	Certificate Signing Request
IKE	Internet Key Exchange
PKI	Internet public key infrastructure

2: Fault Management for A00012183

This document describes the fault management details for all the components of feature A00012183 - IPSEC PKI Support. This document includes the following components:

- PKManager

- WebPKProxy
- GWCEM
- MG9kEM
- SSM

2.1 Fault management strategy

PKManager applies the following strategy:

- Security logs are monitored by security personnel and are first to be notified of impending expiring certificates via logs. Alarms are monitored by maintenance / fault personnel so alarms are last resort signals.
- Security logs are generated for any changes to alarm level or alarm threshold configuration. PKManager certificate generation activity or replacement (distribution) activities, revocation and certificate request generation.
- Generate standard audit logs and SSPFS security logs for all operations that involve security parameters, any key input by an operator, any change to which key to use (imported vs. internally generated).
- Generate major alarm when key generation fails and when certificate distribution fails.
- Generate security logs and escalating alarms as indicated below when certificate approaches its expiration date based on configured major alarm in advance time and configured minor alarm in advance time.
- PKManager will alarm imported certificate expirations only. Expiration of internally generated certificate results in generation and distribution of new certificate to EM. A log is generated not an alarm.
- Clear alarm and generate security log when alarmed certificate is replaced.

Thresholds for alarm level escalation for certificates with impending expiration dates are listed below. The maximum severity for non-call process service affecting certificates is a major alarm. Only certificates whose expiration is impending that are used as part of call control or call processing operations are to escalate to a critical alarm level.

Minor alarm - default threshold is 168 hours. This time is configurable by an operator at the PKGUI.

Major alarm - default threshold is 72 hours. This time is configurable by an operator at the PKGUI but must be less than minor alarm. Highest level for non-call control related certificates i.e. OAM&P, HTTPS

Critical alarm - call control related certificate has expired.

WebPKProxy applies the following strategy:

- Security logs are monitored by security personnel and are first to be notified of impending expiring certificates via logs.

GWCEM applies the following strategy:

GWCEM uses existing SESM fault management structure.

MG9kEM applies the following strategy:

Existing Mg9kEM fault management framework and structure is followed.

SSM applies the following strategy:

The existing Fault Management strategy will apply to the faults for SSM PKI.

2.2 Fault management tools and utilities

PKManager -

The PKI GUI provides the ability for users to browse outstanding alarms generated by the PKManager.

WebPKProxy -

No special tools required.

GWCEM -

GWCEM uses existing SESM Alarm Manager to support alarm reporting, alarm history retrieval and browsing.

Mg9kEM -

MG9kEM alarms can be viewed from the Alarm Browser GUI.

SSM -

No special tools required for SSM logs.

2.3 Logs

PKManager Log Section:

Security logs are generated for any changes to alarm level or alarm threshold configuration or replacement (distribution) activities, revocation and certificate request generation. A log is generated when an internally generated certificate expires. Security personnel and are notified of impending expiring certificates via logs.

Security Log location

The Security Log file is stored at:

/var/log/securitylog

2.3.1 PKManager Certificate Generation Logs

2.3.1.1 Certificate Request Created

PKManager will log creation of a certificate request for export.

2.3.1.1.1 Security Log output

Sep 23 16:58:54 wnc0s0jd PROG=PKManager SRC.USR=PKBROKER
SRC=wnc0s0jd STAT=Success EVNT.TYPE=SYSTEM_EVENT_EMS
CMD="Generate CSR" MESSAGE="Certificate signing request was created
for CN, GWC-10 47.142.33.5"

2.3.1.2 Certificate Request Received

PKManager will log reception of a certificate request from integrated client applications.

2.3.1.2.1 Security Log output

Sep 28 14:25:37 wnc0s0jd PROG=PKManager SRC.USR=PKBROKER
SRC=wnc0s0jd STAT=Start EVNT.TYPE=SYSTEM_EVENT_EMS
CMD="Generate Certif" MESSAGE="Processing a request to create a
certificate for CN, wnc0s0r8.us.nortel.com 47.142.148.6"

2.3.1.3 Certificate Created

PKManager will log successful creation of an X509 certificate.

2.3.1.3.1 Security Log output

Sep 30 14:57:15 wnc0s0jd PROG=PKManager SRC.USR=PKBROKER
SRC=wnc0s0jd STAT=Success EVNT.TYPE=SYSTEM_EVENT_EMS
CMD="Certif Created" MESSAGE="Certificate was created for CN,
TestCert1 47.133.32.16"

2.3.1.4 Certificate Delivered

PKManager will log successful delivery of an X509 certificate.

2.3.1.4.1 Security Log output

Sep 28 14:30:49 wnc0s0jd PROG=PKManager SRC.USR=PKBROKER
SRC=wnc0s0jd STAT=Success EVNT.TYPE=SYSTEM_EVENT_EMS
CMD="Certif Delivered" MESSAGE="Certificate was created for CN,
wnc0s0jd.us.nortel.com 47.142.94.74"

2.3.1.5 Certificate Request Rejected

PKManager will log invalid and rejected certificate requests.

2.3.1.5.1 Security Log output

Sep 28 14:24:50 wnc0s0jd PROG=PKManager SRC.USR=PKBROKER
SRC=wnc0s0jd STAT=Failure EVNT.TYPE=SYSTEM_EVENT_EMS
CMD="Generate Certif" MESSAGE="Invalid certificate request for CN,
wnc0s0r8.us.nortel.com 47.142.148.6"

2.3.2 Certificate Revocation and Replacement

2.3.2.1 Certificate Revoked

PKManager will log revocation of certificates.

2.3.2.1.1 Security Log output

Sep 30 15:49:55 wnc0s0jd PROG=PKManager SRC.USR=PKBROKER
SRC=wnc0s0jd STAT=Success EVNT.TYPE=SYSTEM_EVENT_EMS
CMD="Revoke Certif" MESSAGE="Revoked certificate CN, TestCert1
47.133.32.16"

2.3.2.2 Replacement Certificate Request

PKManager will log X509 certificate replacement requests.

2.3.2.2.1 Security Log output

Sep 30 15:53:22 wnc0s0jd PROG=PKManager SRC.USR=PKBROKER
SRC=wnc0s0jd STAT=Start EVNT.TYPE=SYSTEM_EVENT_EMS
CMD="Replace Certif" MESSAGE="Processing request to replace certificate
for CN, GWC-10 47.142.33.5"

2.3.3 Invalid, Expiring and Expired Certificate

2.3.3.1 Invalid Certificate

PKManager will log certificates that fail validation.

2.3.3.1.1 Security Log output

Sep 28 14:24:50 wnc0s0jd PROG=PKManager SRC.USR=PKBROKER
SRC=wnc0s0jd STAT=Failure EVNT.TYPE=SYSTEM_EVENT_EMS
CMD="Validate Certificate" MESSAGE="Certificate serial number 262 CN,
wnc0s0r8.us.nortel.com 47.142.148.6 is invalid"

2.3.3.2 Approaching Certificate Expiration

PKManager will log certificates approaching expiration in advance of expiration as configured in the system.

2.3.3.2.1 Security Log output

Sep 28 16:58:45 wnc0s0jd PROG=PKManager SRC.USR=PKBROKER
SRC=wnc0s0jd STAT=Success EVNT.TYPE=SYSTEM_EVENT_EMS
CMD="Advance Notice" MESSAGE="Certificate serial number 261, CN,
GWC-10 47.142.33.5 will expire on 2005-10-04 00:00:00.0"

2.3.3.3 Last Notice Before Certificate Expiration

PKManager will log a final notice in advance of expiration as configured in the system.

2.3.3.3.1 Security Log output

```
Sep 28 17:10:47 wnc0s0jd PROG=PKManager SRC.USER=PKBROKER  
SRC=wnc0s0jd STAT=Success EVNT.TYPE=SYSTEM_EVENT_EMS  
CMD="Last Notice" MESSAGE="Certificate serial number 261, CN,  
GWC-10 47.142.33.5 will expire on 2005-10-01 00:00:00.0"
```

2.3.3.4 Expired Certificate

PKManager will log expired X509 certificates.

2.3.3.4.1 Security Log output

```
Sep 28 17:18:49 wnc0s0jd PROG=PKManager SRC.USER=PKBROKER  
SRC=wnc0s0jd STAT=Success EVNT.TYPE=SYSTEM_EVENT_EMS  
CMD="Certif Expired" MESSAGE="Certificate serial number 261, CN,  
GWC-10 47.142.33.5 has expired"
```

WebPKProxy Log Section:

A Security log is generated when new certificates have been sent from PKManager for replacement on the application client box. PKManager only sends new certificates if they are impending expiring.

Security Log location

The Security Log file is stored at:

/var/log/securitylog

2.3.4 WebPKProxy Certificate Generation Logs

2.3.4.1 Certificate Request Created

WebPKProxy will log that the new certificates have been received and are ready to be replaced by the crafts person.

2.3.4.1.1 Security Log output

```
securitylog:Nov 22 14:07:48 wnc0s0r8 PROG=WebPKProxy SRC.USER=root  
SRC=wnc0s0r8 STAT=Success PROT=SOAP EVNT.TYPE=Restart  
MESSAGE="New certificates for Apache and Tomcat have been downloaded  
from PKManager. Follow the install process for WebPKProxy certificate  
replacement."
```

GWCEM Log Section:

No new customer logs.

MG9kEM Log Section:

2.3.5 New MGEM 715 audit log

2.3.5.1 Formats

This audit log is generated whenever a user initiates a certificate download request for the NE. The audit can be found at: /var/log/auditlog.

Here is an example of the new MGEM 715 log:

```
Jun 25 15:07:28 wnc1s04n MGEM: joeuser 715
Download NE certificate request
```

Here is the description of the fields:

Table 1 Field descriptions

Field	Description	Example
Date/Time	Date and Time stamp of the log	Jun 25 15:07:28
Host Name	Host machine name	wnc1s04n
Application Name	Specifies the application producing the log.	MGEM
User Name	User name attempting the action	joeuser
Log number	The log number	715
Log Text	Specifies the action attempted and any associated details.	Download NE certificate request

2.3.5.2 Action

This log is informational, no action is required.

SSM Log Section:

No new logs added.

2.4 Alarms

PKManager Alarm Section:

2.4.1 Key/Certificate Generation Failure Major Alarm Log

Log Title:PKM300

2.4.1.1 Formats

NTSTD log format:

RTP2 ** PKM300 SEP23 17:25:00 0401 TBL PKM Certificate generation failure

Location: PKManager=wnc0s0jd

NotificationID: 2000091

State: Raise

Category: Processing Error

Cause: Failed to create X509 certificate

Time: SEP23 17:25:00 2005

Component Id: PKManager

Specific Problem: Failed to create valid certificate for CN, GWC-1
42.45.123.56

Description: Attempt to create and validate an X509 certificate failed.

Table 2 Log Field descriptions

Field	Value
Category	Trouble
Severity	MAJ
LogName	PKM
LogNumber	300
Day Time	mmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	Certificate generation failure
Location	PKManager=hostname
Notification Id	0-65535
Category	Processing error
Cause	Failed to create X509 certificate
Day Time Year	MMdd hh:mm:ss YYYY
Component Id	PKManager
SpecificProblem	Failed to create valid certificate for CN, GWC-1 42.45.123.56
Description	Attempt to create and validate an X509 certificate failed

2.4.1.2 Explanation

This Log is generated when an attempt to create and validate an X509 certificate has failed.

2.4.1.3 Action

Verify that the PKManager has been installed and initially configured properly.
Review installation procedures and initial configuration procedures.

2.4.2 Key/Certificate Generation Failure Alarm Cleared Log

Log Title:PKM300

2.4.2.1 Formats

NTSTD log format:

RTP2 PKM300 SEP23 17:35:00 0401 TBL PKM Certificate generation failure

Location: PKManager=wnc0s0jd

NotificationID: 2000091

State: Cleared

Time: SEP23 17:35:00 2005

Table 3 Log Field descriptions

Field	Value
Category	Trouble
Severity	INFO
LogName	PKM
LogNumber	300
Day Time	mmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	Certificate generation failure
Location	PKManager=hostname
NotificationID	0-65535
State	Cleared
Day Time Year	MMdd hh:mm:ss YYYY

2.4.2.2 Explanation

This Log is generated when a X509 certificate creation and validation succeeded after previously having failed.

2.4.2.3 Action

None.

2.4.3 Key/Certificate Delivery Failure Major Alarm Log

Log Title:PKM301

2.4.3.1 Formats

NTSTD log format:

RTP2 ** PKM301 SEP23 18:25:00 0401 TBL PKM Certificate delivery failure

Location: PKManager=wnc0s0jd

NotificationID: 2000092

State: Raise

Category: Processing Error

Cause: Failed to deliver an X509 certificate

Time: SEP23 18:25:00 2005

Component Id: PKManager

Specific Problem: Failed to deliver a certificate for CN, GWC-2

42.45.123.16

Description: Attempt deliver a certificate to an application for a device failed.

Table 4 Log Field descriptions

Field	Value
Category	Trouble
Severity	MAJ
LogName	PKM
LogNumber	301
Day Time	mmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	Certificate delivery failure
Location	PKManager=hostname
Notification Id	0-65535
Category	Processing error
Cause	Failed to deliver a certificate
Day Time Year	MMdd hh:mm:ss YYYY
Component Id	PKManager

Table 4 Log Field descriptions

Field	Value
SpecificProblem	Failed to deliver a certificate for CN, GWC-2 42.45.123.16
Description	Attempt to deliver a certificate to an application for a device failed

2.4.3.2 Explanation

This Log is generated when an attempt to deliver an X509 certificate to an application has failed.

2.4.3.3 Action

Verify that network communication among the system servers is operational.
Retry provisioning the device.

2.4.4 Key/Certificate Delivery Failure Major Alarm Cleared Log

Log Title:PKM301

2.4.4.1 Formats

NTSTD log format:

RTP2 PKM301 SEP23 18:35:00 0401 TBL PKM Certificate delivery failure
Location: PKManager=wnc0s0jd
NotificationID: 2000092
State: Cleared
Time: SEP23 18:35:00 2005

Table 5 Log Field descriptions

Field	Value
Category	Trouble
Severity	INFO
LogName	PKM
LogNumber	301
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	Certificate delivery failure
Location	PKManager=hostname

Table 5 Log Field descriptions

Field	Value
NotificationID	0-65535
State	Cleared
Day Time Year	MMMdd hh:mm:ss YYYY

2.4.4.2 Explanation

This Log is generated when delivery of an X509 certificate has succeeded after previously having failed.

2.4.4.3 Action

None.

2.4.5 Certificate Expired Critical Alarm Log

Log Title:PKM302

2.4.5.1 Formats

NTSTD log format:

RTP2 *** PKM302 SEP24 18:25:00 0401 TBL PKM Certificate expired
Location: PKManager=wnc0s0jd
NotificationID: 2000192
State: Raise
Category: Processing Error
Cause: An X509 certificate has expired
Time: SEP24 18:25:00 2005
Component Id: PKManager
Specific Problem: Expired certificate for CN, GWC-2 42.45.123.16
Description: A certificate used during call control operations has expired

Table 6 Log Field descriptions

Field	Value
Category	Trouble
Severity	CRT
LogName	PKM
LogNumber	302
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL

Table 6 Log Field descriptions

Field	Value
Device ID	PKM
EventLabel	Certificate expired
Location	PKManager=hostname
Notification Id	0-65535
Category	Processing error
Cause	An X509 certificate has expired
Day Time Year	MMMdd hh:mm:ss YYYY
Component Id	PKManager
SpecificProblem	Expired certificate for CN, GWC-2 42.45.123.16
Description	A certificate used during call control operations has expired

2.4.5.2 Explanation

This Log is generated when an X509 certificate used by a device to authenticate itself during call control operations has expired. The device cannot send or receive call control messages.

2.4.5.3 Action

Verify the status for the device's certificate. If the certificate is PKManager generated certificate and the status is delivery failure. Determine why it has failed to be delivered. If the certificate is an imported certificate and the status is expired. Generate a new certificate for the device, import the certificate, verify the PKManager successfully delivers the certificate.

2.4.6 Certificate Expired Critical Alarm Cleared Log

Log Title:PKM302

2.4.6.1 Formats

NTSTD log format:

RTP2 PKM302 SEP24 19:35:00 0401 TBL PKM Certificate expired
Location: PKManager=wnc0s0jd
NotificationID: 2000192
State: Clear
Time: SEP24 19:35:00 2005

Table 7 Log Field descriptions

Field	Value
Category	Trouble
Severity	INFO
LogName	PKM
LogNumber	302
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	Certificate expired
Location	PKManager=hostname
NotificationID	0-65535
State	Clear
Day Time Year	MMMdd hh:mm:ss YYYY

2.4.6.2 Explanation

This Log is generated when a X509 certificate for a call control device that was expired has been replaced with a new valid certificate.

2.4.6.3 Action

None.

2.4.7 Certificate Expired Major Alarm Log

Log Title:PKM305

2.4.7.1 Formats

NTSTD log format:

RTP2 ** PKM305 SEP28 18:25:00 0401 TBL PKM Certificate expired
Location: PKManager=wnc0s0jd
NotificationID: 2001192
State: Raise
Category: Processing Error
Cause: An X509 certificate has expired
Time: SEP24 18:25:00 2005
Component Id: PKManager
Specific Problem: Expired certificate for CN, GWC-26 42.45.123.32

Description: A certificate used for OAM&P functions has expired

Table 8 Log Field descriptions

Field	Value
Category	Trouble
Severity	MAJ
LogName	PKM
LogNumber	305
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	Certificate expired
Location	PKManager=hostname
Notification Id	0-65535
Category	Processing error
Cause	An X509 certificate has expired
Day Time Year	MMMdd hh:mm:ss YYYY
Component Id	PKManager
SpecificProblem	Expired certificate for CN, GWC-26 42.45.123.32
Description	A certificate used for OAM&P functions has expired

2.4.7.2 Explanation

This Log is generated when an X509 certificate used by a device to authenticate itself for OAM&P functions has expired. The device cannot send or receive OAM&P commands.

2.4.7.3 Action

Verify the status for the device's certificate. If the certificate is PKManager generated certificate and the status is delivery failure. Determine why it has failed to be delivered. If the certificate is an imported certificate and the status is expired. Generate a new certificate for the device, import the certificate, verify the PKManager successfully delivers the certificate.

2.4.8 Certificate Expired Major Alarm Cleared Log

Log Title:PKM305

2.4.8.1 Formats

NTSTD log format:

RTP2 PKM305 SEP28 19:35:00 0401 TBL PKM Certificate expired

Location: PKManager=wnc0s0jd

NotificationID: 2001192

State: Cleared

Time: SEP28 19:35:00 2005

Table 9 Log Field descriptions

Field	Value
Category	Trouble
Severity	INFO
LogName	PKM
LogNumber	305
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	Certificate expired
Location	PKManager=hostname
NotificationID	0-65535
State	Cleared
Day Time Year	MMMdd hh:mm:ss YYYY

2.4.8.2 Explanation

This Log is generated when a X509 certificate for an OAM&P device that was expired has been replaced with a new valid certificate.

2.4.8.3 Action

None.

2.4.9 Certificate Forewarning of Expiration Major Alarm Log

Log Title:PKM303

2.4.9.1 Formats

NTSTD log format:

RTP2 ** PKM303 SEP25 18:25:00 0401 TBL PKM Last Alarm Before a Certificate Expiration
 Location: PKManager=wnc0s0jd
 NotificationID: 2000392
 State: Raise
 Category: Advanced Warning
 Cause: Last alarm before X509 certificate expires
 Time: SEP25 18:25:00 2005
 Component Id: PKManager
 Specific Problem: A certificate will expire soon CN, GWC-2 42.45.123.16
 Description: Last forewarning of an impending certificate expiration

Table 10 Log Field descriptions

Field	Value
Category	Trouble
Severity	MAJ
LogName	PKM
LogNumber	303
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	Last Alarm Before a Certificate Expiration
Location	PKManager=hostname
Notification Id	0-65535
Category	Advanced Warning
Cause	Last alarm before X509 certificate expires
Day Time Year	MMMdd hh:mm:ss YYYY
Component Id	PKManager
SpecificProblem	A certificate will expire soon CN, GWC-2 42.45.123.16
Description	Last forewarning of an impending certificate expiration

2.4.9.2 Explanation

This Log is generated when the expiration date of an X509 certificate has reached the forewarning date for the last alarm before expiration. A previous forewarning date has already passed. The alarm raised at that time has being escalated.

2.4.9.3 Action

- 1) Check that the in advance of expiration thresholds are configured properly. If not correct these.(ie. they are invalid or set too soon)
- 2) Verify the status and expiration date for the device's certificate. If the certificate is a PKManager generated certificate and the status is delivery failure. Determine why it has failed to be delivered. If the certificate is an imported certificate. Generate a new certificate for the device, import the certificate, verify the PKManager successfully delivers the certificate.

2.4.10 Certificate Forewarning of Expiration Major Alarm Cleared Log

Log Title:PKM303

2.4.10.1 Formats

NTSTD log format:

RTP2 PKM303 SEP24 19:35:00 0401 TBL PKM Last Alarm Before a
Certificate Expiration
Location: PKManager=wnc0s0jd
NotificationID: 2000392
State: Cleared
Time: SEP24 19:35:00 2005

Table 11 Log Field descriptions

Field	Value
Category	Trouble
Severity	INFO
LogName	PKM
LogNumber	303
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	Last Alarm Before a Certificate Expiration

Table 11 Log Field descriptions

Field	Value
Location	PKManager=hostname
NotificationID	0-65535
State	Cleared
Day Time Year	MMMdd hh:mm:ss YYYY

2.4.10.2 Explanation

This Log is generated when an X509 certificate has been replaced and delivered successfully to the device after the replaced certificate had reached the last alarm before expiration date.

2.4.10.3 Action

None.

2.4.11 Certificate Forewarning of Expiration Minor Alarm Log

Log Title:PKM304

2.4.11.1 Formats

NTSTD log format:

RTP2 * PKM304 SEP26 18:25:00 0401 TBL PKM First Alarm Forewarning of a Certificate Expiration
Location: PKManager=wnc0s0jd
NotificationID: 2000492
State: Raise
Category: Advanced Warning
Cause: First alarm warning of impending X509 certificate expiration
Time: SEP26 18:25:00 2005
Component Id: PKManager
Specific Problem: A certificate will expire soon CN, GWC-2 42.45.123.16
Description: Initial forewarning of an impending certificate expiration

Table 12 Log Field descriptions

Field	Value
Category	Trouble
Severity	MINOR
LogName	PKM
LogNumber	304
Day Time	mmmdd hh:mm:ss

Table 12 Log Field descriptions

Field	Value
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	Certificate expired
Location	PKManager=hostname
Notification Id	0-65535
Category	Advanced Warning
Cause	First Alarm Forewarning of a Certificate Expiration
Day Time Year	MMMdd hh:mm:ss YYYY
Component Id	PKManager
SpecificProblem	A certificate will expire soon CN, GWC-2 42.45.123.16
Description	Initial forewarning of an impending certificate expiration

2.4.11.2 Explanation

This Log is generated when the expiration date of an X509 certificate has reached the date for initial alarm forewarning its expiration.

2.4.11.3 Action

- 1) Check that the in advance of expiration thresholds are configured properly. If not correct these.(ie. they are invalid or set too soon)
- 2) Verify the status and expiration date for the device's certificate. If the certificate is a PKManager generated certificate and the status is replaced then check the status again in an hour. Should the status change to delivery failure. Determine why it has failed to be delivered. If the certificate is an imported certificate. Generate a new certificate for the device, import the certificate, verify the PKManager successfully delivers the certificate.

2.4.12 Certificate Forewarning of Expiration Minor Alarm Cleared Log

Log Title:PKM304

2.4.12.1 Formats

NTSTD log format:

RTP2 PKM304 SEP24 19:35:00 0401 TBL PKM First Alarm Forewarning of a Certificate Expiration

Location: PKManager=wnc0s0jd

NotificationID: 2000492

State: Cleared

Time: SEP24 19:35:00 2005

Table 13 Log Field descriptions

Field	Value
Category	Trouble
Severity	INFO
LogName	PKM
LogNumber	304
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
EventType	TBL
Device ID	PKM
EventLabel	First Alarm Forewarning of a Certificate Expiration
Location	PKManager=hostname
NotificationID	0-65535
State	Cleared
Day Time Year	MMMdd hh:mm:ss YYYY

2.4.12.2 Explanation

This Log is generated when an X509 certificate has been replaced and delivered successfully to the device after the replaced certificate had triggered the initial forewarning alarm before expiration log.

2.4.12.3 Action

None.

GWCEM Alarm Section:

2.4.13 New Alarm: CMT304 GWCEM fail to retrieve the cert.

This new alarm will be raised when GWCEM fail to retrieve the certificates from PKBClient.

2.4.13.1 Cause and condition

This scenario will happen if the PKBM is not ready for certificate retrieve or communication errors.

2.4.13.2 Alarm format

The format of this alarm should be:

Network Element: CS2K Config Manager
Alarm Level: Critical
Category: Environment
Alarm Time: <Data and time when the alarm was raised>
Probable Cause: PKBM is not ready for certificate retrieve or communication errors.
Description: GWCEM fail to retrieve the certificates.

Here is an example of this alarm:

<OFFICE> *** CMT304 MMMDD hh:mm:ss <sequence number> TBL
CMT Fault

Location: gwcem

NotificationID: <Notification ID>

State: Raise

Category: processingError

Cause: corruptData

Time: Mmm DD hh:mm:ss YYYY

Component Id:
SESM=GWCEMalarm;GWCEM=GWCGetCertAlarm;GWC=<GWC
node/unit>

Specific Problem: GWCEM can not get the certificates from IEMS.

Description: Failed to get certificates from IEMS.

Clear example:

<OFFICE> CMT399 MMMDD hh:mm:ss <sequence number> INFO CMT
Fault

Location: gwcem

NotificationID: <Notification ID>

State: Clear

Time: Mmm DD hh:mm:ss YYYY

Component Id:
SESM=GWCEMalarm;GWCEM=GWCGetCertAlarm;GWC=<GWC
node/unit>

Description: Clearing Get Certificate Alarm Type FAIL GET CERT

2.4.13.3 Response Action

Action is required to check the communication between GWCEM and PKBClient or between PKBClient and PKBroker.

Mg9kEM Alarm Section:

2.4.14 New IPSC 307 - 313 alarms

2.4.14.1 Formats

The following alarms are raised or cleared when the Mg9kEM receives the “nnIpssecCertifFault” trap from the gateway:

Alarm ID	Fault Type Description
IPSC 307	certificate has expired
IPSC 308	certificate is about to expire in 4 days
IPSC 309	certificate has invalid from date
IPSC 310	certificate not installed
IPSC311	remote certificate verification failed
IPSC 312	certificate is missing Subject Alt. Name
IPSC 313	certificate processing failed

The above alarms have the same basic format. The fault type received from the “nnIpssecCertifFault” determines the alarm id and fault description. Here is an example of a IPSC 311 alarm:

MSH10_I06BR IPSC 310 JUN2 13:35:15 6550 Major TBL MG9K nnIpssecCertifFault

Location: 1-RM9K-Frame007.Shelf1.Slot13

Notification Id: 57493

State: cleared

Category: Equipment Alarm

Cause: remote certificate verification failed

Time: May 30 15:18:48 2003

Component Id: Card.frame0.shelf1.slot13.ITY

Specific Problem: Ipssec Cert Fault

Description: remote certificate verification failed

Site Flr RPos Bay_id

CARY 02 BB17 MG9F 007

Here are the descriptions of the fields:

Field	Value
LogName	IPSC
LogNumber	307 - 313
Day Time	mmmdd hh:mm:ss
Sequence Number	sequential log number
Severity	Major
Alarm Category	Trouble
Device ID	Mg9k
EventType	nnIpssecCertifFault
Location	equipment location
NotificationID	0-65535
State	Raise or Clear
Day Time Year	MMMdd hh:mm:ss YYYY
Category	Equipment alarm
Cause	reason for fault
Day Time Year	MMMdd hh:mm:ss YYYY
Component Id	Equipment description
SpecificProblem	problem description

Field	Value
Description	fault description
Frame location Info	physical location of the equipment

2.4.14.2 Action

Correct the reported error condition associated with the alarm. For example, ensure the certificates used are current and valid.

2.4.15 New IPSC 314 alarm

2.4.15.1 Formats

The IPSC 314 alarm is raised when the EM attempts but fails to deliver certificates to the gateway. This alarm is cleared when a subsequent delivery attempt succeeds.

Here is an example of a IPSC 314 alarm:

MSH10_I06BR IPSC 314 JUN2 13:35:15 6551 Major TBL MG9KEM CERT DELIVERY ERROR

Location: 1-RM9K-Frame007.Shelf1.Slot13

Notification Id: 57494

State: raised

Category: System Alarm

Cause: error delivering certificates

Time: May 30 15:18:48 2003

Component Id: Card.frame0.shelf1.slot13.ITY

Specific Problem: delivery error

Description: error delivering certificates

Site Flr RPos Bay_id

CARY 02 BB17 MG9F 007

Here are the descriptions of the fields:

Field	Value
LogName	IPSC
LogNumber	314
Day Time	mmdd hh:mm:ss
Sequence Number	sequential log number
Severity	Major

Field	Value
Alarm Category	Trouble
Device ID	MG9KEM
EventType	CERT DELIVERY ERROR
Location	equipment location
NotificationID	0-65535
State	Raise or Clear
Day Time Year	MMMdd hh:mm:ss YYYY
Category	System alarm
Cause	reason for fault
Day Time Year	MMMdd hh:mm:ss YYYY
Component Id	Equipment description
SpecificProblem	problem description
Description	fault description
Frame location Info	physical location of the equipment

2.4.15.2 Action

Correct the reported error condition associated with the alarm then retry the download request.

SSM Alarms Section:

No new alarms added.

3: Configuration Management for A00012183

This section discusses the following configurations:

- WebPKProxy Configuration
- PKManager Configuration
- MG9KEM Configuration
- MG9K Configuration
- GWC-EM Configuration
- SSM Certificate Handling

WebPKProxy Configuration

3.1 Hardware and Software Requirements

WebPKProxy is delivered as part of the SSPFS installation. This application requires a local or remote PKManager application to be functional.

3.2 Initial Configuration

WebPKProxy is an application client of PKManager that manages the Apache and Tomcat certificates on the local box.

Initial installation of the WebPKProxy will be performed as part of the SSPFS installation. WebPKProxy cannot be configured without a working PKManager application. PKManager can be running on the same box or on a internet accessible box.

The Certificate Manager delivers certificates to client applications via a star network secured by WEBPKPROXY type certificates. At the center of the star network is the WEBPKPROXY certificate for the server that hosts the Certificate Manager. This certificate is labeled the TRUSTED certificate. Each client server in the network must install along with its own WEBPKPROXY certificate a copy of the TRUSTED certificate.

Create and install the WEBPKPROXY certificate for the Certificate Manager prior to attempting to configure any other servers into the Certificate Manager network with a WEBPKPROXY certificate. See PKGUI section below.

3.2.1 Applying Certificates generated from PKManager's GUI

For initial configuration, certificates are generated on the PKManager box and ftped to the application client box and applied to Apache and Tomcat.

Note the steps that follow assume that the WEBPKPROXY certificate for the Certificate Manager host machine referred to here as the TRUSTED certificate was the first certificate to be created and installed.

1. Log into PKGUI Public Key Manager via a web browser.

Select the Import Export function.

Select Generate Cert

Enter the FQDN of the application client box into the Entity ID field.

Enter the IP of the application client box into the IP Address field.

Select WEBPKPROXY for the Entity Type.

Select the Submit button twice.

2. Telnet into the PKManager box and become root.

3. Go to the output directory specified on the web page

ftp the CA*.pem, TRUSTED*.pem, and 'test box hostname'*.pem to your application client box at /data/ pkclient/certificates

3. Telnet into your application client box and become root.

4. From the cli; select Configuration, Security Services Configuration, PKManager Certificate Installation, install_certs

Wait for the script to finish and verify no errors were seen.

5. From the UNIX prompt, type top and watch the CPU load. Wait for the Java process to fall below 10% before proceeding to WebPKProxy registration.

3.2.2 WebPKProxy Registration

The registration configuration step is required to identify which box will serve as your PKManager server.

1. From the cli; select Configuration, Security Services Configuration, WebPKProxy/PKClient Configuration, register_pkclient

Enter the hostname of the PKManager box. Note, PKManager box must be fully functional or this step will fail.

2. Wait for the script to finish and verify no errors or warnings were seen.

3.3 Certificate Replacement Notification

Before the Apache and Tomcat certificates expire, PKManager will notify WebPKProxy. WebPKProxy will download the certificates from PKManager and generate a Security Log to notify the crafts person of the required action. WebPKProxy does not automatically apply the certificates, the crafts person is required to determine the appropriate maintenance window since Apache and Tomcat will be restarted.

The log will look like:

```
securitylog:Nov 22 14:07:48 wnc0s0r8 PROG=WebPKProxy SRC.USER=root  
SRC=wnc0s0r8 STAT=Success PROT=SOAP EVNT.TYPE=Restart  
MESSAGE="New certificates for Apache and Tomcat have been downloaded  
from PKManager. Follow the install process for WebPKProxy certificate  
replacement."
```

3.3.1 Certificate Replacement

1. Telnet into your application client box and become root.
2. From the cli; select Configuration, Security Services Configuration, PKManager Certificate Installation, install_certs

Wait for the script to finish and verify no errors were seen.

3. From the UNIX prompt, type top and watch the CPU load. Wait for the Java process to fall below 10% before proceeding to WebPKProxy registration.

3.3.2 WebPKProxy Registration

The registration configuration step is required to identify which box will serve as your Certificate Manager server.

1. From the cli; select Configuration, Security Services Configuration, WebPKProxy/PKClient Configuration, register_pkclient

Enter the hostname of the Certificate Manager box. Note, Certificate Manager box must be fully functional or this step will fail.

2. Wait for the script to finish and verify no errors or warnings were seen.

3.4 Upgrade Considerations

3.4.1 Dump and Restore (CM)

N/A

3.4.2 Element Management Upgrade

N/A

3.4.3 Downgrade impact

N/A

4: Certificate Manager Configuration

4.1 Hardware and Software Requirements

Certificate Manager is bundled as part of the IEMS package. The manager application shares the IEMS platform dependencies.

4.2 Initial Configuration

Initial installation of the Certificate Manager will be performed as part of the IEMS installation. The installation procedure will require changes to allow the PKManager servlet and web clients to be launched securely on initial startup.

Currently, the certificate for Apache on SSPFS must be manually installed before secure communications over HTTPS can occur.

The IEMS installation script currently checks for an Apache certificate before allowing installation to proceed. With Certificate Manager, the user now has the option to use their own certificate (from a third party - for example) or to request the Certificate Manager to create them.

The user will have the ability to change default settings for the certificate authority's distinguished name through the PKGUI. See Section 4.5.4.2 on page 1004 for screen details.

Once the installation of the software is completed a secure Certificate Manager network must be established that includes all the servers that obtain X509 certificates from the Certificate Manager some of these servers are: IEMS/CMT combo, MG9kEM and CBM. Any server with SSPFS installed can be part of the Certificate Manager network. However, only include servers that host applications that are clients of the Certificate Manager. In SN09FF these applications are MG9KEM, GWCEM, SSM and WEBPKPROXY (Tomcat and Apache).

The Certificate Manager delivers certificates to client applications via a star network secured by WEBPKPROXY type certificates. At the center of the star network is the WEBPKPROXY certificate for the server that hosts the Certificate Manager. This certificate is labeled the TRUSTED certificate. Each client server in the network must install along with its own WEBPKPROXY certificate a copy of the TRUSTED certificate.

Create and install the WEBPKPROXY certificate for the Certificate Manager prior to attempting to configure any other servers into the Certificate Manager network with a WEBPKPROXY certificate. See PKGUI section below.

4.3 Upgrade Considerations

4.3.1 Dump and Restore (CM)

N/A

4.3.2 Element Management Upgrade

N/A

4.3.3 Downgrade impact

N/A

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

N/A

4.5 Element Management

4.5.1 IEMS

This feature integrates the Public Key Manager application with IEMS to provide the following capabilities from the IEMS GUI:

- Add the Certificate Manager as an application to IEMS topology
- View Certificate Manager alarms on IEMS
- Launch the Certificate Manager GUI client from IEMS using single sign-on.

4.5.2 Certificate Manager GUI (PKGUI)

The PKGUI is a web-based user interface that provides a set of user screens for certificate administration and management tasks. On successful login, the user is directed to a home page presenting links to various functions and displaying configuration and state information for the application and its registered clients.

User Authorization Note: This tool restricts access to users belonging to the authorization groups “secadm” and “secro”. All operations in the GUI will check for group membership before allowing access to a given operation. The group “secadm” is used to permit all operations in this tool; while “secro” is used to permit viewing and browsing only. See “PKGUI Auth Groups and Operations Mapping” on page 1043 for mapping details.

4.5.3 New/modified GUIs

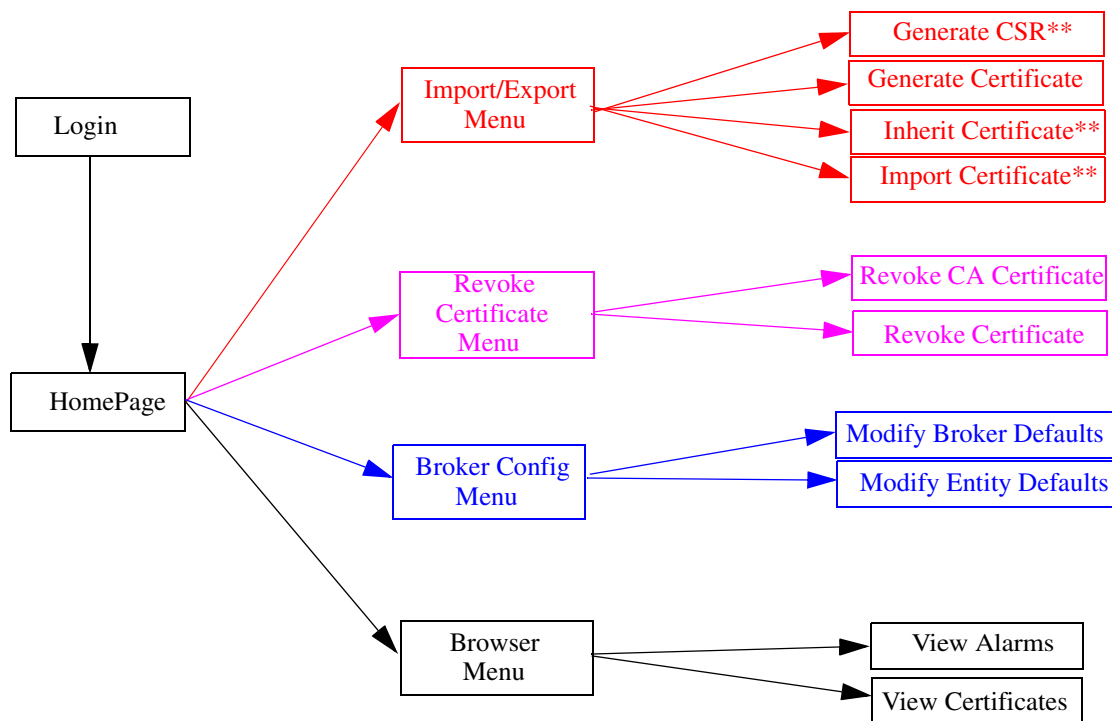
Table 1 New GUIs for PKManager Web Application

GUI name	NEW, CHANGED, DELETED
1. PK Manager Home	NEW
2. Broker Configuration Menu	NEW
3. Import/Export Menu	NEW
4. Revoke Certificate Menu	NEW
5. Browser menu (read-only)	NEW
6. Modify Broker Defaults - Section 4.5.4.1 on page 1002	NEW
7. Configure Entity Defaults -Section 4.5.4.2 on page 1004	NEW
8. Generate CSR for Export -Section 4.5.4.3 on page 1006	NEW
9. Import Certificate for Integrated/NonIntegrated Client - Section 4.5.4.4 on page 1010	NEW

Table 1 New GUIs for PKManager Web Application

GUI name	NEW, CHANGED, DELETED
10. Create Integrated/Non-Integrated Certificate for Export - Section 4.5.4.5 on page 1014	NEW
11. Inherit Certificate - Section 4.5.4.6 on page 1019	NEW
12. Revoke Certificate - Section 4.5.4.7 on page 1020	NEW
13. Revoke CA Certificate - Section 4.5.5.1 on page 1024	NEW
14. View Certificates - Section 4.5.6.1 on page 1029	NEW
15. View Certificate Details - Section 4.5.6.2 on page 1034	
16. View Alarms - Section 4.5.6.3 on page 1036	NEW
17. View Alarm Details - Section 4.5.6.4 on page 1039	NEW

PKGUI Screen Flow



** available in MANAGER mode only

4.5.4 GUI information

4.5.4.1 GUI name: **Modify Broker Defaults**

4.5.4.1.1 Functional description

The Modify Broker Defaults screen is accessed from the Broker Configuration link in the menu panel on the left side of the Home page. This menu will be displayed as the top-level or entry screen to the application.

This screen is intended for use during initial setup of the PKBroker application on SSPFS. It provides a simple form that allows the user to set default values for PKBroker alarm thresholds for each supported entity type.

Modify Broker Defaults Form



Public Key Manager

[logout](#)

User: secadmu
Access: secadm
PKMgr Mode: CA

Edit Defaults

Modify Broker Defaults

[Entity Settings](#)
[Broker Settings](#)
[Previous](#)
[Home](#)

Device	Minor Alarm	Major Alarm	Cert. Expiry
GWC	168	72	Days Valid 365
MG9KVMG	168	72	
WEBPKPROXY	168	72	
MG9KNE	168	72	
SSM	168	72	



4.5.4.1.2 GUI usage and implications

This GUI is used to change alarm thresholds and certificate lifespans for generated certificates.

4.5.4.1.3 GUI fields

The following table lists fields for GUI or pull down menu “Modify Broker Defaults”.

Table 2 PKGUI - Modify Broker Defaults

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Minor Alarm Threshold	NEW			this field defines the alarm threshold in hours to generate a minor alarm	

Table 2 PKGUI - Modify Broker Defaults

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Major Alarm threshold	NEW			this field defines the alarm threshold in hours to generate a minor alarm	
Days Valid	NEW			Defines the number of days a generated certificate will be valid in the system. The certificate will expire after this period.	

4.5.4.1.4 Usage example

See screen shot above.

4.5.4.1.5 GUI release history update**4.5.4.1.6 Context sensitive launching information**

This GUI is launched by clicking the “Modify Entity Defaults” link from the “Broker Config Sub-menu”.

4.5.4.1.7 Supplementary information

NONE

4.5.4.2 GUI name: **Modify Entity Defaults****4.5.4.2.1 Functional description**

This screen allows the user to change the default Distinguished Name components used by the Certificate Manager to generate certificates and requests.

This screen is intended for use during initial setup of the PKBroker application on SSPFS. It provides a simple form that allows the user to set default values for Distinguished Name parameters used for certificate management and generation. **Configure Entity Defaults Form**

Entity Defaults



Public Key Manager

[logout](#)

User: les
Access: secadm
PKMgr Mode: MANAGER

Edit Defaults

[Entity Settings](#)
[Broker Settings](#)

[Previous](#)
[Home](#)

Entity Profiles

Entity Profiles	Modify Entity Defaults
GWC ☐ EXTERNAL ▼	Country Code US
MG9KVMG ☐ EXTERNAL ▼	State North Carolina
WEBPKPROXY ☐ EXTERNAL ▼	Locality Research Triangle Park
MG9KNE ☐ EXTERNAL ▼	Org Name Security
SSM ☐ EXTERNAL ▼	Org Unit Name 3X20

Changing these values will require a CA certificate replacement.

4.5.4.2.2 GUI usage and implications

This screen is intended for use during initial setup of Certificate Manager - before it is used to generate a managed certificate or CSR. The customer has the option to set subject ID components to their own custom values. These default values should not be changed once they are set. Changing these values will require ALL managed certificates to be regenerated. During the CA replacement operation, GUI operations will be restricted to read-only for the duration (potentially measured in hours depending on the number of certificates in the database)

4.5.4.2.3 GUI fields

The following table lists fields for GUI or pull down menu “Modify Entity Defaults”.

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Country	NEW			2 character country code	
Region	NEW			State/Province/other	
Locality	NEW			City	
Org Name	NEW			Organization Name	
Org Unit Name	NEW			Organization Unit Name	

4.5.4.2.4 Usage example

The following example shows sample datafill or menu selection for GUI “Modify Entity Defaults” (also see screenshot above):

- Country: *US*
- Region: *North Carolina*
- Locality: *Raleigh*
- Organization Name: *Succession*
- Organization Unit Name: *OAM Security*

4.5.4.2.5 GUI release history update

4.5.4.2.6 Context sensitive launching information

This GUI is launched by clicking the “Modify Entity Defaults” link from the “Broker Config Sub-menu”.

4.5.4.2.7 Supplementary information

NONE

4.5.4.3 GUI name: **Generate CSR for Export**

4.5.4.3.1 Functional description

This screen will allow the user to generate a certificate request for submission to an external certificate authority. The user is required to manually enter the Entity ID and IP address of the certificate host. The EntityType will be selected from a drop-down menu containing the list of integrated devices to choose from.

Generate CSR for Export



Public Key Manager

[logout](#)

ur: les
ess: secadm
lgr Mode: MANAGER

Import/Export

[Generate Cert](#)
[Generate CSR](#)
[Import Cert](#)

[Previous](#)
[Home](#)

Generate CSR for Export

DN Defaults

Common Name
Country Code
State
Locality
Subject Alt
Org Name
Org Name Unit

Entity Info

Entity ID
IP Address
Entity Type

Export Targets

Export Directory:



Generate CSR (drop-down menu)



Public Key Manager

[logout](#)
[User: les](#)
[Session: secadm](#)
[Manager Mode: MANAGER](#)

Import/Export

[Generate Cert](#)
[Generate CSR](#)
[Import Cert](#)
[Previous](#)
[Home](#)

Generate CSR for Export

DN Defaults

Common Name
Country Code
State
Locality
Subject Alt
Org Name
Org Unit Name

Entity Info

Entity ID
IP Address
Entity Type

Export Directory:

- GWC
- MG9KVMG
- MG9KNE
- WEBPKPROXY**
- GENERICINTERNAL
- GENERICEXTERNAL
- INHERITINTEGRATED
- CA



Screen Legend:

User Input Fields

Derived Values

Defaults or fixed values

4.5.4.3.2 GUI usage and implications

4.5.4.3.3 GUI fields

The following table lists fields for GUI or pull down menu “Generate CSR for Export”.

Table 4 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
EntityType	NEW		MG9KEM, MG9K, GWCEM, GWC, WebPKProxy	Selector (integrated devices only)	
EntityID	NEW			hostname of entity	
IP Address	NEW			IP address of entity	
Common Name	NEW			Derived value == <entityID> <IPAddress>	
Subject Alt Name	NEW			Derived value== <IP Address>	
Cert Request				Certificate request output file. Derived value == <entityID>CSR.pem	

Note: All Subject fields in the GUI are read-only and provided by the values set in the “Modify Entity Defaults” screen.

4.5.4.3.4 Usage example

The following example shows sample datafill or menu selection for GUI “Generate CSR for Export”:

The user is required to enter data for the following fields:

- **Entity Type** - supported entity types
- **EntityID** - this is a typically a hostname by convention
- **IP address** - (e.g.: 47.142.144.127)

The following fields comprise the Subject and are **NOT** configurable by the user from this screen. Values for these fields are loaded from the *EntityDefault* table.

Defaulted Fields (Subject)

Country Code

Region
Locality
Organization Name
Organization Unit Name

**Note: the above defaults are set during initial setup of the PKBroker and should NOT be changed. This is done through the “Configure Broker Defaults” screen.

Derived Fields:

The following fields are derived from the entered data. They include the following:

Common Name - derived by concatenating the entityID and IP address fields. The combined fields are delimited by the space character.

Example:

entityID = wnc0s0qh.us.nortel.com

IP=47.142.144.127

Common Name = “wnc0s0qh.us.nortel.com 47.142.144.127”

Subject Alternate Name - this field is assigned the IP address entered.

Certificate Request Output file - certificate request output files will always end with the suffix: “**CSR.pem**”. The suffix is appended to the Entity ID to derive the final file name.

example: EntityID = wnc0s0qh

CSR file = wnc0s0qh**CSR.pem**

The files are generated to the default target directory: **/opt/pkmgr/csr/export**.

4.5.4.3.5 GUI release history update

4.5.4.3.6 Context sensitive launching information

This GUI is launched by clicking the “Generate CSR for Export” link from the “Import/Export Sub-menu”.

4.5.4.3.7 Supplementary information

NONE

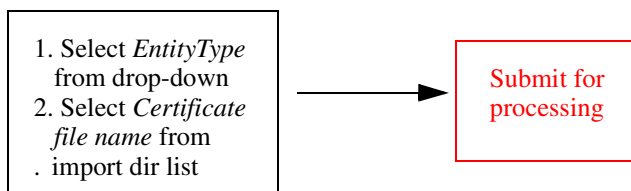
4.5.4.4 GUI name: **Import Certificate**

4.5.4.4.1 Functional description

This screen will allow the user to manually import certificates for expiration monitoring for a supported device. Most fields on this screen are common for both **integrated and non-integrated** devices. Certificates to be imported for

integrated devices will be matched automatically with a corresponding CSR from the database. The operation integration “type” will be determined by the Entity Type selected by the user and set appropriately in the PKBRequest object passed to the server.

Import Certificate - GUI Datafill Flow



Import Integrated Device



Public Key Manager

[logout](#)

User: les
Access: secadm
PKMgr Mode: MANAGER

Import

[Integrated Device \(match CSR\)](#)
[Non-Integrated Device](#)

[Previous](#)
[Home](#)

Import Integrated Device Certificate

DN Defaults	Entity Info
Common Name	Entity ID
Country Code	IP Address
State	Entity Type GENERICEXTERNAL
Locality	Import Directory: /data/NTPkmgr/cert/import
Subject Alt	Import File
Org Name	
Org Unit Name	

Submit Cancel



Import Non-Integrated device



Public Key Manager

[logout](#)

User: les

Access: secadm

PKMgr Mode: MANAGER

Import

[Integrated Device \(match CSR\)](#)
[Non-Integrated Device](#)
[Previous](#)
[Home](#)

Import Non-Integrated Device Certificate

DN Defaults

Common Name
Country Code
State
Locality
Subject Alt
Org Name
Org Unit

Entity Info

Entity ID
IP Address
Entity Type
Import Directory: /data/NTPkmgr/cert/import
Import File



4.5.4.4.2 GUI usage and implications

The import screens are launched when selected from the Import/Export menu page.

Main Menu --> Import/Export Menu-->Import Cert-->Integrated Device

Main Menu --> Import/Export Menu-->Import Cert-->NonIntegrated Device

4.5.4.4.3 GUI fields

The following table lists fields for GUI or pull down menu “Import Certificate”.

Table 5 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Entity Type			GENERIC EXTERN AL	select from drop-down	
Device Certificate file				file name of Device certificate in default import directory	
CSR Common Name				Integrated devices - selected from drop-down NonIntegrated devices - entered manually by user to match import certificate	
CA Certificate file				Integrated Entity Type only - file name of CA certificate in default import directory	
EntityID				NonIntegrated devices only - entered manually by user according to import certificate	
Status			Available, Unavailable	NonIntegrated devices only - select from drop-down	

4.5.4.4.4 Usage example

The following example shows sample datafill or menu selection for GUI “Import Certificate”:

User Input Fields

The user is initially presented with a single drop-down menu to select the entity type and a text box for specifying the certificate path on the server.

Common Fields:

- *Entity Type* - select from drop-down list
- *Device Certificate path* - this field is required for both import types (selected from drop-down menu).

When selected, the integration “type” will be determined and the screen will change as follows:

Integrated device fields:

- *CSR Common Name* - from drop-down list
- *CA Certificate path* - the file path to the CA certificate for the device cert to be imported (selected from drop-down menu).

If an integrated device is selected, the server will automatically attempt to match the imported device with an existing CSR in the database.

Entity ID

Non-Integrated Device Fields:

If the entity type selected is not integrated, then additional text boxes will appear on the screen prompting the user for the following data fields:

- *Common Name*
- *Entity ID*

Note: The default certificate import directory for all import types is:

/opt/pkmgr/cert/import.

**The user is required to place the certificate there for import. Currently, the certificate file names MUST end with the suffix “Ent_cert” to be recognized in the drop-down menu:

<entityName>Ent_cert

example: host1.us.nortel.comEnt_cert

4.5.4.4.5 GUI release history update

4.5.4.4.6 Context sensitive launching information

This GUI is launched by clicking the “Import CSR” link from the “Import/Export Sub-menu”.

4.5.4.4.7 Supplementary information

NONE

(No screenshot available)

4.5.4.5 GUI name: **Create Certificate for Export**

Create Integrated/Non-Integrated Certificate for Export

4.5.4.5.1 Functional description

Integrated and Non-Integrated devices

This screen will allow the user to generate a private key and certificate for use with a supported device. This screen is common for both Integrated and non-integrated devices. The operation integration “type” will be determined by the Entity Type selected by the user and set appropriately in the PKBRequest object passed to the server.

4.5.4.5.2 GUI usage and implications

4.5.4.5.3 GUI fields

The following table lists fields for GUI or pull down menu Create Certificate for Export.

- **Entity Type** - select from drop-down list
- **EntityID** - this is a typically a hostname by convention
- **IP address** - (e.g.: 47.142.144.127)

Table 6 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
EntityType	NEW		MG9KEM, MG9K, GWCEM, GWC, WebPKProxy	Selector (integrated devices only)	
EntityID	NEW			hostname of entity	
IP Address	NEW			IP address of entity	
Common Name	NEW			Derived value == <entityID> <IPAddress>	
Subject Alt Name	NEW			Derived value== <IP Address>	
Cert Output file	NEW			Certificate output file. Derived value == <entityID>Cert.pem	
Private Key file	NEW			Private Key output file. Derived value == <entityID>Key.pem	

User Input Fields

The user is required to enter data for the following fields:

- *Entity Type* - select from drop-down list
- *EntityID* - this is typically a hostname by convention
- *IP address* - (e.g.: 47.142.144.127)

The following fields comprise the Subject ID and are **NOT** configurable by the user from this screen. Values for these fields are loaded from the *EntityDefault* table.

Defaulted Fields (Subject)

Country Code

Region

Locality

Email Address

Organization Name

Organization Unit Name

Company Name

**Note: the above read-only defaults are set during initial setup of the PKBroker and should NOT be changed. This is done through the “Configure Entity Defaults” screen.

Derived Fields:

The following fields are derived from the entered data. They include the following:

Common Name - derived by concatenating the entityID and IP address fields. The combined fields are delimited by the space character.

Example:

entityID = wnc0s0qh.us.nortel.com

IP=47.142.144.127

Common Name = “wnc0s0qh.us.nortel.com 47.142.144.127”

Subject Alternate Name - this field is assigned the IP address entered.

Certificate Output file - certificate output files will always end with the suffix: “**Cert.pem**”. The suffix is appended to the Entity ID to derive the final file name.

Private Key Output File - certificate output files will always end with the suffix: “**Key.pem**”. The suffix is appended to the Entity ID to derive the final file name.

example: EntityID = **wnc0s0qh**
cert file = **wnc0s0qhCert.pem**
key file = **wnc0s0qhKey.pem**

Note: Output files are saved in the export directory specified in the Broker Defaults screen. The default target directory is: **/opt/pkmgr/cert/export**.

4.5.4.5.4 Usage example

The following example shows sample datafill or menu selection for GUI “Create Certificate for Export”:

Generate Certificate for Export 1

Public Key Manager

[logout](#)

ser: secadmu
ccess: secadm
KMGr Mode: CA

Import/Export

[Generate Cert](#)[Previous](#)[Home](#)

Generate Certificate for Export

DN Defaults

Common Name
Country Code
State
Locality
Subject Alt
Org Name
Org Unit

Entity Info

Entity ID
IP Address
Entity Type

Export Targets

Export Directory: **/data/NTPkmgr/cert/export**



Screen Legend:

User Input Fields
Derived Values
Defaults or fixed values

Generate Certificate for Export 2



NortelNetworks

Public Key Manager

[logout](#)

er: secadmu
ess: secadm
Mgr Mode: CA

Import/Export

[Generate Cert](#)[Previous](#)[Home](#)

Generate Certificate for Export

DN Defaults

Common Name
Country Code
State
Locality
Subject Alt
Org Name
Org Unit

Entity Info

Entity ID
IP Address
Import File

Export Targets

Export Directory:
Certificate:
Private Key:



Generate Certificate for Export 3



Public Key Manager

[logout](#)

ser: secadmu
ccess: secadm
<Mgr Mode: CA

Certificate Details

[Previous](#)[Home](#)

Field Name	Info
Common Name	test.host.com 10.11.12.13
Serial#	344
Active Date	2005-11-29 00:00:00.0
Expiry Date	2006-11-29 00:00:00.0
Issuer	OU=3X20, O=Security, L=Research Triangle Park, C=US, ST=North Carolina, CN=PKBCA05
Type	CA
Manager ID	NA
Cert State	CREATED

Operation successful.



4.5.4.5.5 GUI release history update

4.5.4.5.6 Context sensitive launching information

This GUI is launched by clicking the “Create Certificate forExport” link from the “Import/Export Sub-menu”.

4.5.4.5.7 Supplementary information

NONE

4.5.4.6 GUI name: **Inherit Certificate**

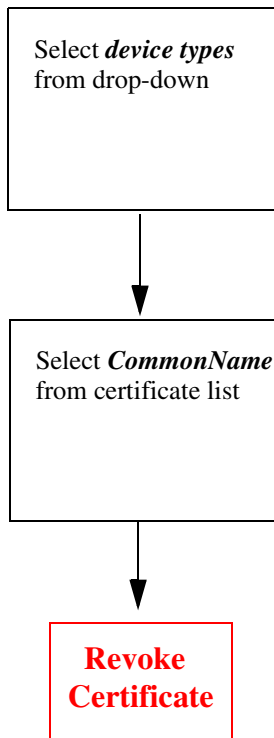
This is covered by the Import Integrated Certificate “GUI name: Import Certificate” on page 1010

4.5.4.7 GUI name: **Revoke Device Certificate**

4.5.4.7.1 Functional description

This screen will allow the user to manually revoke any certificate that is monitored by the PKManager. *Integrated device certificates* that are revoked result in creation and delivery of replacement certificates to their original downstream clients.

Revoke Certificate - GUI Datafill Flow



4.5.4.7.2 GUI usage and implications

4.5.4.7.3 GUI fields

The following table lists fields for GUI or pull down menu “Revoke Certificate”.

Table 7 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Input Type	NEW		Radio Button	activates the input field to use: drop-down or text box	

Table 7 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Common Name	NEW		activated by radio button	Selector - drop-down list of certificate common names is presented for selection	
Serial Number	NEW		activated by radio button selection	User has option to directly enter the serial number of the certificate to revoke	

4.5.4.7.4 Usage example

The following example shows sample datafill or menu selection for GUI “Revoke Certificate”:

Revoke Device Certificate 1



Public Key Manager

[logout](#)

er: secadmu
cess: secadm
Mgr Mode: CA

Certificate Types

GWC

MG9KVMG

MG9KNE

WEBPKPROXY

SSM

certListing



[Previous](#)
[Home](#)



CARRIER GRADE SECURITY FORTIFIED

Revoke Device Certificate 2



Public Key Manager

[logout](#)

er: secadmu
cess: secadm
Mgr Mode: CA

[Previous](#)[Home](#)

Revoke Device Certificate

Common Name		Serial#	Cert State
☐	comp5iems.us.nortel.com 47.142.128.85	327	DELIVERED
☐	emdesign.us.nortel.com 47.142.92.52	337	DELIVERED
☐	rtphmg9kem.us.nortel.com 47.142.101.137	330	CREATED
☒	test.host.com 10.11.12.13	344	DELIVERED
☐	wnc0s0r8.us.nortel.com 47.142.148.6	336	DELIVERED
☐	znc0s0ky.us.nortel.com 47.142.106.232	328	CREATED
☐	znc0s0uc.us.nortel.com 47.142.106.232	329	DELIVERED



Revoke Device Certificate 3



Public Key Manager

[logout](#)

er: secadmu
cess: secadm
Mgr Mode: CA

[Previous](#)[Home](#)

Revoke Device Certificate

Common Name			Serial#	Cert State
☐	comp5iems.us.nortel.com	47.142.128.85	327	DELIVERED
☐	emdesign.us.nortel.com	47.142.92.52	337	DELIVERED
☐	rtphmg9kem.us.nortel.com	47.142.101.137	330	CREATED
☒	test.host.com	10.11.12.13	344	REPLACE
☐	wnc0s0r8.us.nortel.com	47.142.148.6	336	DELIVERED
☐	znc0s0ky.us.nortel.com	47.142.106.232	328	CREATED
☐	znc0s0uc.us.nortel.com	47.142.106.232	329	DELIVERED

Operation successful.



The user can specify a certificate to revoke:

- Select the certificate from a drop-down menu of certificate Common Names

If only one field is used (as is the intended use - for convenience), then the certificate information is retrieved for the selected or entered certificate and used to populate the missing data in the other field.

4.5.4.7.5 GUI release history update

4.5.4.7.6 Context sensitive launching information

This GUI is launched by clicking the “Revoke Certificate” link from the “Revoke Certificate Menu”.

4.5.4.7.7 Supplementary information

4.5.5 GUI information

4.5.5.1 GUI name: **Revoke CA Certificate**

4.5.5.1.1 Functional description

Revoke CA Certificate is used to immediately revoke a CA certificate that is monitored by the PKManager. *This operation should be used with extreme caution* as it will cause the PKManager to initiate certificate replacements for **ALL** certificates generated and managed by the Certificate Manager.

This screen will allow the user to select a root CA from a drop-down menu. This selection will be limited to one of the following

Common Names: (static drop-down)

- **PKBRoot**
- **PKBCA**

The initial screen will also display a warning to the user about the potential danger of this operation.

Once a selection has been made and the user submits the form data, an pop-up window will be presented asking the user to confirm the operation should proceed.

Since this operation could take a significant amount of time to run, all other GUI operations that modify data will be blocked. An error message will be displayed in the footer panel during this time for such operations. “View Certificates” and “View Alarms” screens will still be available for use.

Note: Only users with “secadm” group membership will be permitted to run this command.

User Input Fields

The user is initially presented with a single drop-down menu to select the root CA certificate by Common Name.

- **None**

Following the application-wide convention, database or system error messages will be added to the request context and displayed in the footer window in red using the <html:errors> tag.

Revoke CA Certificate1



Public Key Manager

[logout](#)

User: secadmu
Access: secadm
PKMgr Mode: CA

Revoke Certificates

[Revoke Device](#)
[Revoke CA](#)
[Home](#)

Revoke CA Certificate

Warning

**This operation replaces ALL integrated device
certificates in the network!
Use with extreme caution**



Revoke CA Certificate2



Public Key Manager

[logout](#)

User: secadmu
Access: secadm
KMgr Mode: CA

Revoke Certificates

[Revoke Device](#)[Revoke CA](#)[Home](#)

Revoke CA Certificate

Warning

**This operation replaces ALL integrated device
certificates in the network!**

Use with extreme caution

The potential for an outage exists with this operation!

Cancel to abort.



Revoke CA Certificate3



Public Key Manager

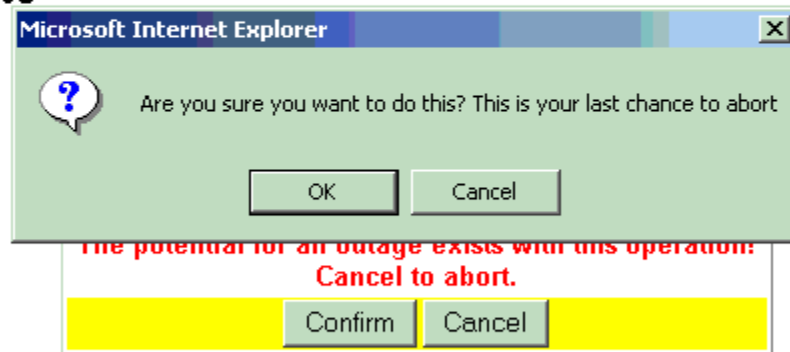
[logout](#)

er: secadmu
cess: secadm
Mgr Mode: CA

Revoke Certificates

Revoke CA Certificate

[Revoke Device](#)
[Revoke CA](#)
[Home](#)



4.5.5.1.2 GUI usage and implications



Public Key Manager

[logout](#)

User: les
Access: secadm
PKMgr Mode: CA

CA Certificate Replacement in Progress
Read-Only Operations Allowed

Revoke Certificates

Revoke CA Certificate

[Home](#)

Warning

**This operation replaces ALL integrated device
certificates in the network!**
Use with extreme caution
The potential for an outage exists with this operation!
Cancel to abort.



4.5.5.1.3 GUI fields

The following table lists fields for GUI or pull down menu “Revoke CA Certificate”.

Table 8 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Common Name	NEW		PKBRoot, PKBCA	Common Name Select from drop-down	

4.5.5.1.4 Usage example

The following example shows sample datafill or menu selection for GUI Revoke CA Certificate:

Following the application-wide convention, database or system error messages will be added to the request context and displayed in the footer window in red using the <html:errors> tag.

4.5.5.1.5 GUI release history update

4.5.5.1.6 Context sensitive launching information

This GUI is launched by clicking the “Revoke Certificate” link from the “Revoke Certificate Menu”.

4.5.5.1.7 Supplementary information

NONE

4.5.6 GUI information

4.5.6.1 GUI name: View Certificates

4.5.6.1.1 Functional description

This screen provides the user with the ability to browse certificates according to their entity type (device) hierarchy. The user has the ability to choose one or more entity types from which a database query will be launched to retrieve the associated data. A table of certificate summary information will be displayed. Next to each item listed will be a “View Details” button that will forward the user to another screen displaying full contents of a specific certificate (see next GUI screen section). Entity types that logically contain sub-components (for example, MG9K contains VMGs), an additional “*List <childEntityType>s*” button will be provided next to the entry to list a summary of the sub-components. When selected, the sub-components summary are listed in the same format as the parent types. Each NE listed for the MG9K, for example, would have a button next to it called “List VMGs”.

View Certificates - Listing

Entity Types

☒ MG9KEM
☒ GWCEM
☐ SSM
☒ WebProxy

Submit 1.

“MG9KEM” Sub-Elements

CommonName	Start Date	Expire Date	Issuer	State
ne1 10.11.12.13 2.	10/15/05	10/15/06	Nortel	OK
vmg3 10.11.12.14	9/15/04	8/15/05	Nortel	MNR

“GWCEM” Sub-Elements

gwc1 10.11.12.13	9/15/04	8/15/05	Nortel	MNR

“WebPKProxy” Certificates

webpkp 10.11.12.13	9/15/04	8/15/05	Nortel	MNR

Links to certificate details

4.5.6.1.2 GUI usage and implications

Certificate Browser usage

1. User selects entity types to list in the certificate summary and clicks on submit to retrieve data. The representation above illustrates the fields retrieved for display and the strategy used to navigate.

2. The certificates are listed according to their manager types or category - if not managed.

4.5.6.1.3 GUI fields

The following table lists fields for GUI or pull down menu View Certificates.

Table 9 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Common Name	NEW		Display field	Common Name of certificate	
Start Date	NEW		Display field	“Not Before” validity date of certificate	
End Date	NEW		Display field	“Not after” validity date of certificate	

Table 9 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Issuer	NEW		Display field	Name of certificate Issuer	
Status	NEW		Display field - must be one of: ok, maj, mnr	certificate expiration state	

4.5.6.1.4 Usage example

The following example shows sample datafill or menu selection for GUI “View Certificates”:

Browse menu



Public Key Manager

[logou](#)

User: secadmu
Access: secadm
PKMgr Mode: CA

Browse Operations

[View Certificates](#)
[View Alarms](#)
[Previous](#)
[Home](#)



CARRIER GRADE SECURITY FORTIFIED



Device Select



Public Key Manager

[logout](#)

User: secadmu

Access: secadm

PKMgr Mode: CA

Certificate Types

MG9KNE	▲
WEBPKPROXY	
SSM	
GENERICINTERNAL	
INHERITINTEGRATED	▼

[certListing](#)[Previous](#)[Home](#)

CARRIER GRADE SECURITY FORTIFIED



Certificate Listing



User: secadmu
Access: secadm
PKMgr Mode: CA

Public Key Manager

[logout](#)

Certificate Types

GWC
 MG9KVMG
 MG9KNE
 WEBPKPROXY
 SSM

[certListing](#)

[Previous](#)
[Home](#)

Certificate Listing

Common Name	Type	Serial#	Active Date	Expiry Date	Cert State
generic.test.com.10.11.22.33	GENERICINTERNAL	345	Nov 2005	29, Nov 2006	29, DELIVERED
comp5iems.us.nortel.com.47.142.128.85	WEBPKPROXY	327	Nov 2005	21, Nov 2006	21, DELIVERED
emdesign.us.nortel.com.47.142.92.52	WEBPKPROXY	337	Nov 2005	28, Nov 2006	28, DELIVERED
rtphmg9kem.us.nortel.com.47.142.101.137	WEBPKPROXY	330	Nov 2005	21, Nov 2006	21, CREATED
test.host.com.10.11.12.13	WEBPKPROXY	344	Nov 2005	29, Nov 2006	29, REPLACE
wnc0s0r8.us.nortel.com.47.142.148.6	WEBPKPROXY	336	Nov 2005	22, Nov 2006	22, DELIVERED
znc0s0ky.us.nortel.com.47.142.106.232	WEBPKPROXY	328	Nov 2005	21, Nov 2006	21, CREATED
znc0s0uc.us.nortel.com.47.142.106.232	WEBPKPROXY	329	Nov 2005	21, Nov 2006	21, DELIVERED



4.5.6.1.5 GUI release history update

4.5.6.1.6 Context sensitive launching information

This GUI is launched by clicking the “View Certificates” link from the “Certificate Browser Menu”.

4.5.6.1.7 Supplementary information

NONE

4.5.6.2 GUI name: **Certificate Details**

4.5.6.2.1 Functional description

This screen displays a form containing a detailed listing of a specified certificate's fields.

4.5.6.2.2 GUI usage and implications

Certificate Details

Public Key Manager



User: secadmu
Access: secadm
PKMgr Mode: CA

[logout](#)

Certificate Details

[Previous](#)

[Home](#)

Field Name	Info
Common Name	comp5iems.us.nortel.com 47.142.128.85
Serial#	327
Active Date	2005-11-21 00:00:00.0
Expiry Date	2006-11-21 00:00:00.0
Issuer	OU=3X20, O=Security, L=Research Triangle Park, C=US, ST=North Carolina, CN=PKBCA05
Type	CA
Manager ID	NA
Cert State	DELIVERED



This screen depends on the “View Certificates” screen in the previous section to specify a certificate to view. It is selected from the listed provided by that screen.

4.5.6.2.3 GUI fields

The following table lists fields for GUI or pull down menu Certificate Details.

Table 10 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Issued to			display only	Common Name	
Version			display only	version (3)	
Serial Number			display only	Serial Number	
Issuer			display only	Issuer	
Valid from			display only	start date of certificate validity	
Valid to			display only	expiry date of certificate	
Subject		Common Name, country, region, locality, org, org unit,	display only	display components of subject	
Constraints			display only	as listed as defined in certificate	
Signature Algorithm			display only	md5RSA	

4.5.6.2.4 Usage example

The following example shows sample datafill or menu selection for GUI “View Details”:

This screen is launched by clicking the “Common Name” link for a listed certificate in the “View Certificates” screen (see **Section 4.5.6.1 on page 1029**) for invocation context.

4.5.6.2.5 GUI release history update**4.5.6.2.6 Context sensitive launching information**

This screen is launched from the view certificates screen by right-clicking on a listed certificate link.

4.5.6.2.7 Supplementary information

NONE

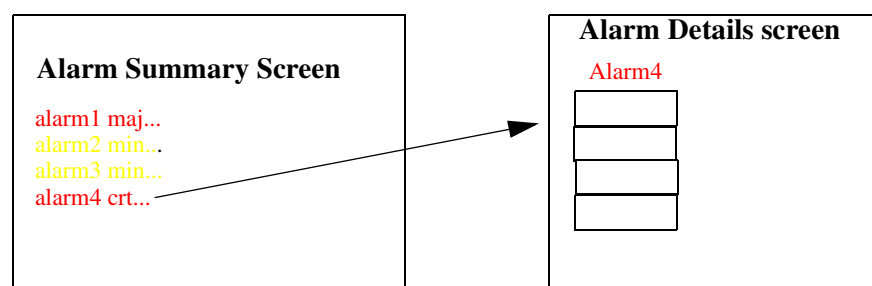
4.5.6.3 GUI name: **View Alarms**

4.5.6.3.1 Functional description

This screen provides a summary listing of the current outstanding alarms generated by the PKManager. The alarm content will be displayed in the “body” portion of the standard screen layout.

This menu selection will display a summary of the current set of active alarms raised by the PKBroker in the main “Body” tile of the display screen. Each alarm listed will be displayed as a hyperlink that will provide full alarm details when clicked. The following tables provide a breakdown of the fields in each.

Alarm Viewer logical screen flow



4.5.6.3.2 GUI usage and implications

This GUI is launched from the “View Alarms” sub-menu of the “Browser Menu”.

4.5.6.3.3 GUI fields

The following table lists fields for GUI or pull down menu “View Alarms”.

Table 11 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
DateTime	NEW		read-only	Date/time of alarm	
LogName	NEW		read-only	Log name as defined in log stream	
Log Number	NEW		read-only	log number as defined in log stream	
Severity	NEW		read-only	Maj, min, info	
Event Label	NEW		read-only	description of fault	

4.5.6.3.4 Usage example

The following example shows sample datafill or menu selection for GUI View Alarms.

PKManager Alarm Summary table

The following alarms will be used to demonstrate the fields displayed in the summary and detail views.

RTP2 * PKM304 SEP26 18:25:00 0401 TBL PKM First Alarm Forewarning of a Certificate Expiration

Location: PKManager=wnc0s0jd
 NotificationID: 20492
 State: Raise
 Category: Advanced Warning
 Cause: First alarm warning of impending X509 certificate expiration
 Time: SEP26 18:25:00 2005
 Component Id: PKManager
 Specific Problem: A certificate will expire soon CN, GWC-2 42.45.123.16
 Description: Initial forewarning of an impending certificate expiration

RTP2 ** PKM301 SEP23 18:25:00 0401 TBL PKM Certificate delivery failure

Location: PKManager=wnc0s0jd
 NotificationID: 20092
 State: Raise
 Category: Processing Error
 Cause: Failed to deliver an X509 certificate
 Time: SEP23 18:25:00 2005
 Component Id: PKManager
 Specific Problem: Failed to deliver a certificate for CN, GWC-2 42.45.123.16
 Description: Attempt deliver a certificate to an application for a device failed.

Table 12 Example Content of Alarm Summary display

DateTime	OfficeID	LogName	LogNum	Severity	EventLabel
SEP23 18:25:00	RTP2	PKM	301	MAJ	Certificate delivery failure
SEP26 18:25:00	RTP2	PKM	304	MIN	First Alarm Forewarning of a Certificate Expiration

Note** - each row will be a hyperlink to display full details described in Section 4.5.6.4 on page 1039. Text color RED for critical and major alarms. Yellow for minor.

Alarm Select



Public Key Manager

[logout](#)

User: secadmu
Access: secadm
PKMgr Mode: CA

Severity

- ☒ Critical
- ☒ Major
- ☒ Minor

alarmListing

[Previous](#)

[Home](#)



CARRIER GRADE SECURITY FORTIFIED



Alarm Listing



Public Key Manager

[log](#)

User: secadmu

Access: secadm

PKMgr Mode: CA

Severity

☒ Critical☒ Major☒ Minor[alarmListing](#)

Active Alarms

Log ID	Common Name	Date	Severity	Category
PKM 305	test.host.com 10.11.12.13	2005-11-29 14:50:43.0	MAJ	timeDomainViolation

[Previous](#)[Home](#)

4.5.6.3.5 GUI release history update

4.5.6.3.6 Context sensitive launching information

4.5.6.3.7 Supplementary information

4.5.6.4 GUI name: **Alarm Details**

4.5.6.4.1 Functional description

4.5.6.4.2 GUI usage and implications

4.5.6.4.3 GUI fields

The following table lists fields for GUI or pull down menu Alarm Details.

Table 13 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Severity	NEW		read-only	Maj, min, info	
Date Time			read-only	MMMMDD hh:mm:ss	
LogName	NEW		read-only	Log name as defined in log stream	
Log Number	NEW		read-only	log number as defined in log stream	
Sequence Number	NEW		read-only	sequence number	
Event Type	NEW		read-only CBSY', 'EXC', 'FAIL', 'FLT', 'INFO', 'INIT', 'LO', 'MANB', 'OFFL', 'PASS', 'PBSY', 'RTS', 'SUMM', 'SYSB', 'TBL', 'TRAN', 'TRAP', 'UNEQ'.	from NTSTD/SCC2 log header	
Device ID	NEW		read-only value: PKM	device identifier for PKManager	
Event Label	NEW	PKManager	read-only	description of fault	
Location	NEW		read-only	device location	
Notification ID	NEW		read-only	id of event sent by PKManager	
Category	NEW		read-only	alarm type category	
Cause	NEW		read-only	cause description	
Component ID	NEW		read-only	fault identifier	
Specific Problem	NEW		read-only	problem text with component info	
Description	NEW		read-only	detailed problem text	

4.5.6.4.4 Usage example

The following example shows sample datafill or menu selection for GUI “Alarm Details”:

This screen is launched by clicking on an entry in the “Alarm Summary” page. A new screen with the following fields will be displayed

Alarm Details



Public Key Manager



User: secadmu
Access: secadm
PKMgr Mode: CA

[Previous](#)

[Home](#)

Alarm Details

Field Name	Info
Common Name	test.host.com 10.11.12.13
Serial#	344
Log ID	PKM 305
Severity	MAJ
Date	2005-11-29 14:50:43.0
Event Type	TBL
Event Label	expiredCert
Location	comp5iems
Category	timeDomainViolation
Cause	keyExpired
Specific Problem	Expired certificate for CN: test.host.com 10.11.12.13
Description	A certificate used for OAM&P functions has expired.



Table 14 Alarm Details Display Contents

Field	Example
Severity	MAJ
LogName	PKM
LogNumber	301
Day Time	SEP23 18:25:00 2005

Table 14 Alarm Details Display Contents

Field	Example
Sequence Number	20092
EventType	TBL
Device ID	PKM
EventLabel	Certificate delivery failure
Location	PKManager=wnc0s0jd
Notification Id	0-65535
Category	Processing error
Cause	Failed to deliver a certificate
Component Id	PKManager
SpecificProblem	Failed to deliver a certificate for CN, GWC-2 42.45.123.16
Description	Attempt deliver a certificate to an application for a device failed

4.5.6.4.5 GUI release history update

4.5.6.4.6 Context sensitive launching information

This screen is launched from the “Alarm Summary” by clicking on one of the summary rows (displayed as a link).

4.5.6.4.7 Supplementary information

NONE

4.5.7 CLUI Interface

NONE

4.6 User interface changes

Refer to GUI discussions above.

4.7 OSSGate Interface Changes

4.8 Security

Security

Login

- standard SSPFS-based central security mechanism. Session management handled by common mechanisms. Inactivity timeout and session ID validation for each requested operation

User Authorization and Operations

Table 15 PKGUI Auth Groups and Operations Mapping

	GUI Operation	Auth Group(s) permitted
1.	Login	secadm, secro
2.	Modify Broker Defaults	secadm
3.	Configure Entity Defaults	secadm
4.	Generate Certificate for Export	secadm
5.	Generate Certificate Request	secadm
6.	Import Certificate	secadm
7.	Revoke Certificate	secadm
8.	Revoke CA Certificate	secadm
9.	Inherit Certificate	secadm
10.	View Certificates	secadm, secro
11.	View Alarms	secadm, secro

4.8.1 Network configuration**4.8.2 Key management****4.8.3 Protocol****4.8.4 Authentication****4.9 PKManager Configuration Walkthrough**

1. User invokes IEMS installation script using existing procedure
2. Installation scripts detect if a managed certificate is already installed and prompts the user to enter one of the following selections:
 - Use existing managed certificate (this is for IEMS upgrade only). Selecting this option will result in no further user input being needed for certificate management.

- Create a new CertificateL - this will prompt the user to enter values for Distinguished name components (see initial config section)
- Import a new, externally generated certificate - the user will be prompted to enter the path of the certificate to be imported and managed for use.
- 3. The appropriate conf script is invoked to ensure a certificate is in place before proceeding
- 4. IEMS installation proceeds as before.

5: MG9KEM Configuration

5.1 Hardware and Software Requirements

5.1.1 MG9kEM

Standard Media Gateway 9000 Element Manager (MG9000 EM) configuration.

5.2 Initial Configuration

5.2.1 MG9kEM

Standard Media Gateway 9000 Element Manager (MG9000 EM) configuration.

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

N/A

5.4 Upgrade Considerations

5.4.1 Dump and Restore (CM)

5.4.2 Element Management Upgrade

5.4.3 Downgrade impact

5.4.3.1 MG9kEM

The new Mg9kEM PKI support capabilities are only supported for Mg9k gateways running SN09.1 or newer software loads. If a Mg9k uses PKI for securing its OAMP or CallP channel, it cannot be downgraded to a SN09 or earlier load unless the PKI option is removed.

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

N/A

5.6 Service Orders (SO) (CM & SESM)

N/A

5.7 Software optionality control (SOC)

N/A

5.8 Element Management - Mg9kEM

5.8.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
MG9000 Provisioning View	CHANGED
NE Properties View	CHANGED
GW Security Config panel	CHANGED

5.8.2 GUI information

5.8.2.1 GUI name: MG9000 Provisioning View

5.8.2.1.1 Functional description

This is an existing view. This view is used for the initial commissioning of a NE.

5.8.2.1.2 GUI usage and implications

The MG9000 Provisioning View is updated to include a new “Download Digital Certificates” option. Using this new “Download Digital Certificates” option, during the initial NE commissioning, the user can download the certificates that the gateway needs to secure the OAMP channel. The “Download Digital Certificates” option only delivers the certificates to the gateway; it does not activate or establish the security association between the Mg9kEM and the gateway. The security configuration between the Mg9kEM and the gateway is provisioned and controlled by the SSM and LCI.

5.8.2.1.3 GUI fields

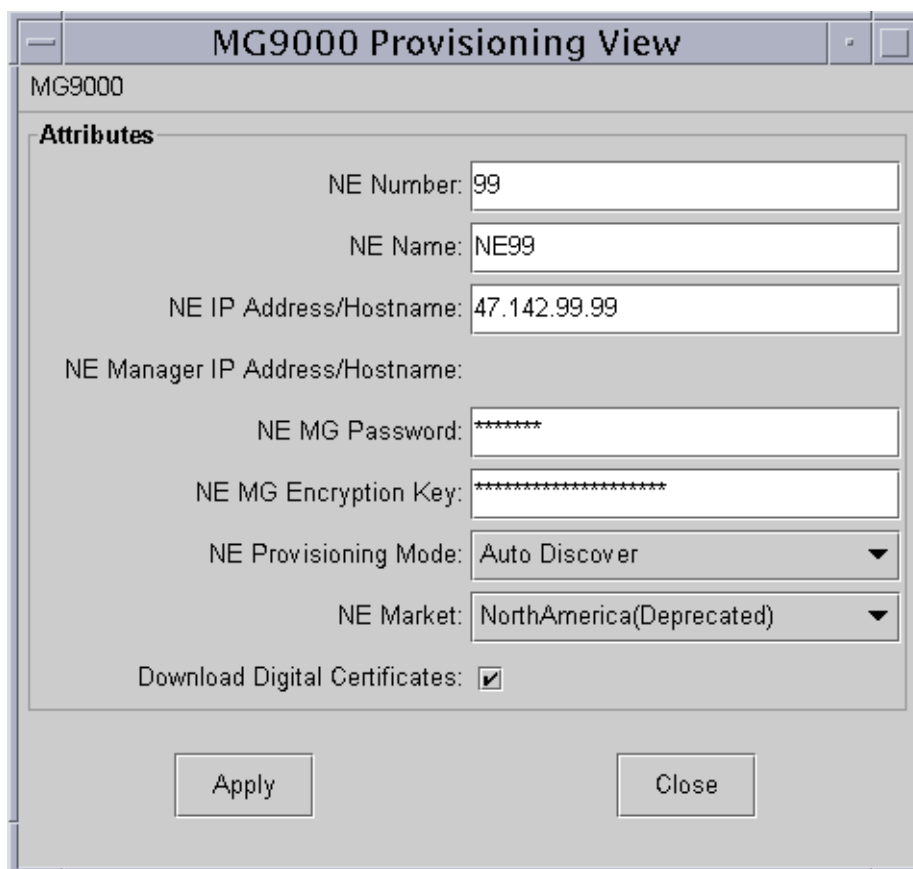
Table 2 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Download Digital Certificates	new			download the certificates to the gateway	

5.8.2.1.4 Usage example

To launch the GUI, from the Mg9kEM Subnet GUI, click on the “Configuration” pulldown menu, then select the “Add new MG9000 NE...” from the list. Once the view is displayed, the user may fill in all the parameters for the NE and if PKI is required for securing the OAMP channel between the EM and the NE, the “Download Digital Certificates” check box should be selected.

Here is an example of the view:



The screenshot shows a window titled "MG9000 Provisioning View". Inside the window, the title "MG9000" is at the top left. Below it is a section labeled "Attributes". This section contains several input fields and dropdown menus: "NE Number:" with the value "99", "NE Name:" with the value "NE99", "NE IP Address/Hostname:" with the value "47.142.99.99", "NE Manager IP Address/Hostname:" (empty), "NE MG Password:" with masked characters "*****", "NE MG Encryption Key:" with masked characters "*****", "NE Provisioning Mode:" with a dropdown menu showing "Auto Discover", and "NE Market:" with a dropdown menu showing "NorthAmerica(Deprecated)". At the bottom of the "Attributes" section is a checkbox labeled "Download Digital Certificates:" which is checked. Below the "Attributes" section are two buttons: "Apply" and "Close".

5.8.2.1.5 GUI release history update

5.8.2.1.6 Context sensitive launching information

This view is accessible from the Mg9kEM Subnet View

5.8.2.1.7 Supplementary information

5.8.3 GUI information

5.8.3.1 GUI name: Properties View

5.8.3.1.1 Functional description

This is an existing view. This view is used to display or modify NE specific attributes.

5.8.3.1.2 GUI usage and implications

The Properties View is updated to include a new “Download Certificates” button. The user can use this view to download the certificates that the gateway needs to secure the OAMP channel. The “Download Certificates” option only delivers the certificates to the gateway; it does not activate or establish the security association between the Mg9kEM and the gateway. The security configuration between the Mg9kEM and the gateway is provisioned and controlled by the SSM and LCI.

Four additional display fields are added to Properties View:

- Gateway Authentication Method
This field displays the current security authentication method used by the gateway.
- Managing Gateway Certificate
This field indicates whether the Mg9kEM is currently managing the gateway’s certificates.
- Last Pushed Certificate
This field displays the serial number of the last device certificate that was successfully downloaded to Mg9k.
- Last Pulled Certificate
This field displays the serial number of the latest device certificate received from the PKBroker.

5.8.3.1.3 GUI fields

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Download Certificates Button	new			download the certificates to the gateway	
Gateway Authentication Method	new			current security authentication method used by the gateway	
Managing Gateway Certificate	new			whether the Mg9kEM is currently managing the gateway’s certificates	

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Last Pushed Certificate	new			the serial number of the last device certificate that was successfully downloaded to Mg9k	
Last Pulled Certificate	new			the serial number of the latest device certificate received from the PKBroker	

5.8.3.1.4 Usage example

To launch the GUI, select a NE from the Mg9kEM Subnet GUI then click on the “Configuration” pulldown menu, then select the “View/Modify NE Properties...” from the list. Once the view is displayed, the user may view security related information or download certificates for the NE by selecting the “NE Security” tab from the GUI. Normally, the “Last Pushed Certificate” and the “Last Pulled Certificate” fields should contain the same serial number. However, if for some reason, the Mg9k does not have the latest certificates available, the “Download Certificates” button can be used to initiate a manual certificate download to the gateway.

Here is an example of the view:

The screenshot shows a window titled "Properties View" for device "MG9000". It has three tabs: "NE Properties", "NE Security", and "IESA PVR Provisioning". The "NE Security" tab is selected. The settings displayed are:

- IPSec Oper Status: Enabled
- IPSec Admin Status: Enabled
- Gateway Authentication Method: Digital Certificate
- Managing Gateway Certificate: Yes
- Last Pulled Certificate: 272
- Last Pushed Certificate: 272

Below these settings is a section titled "Discovery Status Info" containing a text box with the message: "This NE was successfully discovered." At the bottom of the window are three buttons: "Download Certificates", "Refresh", and "Close".

5.8.3.1.5 GUI release history update

5.8.3.1.6 Context sensitive launching information

This view is accessible from the Mg9kEM Subnet View

5.8.3.1.7 Supplementary information

5.8.4 GUI information

5.8.4.1 GUI name: GW Security Config panel

5.8.4.1.1 Functional description

This is an existing view. This view is used to configure security information for the call control channel between the Mg9k and the GWC.

5.8.4.1.2 GUI usage and implications

The GW Security Config panel is updated to include a new “Security Infrastructure” selector where the user can specify whether the VMG intends to use certificate or preshared key for securing its callp link. When the “Certificate” option is specified, the EM will start the process to retrieve and download the certificates to the gateway. The user can continue with the remaining VMG provisioning steps without waiting for the certificate download to complete. However, the gateway will not enable call processing for this VMG until it has successfully received and processed the VMG certificates from the EM.

The GW Security panel will also contain a new option to allow the user to explicitly trigger a certificate download request.

Prior to this feature, the GW Security Config panel is an optional panel during VMG provisioning. With this feature, this panel will become a required step during VMG provisioning. When provisioning a new VMG, the GW Security Config panel will be presented as part of the VMG provisioning process. The user will have to provision the security data for the VMG.

5.8.4.1.3 GUI fields

Table 4 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Security Infrastructure	new	Certificates or Preshared Key		whether the VMG intends to use PKI or PSK for securing its callp channel	
Push Serial	new			the serial number of the last device certificate that was successfully downloaded to Mg9k	
Pull Serial	new			the serial number of the latest device certificate received from the PKBroker	

Table 4 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Download Button	new			initiate a certificate download to the gateway	

5.8.4.1.4 Usage example

Here is an example of the view:

Switched Line Services for MG9000 Element 16

MG9000 Services

Select a Virtual Media Gateway

Create

Delete

MG16000-0-0

MG16000-0-1

MG16000-0-2

MG16000-0-3

Provisioning Information for: MG16000-0-3 Frame : 0 Shelf : 3 Mated Slots : 12/13

GW Security Config GW Market Config GW Status Config GW Termination Config

ESA Config GW Config GW Controller Config

Operational State: Disabled

Security State: On

Security Infrastructure: Certificates

IKE Preshared Key:

IKE Preshared Key (Verify):

IKE Lifetime: 8

IKE Lifetime Units: Hours

IPsec Lifetime: 8

IPsec Lifetime Units: Hours

Push Serial: 261

Pull Serial: 261

Apply Download Use Defaults Refresh

5.8.4.1.5 GUI release history update

5.8.4.1.6 Context sensitive launching information

This view is accessible from the Mg9kEM Switched Line Services View.

5.8.4.1.7 Supplementary information

5.8.5 CLUI Interface

5.9 User interface changes

N/A

5.10 OSSGate Interface Changes

N/A

5.11 Security

5.11.1 MG9kEM

Only users in the “emsrw” or “emsadm” group are authorized to download certificates for the NE (i.e. OAMP link). This is consistent with other NE specific provisioning actions.

Only users in the “emssprov”, “emsrw” or “emsadm” group are authorized to setup or modify the PKI related options for the VMGs (i.e. Callp links). This is consistent with other VMG specific provisioning actions.

5.12 Configuration Walkthrough

5.12.1 Mg9kEM - OAMP link with PKI

The security configuration between the Mg9kEM and the gateway is provisioned and controlled by the SSM and Mg9k LCI. Before the security association using PKI can be established between the Mg9kEM and the gateway, the gateway must install its appropriate digital certificates. The Mg9kEM is used to deliver these certificates to the gateway. The certificate delivery can be initiated during the initial NE commissioning or any time after the NE is provisioned. Once the certificates are delivered to the gateway, the Mg9kEM will update the certificates whenever the certificates change. The user can also manually initiate a certificate download request and send down the current set of certificates to the gateway.

Please refer to SSM and LCI documentation for details on provisioning security for the OAMP channel.

6: MG9K Configuration

6.1 Hardware and Software Requirements

6.1.1 MG9K

Standard Media Gateway 9000 configuration.

6.2 Initial Configuration

6.2.1 MG9K

Standard Media Gateway 9000 Element Manager (MG9000 EM) configuration.

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

N/A

6.4 Upgrade Considerations

6.4.1 Dump and Restore (CM)

6.4.2 MG9K Upgrade

6.4.3 Downgrade impact

6.4.3.1 MG9K

PKI support is available in SN09.x loads.

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

N/A

6.6 Service Orders (SO) (CM & SESM)

N/A

6.7 Software optionality control (SOC)

N/A

6.8 MG9K

6.8.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
IPSec Control	CHANGED

6.8.2 GUI information

6.8.2.1 GUI name: LCI IPsec Control

The LCI is used to configure and control IP Security on the MG9K's Data Controller Card (DCC).

6.8.2.1.1 Functional description

This is an existing view which allows a user to select the 'Authentication Type' used by IPsec to secure the node's external IP interface.

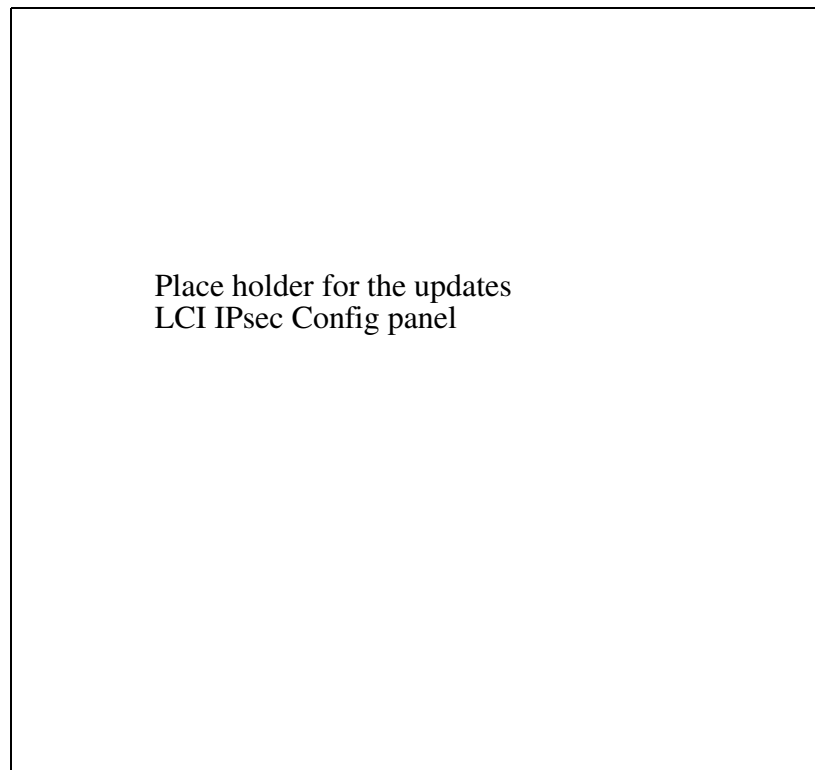
6.8.2.1.2 GUI usage and implications

The IPsec Configuration View is updated to allow the user to select authentication type of pre-shared key or Digital Certificate.

6.8.2.1.3 Usage example

The LCI is used to manage the IPsec options on the DCC card of the MG9K. Optionally, it can be used to also configure and control IP security for VMGs. For the DCC, the LCI is essential to bring a node in service with IP security enabled.

Here is an example of the view:



6.8.3 GUI information

6.8.3.1 GUI name: LCI OAMP Control Panel

This screen is mainly used to configure the OAMP link's network parameters. It also allows the user to configure a preshared encryption key. This key is used to encrypt/decrypt sensitive data transferred between the MG9K and its element manager. When digital certificates are used to authenticate the IPsec

channels between the MG9K and its manager, a pre-shared key is no longer required as sensitive data can be encrypted with the device certificate.

6.8.3.1.1 Functional description

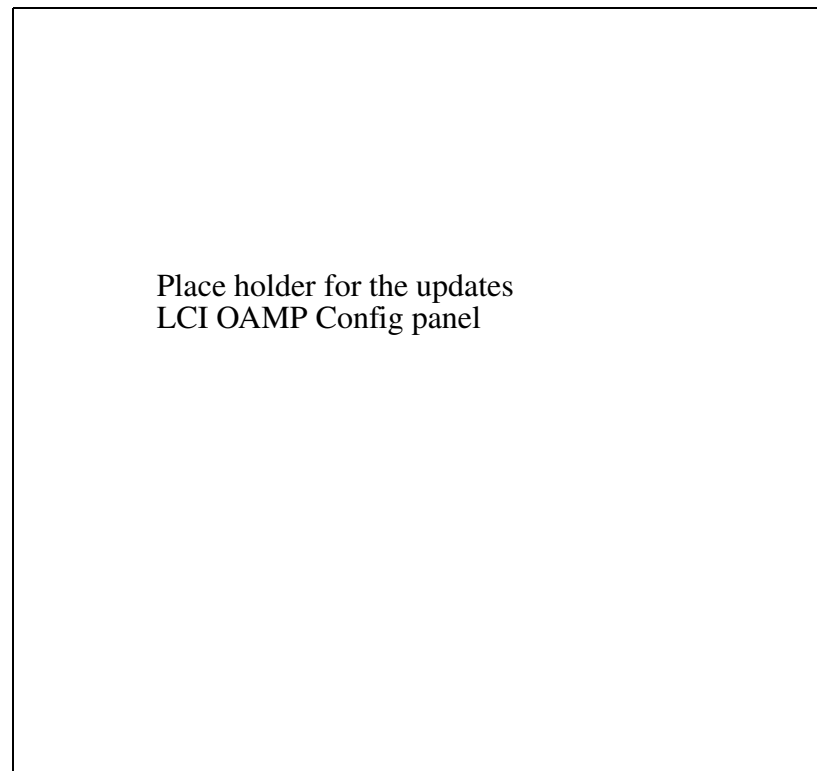
Given that it is a customer preference to authenticate IPsec with digital certificates, the OAMP config screen will no longer enforce the a key to be entered unless there is no authentication type selected.

6.8.3.1.2 GUI usage and implications

If the user chooses to configure the OAMP screen before configuring the IPsec screen, they will be asked to either enter a PSK or go back to the IPsec control screen and configure IPsec.

6.8.3.1.3 Usage example

Here is an example of the view:



6.9 OSSGate Interface Changes

N/A

6.10 Security

6.10.1 MG9K LCI

LCI users are ‘administrative’ users and currently have permissions for node wide changes.

6.11 Configuration Walkthrough

See “PKManager Configuration Walkthrough” on page 1043.

7: GWC-EM Configuration

7.1 Hardware and Software Requirements

7.2 Initial Configuration

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

N/A

7.4 Upgrade Considerations

7.4.1 Dump and Restore (CM)

7.4.2 Element Management Upgrade

7.4.3 Downgrade impact

When SN09.1 SESM has detected an earlier GWC load, it should only allow provisioning of a single preshared key in the new IKE Authentication dialog. Any SNMP SETs to the older GWC load must use the existing MIB tables, not the new definitions.

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

7.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
ikepreferenceentry	changed	
connectionpolicyentry	changed	

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
IKEauthenticationentry	new	
certificatefileentry	changed	
privatekeyfileentry	new	
GWC-SPD-MIB	changed	

7.5.2 Table/MIB/Remote Database Schema information

7.5.2.1 Name: MIB GWC-SPD-MIB table ikePreferenceTableV1

7.5.2.1.1 Functional description

This table clones the table ikePreferenceTable and removes the field “ikePrefAuthMethod”

7.5.2.1.2 Usage sequence and implications (CM Only)

N/A

7.5.2.1.3 Size

N/A

7.5.2.1.4 Fields/OIDs

The table oid is .1.3.6.1.4.1.562.28.0.1.4.1.7.1.18.

7.5.2.1.5 Datafill example

7.5.2.1.6 Table release history update

N/A

7.5.2.1.7 Supplementary information

N/A

7.5.2.1.8 Translation verification and other tools

N/A

7.5.2.2 Name: ikepreferenceentry

IKE preference entry

7.5.2.2.1 Functional description

This table stores the ike preference configuration by the customer. It removes the field “ikeprefauthmethod”

7.5.2.2.2 Usage sequence and implications (CM Only)

N/A

7.5.2.2.3 Size

N/A

7.5.2.2.4 Fields/OIDs

It removes the field “ikeprefauthmethod”.

7.5.2.2.5 Datafill example

Column Name	Type	Content
gwcid	VARCHAR2(32) NOT NULL	GWC-2
ikepreferenceid	NUMBER	1
ikeprefciphalg	NUMBER	1
ikeprefhashalg	NUMBER	1
ikeprefpfsgroupid	NUMBER	1
ikepreflifetimesec	NUMBER	600
ikepreflifetimekb	NUMBER	0
ikeprefphase1only	NUMBER	0
ikeprefcommit	NUMBER	0
ikeprefcom- pathashid	NUMBER	0
ikeprefcompatalignpayl	NUMBER	0
ikeprefippcp4bytespi	NUMBER	0
ikeprefusecertid	NUMBER	0
ikeprefnocert	NUMBER	0
ikeprefnocertreq	NUMBER	0
ikeprefnoinitcont	NUMBER	0
ikepreferenceidstring	VARCHAR2(255)	IKE-preference

7.5.2.2.6 Table release history update

N/A

7.5.2.2.7 Supplementary information

N/A

7.5.2.2.8 Translation verification and other tools

N/A

7.5.2.3 Name: MIB GWC-SPD-MIB table connectionPolicyTableV1**7.5.2.3.1 Functional description**

This table clones the table connectionPolicyTableV1 and removes the field “ipsecConnIkeRemGwId” and “IPSECCONNIKEPREFLISTID.” It adds the fields “IPSECCONNFLAG” (not currently used) and “IPSECCONNIKEAUTHMETHODIDV1.”

7.5.2.3.2 Usage sequence and implications (CM Only)

N/A

7.5.2.3.3 Size

N/A

7.5.2.3.4 Fields/OIDs

The table oid is .1.3.6.1.4.1.562.28.0.1.4.1.7.1.19.

7.5.2.3.5 Datafill example**7.5.2.3.6 Table release history update**

N/A

7.5.2.3.7 Supplementary information

N/A

7.5.2.3.8 Translation verification and other tools

N/A

7.5.2.4 Name: connectionpolicyentry

Connection Policy entry

7.5.2.4.1 Functional description

This table stores the connection policy configuration by the customer. It removes the field “IPSECCONNIKEREMGWID” and “IPSECCONNIKEPREFLISTID.” It adds the fields “IPSECCONNFLAG” (not currently used) and “IPSECCONNIKEAUTHMETHODIDV1.”

7.5.2.4.2 Usage sequence and implications (CM Only)

N/A

7.5.2.4.3 Size

N/A

7.5.2.4.4 Fields/OIDs

Remove the fields “ipseconnikeremgwId” and “ipseconnikepreflistid”. Add a new field “ipseconnikeauthmethodidV1” and “ipsecConnFlagV1”

7.5.2.4.5 Datafill example

Column Name	Type	Content
gwcid	VARCHAR2(32) NOT NULL	GWC-2
ipseconnpolicyid	NUMBER	1
ipseconntansprotoc	NUMBER	0
ipseconnlhostport	NUMBER	8999
ipseconnlhostform	NUMBER	0
ipseconnllocipsasel	NUMBER	0
ipseconnllocportsasel	NUMBER	0
ipseconnlrmipsasel	NUMBER	0
ipseconnlrmportsasel	NUMBER	0
ipseconnltranprotsasel	NUMBER	0
ipseconnlremgwaddr	VARCHAR2(255)	
ipseconnpolrhost	VARCHAR2(255)	5.6.7.8
ipseconnpolprofileid	NUMBER	1
ipseconnpreflistid	NUMBER	1
ipseconncertalias	VARCHAR2(255)	
ipseconnppeer certfile	VARCHAR2(255)	
IPSECCONNIKEREMGWID	VARCHAR2(255)	
IPSECCONNCOMMENT	VARCHAR2(255)	
IPSECCONNIKEPREFLISTID	NUMBER	
IPSECCONNFLAG	NUMBER	

7.5.2.4.6 Table release history update

N/A

7.5.2.4.7 Supplementary information

N/A

7.5.2.4.8 Translation verification and other tools

N/A

7.5.2.5 Name: MIB GWC-SPD-MIB table ikeAuthenticationTable**7.5.2.5.1 Functional description**

This table is new table and stores the ike authentication method setting.

7.5.2.5.2 Usage sequence and implications (CM Only)

N/A

7.5.2.5.3 Size

N/A

7.5.2.5.4 Fields/OIDs

The table oid is .1.3.6.1.4.1.562.28.0.1.4.1.7.1.20.

7.5.2.5.5 Datafill example**7.5.2.5.6 Table release history update**

N/A

7.5.2.5.7 Supplementary information

N/A

7.5.2.5.8 Translation verification and other tools

N/A

7.5.2.6 Name: IKEauthenticationentry

IKE authentication entry

7.5.2.6.1 Functional description

This table stores the ike authentication configuration by the customer. It is a new table.

7.5.2.6.2 Usage sequence and implications (CM Only)

N/A

7.5.2.6.3 Size

N/A

7.5.2.6.4 Fields/OIDs

A new table.

7.5.2.6.5 Datafill example

Column Name	Type	Content
gwcid	VARCHAR2(32) NOT NULL	
ikeauthenremgwid	VARCHAR2(255)	
ikeauthpreflistid	NUMBER	
ikeauthpki	NUMBER	Disabled (0) or Enabled (1)
ikeAuthPsk1	NUMBER	Disabled (0) or Enabled (1)
ikeAuthPskHexFmt1	NUMBER	False (0), True (1)
ikeAuthPskData1	VARCHAR2(255)	
ikeAuthPskTime1	NUMBER	
ikeAuthPsk2	NUMBER	
ikeAuthPskHexFmt2	NUMBER	
ikeAuthPskData2	VARCHAR2(255)	
ikeAuthPskTime2	NUMBER	
IKEAUTHFLAG	NUMBER	

7.5.2.6.6 Table release history update

N/A

7.5.2.6.7 Supplementary information

N/A

7.5.2.6.8 Translation verification and other tools

N/A

7.5.2.7 Name: MIB GWC-SPD-MIB table certificateFileTableV1**7.5.2.7.1 Functional description**

This table is new table and stores the certificates.

7.5.2.7.2 Usage sequence and implications (CM Only)

N/A

7.5.2.7.3 Size

N/A

7.5.2.7.4 Fields/OIDs

The table oid is .1.3.6.1.4.1.562.28.0.1.4.1.7.1.21.

7.5.2.7.5 Datafill example**7.5.2.7.6 Table release history update**

N/A

7.5.2.7.7 Supplementary information

N/A

7.5.2.7.8 Translation verification and other tools

N/A

7.5.2.8 Name: Certificatefileentry**7.5.2.8.1 Functional description**

This table stores the certificates file data.

7.5.2.8.2 Usage sequence and implications (CM Only)

N/A

7.5.2.8.3 Size

N/A

7.5.2.8.4 Fields/OIDs

New table.

7.5.2.8.5 Datafill example

Column Name	Type	Content
gwcid	VARCHAR2(32) NOT NULL	
CERTFILENAME	VARCHAR2(255)	
CERTFILESEQNUMBER	NUMBER	
CERTFILESEQTOTAL	NUMBER	

Column Name	Type	Content
CERTORCRLDATA	VARCHAR2(330)	

7.5.2.8.6 Table release history update

N/A

7.5.2.8.7 Supplementary information

N/A

7.5.2.8.8 Translation verification and other tools

N/A

7.5.2.9 Name: MIB GWC-SPD-MIB table privatekeyFileTableV1**7.5.2.9.1 Functional description**

This table is new table and stores the device private key.

7.5.2.9.2 Usage sequence and implications (CM Only)

N/A

7.5.2.9.3 Size

N/A

7.5.2.9.4 Fields/OIDs

The table oid is .1.3.6.1.4.1.562.28.0.1.4.1.7.1.22.

7.5.2.9.5 Datafill example**7.5.2.9.6 Table release history update**

N/A

7.5.2.9.7 Supplementary information

N/A

7.5.2.9.8 Translation verification and other tools

N/A

7.5.2.10 Name: privatekeyfileentry**7.5.2.10.1 Functional description**

This table stores the private key file data.

7.5.2.10.2 Usage sequence and implications (CM Only)

N/A

7.5.2.10.3 Size

N/A

7.5.2.10.4 Fields/OIDs

New table.

7.5.2.10.5 Datafill example

Column Name	Type	Content
gwcid	VARCHAR2(32) NOT NULL	
PRIVATEKEYFILENAME	VARCHAR2(255)	
PRIVATEKEYFILESEQNUMBER	NUMBER	
PRIVATEKEYFILESEQTOTAL	NUMBER	
PRIVATEENKEYDATA	VARCHAR2(660)	

7.5.2.10.6 Table release history update

N/A

7.5.2.10.7 Supplementary information

N/A

7.5.2.10.8 Translation verification and other tools

N/A

7.6 Service Orders (SO) (CM & SESM)

N/A

7.7 Software optionality control (SOC)

N/A

7.8 Element Management

GWCEM

7.8.1 New/modified GUIs**Table 2 New or modified GUIs**

GUI name	NEW, CHANGED, or DELETED
IKE Preference Panel	changed
Add/Change IKE Preference dialog	changed

Table 2 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Connection Policy Panel	changed
Add/Change Connection Policy dialog	changed
IKE Authentication panel	new
Add/Change IKE Authentication dialog	new
IKE certificate panel	new
View IKE certificate dialog	new

7.8.2 GUI information

User Authorization Note: The IPsec actions restricts access to users belonging to the authorization groups “*mgcrw*”, “*secrw*”, “*mgcro*” and “*secro*”. All operations in the GUI will check for group membership before allowing access to a given operation. The group “*mgcrw*”/“*secarw*” is used to permit all operations in this tool; while “*mgcro*”/“*secro*” is used to permit viewing and browsing only. See “Table 3 IPsec GUI Auth Groups and Operations Mapping” on page 1079 for mapping details.

7.8.2.1 GUI name: IKE Preference Panel

7.8.2.1.1 Functional description

Profile	IPSec Preference	IPSec Preference List	IKE Preference	IKE Preference List	Connection Policy	Ker
Preference name	Cipher algorithm	Hash algorithm	Authentication method	Lifetime (seconds)	Diffie-	
KE	DES-CBC	MD5	PRESHARED	0	1	

This panel displays the IKE preference configuration data.

7.8.2.1.2 GUI usage and implications

Provisioning a GWC with IPsen supported, then configure this IPsen configuration.

7.8.2.1.3 GUI size

N/A

7.8.2.1.4 GUI fields

The column “Authentication method” is deleted.

7.8.2.1.5 Usage example

At first, configure a IKE preference, then the configured item will be shown in the panel.

7.8.2.1.6 GUI release history update

N/A

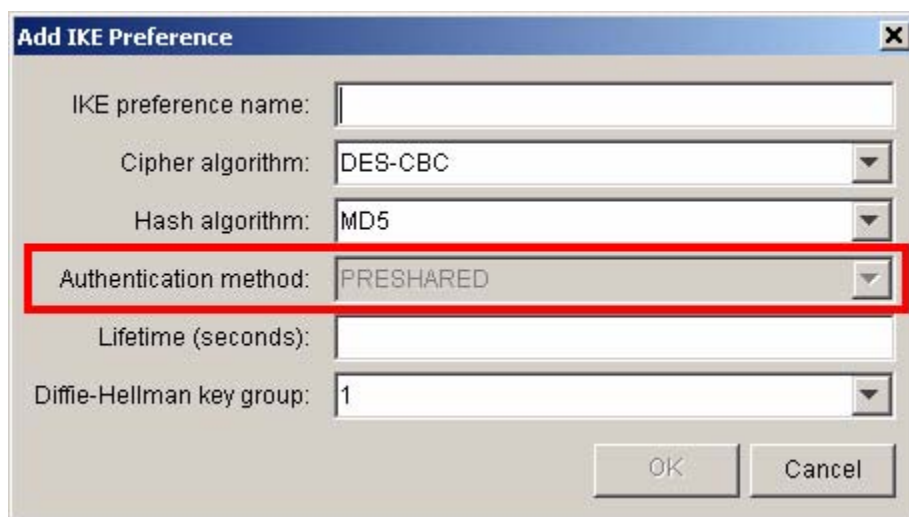
7.8.2.1.7 Context sensitive launching information

N/A

7.8.2.1.8 Supplementary information

N/A

7.8.2.2 GUI name: Add/Change IKE Preference dialog



7.8.2.2.1 Functional description

This dialog shows the IKE preference configuration parameter list and used to configure these parameters.

7.8.2.2.2 GUI usage and implications

Provisioning a GWC with IPsen supported, then configure IKE preference.

7.8.2.2.3 GUI size

N/A

7.8.2.2.4 GUI fields

The parameter “Authentication method” is deleted.

7.8.2.2.5 Usage example

In IKE preference panel, click “Add/Change” button, the dialog will be shown. You can configure /change an IKE preference.

7.8.2.2.6 GUI release history update

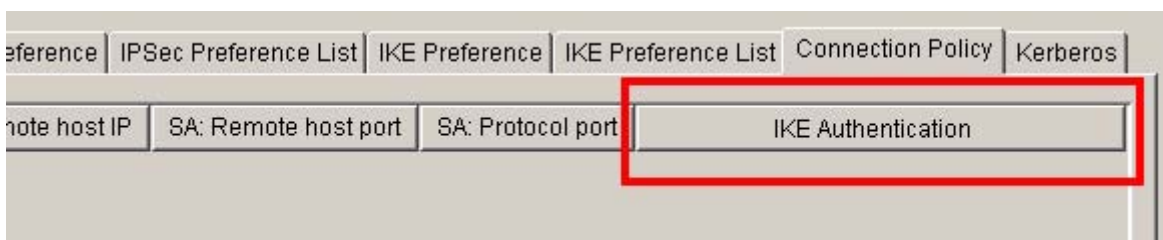
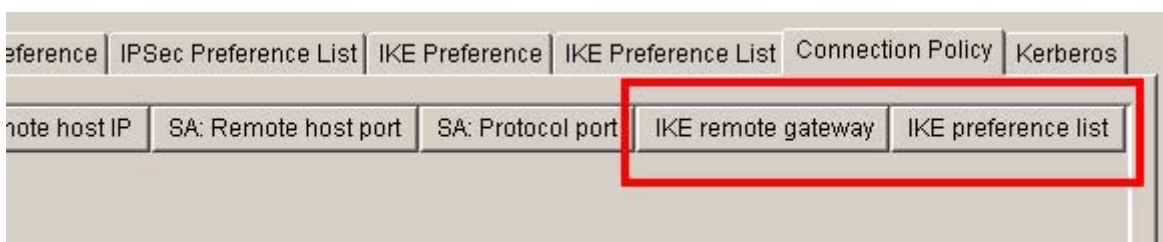
N/A

7.8.2.2.7 Context sensitive launching information

N/A

7.8.2.2.8 Supplementary information

N/A

7.8.2.3 GUI name: Connection Policy Panel**7.8.2.3.1 Functional description**

This panel displays the connection policy configuration data.

7.8.2.3.2 GUI usage and implications

Provisioning a GWC with IPsen supported, then click the IPsen tab and click this panel.

7.8.2.3.3 GUI size

N/A

7.8.2.3.4 GUI fields

The column “IKE remote gateway” and “IKE preference list” is deleted and adds a new column “IKE Authentication”.

7.8.2.3.5 Usage example

At first, configure a connection policy, then the configured item will be shown in the panel.

7.8.2.3.6 GUI release history update

N/A

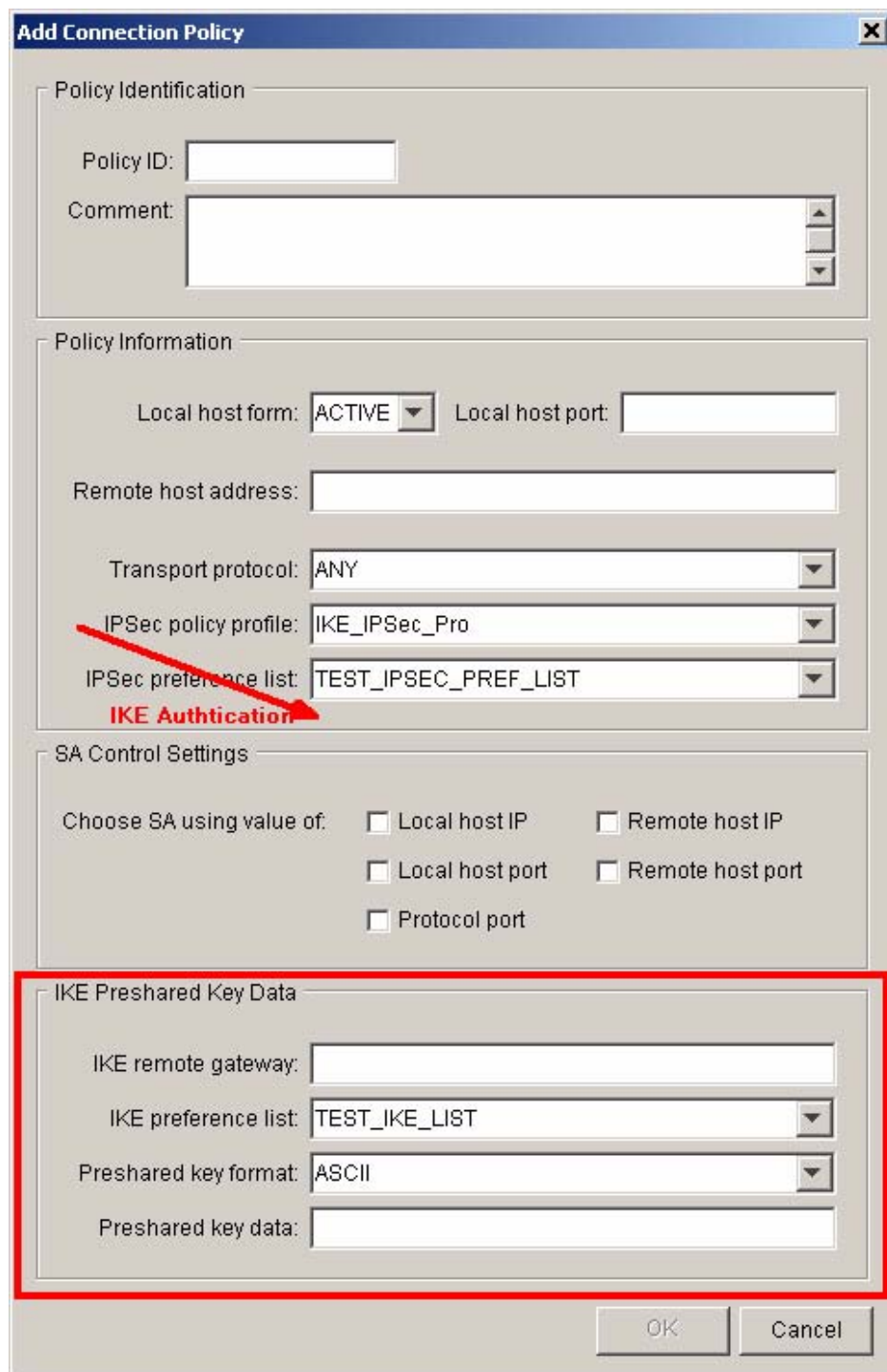
7.8.2.3.7 Context sensitive launching information

N/A

7.8.2.3.8 Supplementary information

N/A

7.8.2.4 GUI name: Add/Change Connection Policy Dialog



The image shows a screenshot of the 'Add Connection Policy' dialog box. The dialog is divided into several sections: 'Policy Identification', 'Policy Information', 'SA Control Settings', and 'IKE Preshared Key Data'. The 'IKE Preshared Key Data' section is highlighted with a red border. A red arrow points to the 'IPSec preference list' dropdown menu, which is labeled 'IKE Authentication' in red text.

Add Connection Policy

Policy Identification

Policy ID:

Comment:

Policy Information

Local host form: **ACTIVE** Local host port:

Remote host address:

Transport protocol: **ANY**

IPSec policy profile: **IKE_IPSec_Pro**

IPSec preference list: **TEST_IPSEC_PREF_LIST**

IKE Authentication

SA Control Settings

Choose SA using value of:

- ☐ Local host IP
- ☐ Remote host IP
- ☐ Local host port
- ☐ Remote host port
- ☐ Protocol port

IKE Preshared Key Data

IKE remote gateway:

IKE preference list: **TEST_IKE_LIST**

Preshared key format: **ASCII**

Preshared key data:

OK Cancel

7.8.2.4.1 Functional description

This dialog shows the connection policy configuration parameter list and used to configure these parameters.

7.8.2.4.2 GUI usage and implications

Provisioning a GWC with IPSen supported, then configure connection policy.

7.8.2.4.3 GUI size

N/A

7.8.2.4.4 GUI fields

The area “IKE Preshared Key Data” will be removed from Add/Change Connection Policy Dialog box. Additional, a new drop down selector “IKE Authentication” will be added into this dialog box.

7.8.2.4.5 Usage example

In connection policy panel, click “Add/Change” button, the dialog will be shown. You can configure /change a connection policy.

7.8.2.4.6 GUI release history update

N/A

7.8.2.4.7 Context sensitive launching information

N/A

7.8.2.4.8 Supplementary information

N/A

7.8.2.5 GUI name: IKE Authentication Panel

IPSec Profile	IPSec Preference	IPSec Preference List	IKE Preference	
IKE Preference List	IKE Authentication	IKE Certificate	Connection Policy	Kerberos
IKE remote gateway	IKE preference list	Method 1	Method 2	
1.1.1.1	DES-MD5-grp1-600s	PKI	PRESHARED	
2.2.2.2	DES-MD5-grp1-600s	PRESHARED	NONE	

Add... Change... Delete

7.8.2.5.1 Functional description

This panel displays the IKE authentication configuration data.

7.8.2.5.2 GUI usage and implications

Provisioning a GWC with IPSen supported, then configure this IPSen configuration.

7.8.2.5.3 GUI size

N/A

7.8.2.5.4 GUI fields

This panel will include 4 columns:

- IKE remove gateway column contains an IPV4 address.
- IKE preference list column contains an index into the “IKE Preference List” panel.
- Method1 column displays either PKI, PRESHARED or NONE.
- Method2 column displays either PKI, PRESHARED or NONE.

and 3 buttons:

- Add
- Change

- Delete.

7.8.2.5.5 Usage example

At first, configure a IKE Authentication, then the configured item will be shown in the panel.

7.8.2.5.6 GUI release history update

N/A

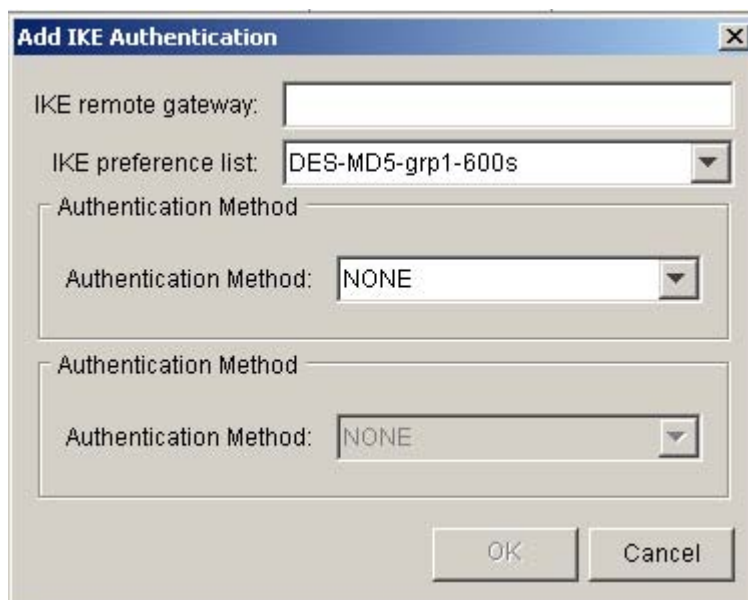
7.8.2.5.7 Context sensitive launching information

N/A

7.8.2.5.8 Supplementary information

N/A

7.8.2.6 GUI name: Add/Change IKE Authentication dialog



7.8.2.6.1 Functional description

This dialog shows the IKE authentication configuration parameter list and is used to configure these parameters.

7.8.2.6.2 GUI usage and implications

Provisioning a GWC with IPsen supported, then configure IKE authentication.

7.8.2.6.3 GUI size

N/A

7.8.2.6.4 GUI fields

This dialog will include 4 fields:

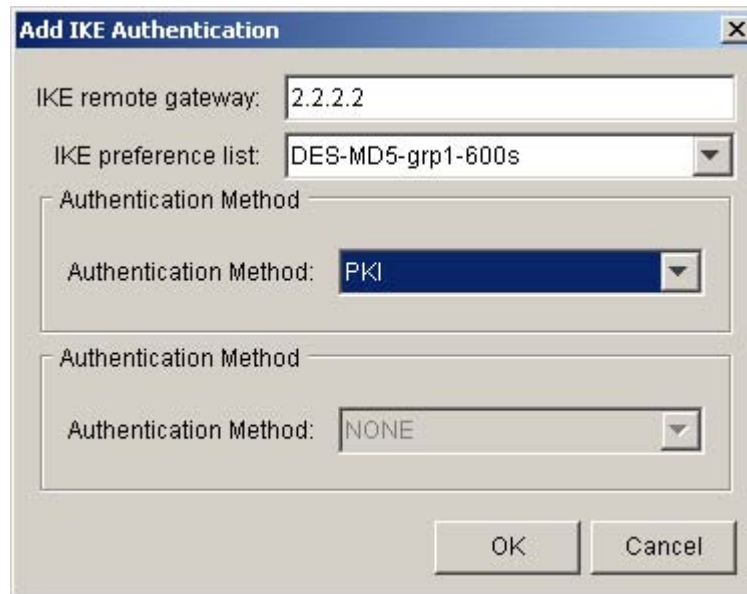
- IKE remove gateway.
- IKE preference list cl.
- Authentication Method (1).
- Authentication Method (2).

7.8.2.6.5 Usage example

In IKE authentication panel, when the “Add” button is clicked, the “Add IKE Authentication” dialog box will appear, which includes following fields:

- IKE remove gateway column contains an IPV4 address.
- IKE preference list column contains an index into the “IKE Preference List” panel.
- Authentication Method field is a drop down selector, available values consisting of “None”, “PRESHARED” and “PKI”.
- Please note that the second Authentication Method only becomes editable after the first Authentication Method is datafilled. They have the same available values.
- In SN9.1, at most one PKI and at most one PRESHARED can be selected in the same IKE Authentication item. E.g. you can select only “PKI”, or only “PRESHARED” as authentication method. Also you can select both “PKI” and “PRESHARED” as authentication methods. But you cannot select two “PKI” or two “PRESHARED”.

If you select PKI as authentication method, just simply save it by clicking “OK” button.

Figure 1 Add IKE Authentication - PKI method

The image shows a Windows-style dialog box titled "Add IKE Authentication". It contains the following fields and controls:

- IKE remote gateway:** A text box containing "2.2.2.2".
- IKE preference list:** A dropdown menu showing "DES-MD5-grp1-600s".
- Authentication Method:** A section containing two dropdown menus. The first dropdown is labeled "Authentication Method:" and is set to "PKI". The second dropdown is also labeled "Authentication Method:" and is set to "NONE".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

If you select “PRESHARED” as authentication method, three more fields will appear on the dialog box:

- Preshared key format field is a drop down selected, only be shown when “PRESHARED” is selected as authentication method. Available values consisting of “ASCII” and “HEX”.
- Preshared key data is a text field, only be shown when “PRESHARED” is selected as authentication method.
- Last modified data is a non editable text field, only be shown when “PRESHARED” is selected as authentication method. SESM will display current time in this field.

Add IKE Authentication - Preshared method

Add IKE Authentication

IKE remote gateway: 2.2.2.2

IKE preference list: DES-MD5-grp1-600s

Authentication Method

Authentication Method: PRESHARED

Preshared key format: ASCII

Preshared key data: DATATEST

Last modified date:

Authentication Method

Authentication Method: NONE

OK Cancel

7.8.2.6.6 GUI release history update

N/A

7.8.2.6.7 Context sensitive launching information

N/A

7.8.2.6.8 Supplementary information

N/A

7.8.2.7 GUI name: PKI Certificate Panel

IKE Preference List		IKE Authentication		IKE Certificate		Connection Policy		Kerberos	
Set No.	Root CA	Chain	Device	Private Key					
1	PKBRoot01	PKBCA01	GWC-6 10.66.17.60	<KEY IS HIDDEN>					

RetrieveViewDeleteRefresh

7.8.2.7.1 Functional description

This panel displays the entire chain (root, intermediate, device certs + private key) in a single row with one piece of info (maybe subject name) on each cert.

7.8.2.7.2 GUI usage and implications

Provisioning a GWC with IPsen supported, then view this panel.

7.8.2.7.3 GUI size

N/A

7.8.2.7.4 GUI fields

TBD.

7.8.2.7.5 Usage example

At first, provision a GWC with IPsec supported, then click “Retrieve” button to get the certificates. After succeed get the certificates, the panel display the entire chain (root, intermediate, device certs + private key) in a single row with one piece of info (subject name) on each cert. Click “Delete” to delete the certificates. Click “Refresh” button to refresh the certificates display.

7.8.2.7.6 GUI release history update

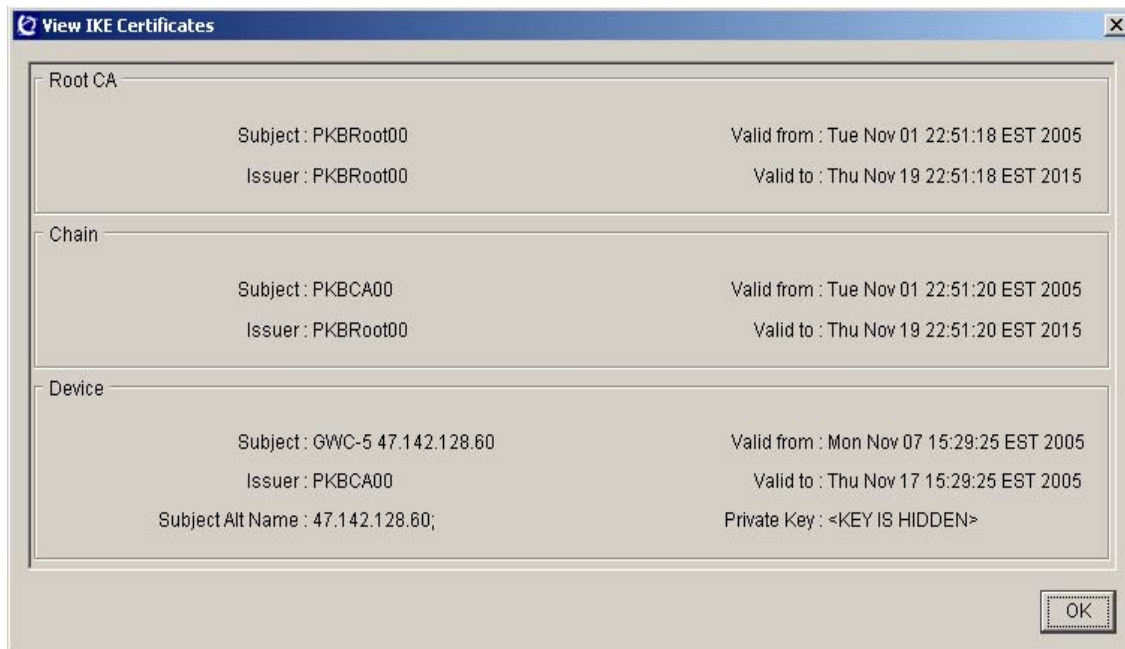
N/A

7.8.2.7.7 Context sensitive launching information

N/A

7.8.2.7.8 Supplementary information

N/A

7.8.2.8 GUI name: IKE Preference Panel**7.8.2.8.1 Functional description**

This dialog displays the entire chain with more info.

7.8.2.8.2 GUI usage and implications

Provisioning a GWC with IPsen supported, then view the entire chain with more info.

7.8.2.8.3 GUI size

N/A

7.8.2.8.4 GUI fields

TBD.

7.8.2.8.5 Usage example

In IKE certificate panel, click "view" button, the dialog will be shown. You can view the entire chain with more info.

7.8.2.8.6 GUI release history update

N/A

7.8.2.8.7 Context sensitive launching information

N/A

7.8.2.8.8 Supplementary information

N/A

7.8.3 CLUI Interface**7.9 User interface changes**

N/A

7.10 OSSGate Interface Changes

N/A

7.11 Security

User Authorization and Operations

Table 3 IPsec GUI Auth Groups and Operations Mapping

	GUI Operation	Auth Group(s) permitted
1.	Add/Change/Delete IPsec Profile	mgcrw, secrw
2.	View IPsec Profile	mgcro, secro
3.	Add/Change/Delete IPsec Preference	mgcrw, secrw
4.	View IPsec Preference	mgcro, secro
5.	Add/Change/Delete IPsec Preference List	mgcrw, secrw
6.	View IPsec Preference List	mgcro, secro
7.	Add/Change/Delete IKE Preference	mgcrw, secrw
8.	View IKE Preference	mgcro, secro
9.	Add/Change/Delete IKE Preference List	mgcrw, secrw
10.	View IKE Preference List	mgcro, secro
11.	Add/Change/Delete IKE Authentication	mgcrw, secrw
12.	View IKE Authentication	mgcro, secro

Table 3 IPsec GUI Auth Groups and Operations Mapping

	GUI Operation	Auth Group(s) permitted
13.	Download/Delete IKE Certificate	mgcrw, secrw
14.	View/Refresh IKE Certificate	mgcro, secro
15.	Add/Change/Delete Connection Policy	mgcrw, secrw
16.	View Connection Policy	mgcro, secro
17.	Add/Change Kerberos	mgcrw, secrw
18.	View Kerberos	mgcro, secro

7.12 Configuration Walkthrough

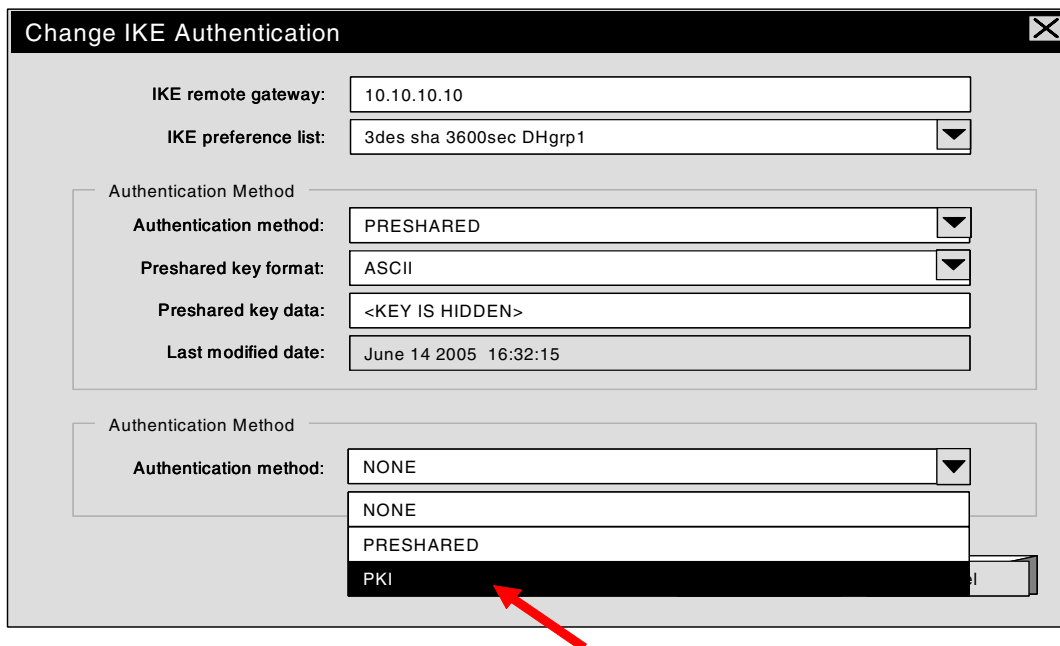
The following transition scenarios are covered by this document:

1. PSK to PKI
2. PKI to PSK

7.12.1 Transition from PSK to PKI

1. In IKE authentication panel, select “Change” button.

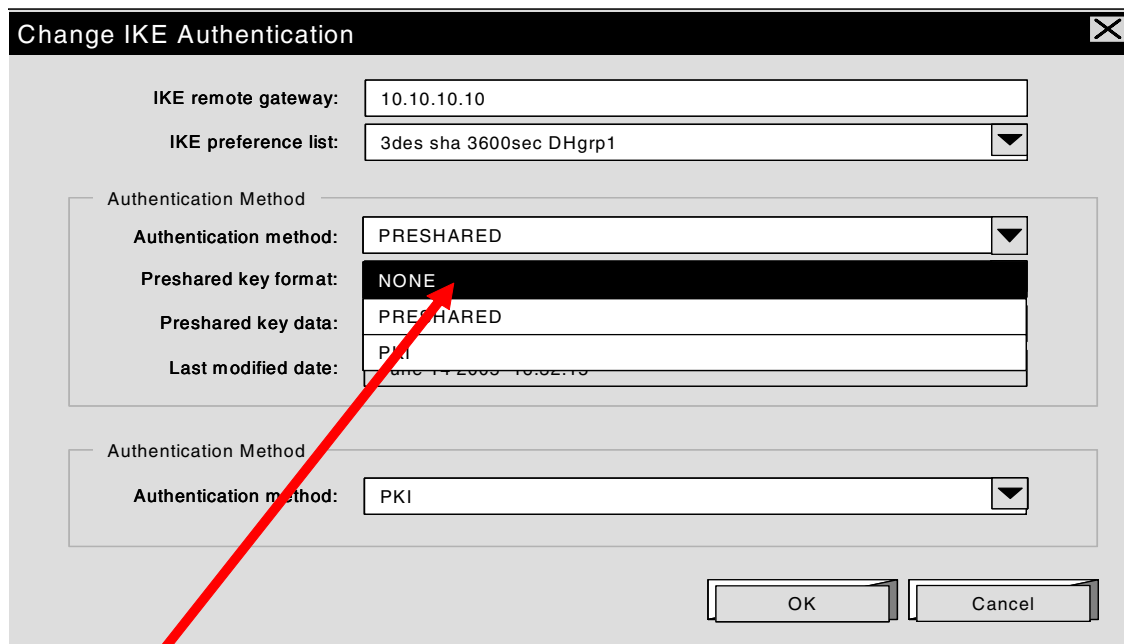
In the IKE authentication change dialog, set the second Authentication Method to PKI: (PSK -to- PSK + PKI)



The dialog box titled "Change IKE Authentication" contains the following fields and options:

- IKE remote gateway: 10.10.10.10
- IKE preference list: 3des sha 3600sec DHgrp1
- Authentication Method section:
 - Authentication method: PRESHARED
 - Preshared key format: ASCII
 - Preshared key data: <KEY IS HIDDEN>
 - Last modified date: June 14 2005 16:32:15
- Authentication Method section (dropdown menu):
 - NONE
 - NONE
 - PRESHARED
 - PKI (highlighted with a red arrow)

2. After the GWC use the PKI as its new profile, the customer will delete the PSK from the IKE authentication setting: (PSK+PKI - to - PKI)



The dialog box titled "Change IKE Authentication" contains the following fields and options:

- IKE remote gateway: 10.10.10.10
- IKE preference list: 3des sha 3600sec DHgrp1
- Authentication Method section:
 - Authentication method: PRESHARED
 - Preshared key format: NONE (highlighted with a red arrow)
 - Preshared key data: PRESHARED
 - Last modified date: PKI
- Authentication Method section (dropdown menu):
 - PKI
- Buttons: OK, Cancel

7.12.2 Transition from PKI to PSK

1. In IKE authentication panel, select “Change” button.

In the IKE authentication change dialog, set the second Authentication Method to PSK: (PKI -to- PKI + PSK)

Change IKE Authentication

IKE remote gateway: 10.10.10.10

IKE preference list: 3des sha 3600sec DHgrp1

Authentication Method

Authentication method: PKI

Authentication Method

Authentication method: PRESHARED

Preshared key format: NONE

Preshared key data: PRESHARED

Last modified date: June 11, 2006 10:02:10

OK Cancel

2. After the GWC use the PSK as its new profile, the customer will delete the PKI from the IKE authentication setting: (PKI+PSK - to - PSK)

Change IKE Authentication

IKE remote gateway: 10.10.10.10

IKE preference list: 3des sha 3600sec DHgrp1

Authentication Method

Authentication method: NONE

Authentication Method

Authentication method: PRESHARED

Preshared key format: ASCII

Preshared key data: KEY IS HIDDEN>

Last modified date: June 14 2005 16:32:15

OK Cancel

8: Configuration - SSM Certificate Handling

8.1 Hardware and Software Requirements

SN09.1 or later software load for SSPFS and the MG9K Element manager.

8.2 Initial Configuration

8.2.1 SSPFS Certificate

From a high-level, here are the steps to install the certificate “chain” on the SSPFS Machine from PKBroker.

1. Load IEMS with the required SN09.1 or later software.
2. Load both SSPFS and MG9000 Element Manager with required SN09.1 or later software.
3. For installing the certificate(s) on the SSPFS machine, thru PKBroker, the craftsperson will perform a certificate signing request from X. This is done by X. Behind scenes, PKBroker sends request to SSM on the SSPFS Machine. SSM generates a certificate signing request and forwards the CSR to PKBroker and the certificate is returned along with all supporting certificates. These certificates are installed in Solaris.
4. To verify the installation of certificates, the craftsperson will press the display all certificates button from the Certificate page.

8.2.2 IKE Entry with certificates

IPSec and IKE configuration parameters that are provisioned, via the Server Security Manager (SSM), must match the corresponding IPSec and IKE parameters on the MG9000, provisioned via the LCI and MG9000 Element Manager.

From a high-level here are the steps to enable security on the OAM&P links.

1. Load both MG9000 and MG9000 Element Manager with required software.
2. When commissioning the MG9000, the craftsperson will enable security using certificates for that network element using the Node Provisioning view of the Element Manager.
3. The craftsperson will then use a web browser and connect to the MG9000 Element Manager server machine (SSM). After logging in, the craftsperson will enable security by creating IPSec and IKE entries using the MG9000 IP address. When provisioning the IKE entry the craftsperson will elect to use certificates instead of pre-shared key.
4. Cold start from MG9000 or manual discovery from Element Manager.
5. This will complete securing the OAM&P link.

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

Not applicable

8.4 Upgrade Impact

8.4.1 Server Security Manager

For SN07 or earlier to SN09.1 upgrades, there are no impacts as IPSec was not available.

For SN08 or SN09 to SN09.1 upgrades, an SSPFS backup and restore will be necessary to move IPSec configuration forward to SN09.1. A restart of the SSPFS machine or a restart of the iked daemon will be necessary to load the IPSec data into Solaris. No data conversion will be necessary.

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

None

8.6 OSS Changes

None

8.7 External Interface Changes

None.

8.8 Server Security Manager

8.8.1 GUI name: Server Security Manager

Server Security Manager

8.8.1.1 Functional description

This HTML webpage is used to define security parameters to secure communications into and out from the SSPFS Machine. This includes MG9000 Element Manager to MG9000 OAM&P communications.

The craftsperson will be presented with two tables representing currently provisioned security parameters. One for IPSec parameters and one for IKE parameters. Options to add and delete entries are available. Adding entries will be performed using HTML forms.

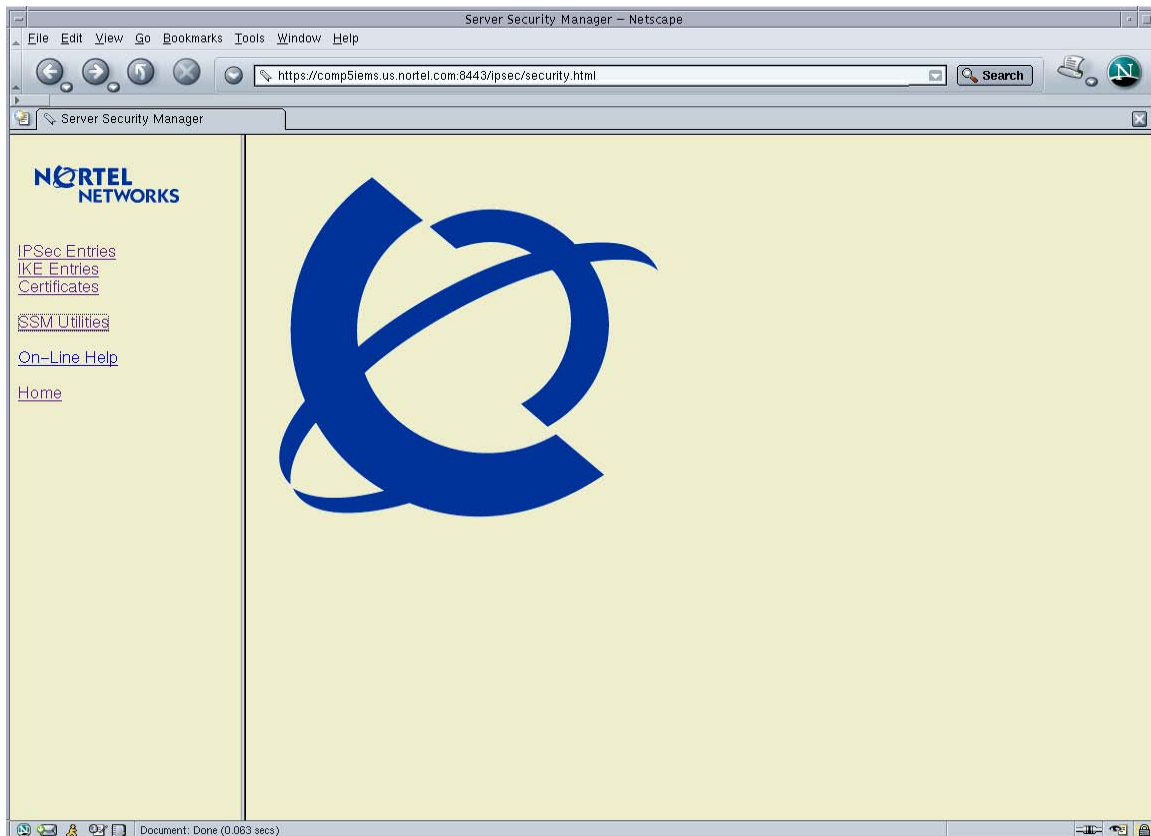
The IPSec Entries page allows retrieval and manipulation of IPSec policies for a host server. Once the policies are configured, all outbound and inbound datagrams are subject to policy checks as they exit and enter the host server. If no entry is found, no policy checks will be completed, and all the traffic will pass through. Depending upon the match of the policy entry, a specific action will be taken.

The IKE Entries page allows retrieval and manipulation of Internet Key Exchange policies for a host server. Once a policy is configured, the IKE daemon running on the host server, discovers a remote host's public encryption key. The local system can then encrypt messages destined for the remote host whose public key it has discovered.

A new "Transforms" button will be available from the IKE Entries page to allow the craftsperson to add, delete, and view multiple transforms per IKE entry. For example, one transform could support a preshared key and another could support certificates.

A new "Certificates" link will be available on the navigation bar on the left. This will access the SSPFS Machine's certificates. Options to perform certificate signing requests to the CA authority and to delete certificates will be found.

The following is the first page presented to the craftsperson upon opening the Security Interface:



Navigation is performed using the links on the left frame. User input is performed or operation output is displayed in the right frame.

8.8.1.2 GUI usage and implications

First, IPSec entries are created using the desired parameters. If the craftsperson has chosen to use the "IPSec" action, the second step is to create a corresponding IKE entry using the desired parameters.

This interface provides for securing all network communications and not just Element Manager communications. Care must be taken when provisioning or deleting the security parameters, so as not to effect other essential communications, such as telnet, ftp, etc.

8.8.1.3 IPSec Entry

No changes are planned.

8.8.1.4 IKE Entry

The following table lists the security fields for IKE parameters.

Table 1 IPSec field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action
Index ID	No	No	Integer	Internal index used by the server to track and reference IKE entries.
Remote Address	No	No	A numeric internet IP address of the form: www.xxx.yyy.zzz	IP address of the remote system communicating with this server.
Local Address	No	No	A numeric internet IP address of the form: www.xxx.yyy.zzz	IP address of this server.
Type	New	No	Preshared Key or Certificate	Selects the type of security negotiation and authentication to use.
Oakley Group	No	No	1 (768-bit), 2 (1024-bit), or 5 (1536-bit).	The Oakley Diffie-Hellman group used for IKE Security Association key derivation.
Authentication Method	No	No	Preshared is the only supported option.	The authentication method used for IKE phase 1.
Encryption	No	No	des, 3des, and blowfish.	Specifies the encryption algorithm for a Security Association.
Authentication	No	No	sha1 and md5.	Specifies the authentication algorithm for a Security Association.
PFS Group ID	No	No	0 (do not use Perfect Forward Secrecy for IPsec SAs), 1 (768-bit), 2 (1024-bit), and 5 (1536-bit).	The Oakley Diffie-Hellman group used for IPsec Security Association key derivation.
Key	No	No	16 - 120 character ASCII string	Specifies the preshared key for this Security Association.
IKE Lifetime	No	No	Maximum allowed value is 2,419,200 seconds, 40,320 minutes, 672 hours or 28 days.	Specifies the lifetime for a IKE phase 1 Security Association.

Table 1 IPsec field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action
IPsec Lifetime	No	No	Maximum allowed value is 2,419,200 seconds, 40,320 minutes, 672 hours or 28 days.	Specifies the lifetime for an IPsec Security Association.

8.8.1.5 IKE provisioned entries example

The following example shows a number of IKE entries for an SSPFS server:

Place holder

8.8.1.6 IKE entry form example

The following example shows a form for creating IKE entries for an SSPFS server:

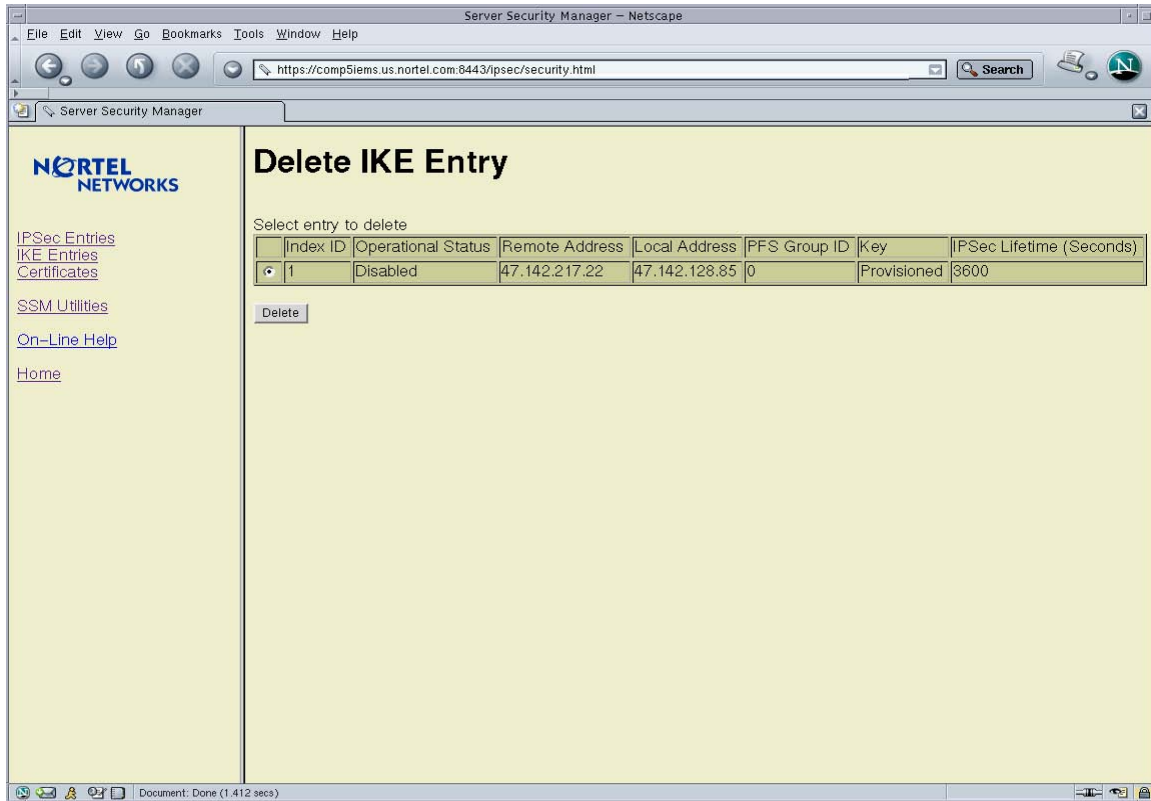
The screenshot shows a Netscape browser window titled "Server Security Manager - Netscape" with the address bar displaying "https://comp5iems.us.nortel.com:8443/ipsec/security.html". The page content is titled "Add IKE Entry" and features the Nortel Networks logo on the left. A sidebar on the left contains links: "IPSec Entries", "IKE Entries", "Certificates", "SSM Utilities", "On-Line Help", and "Home". The main form area contains the following fields and controls:

- Remote Address :
- Local Address :
- PFS Group ID :
- IPSec Lifetime :
- IPSec Lifetime Unit :
- IKE Preshared Key
 - Key Type : ☒ ASCII ☐ Hex
 - Key :
 - Verify Key :

At the bottom of the form are "Apply" and "Clear" buttons. The status bar at the bottom of the browser window indicates "Document: Done (0.826 secs)".

8.8.1.7 IKE entry deletion example

The following example shows a table for deleting IKE entries for an SSPFS server:



The screenshot shows a Netscape browser window titled "Server Security Manager - Netscape". The address bar displays "https://comp5iems.us.nortel.com:8443/ipsec/security.html". The page content is titled "Delete IKE Entry". On the left, there is a sidebar with the Nortel Networks logo and links: "IPSec Entries", "IKE Entries", "Certificates", "SSM Utilities", "On-Line Help", and "Home". The main content area has the heading "Delete IKE Entry" and a sub-heading "Select entry to delete". Below this is a table with the following data:

☐	Index ID	Operational Status	Remote Address	Local Address	PFS Group ID	Key	IPSec Lifetime (Seconds)
☒	1	Disabled	47.142.217.22	47.142.128.85	0	Provisioned	3600

Below the table is a "Delete" button. The status bar at the bottom of the browser window shows "Document: Done (1.412 secs)".

8.8.1.8 IKE entry adding transform example

The following example shows a form for adding a transform to from IKE entry for an SSPFS server:

The screenshot shows a Netscape browser window titled "Server Security Manager - Netscape". The address bar displays "https://comp5iems.us.nortel.com:8443/ipsec/security.html". The page content is divided into a left sidebar and a main area. The sidebar contains the Nortel Networks logo and a list of links: "IPSec Entries", "IKE Entries", "Certificates", "SSM Utilities", "On-Line Help", and "Home". The main area is titled "Add Transform" and contains a form with the following fields:

- Oakley Group :
- Authentication Method :
- Encryption Algorithm :
- Authentication Algorithm :
- IKE Lifetime :
- IKE Lifetime Unit :

At the bottom of the form are three buttons: "Apply", "Clear", and "Cancel". The status bar at the bottom of the browser window shows "Document: Done (0.593 secs)".

8.8.1.9 IKE entry view with transform example

The following example shows a form detailing all transform information for an IKE entry for an SSPFS server:

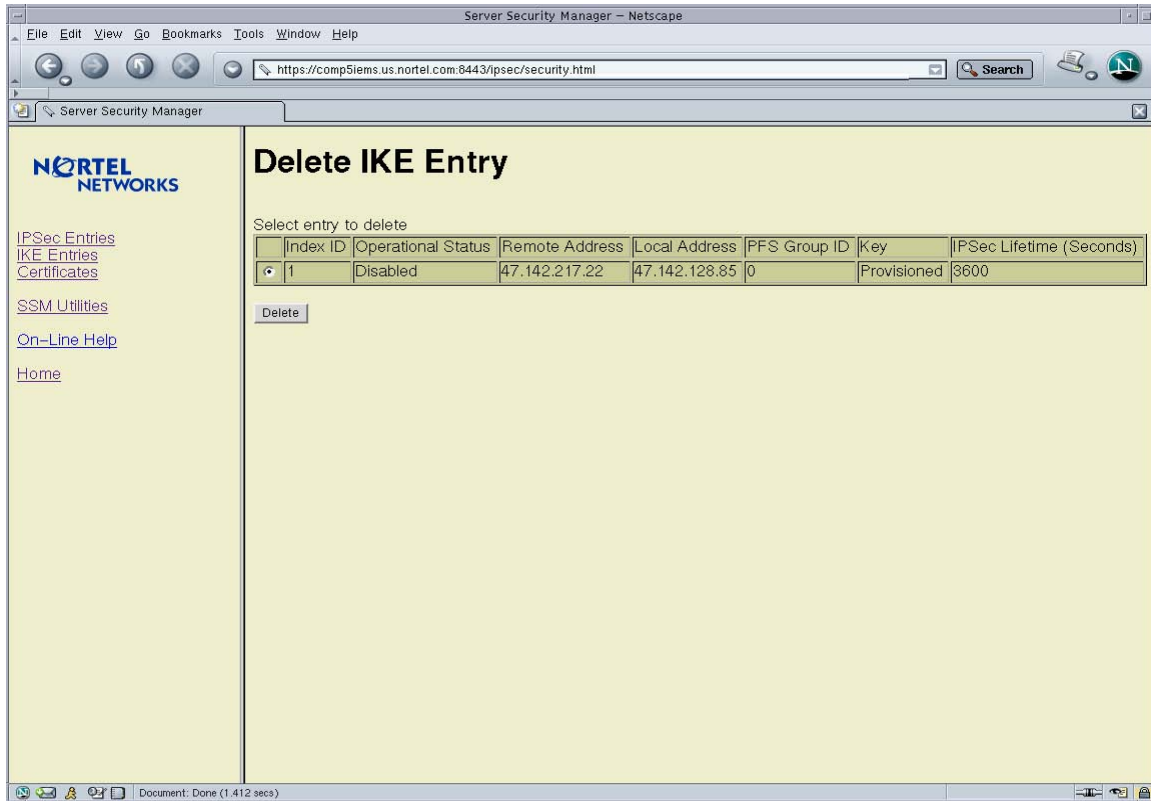
The screenshot shows a Netscape browser window titled "Server Security Manager - Netscape". The address bar displays "https://comp5iems.us.nortel.com:8443/ipsec/security.html". The page content is titled "IKE Transforms" and includes the Nortel Networks logo. A sidebar on the left contains links: "IPSec Entries", "IKE Entries", "Certificates", "SSM Utilities", "On-Line Help", and "Home". The main content area states "These are the currently provisioned xform for IKE entry 1" and displays a table with the following data:

Index ID	Xform ID	Oakley Group	Authentication Method	Encryption	Authentication	IKE Lifetime (Seconds)
1	1	1	rsa_sig	3des	sha1	3600
1	2	1	preshared	des	sha1	1

Below the table are two buttons: "Add Xform" and "Delete Xform". The status bar at the bottom indicates "Document: Done (1.313 secs)".

8.8.1.10 IKE entry delete transform example

The following example shows a form for deleting a transform from IKE entry for an SSPFS server:



8.8.1.11 Add preshared key IKE entry example

The following example shows a form for adding a preshared key to an IKE entry for an SSPFS server:

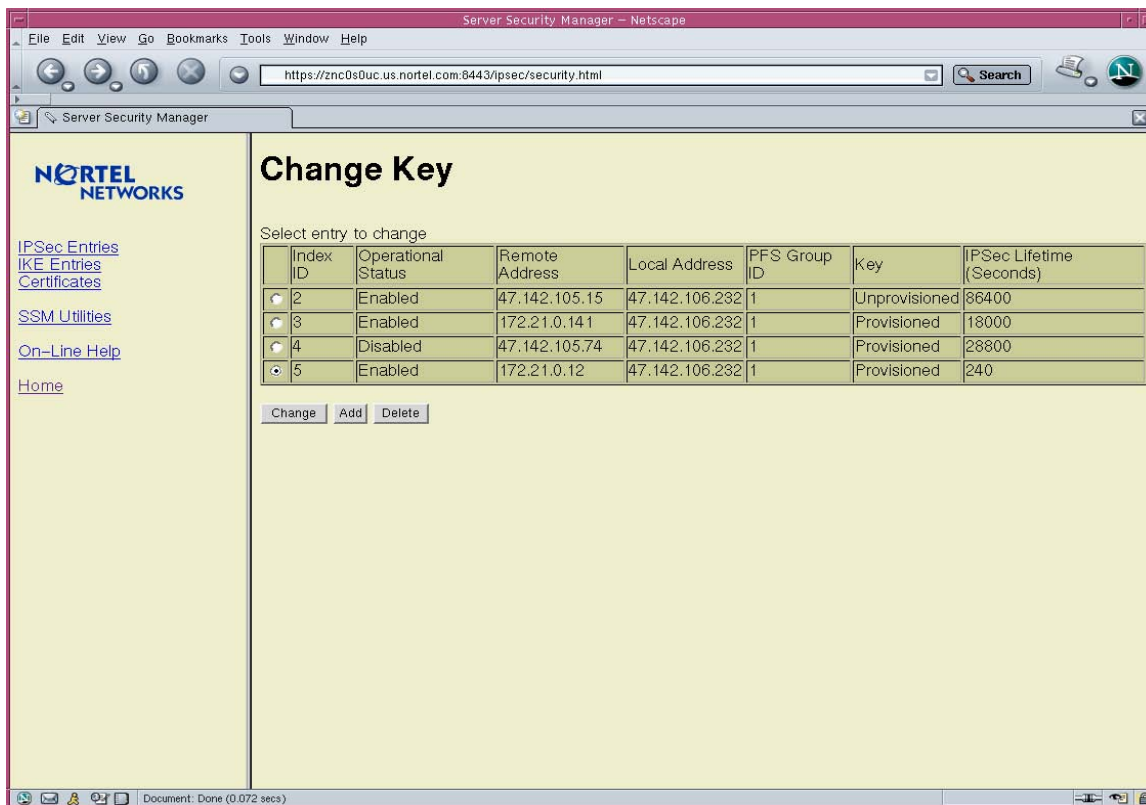
The screenshot displays a Netscape browser window titled "Server Security Manager - Netscape". The address bar shows the URL "https://znc0s0uc.us.nortel.com:8443/ipsec/security.html". The page content is titled "Add Preshared Key". On the left side, there is a navigation menu with the following links: [IPSec Entries](#), [IKE Entries](#), [Certificates](#), [SSM Utilities](#), [On-Line Help](#), and [Home](#). The main content area contains a form with the following fields and controls:

- Key Type :** A radio button selection with "ASCII" selected and "Hex" as an option.
- New Key :** A text input field.
- New Key (again) :** A second text input field for confirmation.
- Buttons:** "Apply" and "Clear" buttons located below the input fields.

The status bar at the bottom of the browser window indicates "Document: Done (0.208 secs)".

8.8.1.12 Delete preshared key IKE entry example

The following example shows a form for deleting a preshared key from an IKE entry for an SSPFS server:



8.8.1.13 Change preshared key IKE entry example

The following example shows a form for changing a preshared key for an IKE entry for an SSPFS server:

The screenshot shows a Netscape browser window titled "Server Security Manager - Netscape". The address bar displays "https://znc0s0uc.us.nortel.com:8443/ipsec/security.html". The page content is titled "Change Key" and features the Nortel Networks logo on the left. A sidebar on the left contains links: "IPSec Entries", "IKE Entries", "Certificates", "SSM Utilities", "On-Line Help", and "Home". The main form area has a "Key Type" section with radio buttons for "ASCII" (selected) and "Hex". Below this are two text input fields labeled "New Key :" and "New Key (again) :". At the bottom of the form are "Apply" and "Clear" buttons. The status bar at the bottom indicates "Document: Done (0.123 secs)".

8.8.1.14 MG9000 IKE Parameter settings

For each MG9000 provisioned and requires IP security, there must be a corresponding IKE entry.

The IKE entry must be provisioned as follows:

1. Remote Address is the address of the MG9000 as seen by the Element Manager.
2. Local Address is the address of the Element Manager as seen by the MG9000.
3. PFS Group ID is "1".
4. IPSec Lifetime is "8".
5. IPSec Lifetime Unit is "hours".
6. Key Type is "ASCII".
7. Key and Verify Key is a user supplied key.

8.8.1.15 MG9000 Certificate Xform Parameter settings

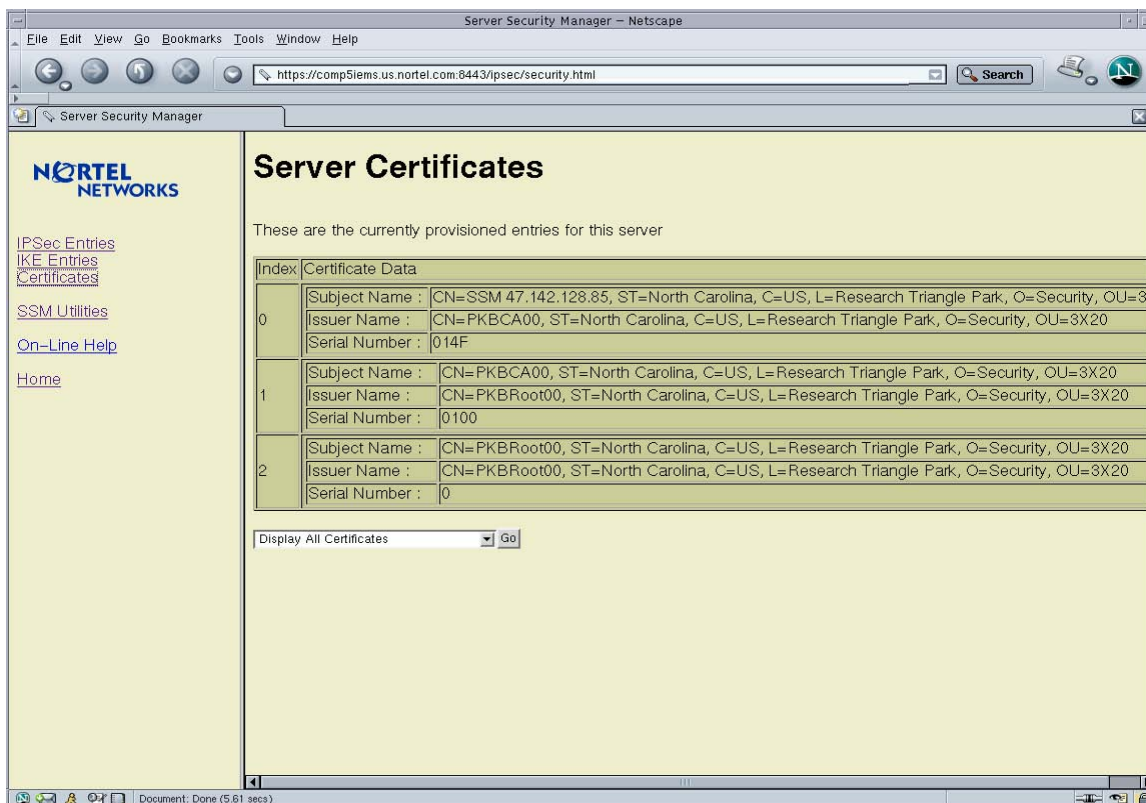
For each IKE entry there must be atleast one Xform entry. These entries specify the parameters for key negotiation.

The Xform entry must be provisioned as follows:

1. Oakley Group is “1”.
2. Authentication Method is “preshared” if using preshared key or “rsa_sig” if using public key certificates.
3. Encryption Algorithm is “3des”.
4. Authentication Algorithm is “sha1”.
5. IKE Lifetime is “8”.
6. IKE Lifetime Unit is “hours”.

8.8.1.16 Certificate Commands example

The following example shows the certificate commands available for an SSPFS server:



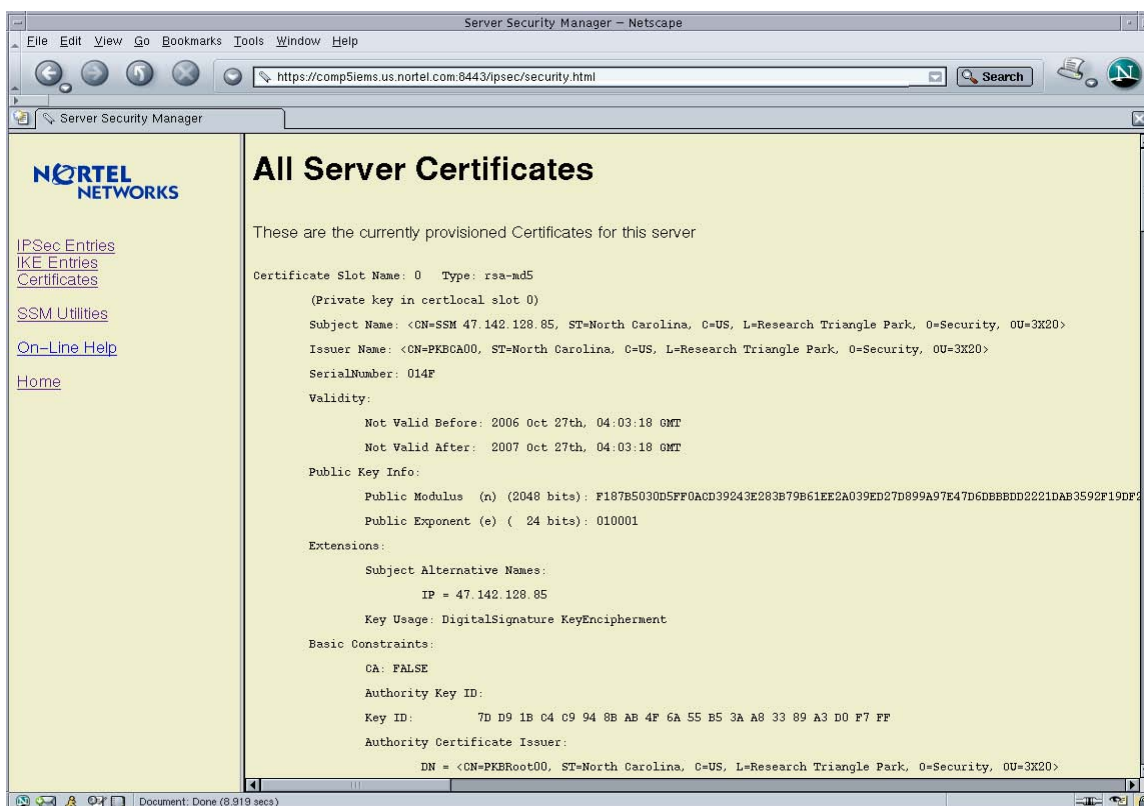
8.8.1.17 Certificate command page

The commands are as follows:

1. Certificate Signing Request - generate a certificate signing request.
2. Clear All - remove all certificates from the machine.
3. Display All - display all certificates currently provisioned.

8.8.1.18 Display All certificate example

The following example shows the Display All certificate page:

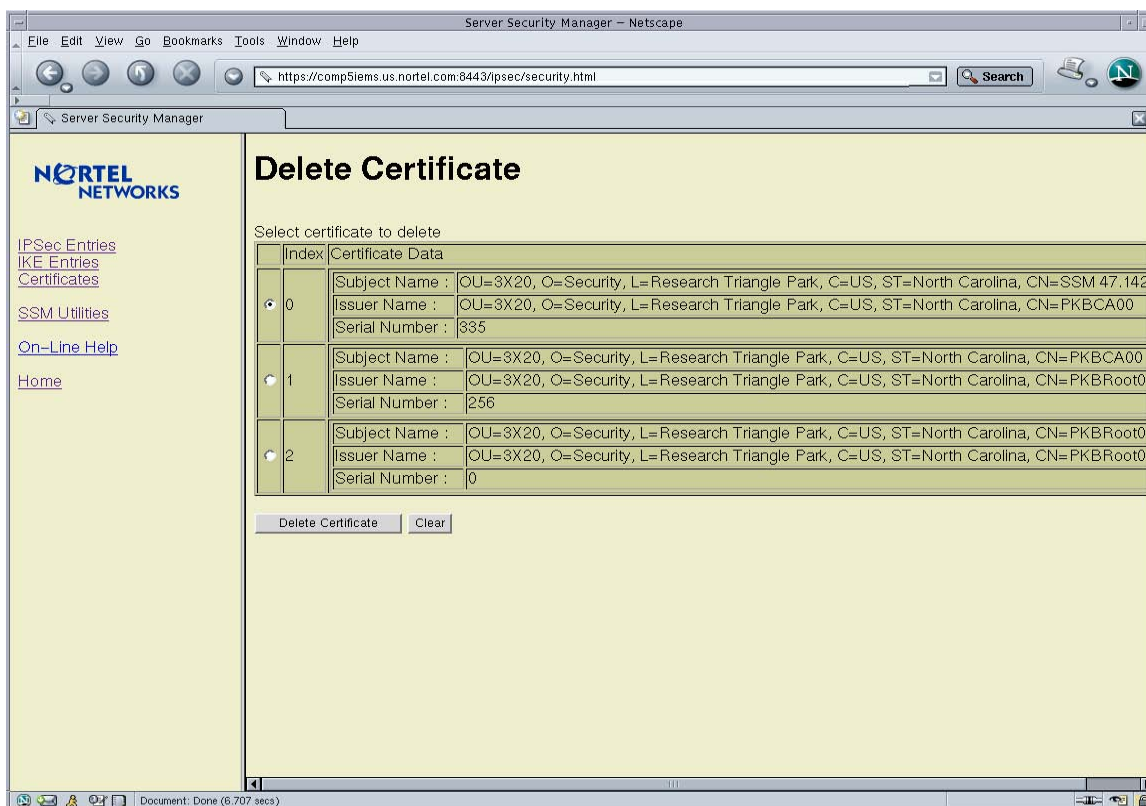


8.8.1.19 Display All certificate page

This page will display all the certificates currently provisioned on the SSPFS machine.

8.8.1.20 Delete certificate example

The following example shows the Delete certificate page:



8.8.1.21 Delete certificate page

This page will show a list of certificates, that can be deleted.

8.8.1.22 GUI release history update

The following information was added:

1. Type field to select Preshared Key or Certificate to IKE entry form and IKE table.
2. New pages for IKE transforms. Add, delete and view transforms.
3. New pages for certificates. Certificate Signing Request, Clear All and Display All.

8.8.1.23 Supplementary information

None

8.8.1.24 CLUI Interface

Not applicable

8.9 Command interface changes

Add, Delete and show IKE Entry transforms.

Certificate signing request command line option.

8.10 Security

8.10.1 Network configuration

No changes to the network are necessary to support the IPsec implementation.

8.10.2 Key management

8.10.2.1 SSPFS IKE Preshared key

The SSPFS IKE preshared key input by the user in the SSPFS Security Servlet. This key is secured by the use of secure http, if configured, from the browser to the server. Solaris stores all keys in a hidden system file not accessible by common users but is available to the ROOT user.

8.10.2.2 SSPFS Certificate Public/Private key

For the SSPFS Certificate Public/Private keys, Solaris stores all keys in a hidden system file not accessible by common users but is available to the ROOT user.

8.10.3 Protocol

IPsec is being used on the Solaris machine.

8.10.4 Authentication

Succession login will still be used for SSPFS Security Servlet.

8.11 Configuration Walkthrough

8.11.1 SSM Certificate Installation (Local)

From a high-level, here are the steps to install the certificate “chain” on the SSPFS Machine from SSM running on the SSPFS Machine.

1. Load IEMS with the required SN09.1 or later software.
2. Load both SSPFS and MG9000 Element Manager with required SN09.1 or later software.
3. For installing the certificate(s) on the SSPFS machine, thru the SSM Servlet, the craftsperson will perform a certificate signing request from the Certificate page. This is done by pressing the Cert Signing Request button. Behind scenes, the certificate is forwarded for signing and returned along with all supporting certificates. These certificates are installed in Solaris.
4. To verify the installation of certificates, the craftsperson will press the display all certificates button from the Certificate page.

8.11.2 SSM Certificate Installation (PKBroker)

From a high-level, here are the steps to install the certificate “chain” on the SSPFS Machine from PKBroker.

1. Load IEMS with the required SN09.1 or later software.
2. Load both SSPFS and MG9000 Element Manager with required SN09.1 or later software.
3. For installing the certificate(s) on the SSPFS machine, thru PKBroker, the craftsperson will perform a certificate signing request from X. This is done by X. Behind scenes, PKBroker sends request to SSM on the SSPFS machine. SSM generates a certificate signing request and forwards the CSR to PKBroker and the certificate is returned along with all supporting certificates. These certificates are installed in Solaris.
4. To verify the installation of certificates, the craftsperson will press the display all certificates button from the Certificate page.

8.11.3 SSM Certificate Removal

From a high-level, here are the steps to remove the certificate “chain” on the SSPFS Machine.

1. Load both SSPFS and MG9000 Element Manager with required software.
2. For removing the certificate(s) from the SSPFS machine, thru the SSM Servlet, the craftsperson will perform a delete all certificates from the Certificate page. This is done by pressing the Clear Certificates button. Behind scenes, the certificates are removed.
3. To verify the deletion of certificates, the craftsperson will press the display all certificates button from the Certificate page.

Product = CS2K Management Tools

A00012223, A00012217, A00012225--SESM Support for SIP Lines, Part 2

Functional Description

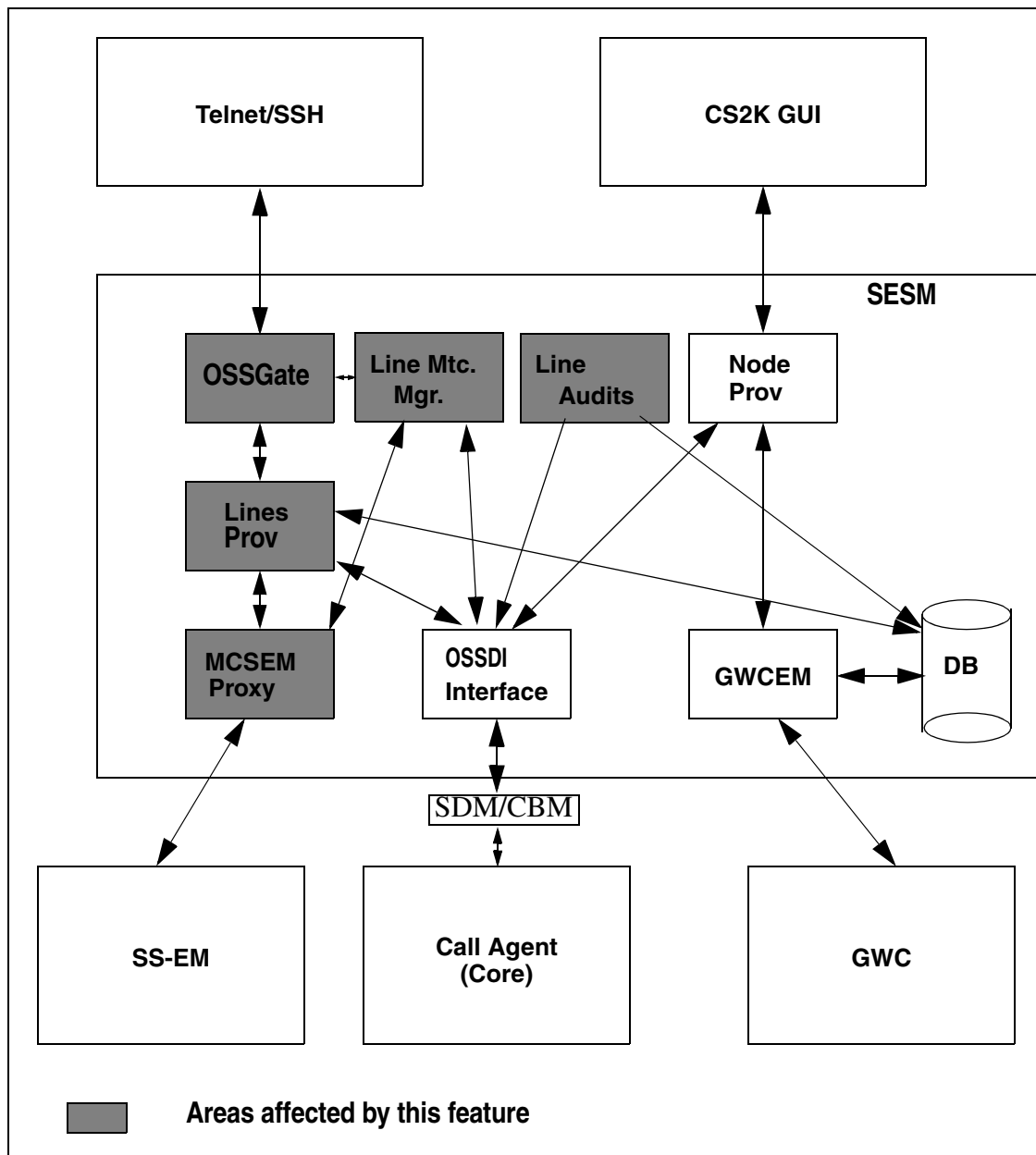
1: Applicable Solution(s)

MCS

1.1 Description

This activity, SESM Support for SIP Lines Part 2, consists of 3 features:

- A00012223 - SESM: SESM: Additional Provisioning for SIP Lines
A richer set of SERVORD+ and query commands will be supported for SIP lines. Some of the newly supported commands and will trigger flowthrough of new data to the Session Server Element Manager (SS-EM). The support of HUNT and MADN commands will entail new flowthrough logic for group information to the SS-EM.
- A00012217 - SESM: SIP Lines - Data Sync Audit
The Line Audit feature component will add auditing coverage of SIP line data on the SS-EM. The data to be audited on the SS-EM includes the Directory Number (DN), the termination name, the Virtual Media Gateway (VMG), and the HUNT/MADN group name information.
- A00012225 - SESM: SIP Lines - Maintenance Enhancements
Maintenance Enhancements introduces a Services Maintenance Command Line User Interface (CLUI) to replace the LMM GUI and eventually the LTP (Lines Test Position) level of the MAPCI.
For the introduction, this CLUI will allow the user to post Succession and non-Succession lines (TDM) and perform functions similar to that of the LTP level. This LMM CLUI defined in this document will be generic, intended for use with line or gateway types other than SIP.

Figure 1 Functional Behavior Diagram

1.1.1 Line Maintenance Manager CLUI

The LMM CLUI performs similar functions as the LMM GUI, providing a human/machine interface to view LMM configurations, generate “Query GW in Trouble” reports and line maintenance commands.

1.1.2 Configure

In the SESM, the /opt/nortel/NTsesm/admin/bin/configure tool must be used to configure SESM access to the Session Server Element Manager (SS-EM). This tool is currently used to provision the OPI link. The OMI link requires similar entries.

SESM-CS2KSS configuration

OPI - Provisioning Manager Interface configuration

Enter OPI transport protocol to EM server (http/https - default: https)

[1] - http
[2] - https
[x] - exit

select - 2

Enter the IP address / Name of the primary CS2KSS prov server (default: 47.142.91.164) : 47.142.91.164

Enter the primary CS2KSS prov server https port (default is 8443): 8443

Enter the IP address / Name of the secondary CS2KSS prov server (default: 47.142.91.164) : 47.142.91.164

Enter the secondary CS2KSS EM server https port (default is 8443): 8443

Enter the OPI administrator user name (default: admin): admin

Enter the OPI administrator password:

Re-enter the OPI administrator password:

OMI - Provisioning Manager Interface configuration

Enter OMI transport protocol to EM server (http/https - default: https)

[1] - http
[2] - https
[x] - exit

select - 2

Enter the IP address / Name of the primary CS2KSS mtc server (default: 47.142.91.164) : 47.142.91.164

Enter the primary CS2KSS mtc server https port (default is 12121): 12121

Enter the IP address / Name of the secondary CS2KSS mtc server (default: 47.142.91.164) : 47.142.91.164

Enter the secondary CS2KSS mtc server https port (default is 12121): 12121

Enter the OMI administrator user name (default: admin): admin

Enter the OMI administrator password:

Re-enter the OMI administrator password:

OPI - Provisioning Manager configuration

```
Transport protocol to EM server           : https://
Primary CS2KSS Provisioning Manager IP / Name : 47.142.91.164
Primary CS2KSS Provisioning Manager port   : 8443
Secondary CS2KSS Provisioning Manager IP / Name : 47.142.91.164
Secondary CS2KSS Provisioning Manager port   : 8443
The administrator user name                : admin
```

OMI - Maintenance Manager configuration

```
Transport protocol to Maintenance Manager : https://
Primary CS2KSS Maintenance Manager IP / Name : 47.142.91.164
Primary CS2KSS Maintenance Manager port   : 12121
Secondary CS2KSS Maintenance Manager IP / Name : 47.142.91.164
Secondary CS2KSS Maintenance Manager port   : 12121
The administrator user name                : admin
```

Is the information correct? (y or n) :

The configuration tool will prompt the user to enter the following for the OMI link information:

- Transport protocol to SS-EM server (https).
- IP address / host name of primary SS-EM server
- IP address / host name of secondary SS-EM server. Some configurations may not include a secondary SS EM server. If so, configure the same information provided for the primary server (by default this should be the case).
- HTTPS communication port to SS EM server (12121).
- SS-EM Provisioning Manager administrator user name
- SS-EM Provisioning Manager administrator password

The OPI version information is not required anymore since it is dynamically determined when the OPI and OMI links come into service.

The IP address and port will be used to generate the SS-EM Provisioning Manager URL which in turn will be added to sesm.properties file.

As part of the configuration, the IP address will be validated for format, range and reachability. Other user entered data will be validated for format, range, values etc.

The user name will be added to sesm.properties as clear text.

The password will be stored separately and accessible only to the root user.

All configuration information (url, username, etc.) except password can be displayed by using the SESM “/opt/nortel/NTsesm/admin/bin/configure” tool.

1.1.3 Audits

The Line Audit will now audit the endpoints of Session Server EM with GWCEM and compare group information in SS EM with core and also compare DN to LEN mapping stored in SS EM with core. See section “2.6.2 Line Audit” for information on changes to GUI, BPT, and audit output data (valid and problem log file)

1.1.4 Line Provisioning

Existing support for provisioning SIP lines at OSSGate via SERVORD+ commands will be extended to include a more robust and richer set of commands. See section “1.5.2 SERVORD+ via OSSGate” on page 1118 for detailed information.

1.2 Hardware Requirements or Dependencies

Not applicable.

1.3 Software Requirements or Dependencies

This activity requires that the following components are loaded with SN09 drop 2 or equivalent loads.

CM, XAC or 3PC

GWC

MSM

1.4 Limitations and restrictions

1.4.1 SERVORD+ via OSSGate

See “1.5.2 SERVORD+ via OSSGate” on page 1118 for the various limitations and restrictions related to the support for the expanded set of SERVORD+ commands.

1.5 Interactions

1.5.1 LMM CLUI

To access the LMM CLUI telnet to OSSGate, enter ^B, “mode MTC”. Once in the MTC level, “LMM” is entered for access to the LMM CLUI.

```
>
? mode MTC

Mode is MTC.
```

The CMCLLI command is used to return the SDM IP and CMCLLI name:

```
>CMCLLI
SDM IP = 47.142.134.124
CM CLLI = RTP2
```



```
>LMM
report <-v>
report <-l> <report name>
report <-gen> <GWC Options>

post <-d, -l, -gw, -u, -r, -set, -display, -count>

bsy <-d, -l, -gw, -set> [inb]
rts <-d, -l, -gw, -set>
tst <-d, -l, -gw, -u, -set>
FRLS <-d, -l>

qdn <dn>
qlen <len>
qsip <dn, len>

help

quit
```

The commands (i.e. report, bsy) can be entered in either upper or lower case. The options (i.e. -d, -l) must be entered in lower case. The parms can be entered in either case but in the case of the GW name, should be in the proper case.

1.5.1.1 REPORT Commands

The REPORT commands are used with the GW in Trouble reports. Using the commands, the user has the ability to list, view and delete any of the reports. The GENERATE or GEN is used to run the process to create a report.

Command format:

```
report <-l>
report <-v> <REPORT NAME>
report <-gen> <GWC List | all>
```

Command usage:

To obtain a list of reports currently available

```
>report -l
The following reports are available:
Report-2005-08-10-22-06-14
```

To view a specific report

```
>report -v Report-2005-08-10-22-06-14
GW Name      Results for GWC-0
t1124ent.us.nortel.com  GW DISABLED

GW Name      Results for GWC-10
test4       GW DISABLED
```

To request a new GW in Trouble report for GWC 1

```
report -gen 1
```

To request a new GW in Trouble report for GWC 1, 2 and 3

```
report -gen 1, 2, 3
```

```

    or
report -gen 1-3

```

```

    or
report -gen 1, 2-3

```

To request a new GW in Trouble report for all valid (small and large line) GWCs

```
report -gen all
```

1.5.1.2 MTC Commands

This set of commands is used to perform operations on either one or a set of lines.

Command format:

```

post -d <DN> [verbose]
post -l <LEN> [verbose]
post -gw <GW/VMG> [verbose]
post -u <URI> [verbose]
post -r <Domain name> [verbose]
post -display [verbose]
post -count

```

```

bsy -d <DN> [inb]
bsy -l <LEN> [inb]
bsy -gw <GW or VMG> [inb]
bsy -set [inb]

```

```

rts -d <DN>
rts -l <LEN>
rts -gw <GW/VMG>
rts -set

```

```

tst -d <DN>
tst -l <LEN>
tst -gw <GW/VMG Name>
tst -u <URI>
tst -set

```

```

frls -d <DN>
frls -l <LEN>

```

1.5.1.2.1 REPORT Commands

The REPORT commands are used with the GW in Trouble reports. Using the commands, the user has the ability to list and view any of the reports. The -gen is used to run the process to create a report.

Command format:

```

report <-l>
report <-v> <REPORT NAME>
report <-gen> <GWC List | all>

```

Command usage:

To obtain a list of reports currently available

```
>report -l
The following reports are available:
Report-2005-11-14-12-12-01
```

To view a specific report

```
>report -v Report-2005-11-14-12-12-01
GWC-14  Number of GWs out of service = 1

R7A20204.rtp7.net status = GW DISABLED

GWC-13  Number of GWs out of service = 11
```

To request a new GW in Trouble report for GWC 1

```
report -gen 1
```

To request a new GW in Trouble report for GWC 1, 2, 3 and 4

```
report -gen 1, 2, 3, 4
```

or

```
report -gen 1-4
```

or

```
report -gen 1, 2-4
```

To request a new GW in Trouble report for all valid (small and large line) GWCs

```
report -gen all
```

1.5.1.2.2 POST

The POST command can be used to generate a set of lines and be used for maintenance (BSY, etc.) actions.

The POST command will list the contents of the post set to the screen using a “brief” format. The information listed will be dn, len, uri, clientIp, gwc, lcc, cm line state, scc line state and MCS line state (if a SIP Line).

The VERBOSE option includes included the above and adds the following, GW/VMG name, GW ipaddress, GW type, endpointName, domain/subdomain.

To post by DN (SIP Line)

```
>post -d 7550505
DN          = 6137550505
LEN         = SS 00 0 00 05
LCC         = IBN
GWC NAME    = GWC-5
GW NAME     = rtp7ssa
EPT NAME    = SS/000/0/0005
GW EPT ST   = ON-HOOK
CM EPT ST   = IDL
SIP URI     = user5@rtp7ssa.com
CLIENT IP   =
SS EPT ST   =
```

Number of endpoints returned = 1

To post by DN, non SIP Line

> post -d 6210010

```
DN          = 6136210010
LEN         = UAIP 00 1 00 00
LCC         = IBN
GWC NAME    = GWC-14
GW NAME     = rtp7-1104b.us.nortel.com
EPT NAME    = aaln/1
GW EPT ST   = ON-HOOK
CM EPT ST   = IDL
```

Number of endpoints returned = 1

To post by LEN:

> post -l ss 0 0 0 5

```
DN          = 6137550505
LEN         = SS 00 0 00 05
LCC         = IBN
GWC NAME    = GWC-5
GW NAME     = rtp7ssa
EPT NAME    = SS/000/0/0005
GW EPT ST   = ON-HOOK
CM EPT ST   = INB
SIP URI     = user5@rtp7ssa.com
CLIENT IP   =
SS EPT ST   =
```

To post by GW:

Note: Since the minimum VMG size for SIP is 1023 endpoints, posting by vmg may take a long time (approx 5 mins per LGRP) and will produce a huge output.

> post -gw rtp7-1104b.us.nortel.com

```
DN          = 6136210010
LEN         = UAIP 00 1 00 00
LCC         = IBN
GWC NAME    = GWC-14
GW NAME     = rtp7-1104b.us.nortel.com
EPT NAME    = aaln/1
GW EPT ST   = ON-HOOK
CM EPT ST   =

DN          = 6136210011
LEN         = UAIP 00 1 00 01
LCC         = IBN
```

```
GWC NAME = GWC-14
GW NAME  = rtp7-1104b.us.nortel.com
EPT NAME = aaln/2
GW EPT ST = ON-HOOK
CM EPT ST =
```

```
DN       = 6136210012
LEN      = UAIP 00 1 00 02
LCC      = RES
GWC NAME = GWC-14
GW NAME  = rtp7-1104b.us.nortel.com
EPT NAME = aaln/3
GW EPT ST = ON-HOOK
CM EPT ST =
```

```
DN       = 6136210013
LEN      = UAIP 00 1 00 03
LCC      = RES
GWC NAME = GWC-14
GW NAME  = rtp7-1104b.us.nortel.com
EPT NAME = aaln/4
GW EPT ST = ON-HOOK
CM EPT ST =
```

To post by URI:

```
> post -u user5@rtp7ssa.com
DN       = 6137550505
LEN      = SS 00 0 00 05
LCC      = IBN
GWC NAME = GWC-5
GW NAME  = rtp7ssa
EPT NAME = SS/000/0/0005
GW EPT ST = ON-HOOK
CM EPT ST =
SIP URI  = user5@rtp7ssa.com
CLIENT IP =
SS EPT ST =
```

To post Registered users by domain. This command will return the users that have registered their clients with their provisioned domains.

Note: This command may take a long time and will produce a huge output.

```
> post -r rtp7ssa.com
DN       = 6137550505
LEN      = SS 00 0 00 05
LCC      = IBN
GWC NAME = GWC-5
GW NAME  = rtp7ssa
EPT NAME = SS/000/0/0005
GW EPT ST =
CM EPT ST =
SIP URI  = user5@rtp7ssa.com
CLIENT IP =
SS EPT ST =

DN       = 6137550510
LEN      = SS 00 0 00 10
LCC      = IBN
GWC NAME = GWC-5
GW NAME  = rtp7ssa
```

```

EPT NAME   = SS/000/0/0010
GW EPT ST  =
CM EPT ST  =
SIP URI    = user10@rtp7ssa.com
CLIENT IP  =
SS EPT ST  =

```

Number of endpoints returned = 2

To display the contents of the post set using the verbose option:

```

> post -display verbose
DN          = 6137550505
LEN         = SS 00 0 00 05
LCC         = IBN
GWC NAME    = GWC-5
GW NAME     = rtp7ssa
EPT NAME    = SS/000/0/0005
GW EPT ST   = ON-HOOK
CM EPT ST   = IDL
SIP URI     = user5@rtp7ssa.com
CLIENT IP   =
SS EPT ST   =
Node Num    = 213
Term Num    = 6
GWC IP      = 47.142.92.172
GW IP       = 47.142.91.154
GW TYPE     =

```

To display the number of entries in the post set:

```

>post -count
Post set size = 104

```

1.5.1.2.3 BSY

The BSY commands informs the CM to perform the requested action. A response message indicates the success or failure of the command. These messages are generated by the CM.

To Maintenance/Manual Busy a line by DN:

```

> bsy -d 7550505
DN = 7550505
CM RETURN CODE = CM_OK

```

To Maintenance/Manual Busy a line by LEN:

```

> bsy -l ss 0 0 0 5
LEN = ss 0 0 0 5
CM RETURN CODE = CM_OK

```

To Maintenance/Manual Busy all lines on a GW:

```

> bsy -gw rtp7-1104b.us.nortel.com
DN = 6136210010
CM RETURN CODE = CM_OK
DN = 6136210011
CM RETURN CODE = CM_OK
DN = 6136210012

```

```
CM RETURN CODE = CM_OK
DN = 6136210013
CM RETURN CODE = CM_OK
```

To Busy by the posted set:

```
> bsy -set
DN = 6136210010
CM RETURN CODE = CM_OK
DN = 6136210011
CM RETURN CODE = CM_OK
DN = 6136210012
CM RETURN CODE = CM_OK
DN = 6136210013
CM RETURN CODE = CM_OK
```

The BSY INB operation performs two operations; first is a BSY then upon success, performs the INB operation. If the line is already in the BSY state then only the INB operation is performed.

If the line is IDL

```
> bsy -d 7550505 inb
DN = 7550505
CM RETURN CODE = CM_OK
DN = 7550505
CM RETURN CODE = CM_OK
```

If the line is BSY

```
> bsy -d 7550505 inb
DN = 7550505
CM RETURN CODE = CM_ALRDY_IN_REQ_STATE
DN = 7550505
CM RETURN CODE = CM_OK
```

1.5.1.2.4 RTS

To return-to-service a line by DN:

```
> rts -d 7550505
DN = 7550505
CM RETURN CODE = CM_OK
```

To return-to-service a line by LEN:

```
> rts -l ss 0 0 0 5
LEN = ss 0 0 0 5
CM RETURN CODE = CM_OK
```

To return-to-service all lines on a GW:

```
> rts -gw rtp7-1104b.us.nortel.com
DN = 6136210010
CM RETURN CODE = CM_OK
DN = 6136210011
CM RETURN CODE = CM_OK
DN = 6136210012
```

```
CM RETURN CODE = CM_OK
DN = 6136210013
CM RETURN CODE = CM_OK
```

To Busy by the posted set:

```
> rts -set
DN = 6136210010
CM RETURN CODE = CM_OK
DN = 6136210011
CM RETURN CODE = CM_OK
DN = 6136210012
CM RETURN CODE = CM_OK
DN = 6136210013
CM RETURN CODE = CM_OK
```

1.5.1.2.5 TST

The TST performs a diag (where possible) depending upon the GW's ability to perform diagnostics on endpoints. Only GCP and MGCP GWs support the TST command.

To test by DN (SIP):

```
> tst -d 7550505

DN = 6137550505
LINE_STATE = PASSED
ENDPOINT_STATE = UNKNOWN
CLIENT = user5@47.142.166.65
TEST RESULT = PASSED
```

To test by DN (MGCP line):

```
> tst -d 6210010

DN = 6136210010
LINE_STATE = ON-HOOK
ENDPOINT_STATE = OK
```

To test using the LEN (SIP)

```
> tst -l ss 0 0 0 5

DN = 6137550505
LINE_STATE = PASSED
ENDPOINT_STATE = UNKNOWN
CLIENT = user5@47.142.166.65
TEST RESULT = PASSED
```

To test using the URI

```
> tst -u user5@rtp7ssa.com

URI = user5@rtp7ssa.com
LINE_STATE = PASSED
ENDPOINT_STATE = UNKNOWN
CLIENT = user5@47.142.166.65
TEST RESULT = PASSED
```

To test by GW (or VMG).

Note: Testing by VMG may take a long time and produce a large amount of information.

MGCP based GW:

```
> tst -gw rtp7-1104b.us.nortel.com
```

```
DN = 6136210010
LINE_STATE = ON-HOOK
ENDPOINT_STATE = OK
DN = 6136210011
LINE_STATE = ON-HOOK
ENDPOINT_STATE = OK
DN = 6136210012
LINE_STATE = ON-HOOK
ENDPOINT_STATE = OK
DN = 6136210013
LINE_STATE = ON-HOOK
ENDPOINT_STATE = OK
```

SIP GW

```
> tst -gw rtp7ssa
```

```
DN = 6137550500
LINE_STATE = FAILED
ENDPOINT_STATE = UNKNOWN
ERROR = Test Executed
```

```
DN = 6137550501
LINE_STATE = FAILED
ENDPOINT_STATE = UNKNOWN
ERROR = Test Executed
```

1.5.1.3 QUERY Commands

The query commands are used to perform various existing queries. These queries are the same as those from Servord.

Command format:

```
qdn <DN>
qlen <LEN>
qsip <DN, LEN>
```

Command usage:

To Query a DN

```
QDN 7201000
```

```
-----
DN: 7201000
TYPE: SINGLE PARTY LINE
SNPA: 619 SIG: DT LNATTIDX: N/A
LINE EQUIPMENT NUMBER: SS 00 2 00 00
END POINT: rtp2sesm1 SS/000/2/0000
LINE CLASS CODE: IBN
IBN TYPE: STATION
CUSTGRP: BNR SUBGRP: 0 NCOS: 0
CARD CODE: RDTLSG GND: N PADGRP: PKNIL BNV: NL MNO: N
```

```

PM NODE NUMBER      :    142
PM TERMINAL NUMBER  :    1
OPTIONS:
CWT DGT DPL Y 10
OFFICE OPTIONS:
SRA

```

```

END POINT DATA:
SIP_CLIENT_TYPE: ont
SIP_EP_NAME: SS/000/2/0000
SIP_VMG_NAME: rtp2sesml
SIP_DN: 6197201000
SIP_LOCATION: rtp2
SIP_PACKAGE: basic
SIP_URI: user0@rtp2.com
-----

```

To query by LEN

```
> qlen SS 0 2 0 0
```

```

-----
LEN:      SS      00 2 00 00
END POINT: rtp2sesml SS/000/2/0000
TYPE: SINGLE PARTY LINE
SNPA: 619
DIRECTORY NUMBER:      7201000
LINE CLASS CODE: IBN
IBN TYPE: STATION
CUSTGRP:      BNR      SUBGRP: 0  NCOS: 0
SIGNALLING TYPE: DIGITONE
CARD CODE: RDTLSG      GND: N  PADGRP: PKNIL  BNV: NL MNO: N
PM NODE NUMBER      :    142
PM TERMINAL NUMBER  :    1
OPTIONS:
CWT DGT DPL Y 10
OFFICE OPTIONS:
SRA
END POINT DATA:
SIP_CLIENT_TYPE: ont
SIP_EP_NAME: SS/000/2/0000
SIP_VMG_NAME: rtp2sesml
SIP_DN: 6197201000
SIP_LOCATION: rtp2
SIP_PACKAGE: basic
SIP_URI: user0@rtp2.com
-----

```

To query using the QSIP command. The parm can be either a DN or LEN.

```
> qsip 7550505
SS      00 0 00 05
SS/00/0/0005
-----
```

```

SIP USER DATA
=====
SIP URI: user5@rtp7ssa.com
ACCOUNT STATUS: ACTIVE
REGISTERED: Y
ALLOW POST BSY TERMINATIONS: Y
NUMBER OF CONTACTS: 1
CONTACTS: user5@47.142.166.65
SERVICE PACKAGE:
basic_package
SERVICES:
ALCLNT N IM SIPLN ADVSCR 3 3 N CLNTCO N N N N ADHOC 4 ADDR BK 50 PRES 10 Y

```

```
20 Y VIDEO N N NWLOG 50 50
```

```
SIP LINE DATA
```

```
=====
```

```
ENDPT ID: SS/000/0/0005
```

```
VMG: rtp7ssa
```

```
ZONE ID(s):
```

```
CLIENT TYPE: ONT
```

```
STATIC CLIENT: Y
```

```
SIP CALL DATA
```

```
=====
```

```
ACTIVE CALL APPEARANCES:
```

```
    NODENO    TERMNO
```

```
NUMBER OF ACTIVE SESSIONS IN CS2000 SESSION SERVER: 0
```

```
-----
```

```
>
```

1.5.1.4 MISC Commands

To quit from the LMM level - the user will remain in the MTC mode.

QUIT

1.5.1.5 Command Parsing

Multiple commands can be input on the same line - they must be separated by a “;”. Up to 4 lens, dns or uris can be specified with the POST, BSY, TST and RTS commands. Due to the potential volume of output, only one GW or VMG can be specified.

The commands are not case sensitive, but the parameters may be, i.e. GW name will be case sensitive.

1.5.2 SERVORD+ via OSSGate

This feature extend existing capabilities of the Succession SERVORD+ system for SIP client provisioning. SIP client commands/data will distributed to the SS-EM from the SERVORD+ system within the SESM. The following commands will trigger data distribution to the SS-EM from SESM SERVORD+ when SS vmgs/endpoints (or associated LENSs) are found within the command:

- NEW
- OUT
- CHF
- ADD
- EST
- DEL
- ADO (for MDN options)

- DEO (for MDN options)
- CDN
- CHF
- CLN/CTP
- QCUST
- QLEN/QTP (show endpoint for HASU SIP LENSs)
- QDNWRK (show SIP_DATA queried from SS-EM)
- QLENWRK (show SIP_DATA queried from SS-EM)
- QSIP

For SIP Line clients, the NEW, OUT and CHF commands are currently supported. New development is required to support the remaining commands in this release.

Note: CHF requires the use of gateway/termination names (or the equivalent LEN) in order to trigger data flow through for SS lines. Use of DN instead of primary LEN or gateway/termination will result in the command being processed only by the CM.

Note: CDN commands which modify the DN assigned to the user will *not* automatically update the SIP_URI. The use of Directory Number in the SIP_URI value (e.g. 2145209999@nortel.com) is not recommended.

Note: EST/ADD/DEL commands support only single SIP LENSs/Endpoints in the command due to the limitation of a single SIP_DATA option being processed in the options area. Use of multiple SIP LENSs/Endpoints in these commands will result in command failure.

Query commands such as QCUST, QLENWRK and QDNWRK (which return formatted line/service information) will include the SIP_DATA options provisioned via the NEW/EST/ADD/CHF commands in their output. The SIP_DATA option information will be appended to the end of the existing QLENWRK/QDNWRK output, but prior to the dashed line (e.g. "-----")query output terminator for each line in the output.

Existing data tags presented in query output with sample values:

END POINT DATA: *(This is the endpoint data header, no info/value associated with this tag)*

SIP_CLIENT_TYPE: sip line

SIP_EP_NAME: SCOT/000/0/0000

SIP_VMG_NAME: vmg1

SIP_DN: 6195209998

SIP_LOCATION: nortel networks.rtp.nc0

SIP_PACKAGE: sip lines

SIP_URI: slynch@mordor.com

New data tags presented in query output with sample values:

SIP_GROUP_DN: 6195209999

SIP_GROUP_TYPE: MLH

SIP_SUBDOMAIN: doom.mordor.com

See query examples in the next section for details on presentation and positioning within query output.

1.5.2.1 SERVORD+ Command Examples

See Configuration Section for SIP_DATA option format details and provisioning rules.

1.5.2.1.1 NEW command Examples:

```
NEW $ 6195209998 1FR LATA1 0 SCOT 00 0 00 00 dgt SIP_DATA
SIP_PACKAGE SIP Lines SIP_URI slynch@mordor.com
SIP_SUBDOMAIN doom.mordor.com SIP_CLIENT_TYPE SIP Line
SIP_LOCATION Nortel Networks.RTP.NC0 SIP_PASSWD scott11 $ DPL Y
10 $
```

```
NEW $ 6195209998 1FR LATA1 0 vmg1 SCOT/000/0/0000 dgt SIP_DATA
SIP_PACKAGE SIP Lines SIP_URI slynch@mordor.com
SIP_SUBDOMAIN doom.mordor.com SIP_CLIENT_TYPE SIP Line
SIP_LOCATION Nortel Networks.RTP.NC0 SIP_PASSWD scott11 $ DPL Y
10 $
```

1.5.2.1.2 CHF Command Examples

The change feature command is currently supported for SIP lines and SIP_DATA except SIP_URI. SIP_URI may be included in the CHF command, but it must match the existing value assigned to the user. Change of the SIP_SUBDOMAIN for the user will be supported.

```
CHF $ SCOT 00 0 00 00 SIP_DATA SIP_PACKAGE siplines SIP_PASSWD
scott11 SIP_CLIENT_TYPE IBN SIP_LOCATION IBM.RTP $ $
```

```
CHF $ vmg1 SCOT/000/0/0000 SIP_DATA SIP_PACKAGE siplines
SIP_PASSWD scott11 SIP_CLIENT_TYPE IBN SIP_LOCATION IBM.RTP
$ $
```

Moving a line/user between domains/subdomains can be accomplished using the CHF command. For example, if user slynch@mordor.com is currently provisioned in the root domain (mordor.com) and needs to be moved to subdomain doom.mordor.com, the following CHF command may be used:

```
CHF $ SCOT 00 0 00 00 SIP_DATA SIP_SUBDOMAIN doom.mordor.com
$ $
```

By simply specifying a SIP_SUBDOMAIN sub-option, the user associated with LEN SCOT 00 0 00 00 will be moved from their currently assigned domain to the value specified by the SIP_SUBDOMAIN sub-option. A user may be moved between root domain and subdomains, between subdomains, or between root domains using this mechanism. However, it is important to note that user moves between domains can have serious consequences on user based data in the Session Server Element Manager. If packages, locations, or group information does not match in the target domain, then the users existing data will be *lost* following the move, replaced by default data in the target domain. **NO WARNING IS GIVEN WHEN THIS OCCURS. Therefore, CHF based user moves should be used with caution as important domain specific data may be lost during the move. QLEN/QDN executed before and after the move should reveal any data mismatch/loss.**

1.5.2.1.3 OUT Command Examples

```
OUT $ 6195209998 SCOT 00 0 00 00 BLDN
```

```
OUT $ 6195209998 vmg1 SCOT/000/0/0000 BLDN
```

1.5.2.1.4 QDN and QLEN Query Examples

The following examples of query output show the newly added SIP_DATA sub-options SIP_SUBDOMAIN, SIP_GROUP_TYPE, and SIP_GROUP_DN.

```
> QLEN SCOT 00 0 00 00
```

```
-----
LEN:      SCOT 00 0 00 00
END POINT: vmg1 SCOT/000/0/0000
TYPE: SINGLE PARTY LINE
SNPA: 619
DIRECTORY NUMBER:      5209998
LINE CLASS CODE:       1FR
SIGNALLING TYPE: DIGITONE
LINE TREATMENT GROUP:  0
LINE ATTRIBUTE INDEX:  0
CARDCODE:  RDTLSG      GND: N  PADGRP: PKNIL  BNV: NL MNO: Y
PM NODE NUMBER      :      87
PM TERMINAL NUMBER  :      1
```

```
OPTIONS:
DGT DPL Y 10
OFFICE OPTIONS:
SRA

END POINT DATA:
SIP_CLIENT_TYPE: sip line
SIP_EP_NAME: SCOT/000/0/0000
SIP_VMG_NAME: vmg1
SIP_DN: 6195209998
SIP_LOCATION: nortel networks.rtp.nc0
SIP_PACKAGE: sip lines
SIP_URI: slynch@mordor.com
SIP_SUBDOMAIN: doom.mordor.com
-----

> qdn 5209998
-----

DN:      5209998
TYPE: SINGLE PARTY LINE
SNPA: 619   SIG: DT   LNATTIDX: 0
LINE EQUIPMENT NUMBER:      SCOT  00 0 00 00
END POINT: vmg1  SCOT/000/0/0000
LINE CLASS CODE:      1FR
LINE TREATMENT GROUP:      0
CARDCODE:  RDTLSG   GND: N  PADGRP: PKNIL  BNV: NL MNO: Y
PM NODE NUMBER      :      87
PM TERMINAL NUMBER :      1
OPTIONS:
DGT DPL Y 10
OFFICE OPTIONS:
SRA

END POINT DATA:
SIP_CLIENT_TYPE: sip line
SIP_EP_NAME: SCOT/000/0/0000
SIP_VMG_NAME: vmg1
SIP_DN: 6195209998
SIP_LOCATION: nortel networks.rtp.nc0
SIP_PACKAGE: sip lines
SIP_URI: slynch@mordor.com
SIP_SUBDOMAIN: doom.mordor.com
-----

>qlen TEST  01 1 09 22
-----
```

```
LEN:      TEST 01 1 09 22
END POINT: vmg1 TEST/001/1/0922
TYPE: MEMBER OF MLH HUNT GROUP
SNPA: 214
HUNT GROUP: 13      HUNT MEMBER: 1
DIRECTORY NUMBER: 5209999      (NON-UNIQUE)
LINE CLASS CODE: 1FR
IBN TYPE: STATION
CUSTGRP:      RES214      SUBGRP: 0  NCOS: 1
SIGNALLING TYPE: DIGITONE
LINE TREATMENT GROUP: 0
LINE ATTRIBUTE INDEX: 520_1FR
XLAPLAN KEY : 214_P520_1      RATEAREA KEY :      RA214_2
CARDCODE: RDTLSG      GND: N  PADGRP: PKLNL  BNV: NL MNO: N
PM NODE NUMBER      : 213
PM TERMINAL NUMBER : 923
OPTIONS:
DGT
RES OPTIONS: NONE
PILOT LEN: TEST 01 1 09 23
GROUP OPTIONS:
RCVD
END POINT DATA:
SIP_CLIENT_TYPE: sip line
SIP_EP_NAME: TEST/001/1/0922
SIP_VMG_NAME: vmg1
SIP_DN:
SIP_LOCATION: nortel networks.rtp.nc0
SIP_PACKAGE: sip lines
SIP_URI: slynch@mordor.com
SIP_SUBDOMAIN: doom.mordor.com
SIP_GROUP_TYPE: MLH
SIP_GROUP_DN: 2145209999
-----
>qlen TEST 01 1 09 23
-----
LEN:      TEST 01 1 09 23
END POINT: vmg1 TEST/001/1/0923
TYPE: MULTIPLE APPEARANCE DIRECTORY NUMBER
SNPA: 214
DIRECTORY NUMBER: 5209999      (NON-UNIQUE)
LINE CLASS CODE: 1FR
IBN TYPE: MADN
MADN INFO - TYPE:SCA  PRIMARY:N  RING:NEVER
```



```

MADN GROUP INFO - DENIAL_TRMT:  TONE  BRIDGING:N
CUSTGRP:          RES214  SUBGRP:0  NCOS: 1
SIGNALLING TYPE:  DIGITONE
LINE TREATMENT GROUP:  0
LINE ATTRIBUTE INDEX:  520_1FR
XLAPLAN KEY :    214_P520_1          RATEAREA KEY :    RA214_2
CARDCODE:  RDTLSG  GND: N  PADGRP: PKLNL  BNV: NL MNO: N
PM NODE NUMBER      :    213
PM TERMINAL NUMBER  :    924
OPTIONS:
DGT
RES OPTIONS: NONE
END POINT DATA:
SIP_CLIENT_TYPE: sip line
SIP_EP_NAME: TEST/001/1/0923
SIP_VMG_NAME: vmg1
SIP_DN:
SIP_LOCATION: nortel networks.rtp.nc0
SIP_PACKAGE: sip lines
SIP_URI: slynch@mordor.com
SIP_SUBDOMAIN: doom.mordor.com
SIP_GROUP_TYPE: MDN
SIP_GROUP_DN: 2145209999

```

1.5.2.1.5 QLEN For HASU LEN

The QLEN command output currently shows endpoint and SIP_DATA information for LENs with assigned service, however no endpoint data is shown for HASU LENs. The output is updated in this release to add the associated endpoint information (if any) to the end of the query output for HASU LENs.

```

>qlen TEST 00 1 01 00
-----
TYPE: HARDWARE ASSIGNED SOFTWARE UNASSIGNED
CARDCODE:  RDTLSG  GND: N  PADGRP: PKLNL  BNV: NL MNO: N
PM NODE NUMBER      :    136
PM TERMINAL NUMBER  :    101
END POINT: ssvmg.42 TEST/000/1/0100
-----

```

1.5.2.1.6 QCUST

Example command and output for a SIP line:

```

>qcust bnr $
1 SS12 00 6 00 07 IBN PKLNL RDTLSG N

```

```

2 7207167 BNR 0 0 613
9 CWT DGT DPL Y 10 $
23 SIP_URI me@mydomain.com SIP_LOCATION my house
99

```

New record type “23” is introduced which contains SIP_DATA information.

1.5.2.1.7 QDNWRK/QLENWRK

QDNWRK and QLENWRK are bulk queries which display all or ranges of working DN's or LEN's. The Detailed output of these commands resembles lists of individual QDN and QLEN query output. A Summary output simply displays a count.

Examples:

```

QDNWRK R 7215554 7215554 NLCC $ D
COMMAND AS ENTERED
QDNWRK R          7215554          7215554 ALL NLCC $ ALL D
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>REPORT ON WORKING DIRECTORY NUMBERS
FROM          6197215554 TO          6197215554
      LCC ALL                      OPTION ALL
-----
DN:          7215554
TYPE: SINGLE PARTY LINE
SNPA: 619   SIG: DT   LNATTIDX: N/A
LINE EQUIPMENT NUMBER:      C411  01 0 02 01
END POINT: vmg1 C411/001/0/0201
LINE CLASS CODE:  IBN
IBN TYPE: STATION
CUSTGRP:          BNR      SUBGRP: 0  NCOS: 0
CARDCODE:  RDTLSG   GND: N  PADGRP: PKLNL  BNV: NL MNO: N
PM NODE NUMBER      :      147
PM TERMINAL NUMBER  :      50
OPTIONS:
DGT
END POINT DATA:
SIP_CLIENT_TYPE: sip line
SIP_EP_NAME: C411/001/0/0201
SIP_VMG_NAME: vmg1
SIP_DN: 6197215554
SIP_LOCATION: nortel networks.rtp.nc0
SIP_PACKAGE: sip lines
SIP_URI: slynch@mordor.com
SIP_SUBDOMAIN: doom.mordor.com
-----

```

```

-----
TOTAL COUNT OF WORKING DN FROM      6197215554 TO      6197215554:      1
>

COMMAND AS ENTERED

QLENWRK R C411  01 0  C411  01 0  ALL  ALL NLCC $ D

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT

>y

WARNING : Queries of all LENS or a large range of LENS
          may run for 30 minutes or more before producing any output

Please confirm ("YES", "Y", "NO", or "N"):

>y

REPORT ON WORKING LINE EQUIPMENT NUMBERS

FROM C411  01 0  TO C411  01 0      DRAWERS ALL

      LCC ALL                      OPTION ALL

-----

LEN:      C411  01 0 02 01

TYPE: SINGLE PARTY LINE

DN 6197215554  LCC  IBN      SIG DT  LNATTIDX N/A

IBN TYPE: STATION

CUSTGRP:      BNR      SUBGRP: 0  NCOS: 0

CARDCODE:  RDTLSG      GND: N  PADGRP: PKLNL  BNV: NL MNO: N

PM NODE NUMBER      :      147

PM TERMINAL NUMBER :      50

OPTIONS:

DGT

END POINT DATA:

SIP_CLIENT_TYPE: sip line

SIP_EP_NAME: C411/001/0/0201

SIP_VMG_NAME: vmg1

SIP_DN: 6197215554

SIP_LOCATION: nortel networks.rtp.nc0

SIP_PACKAGE: sip lines

SIP_URI: slynch@mordor.com

SIP_SUBDOMAIN: doom.mordor.com

-----

TOTAL:      1

```

1.5.2.1.8 ADO and DEO for MADN

For most forms of ADO/DEO, a SIP line would be unaffected, however adding a MDN option to an existing line may change that line's directory number (set to empty on the Session Server). Adding the MDN option may also trigger group creation on the Session Server if the line is the first Session Server line in the MDN group.

Examples:

```
NEW $ 7215555 IBN BNR 0 0 619 NILLATA 0 C411 01 0 02 00 SIP_DATA SIP_PACKAGE SIP Lines
SIP_URI user2@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0
SIP_PASSWD user21 $ DPL Y 10 dgt $
```

```
ADO $ c411 1 0 2 0 MDN SCA Y Y 6197215555 TONE N $
```

C411 01 0 02 00 is now the Primary member of the MADN group 6197215555. A MDN group named “6197215555” is created on the Session Server element manager and user “user2@mordor.com” is added to the group. The DN of user “user2@mordor.com” is cleared (blanked) in the Session Server element manager.

A second line is added with a different DN, 6197215554:

```
NEW $ 7215554 IBN BNR 0 0 619 NILLATA 0 C411 01 0 02 1 SIP_DATA SIP_PACKAGE SIP Lines
SIP_URI user3@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0
SIP_PASSWD user21 $ DPL Y 10 dgt $
```

Now the MDN option is added to this second line specifying a different DN (6197215555) and a treatment (BLDN) for the original DN (6197215554):

```
ADO $ C411 01 0 02 01 MDN SCA N Y 6197215555 BLDN $
```

The end result of this is that the DN for C411 01 0 02 01 changed from 6197215554 to 6197215555 on the core and the line is now a member of MADN group 6197215555 on the Session Server element manager. Now, delete the MDN option from this newly added member and specify it's new DN.

```
DEO $ C411 01 0 02 01 MDN 6197215554 $
```

Following the DEO of the MDN option, the DN for C411 01 0 02 01 is changed from 6197215555 to 6197215554 on the core and the line is no longer a member of MADN group 6197215555 in the Session Server element manager. User “user3@mordor.com” will have a DN assignment of 6197215554 on the Session Server element manager.

1.5.2.1.9 NEW, OUT and CDN for MADN

MADN groups may be created and populated using the NEW command.

Examples:

```
NEW $ 7215554 IBN BNR 0 0 619 NILLATA 0 C411 01 0 02 01 DGT MDN SCA Y Y TONE N SIP_DATA
SIP_PACKAGE SIP Lines SIP_URI user1@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION
Nortel Networks.RTP.NC0 SIP_PASSWD user11 SIP_SUBDOMAIN doom.mordor.com $ $
```

```
NEW $ 7215554 IBN BNR 0 0 619 NILLATA 0 C411 01 0 02 02 DGT MDN SCA N Y SIP_DATA SIP_PACKAGE
SIP Lines SIP_URI user2@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel
Networks.RTP.NC0 SIP_PASSWD user11 SIP_SUBDOMAIN doom.mordor.com $ $
```

```
CDN $ 6197215554 6197215555 BLDN
```

```
OUT $ 7215555 C411 01 0 02 02 BLDN
```

```
OUT $ 7215555 C411 01 0 02 01 BLDN
```

A group with type “MDN” and name “6197215554” is created during processing of the first NEW command and user “user1@mordor.com” is

added to that group. The second NEW command adds user “user2@mordor.com” to the same group. The CDN command results in the DN for the MDN group being changed in the core for all members and also the group name changing from “6197215554” to “6197215555” in the Session Server element manager.

On the SS-EM, the OUT command will removed the line/user from the MDN group, and if the user is the last member of the group, the group will also be removed.

1.5.2.1.10 EST, ADD, DEL,CHDN

Huntgroup flowthrough architecture only triggers flowthrough for hunt flavors which can assign service to a HASU line: MLH, DLH, and DNH. MPH can also be used to assign service to a HASU line, however MPH is not supported for SIP line. Other flavors such as CPU, CMG, SIMRING, and BNN are assigned to lines with existing service and therefore trigger no flowthrough and hence no group creation/deletion on the Session Server element manager.

Examples:

DLH:

```
EST $ DLH 6195209998 1FR LATA1 0 SCOT 00 0 00 00 $ dgt SIP_DATA SIP_PACKAGE SIP Lines
SIP_URI user1@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0
SIP_PASSWD user11 SIP_SUBDOMAIN doom.mordor.com $ DPL Y 10 $

ADD $ DLH SCOT 00 0 00 00 SCOT 00 0 00 01 $ dgt SIP_DATA SIP_PACKAGE SIP Lines SIP_URI
user2@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0 SIP_PASSWD
user21 SIP_SUBDOMAIN doom.mordor.com $ DPL Y 10 $

DEL $ DLH SCOT 00 0 00 01 $

OUT $ 6195209998 SCOT 00 0 00 00 BLDN
```

With these commands, a group is created on the Session Server named “6195209998” (GROUP_DN in query output for these lines) with a type of “DLH” (GROUP_TYPE in query output for these lines). The Session Server group is created when the EST command is processed and user “user1@mordor.com” is added to the group. The ADD command triggers no group creation, but user “user2@mordor.com” is added to group “6195209998” on the Session Server Element Manager. The DEL command removes user “user2@mordor.com” from the group and from the Session Server element manager in general. Finally, the OUT command removes group “6195209998” from the Session Server element manager and also removes user “user1@mordor.com”.

MLH:

```
EST $ MLH 6195209998 1FR LATA1 0 SCOT 00 0 00 00 $ dgt SIP_DATA SIP_PACKAGE SIP Lines
SIP_URI user1@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0
SIP_PASSWD user11 SIP_SUBDOMAIN doom.mordor.com $ DPL Y 10 $
```

```
ADD $ MLH SCOT 00 0 00 00 SCOT 00 0 00 01 $ dgt SIP_DATA SIP_PACKAGE SIP Lines SIP_URI
user2@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0 SIP_PASSWD
user21 SIP_SUBDOMAIN doom.mordor.com $ DPL Y 10 $

CHDN $ SCOT 00 0 00 01 2145200999

DEL $ MLH SCOT 00 0 00 01 $
```

The CHDN command shown above results in the DN change of member SCOT 00 0 00 00 to 2145200999 in the core but no change to the currently blank DN assigned to user “user2@mordor.com” in the Session Server element manager. The user’s DN will remain blank in the Session Server as long as it is a member of a group regardless of DN changes which occur in the Core.

DNH:

```
EST $ DNH 2145200998 1FR LATA1 0 SCOT 00 0 00 00 $ DGT SIP_DATA SIP_PACKAGE SIP Lines
SIP_URI user1@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0
SIP_PASSWD user11 SIP_SUBDOMAIN doom.mordor.com $ DPL Y 10 $ 5

ADD $ DNH 2145200998 2145200997 SCOT 00 0 00 01 $ DGT SIP_DATA SIP_PACKAGE SIP Lines
SIP_URI user2@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0
SIP_PASSWD user21 SIP_SUBDOMAIN doom.mordor.com $ DPL Y 10 $ 5

DEL $ DNH 2145200997 SCOT 00 0 00 01 $ bldn
```

Note that the SERVORD+ format requires insertion of GW/EP or LEN in the DEL command for DNH groups. This is normally not required in Core SERVORD.

Only ONE SIP LEN/gw-ep is supported in any EST or ADD command since only one SIP_DATA option is allowed in the options area of the command. Use of more than one SIP LEN/gw-ep in the EST/ADD command will result in command failure.

1.5.2.1.11 CDN

SESM logic will support flow through of change DN requests for SIP Lines, however the CDN command will be blocked for MLH/DLH hunt pilots/members but will be supported for MADN and DNH group pilot/link/members (this is a legacy implementation restriction on CDN commands).

Example:

```
NEW $ 7215555 IBN BNR 0 0 619 NILLATA 0 C411 01 0 02 00 SIP_DATA SIP_PACKAGE SIP Lines
SIP_URI user2@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0
SIP_PASSWD user21 $ DPL Y 10 dgt $

CDN $ 6197215555 6197215554 BLDN
```

CDN commands which modify the DN assigned to the user will *not* automatically update a SIP_URI containing directory number information. The use of Directory Number in the SIP_URI value (e.g. 2145209999@nortel.com) is not recommended.

1.5.2.1.12 CLN

A limited OSSGate/SERVORD+ infrastructure is provided to process flowthrough for CLN commands for SIP lines, however the processing is limited to changes between SIP lines only. For CLN of SIP lines, the from_value and to_value in the CLN command must both contain SIP LENS/endpoints, otherwise the command will fail.

Examples:

```
CLN $ C411 01 0 0 02 00 C411 01 0 0 02 01  
CLN $ C411 00 0 0 00 00 C411 01 0 0 02 01
```

1.5.3 Line Audit:

In this feature, the line audit will also audit the data in Session Server EM. The audit GUI look and feel does not change, except that few checks are added to warn the user of system load. Also the audit output file (both valid and problem files) will have extra information pertaining to the Session Server audit.

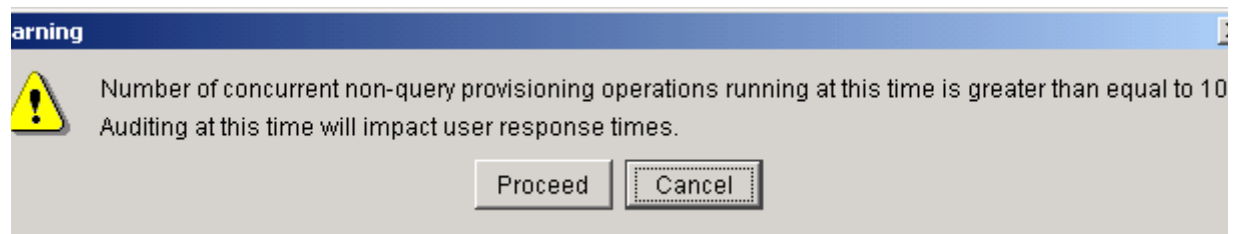
1.5.3.1 Warning Dialogues in Audit GUI

One of the requirements in this feature is to avoid running (atleast warn) line audit when the system is loaded, as the audit might impact more important provisioning activities. In this feature, the manual line audit will check for the system load and warn the user if its not an appropriate time to run audit.

When the user choose line audit from GUI and clicks RunAudit button, the GUI first checks with Audit server if its ready to run the audit. The server does three checks to determine if its ready or not. If any of the three checks is true, then the server will return 'not ready' with details to the GUI, which in turn will pop a dialogue box to warn user of system load and gives him a chance to decide if he wants to run the audit at a later time, since running audit has the potential to slow down the system impacting higher priority provisioning activities.

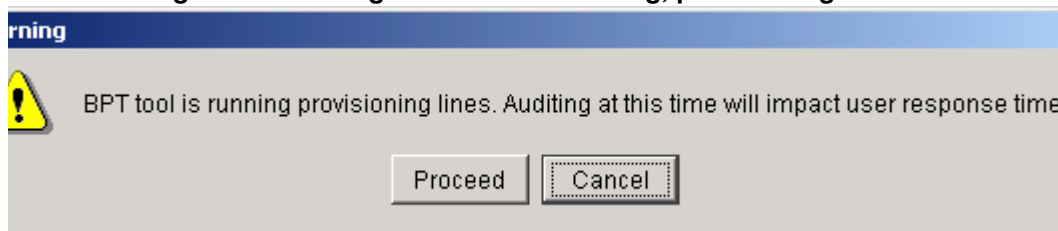
First check done by the server is to see if there are 10 or more concurrent non-read-only operations in progress. If yes, the audit server returns 'not ready' with details to the GUI. Shown below is example dialogue box.

Figure 2 Warning if 10 or more non-query type line provisioning in progress



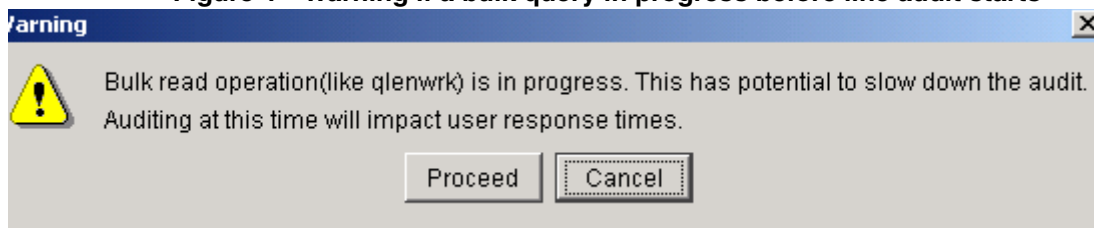
The second check is to see whether BPT tool is running a lines batch operation. If yes, the server returns 'not ready' with details to GUI. Shown below is example dialogue box in this condition.

Figure 3 Warning if BPT tool is running, provisioning lines



The third check is to see whether any bulk query operation (like qlenwrk, qdnwrk etc) is already in progress. If yes, the server will return 'not ready' to the GUI. Shown below is example dialogue box in this scenario.

Figure 4 Warning if a bulk query in progress before line audit starts



1.5.3.2 Warning in BPT on Audit Running

In addition to the line Audit GUI warnings(2.6.2.1), a check is introduced in BPT tool where it determines if Line Audit is currently running. If yes, BPT tool will warn the user that line audit is in progress and gives the user a chance to run the lines batch later, as the throughput of the Lines batch could be slower due to line audit running.

Screen shot from BPT tool when lines batch is started while line audit is in progress.

***** WARNING *****

Line Audit is currently in progress.

This lines batch may run slower and may also invalidate audit results

Do you still want to proceed with lines batch? <y/n>:

The above warning tells the user that line audit is in progress and perhaps the lines batch should be run after the audit is finished

1.5.3.3 Line Data Audit Valid Data output:

After the line data audit finishes, the ValidLineData.log file will have additional information obtained by auditing the Session Server EM.

The endpoints in GWCEM will be compared with SS EM, the group DN and its member DN information will be compared with the core and the DN to len mapping will also be compared with the core.

In the first screen shot is shown, valid data w.r.t the Session server will be at bottom. In the following screen shot, the group DN and its type and the member DNs are printed on screen, which is new audit data added by this feature if SIP MGs are provisioned.

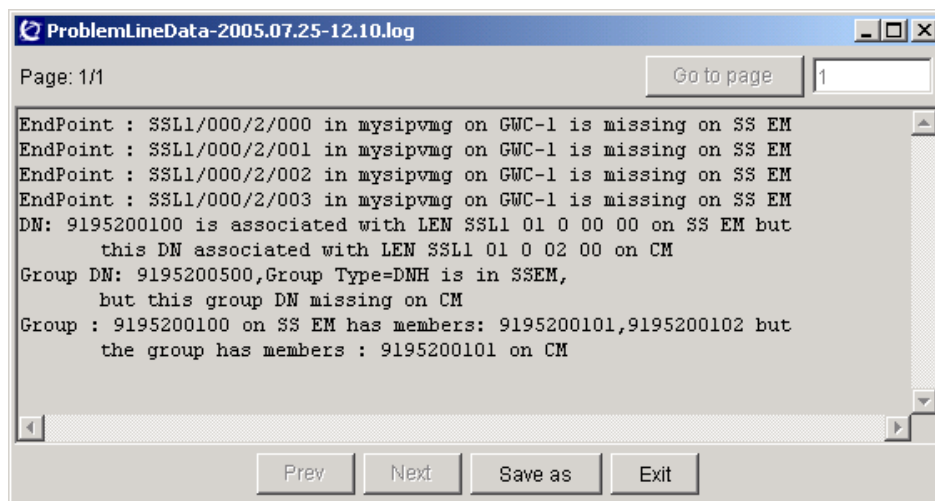
EP NAME	LEN	DN	TN
tp/0/0001	CICM 02 0 00 01	HASU - No DN on CM	2
tp/0/0002	CICM 02 0 00 02	HAS DN	3
tp/0/0003	CICM 02 0 00 03	HAS DN	4
tp/0/0004	CICM 02 0 00 04	HAS DN	5
tp/0/0005	CICM 02 0 00 05	HAS DN	6
tp/0/0006	CICM 02 0 00 06	HAS DN	7
Group DN Group Type Member DNs or LENS (comma seperated)			
9195200100	MDN	CICM 02 0 00 03	<<-NEW Data added in this feature
9195200200	DNH	9195200201,9195200202	

1.5.3.4 Line Data Audit Problem Data output:

Shown below is screen shot of problem line data results. The problems could be in following areas

1. Endpoint exists in GWCEM, but not in Session server EM
2. DN associated with endpointId (len) in SS EM, while that same DN maps to different LEN on core
3. group DN in SS EM but that group information is missing in core

4. member DN/LENs in SS EM belonging to a group do not match the member list in that group on core.



1.6 Glossary

Term	Description
New term	Definition

2: Configuration Management for A00012223, 12217, 12225

2.1 Hardware and Software Requirements

This feature requires the 905-240 GWC card, pec code NTRX51DL. It also requires that the CM, GWC SESM and MCS gateways are on a SN09 drop 2 load for all documented functionality to be available (otherwise the SN09 functionality is the default).

2.2 Initial Configuration

2.2.1 SESM-CS2K Prov Mgr EM Server Configuration

SESM-CS2KSS configuration

OPI - Provisioning Manager Interface configuration

Enter OPI transport protocol to EM server (http/https - default: https)

- [1] - http
- [2] - https
- [x] - exit

```
select - 2
```

```
Enter the IP address / Name of the primary CS2KSS prov server (default:
47.142.91.164) : 47.142.91.164
```

```
Enter the primary CS2KSS prov server https port (default is 8443): 8443
```

```
Enter the IP address / Name of the secondary CS2KSS prov server (default:
47.142.91.164) : 47.142.91.164
```

```
Enter the secondary CS2KSS EM server https port (default is 8443): 8443
```

```
Enter the OPI administrator user name (default: admin): admin
```

```
Enter the OPI administrator password:
```

```
Re-enter the OPI administrator password:
```

OMI - Provisioning Manager Interface configuration

```
Enter OMI transport protocol to EM server ( http/https - default: https)
```

```
[1] - http
```

```
[2] - https
```

```
[x] - exit
```

```
select - 2
```

```
Enter the IP address / Name of the primary CS2KSS mtc server (default:
47.142.91.164) : 47.142.91.164
```

```
Enter the primary CS2KSS mtc server https port (default is 12121): 12121
```

```
Enter the IP address / Name of the secondary CS2KSS mtc server (default:
47.142.91.164) : 47.142.91.164
```

```
Enter the secondary CS2KSS mtc server https port (default is 12121): 12121
```

```
Enter the OMI administrator user name (default: admin): admin
```

```
Enter the OMI administrator password:
```

```
Re-enter the OMI administrator password:
```

OPI - Provisioning Manager configuration

```
Transport protocol to EM server      : https://
Primary CS2KSS Provisioning Manager IP / Name : 47.142.91.164
Primary CS2KSS Provisioning Manager port   : 8443
Secondary CS2KSS Provisioning Manager IP / Name : 47.142.91.164
Secondary CS2KSS Provisioning Manager port   : 8443
The administrator user name           : admin
```

OMI - Maintenance Manager configuration

```
Transport protocol to Maintenance Manager : https://
Primary CS2KSS Maintenance Manager IP / Name : 47.142.91.164
Primary CS2KSS Maintenance Manager port   : 12121
Secondary CS2KSS Maintenance Manager IP / Name : 47.142.91.164
Secondary CS2KSS Maintenance Manager port   : 12121
The administrator user name               : admin
```

```
Is the information correct? (y or n) :y
```

The configuration tool will prompt the user to enter the following for the OMI link information:

- Transport protocol to SS-EM server (https).
- IP address / host name of primary SS-EM server
- IP address / host name of secondary SS-EM server. Some configurations may not include a secondary SS EM server. If so, configure the same information provided for the primary server (by default this should be the case).
- HTTPS communication port to SS EM server (12121).
- SS-EM Provisioning Manager administrator user name
- SS-EM Provisioning Manager administrator password

The OPI version information is not required anymore since it is dynamically determined when the OPI and OMI links come into service.

The IP address and port will be used to generate the SS-EM Provisioning Manager URL which in turn will be added to sesm.properties file.

As part of the configuration, the IP address will be validated for format, range and reachability. Other user entered data will be validated for format, range, values etc.

The user name will be added to sesm.properties as clear text.

The password will be stored separately and accessible only to the root user.

All configuration information (url, username, etc.) except password can be displayed by using the SESM “/opt/nortel/NTsesm/admin/bin/configure” tool.

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

Not Applicable.

2.4 Upgrade Considerations

Initial support for Session Server SIP lines gateways was delivered in SN09. This feature will extend that support in various areas (provisioning, audits, and maintenance) and will therefore be required to implement a backwards compatibility mechanism in order to allow interactions with older Session Server element manager loads which do not support the new functionality.

2.4.1 Dump and Restore (CM)

Not Applicable.

2.4.2 Element Management Upgrade

Upgrading the SESM from SN09 to SN09 drop 2 loads while the Session Server remains on SN09 level software can be done without the need for manual interactions. The backwards compatibility logic within SESM should be able to query any existing Session Server element managers for its load version and implement the backwards compatible interface accordingly.

Some new configuration will be required for the SESM application following either the upgrade of the Session Server or the upgrade of the SESM in order to allow SESM connections to the maintenance system on the Session Server element manager. These new connections are necessary to enable SN09 drop 2 maintenance, audit and provisioning capabilities following system upgrade.

2.4.3 Downgrade impact

No impact - works as per current process.

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

N/A

2.6 Service Orders (SO) (CM & SESM)

No new service orders are created under this activity, however a new suboption for the SIP_DATA option is defined which can be used in NEW/CHF/EST/ADD commands applicable to SIP lines hosted off of Session ServerVMGs.

All listed may also be used via the Bulk Provisioning Tool.

2.6.1 Service order change details

LCC and options

A new SIP_DATA suboption is introduced by this feature. The SIP_DATA suboption SIP_SUBDOMAIN, like the existing suboptions, is not presented to XACore SERVORD (it is removed from the command prior to XACore SERVORD command processing).

2.6.1.1 Option Format:

SIP_DATA sub-options-and-values \$

where

sub-options = SIP_CLIENT_TYPE, SIP_URI, SIP_PASSWD,
SIP_PACKAGE, SIP_LOCATION, *SIP_SUBDOMAIN*

The SIP_DATA option and sub-option tags and values may be entered in either lower or upper case transparently.

Note: sub-option values have external case restrictions. See “2.6.1.4 Usage/Format Validation and Rules” on page 1137.

2.6.1.2 Sub-option value formats:

SIP_SUBDOMAIN option value format = {token_string_value}

2.6.1.3 SIP_DATA Sub-option and Value Examples:

“SIP_DATA SIP_PACKAGE test package SIP_URI someone@nortel.com

SIP_SUBDOMAIN rtp.nortel.com SIP_CLIENT_TYPE SIP Line

SIP_LOCATION Nortel Networks.RTP.NC0 SIP_PASSWD test1password \$”

2.6.1.4 Usage/Format Validation and Rules

OSSGate/SERVORD+ SIP_DATA SIP_SUBDOMAIN validation will be limited. The Session Server element manager will be responsible for validating the actual value contents.

When the SIP_SUBDOMAIN suboption is specified in provisioning commands (e.g. NEW, EST, etc.), subsequent queries (e.g. QLEN/QDN/etc.) will include a SIP_SUBDOMAIN data in output.

Queries showing SIP_URI information will always include the domain (not sub-domain) information formatted as <user>@<domain>. If a subdomain value is used in the SIP_URI suboption (<user>@<subdomain>) in provisioning commands, subsequent queries will show the SIP_URI with the domain, <user>@<domain>.

Prior to delivery of this feature content, if the customer has more than 35000 lines (> 1 Session Server for lines) the SIP_URI suboption in the command must include the subdomain. Subsequent queries will not display information about subdomains.

The use of Directory Number in the SIP_URI value (e.g. 2145209999@nortel.com) is discouraged. CDN commands which modify the DN assigned to the user will *not* automatically update the SIP_URI.

2.6.1.4.1 Rules Enforced for SIP_DATA by OSSGate/SERVORD+

Breaking these rules causes immediate command failure/rejection by OSSGate/SERVORD+:

- One or more sub-options are REQUIRED when the SIP_DATA option is specified.
- Sub-option tags are reserved words and may not be used as values for other sub-options or for any non-related types (e.g. CM customer group, gateway names, etc.). For example, “SIP_PASSWORD sip_password” is an invalid option and value pair. “sip_password” may not be used as the value specified for the SIP_PASSWORD sub-option. “sip_password” may not

be used as a part or whole value for any other sub-option (e.g. “SIP_LOCATION sip_passwd” will be rejected).

- The SIP_DATA terminator, “\$”, is a reserved token and may not be used as a value of any SIP_DATA sub-option. If a sub-option is present in the SIP_DATA options list, then it must have a valid value other than “\$”.
- The tag-value pair relationship for the options/sub-options will be enforced from a simple format perspective. All sub-options must have associated values. The overall SIP_DATA option must be terminated by a “\$”.
- Multiple/extraneous SIP_DATA options or sub-options found in a single NEW/CHF/EST/ADD command, will result in rejection of the command by OSSGate/SERVORD+. This limits the number of SIP LENs/endpoint which can be included in EST/ADD group commands to **ONE**.
- SIP_URI must be of the format user@domain. The domain information is parsed from the URI value. A missing domain (e.g. missing @ delimiter or domain information) will cause immediate command failure. An invalid domain name specified will be rejected by the Session Server Provisioning Manager.
- SIP_LOCATION must be included in the SIP_DATA option when the command issued results in the creation of a new user on the Session Server.
- SIP_SUBDOMAIN is an optional suboption and if not present, the domain parsed from the URI is used when creating the user on the Session Server element manager

2.6.1.4.2 Rules NOT Explicitly Enforced for SIP Data by OSSGate/SERVORD+

These rules are not explicitly enforced by OSSGate/SERVORD+. Breaking these rules may cause command failures or other unintended consequences:

- SIP_DATA and the associated sub-option tags are reserved words and may not be used as values for any non-related types (e.g. CM customer group, gateway names, etc.). Use of the reserved keywords in this manner may cause unexpected problems when attempting to use OSSGate/SERVORD+ for provisioning ANY type of line.
- CHF commands affecting SIP_DATA on SIP lines requires that gateway/termination names (or associated LEN) be used in the command instead of DN. Use of DN will result in the command being processed only by the CM, which is undesirable when SIP_DATA is present in the command.
- ADO and DEO commands for SIP lines affecting MDN data requires that gateway/termination names (or associated LEN) be used in the command instead of DN (e.g. “ADO \$ <DN or LEN> <OPTIONS>”). Use of DN will result in the command being processed only by the Core/CM, which will result in group data misalignment between the Core/CM and the SS-EM.

- Use of the SIP_DATA option is not supported in commands which do not affect SIP lines or in commands which are not supported for flowthrough for SIP lines. Use of the SIP_DATA option in these commands may cause unintended command failures.
- The SIP_DATA option may fall anywhere in the command string except as the first token (which is reserved for the command name), however it is **highly recommended** that the SIP_DATA option be placed in the normal option field range of the command.
- The values assigned to sub-options SIP_CLIENT_TYPE, SIP_PACKAGE, and SIP_LOCATION are *case sensitive*. **When commissioning these associated values on the Session Server Provisioning Manager, you MUST use the case which will be sent from the OSS (some OSS support only upper case, some lower case, and yet others mixed case).** Failure to commission these values in the Session Server Provisioning Manager using the case text supported by the OSS will result in command failures at OSSGate/SERVORD+.
- SIP_URI is normalized to lower case by the Session Server Provisioning Manager when received from OSSGate/SERVORD+. Caseless comparisons are performed by the Session Server Provisioning Manager when determining if a URI entered at OSSGate is already in use (e.g. "Slynch@Nortel.com" is considered identical to "slynch@nortel.com" from the Session Server Provisioning Manager's perspective). Only the normalized/lower-case URI is stored by the Session Server Provisioning Manager (e.g. "USERname1@Domain1.net" received from OSSGate/SERVORD+ would be stored as "username1@domain1.net" in the Session Server Provisioning Manager).

2.6.1.5 Data Mapping Example

In the following command,

LEN: MSM1 00 0 00 00

is mapped to

VMG: TestMSMVMG.1

termination/endpoint: MSM1/000/0/0000

OSSGate command:

```
NEW $ 9195200500 IBN PRADEFAULT 0 0 LATA1 0 MSM1 00 0 00 00 DPL
Y 10 SIP_DATA SIP_PACKAGE test package SIP_PASSWD test1Password
SIP_URI someone@somecompany.com SIP_CLIENT_TYPE SIP Line
SIP_LOCATION Nortel Networks.RTP SIP_SUBDOMAIN
local1.somecompany.com $ MDN SCA Y Y TONE N $
```


XACore SERVORD command derived from OSSGate command:

```
NEW $ 9195200500 IBN PRAEFAULT 0 0 LATA1 0 MSM1 00  
0 00 00 DPL Y 10 MDN SCA Y Y TONE N $
```

Data sent to SS-EM:

VMG: TestMSMVMG.1

termination: MSM1/000/0/0000

Domain: somecompany.com

Subdomain: local.somecompany.com

User: someone

Password: test1Password

firstName: SIPLineUser (default value)

lastName: SIPLineUser (default value)

Package: test package

locale: English (default value)

timezone: Eastern Standard Time (default value)

clientType: sip line

DN: 9195200500

location: nortel networks.rtp

status: ACTIVE (default value)

group type: MDN

group name: 9195200500

2.6.2 New commands

Not Applicable.

2.6.3 Line equipment format changes

2.6.3.1 LEN

No LEN format changes are introduced by this feature. Typical LEN format for SS LENS:

SITE FFF G TT tt

SITE = SITE name

FFF = frame number, 0-511

G = group number, 0-9

TT tt = terminal, 00 00 - 10 23

2.6.3.2 Media gateway endpoint format

No gateway/endpoint format changes are introduced by this feature. Typical SS VMG and endpoint formats:

VMG = 64 character free-form string (e.g. TestSSVMG.1)

endpoint/termination = SITE/FFF/G/TTtt

where SITE, FFF, G, and TTtt value are as specified in the SS LEN format with the following conversion padding rules:

- The LEN's individual TT tt values will always be zero-padded to 2 digits when converted to an endpoint/termination name (e.g. TT tt value "2 7" would be converted to an endpoint/termination TTtt value of "0207").
- The LEN's FFF value will always be zero-padded to 3 digits (e.g. FFF value "6" would be converted to endpoint/termination FFF value "006").

2.7 Software optionality control (SOC)

2.8 Element Management

SESM

2.8.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Line Data Audit	CHANGED

2.8.2 GUI information

2.8.2.1 GUI Name: Line Data Audit

In this feature, the line audit will also audit the data in Session Server EM. The audit GUI look and feel does not change, except that few checks are added to warn the user of system load. Also the audit output file (both valid and problem files) will have extra information pertaining to the Session Server audit.

2.8.2.1.1 Functional description

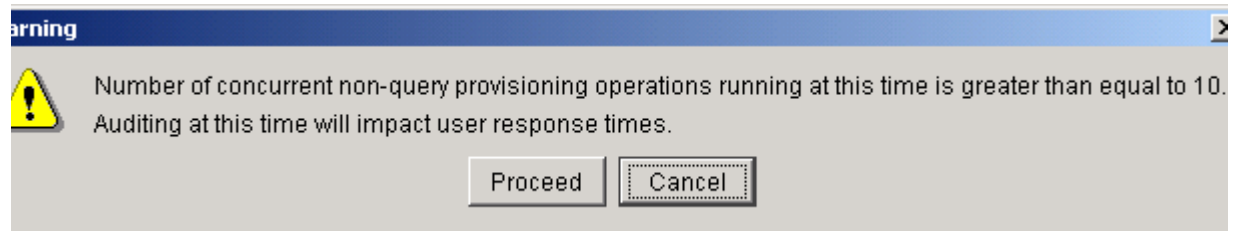
Warning Dialogues in Audit GUI:

One of the requirement in this feature is to avoid running (atleast warn) line audit when the system is loaded, as the audit might impact more important provisioning activities. In this feature, the manual line audit will check for the system load and warn the user if its not an appropriate time to run audit.

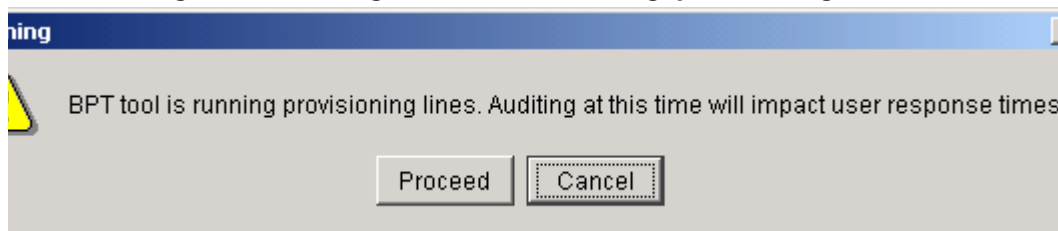
If any of the three checks is true, then the server will return 'not ready' with details to the GUI, which in turn will pop a dialogue box to warn user of system load and gives him a chance to decide if he wants to run the audit at a later time, since running audit has the potential to slow down the system impacting higher priority provisioning activities.

First check done by the server is to see if there are 10 or more concurrent non-read-only operations in progress. If yes, the audit server returns 'not ready' with details to the GUI. Shown below is example dialogue box.

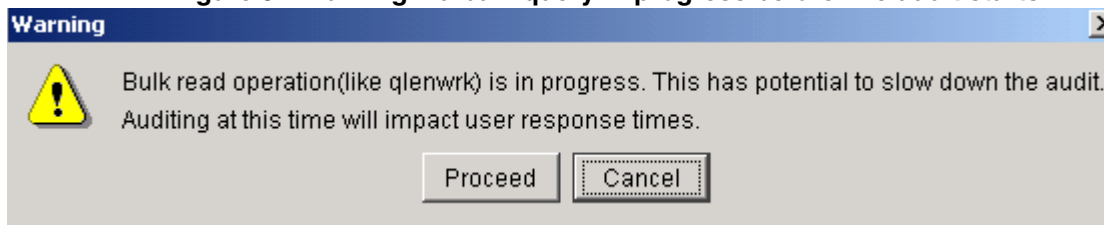
Figure 1 Warning if 10 or more non-query type line provisioning in progress



The second check is to see whether BPT tool is running a lines batch operation. If yes, the server returns 'not ready' with details to GUI. Shown below is example dialogue box in this condition.

Figure 2 Warning if BPT tool is running, provisioning lines

The third check is to see whether any bulk query operation (like qlenwrk, qdnwrk etc) is already in progress. If yes, the server will return 'not ready' to the GUI. Shown below is example dialogue box in this scenario.

Figure 3 Warning if a bulk query in progress before line audit starts**Line Data Audit Valid Data output:**

After the line data audit finishes, the ValidLineData.log file will have additional information obtained by auditing the Session Server EM.

The endpoints in GWCEM will be compared with SS EM, the group DN and its member DN information will be compared with the core and the DN to len mapping will also be compared with the core.

In the first screen shot is shown, valid data w.r.t the Session server will be at bottom. In the following screen shot, the group DN and its type and the member DNs are printed on screen, which is new audit data added by this feature if SIP MGs are provisioned.

Page: 1/1

Go to page 1

EP NAME	LEN	DN	TN
tp/0/0001	CICM 02 0 00 01	HASU - No DN on CM	2
tp/0/0002	CICM 02 0 00 02	HAS DN	3
tp/0/0003	CICM 02 0 00 03	HAS DN	4
tp/0/0004	CICM 02 0 00 04	HAS DN	5
tp/0/0005	CICM 02 0 00 05	HAS DN	6
tp/0/0006	CICM 02 0 00 06	HAS DN	7

Group DN	Group Type	Member DNs or LENs (comma seperated)
9195200100	MDN	CICM 02 0 00 03
9195200200	DNH	9195200201,9195200202

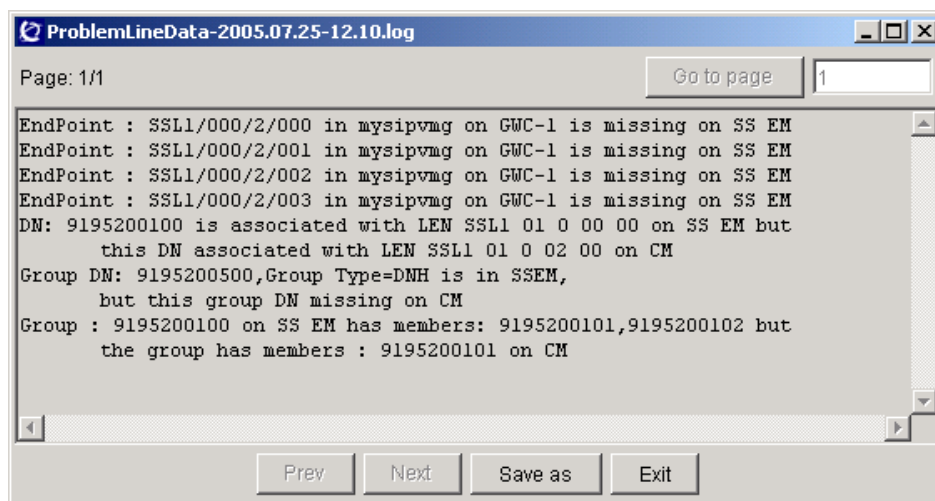
<<-NEW data added by this feature

Prev Next Save as Exit

2.8.2.2 Line Data Audit Problem Data output:

Shown below is screen shot of problem line data results. The problems could be in following areas

1. Endpoint exists in GWCEM, but not in Session server EM
2. DN associated with endpointId (len) in SS EM, while that same DN maps to different LEN on core
3. group DN in SS EM but that group information is missing in core
4. member DN/LENs in SS EM belonging to a group do not match the member list in that group on core.



2.8.2.3 GUI usage and implications

2.8.2.3.1 GUI size

Not applicable.

2.8.2.3.2 GUI fields

Table 2 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry

2.8.2.3.3 Usage example

2.8.2.3.4 GUI release history update

2.8.2.3.5 Context sensitive launching information

Not impacted, no changes

2.8.2.3.6 Supplementary information

None

2.8.2.4 CLUI Interface

Warning in BPT on Audit Running:

A check is introduced in BPT tool where it determines if Line Audit is currently running. If yes, BPT tool will warn the user that line audit is in

progress and gives the user a chance to run the lines batch later, as the throughput of the Lines batch could be slower due to line audit running.

Screen shot from BPT tool when lines batch is started if line audit is in progress.

***** WARNING *****

Line Audit is currently in progress.

This lines batch may run slower and may also invalidate audit results

Do you still want to proceed with lines batch? <y/n>:

The above warning tells the user that line audit is in progress and perhaps the lines batch should be run after the audit is finished.

2.8.3 LMM CLUI

To access the LMM CLUI telnet to OSSGate, enter ^B, “mode MTC”. Once in the MTC level, “LMM” is entered for access to the LMM CLUI.

```
>
? mode MTC

Mode is MTC.
```

The CMCLLI command is used to return the SDM IP and CMCLLI name:

```
>CMCLLI
SDM IP = 47.142.134.124
CM CLLI = RTP2

>LMM
report <-v>
report <-l> <report name>
report <-gen> <GWC Options>

post <-d, -l, -gw, -u, -r, -set, -display, -count>

bsy <-d, -l, -gw, -set> [inb]
rts <-d, -l, -gw, -set>
tst <-d, -l, -gw, -u, -set>
FRLS <-d, -l>

qdn <dn>
qlen <len>
qsip <dn, len>

help

quit
```

The commands (i.e. report, bsy) can be entered in either upper or lower case. The options (i.e. -d, -l) must be entered in lower case. The parms can be entered in either case but in the case of the GW name, should be in the proper case.

2.8.3.1 REPORT Commands

The REPORT commands are used with the GW in Trouble reports. Using the commands, the user has the ability to list, view and delete any of the reports. The GENERATE or GEN is used to run the process to create a report.

Command format:

```
report <-l>
report <-v> <REPORT NAME>
report <-gen> <GWC List | all>
```

Command usage:

To obtain a list of reports currently available

```
>report -l
The following reports are available:
Report-2005-08-10-22-06-14
```

To view a specific report

```
>report -v Report-2005-08-10-22-06-14
GW Name      Results for GWC-0
t1124ent.us.nortel.com  GW DISABLED

GW Name      Results for GWC-10
test4       GW DISABLED
```

To request a new GW in Trouble report for GWC 1

```
report -gen 1
```

To request a new GW in Trouble report for GWC 1, 2 and 3

```
report -gen 1, 2, 3
```

or

```
report -gen 1-3
```

or

```
report -gen 1, 2-3
```

To request a new GW in Trouble report for all valid (small and large line) GWCs

```
report -gen all
```

2.8.3.2 MTC Commands

This set of commands is used to perform operations on either one or a set of lines.

Command format:

```
post -d <DN> [verbose]
post -l <LEN> [verbose]
```



```
post -gw <GW/VMG> [verbose]
post -u <URI> [verbose]
post -r <Domain name> [verbose]
post -display [verbose]
post -count
```

```
bsy -d <DN> [inb]
bsy -l <LEN> [inb]
bsy -gw <GW or VMG> [inb]
bsy -set [inb]
```

```
rts -d <DN>
rts -l <LEN>
rts -gw <GW/VMG>
rts -set
```

```
tst -d <DN>
tst -l <LEN>
tst -gw <GW/VMG Name>
tst -u <URI>
tst -set
```

```
frls -d <DN>
frls -l <LEN>
```

2.8.3.2.1 REPORT Commands

The REPORT commands are used with the GW in Trouble reports. Using the commands, the user has the ability to list and view any of the reports. The -gen is used to run the process to create a report.

Command format:

```
report <-l>
report <-v> <REPORT NAME>
report <-gen> <GWC List | all>
```

Command usage:

To obtain a list of reports currently available

```
>report -l
The following reports are available:
Report-2005-11-14-12-12-01
```

To view a specific report

```
>report -v Report-2005-11-14-12-12-01
GWC-14 Number of GWs out of service = 1

R7A20204.rtp7.net status = GW DISABLED

GWC-13 Number of GWs out of service = 11
```

To request a new GW in Trouble report for GWC 1

```
report -gen 1
```

To request a new GW in Trouble report for GWC 1, 2, 3 and 4

```
report -gen 1, 2, 3, 4
```

or

```
report -gen 1-4
```

or

```
report -gen 1, 2-4
```

To request a new GW in Trouble report for all valid (small and large line) GWCs

```
report -gen all
```

2.8.3.2.2 POST

The POST command can be used to generate a set of lines and be used for maintenance (BSY, etc.) actions.

The POST command will list the contents of the post set to the screen using a “brief” format. The information listed will be dn, len, uri, clientIp, gwc, lcc, cm line state, scc line state and MCS line state (if a SIP Line).

The VERBOSE option includes included the above and adds the following, GW/VMG name, GW ipaddress, GW type, endpointName, domain/subdomain.

To post by DN (SIP Line)

```
>post -d 7550505
DN          = 6137550505
LEN         = SS 00 0 00 05
LCC         = IBN
GWC NAME    = GWC-5
GW NAME     = rtp7ssa
EPT NAME    = SS/000/0/0005
GW EPT ST   = ON-HOOK
CM EPT ST   = IDL
SIP URI     = user5@rtp7ssa.com
CLIENT IP   =
SS EPT ST   =
```

Number of endpoints returned = 1

To post by DN, non SIP Line

> post -d 6210010

```
DN          = 6136210010
LEN         = UAIP 00 1 00 00
LCC         = IBN
GWC NAME    = GWC-14
GW NAME     = rtp7-1104b.us.nortel.com
EPT NAME    = aaln/1
GW EPT ST   = ON-HOOK
CM EPT ST   = IDL
```

Number of endpoints returned = 1

To post by LEN:

```
> post -l ss 0 0 0 5
DN          = 6137550505
LEN         = SS 00 0 00 05
LCC         = IBN
GWC NAME    = GWC-5
GW NAME     = rtp7ssa
EPT NAME    = SS/000/0/0005
GW EPT ST   = ON-HOOK
CM EPT ST   = INB
SIP URI     = user5@rtp7ssa.com
CLIENT IP   =
SS EPT ST   =
```

To post by GW:

Note: Since the minimum VMG size for SIP is 1023 endpoints, posting by vmg may take a long time (approx 5 mins per LGRP) and will produce a huge output.

```
> post -gw rtp7-1104b.us.nortel.com
DN          = 6136210010
LEN         = UAIP 00 1 00 00
LCC         = IBN
GWC NAME    = GWC-14
GW NAME     = rtp7-1104b.us.nortel.com
EPT NAME    = aaln/1
GW EPT ST   = ON-HOOK
CM EPT ST   =
```

```
DN          = 6136210011
LEN         = UAIP 00 1 00 01
LCC         = IBN
GWC NAME    = GWC-14
GW NAME     = rtp7-1104b.us.nortel.com
EPT NAME    = aaln/2
GW EPT ST   = ON-HOOK
CM EPT ST   =
```

```
DN          = 6136210012
LEN         = UAIP 00 1 00 02
LCC         = RES
GWC NAME    = GWC-14
GW NAME     = rtp7-1104b.us.nortel.com
EPT NAME    = aaln/3
GW EPT ST   = ON-HOOK
CM EPT ST   =
```

```
DN          = 6136210013
LEN         = UAIP 00 1 00 03
LCC         = RES
GWC NAME    = GWC-14
GW NAME     = rtp7-1104b.us.nortel.com
EPT NAME    = aaln/4
GW EPT ST   = ON-HOOK
CM EPT ST   =
```

To post by URI:

```
> post -u user5@rtp7ssa.com
DN          = 6137550505
LEN         = SS 00 0 00 05
LCC         = IBN
GWC NAME    = GWC-5
GW NAME     = rtp7ssa
EPT NAME    = SS/000/0/0005
GW EPT ST   = ON-HOOK
CM EPT ST   =
SIP URI     = user5@rtp7ssa.com
CLIENT IP   =
SS EPT ST   =
```

To post Registered users by domain. This command will return the users that have registered their clients with their provisioned domains.

Note: This command may take a long time and will produce a huge output.

```
> post -r rtp7ssa.com
DN          = 6137550505
LEN         = SS 00 0 00 05
LCC         = IBN
GWC NAME    = GWC-5
GW NAME     = rtp7ssa
EPT NAME    = SS/000/0/0005
GW EPT ST   =
CM EPT ST   =
SIP URI     = user5@rtp7ssa.com
CLIENT IP   =
SS EPT ST   =

DN          = 6137550510
LEN         = SS 00 0 00 10
LCC         = IBN
GWC NAME    = GWC-5
GW NAME     = rtp7ssa
EPT NAME    = SS/000/0/0010
GW EPT ST   =
CM EPT ST   =
SIP URI     = user10@rtp7ssa.com
CLIENT IP   =
SS EPT ST   =
```

Number of endpoints returned = 2

To display the contents of the post se using the verbose option:

```
> post -display verbose
DN          = 6137550505
LEN         = SS 00 0 00 05
LCC         = IBN
GWC NAME    = GWC-5
GW NAME     = rtp7ssa
EPT NAME    = SS/000/0/0005
GW EPT ST   = ON-HOOK
CM EPT ST   = IDL
SIP URI     = user5@rtp7ssa.com
CLIENT IP   =
SS EPT ST   =
```

```
Node Num   = 213
Term Num   = 6
GWC IP     = 47.142.92.172
GW IP      = 47.142.91.154
GW TYPE    =
```

To display the number of entries in the post set:

```
>post -count
Post set size = 104
```

2.8.3.2.3 BSY

The BSY commands informs the CM to perform the requested action. A response message indicates the success or failure of the command. These messages are generated by the CM.

To Maintenance/Manual Busy a line by DN:

```
> bsy -d 7550505
DN = 7550505
CM RETURN CODE = CM_OK
```

To Maintenance/Manual Busy a line by LEN:

```
> bsy -l ss 0 0 0 5
LEN = ss 0 0 0 5
CM RETURN CODE = CM_OK
```

To Maintenance/Manual Busy all lines on a GW:

```
> bsy -gw rtp7-1104b.us.nortel.com
DN = 6136210010
CM RETURN CODE = CM_OK
DN = 6136210011
CM RETURN CODE = CM_OK
DN = 6136210012
CM RETURN CODE = CM_OK
DN = 6136210013
CM RETURN CODE = CM_OK
```

To Busy by the posted set:

```
> bsy -set
DN = 6136210010
CM RETURN CODE = CM_OK
DN = 6136210011
CM RETURN CODE = CM_OK
DN = 6136210012
CM RETURN CODE = CM_OK
DN = 6136210013
CM RETURN CODE = CM_OK
```

The BSY INB operation performs two operations; first is a BSY then upon success, performs the INB operation. If the line is already in the BSY state then only the INB operation is performed.

If the line is IDL

```
> bsy -d 7550505 inb
DN = 7550505
CM RETURN CODE = CM_OK
DN = 7550505
CM RETURN CODE = CM_OK
```

If the line is BSY

```
> bsy -d 7550505 inb
DN = 7550505
CM RETURN CODE = CM_ALRDY_IN_REQ_STATE
DN = 7550505
CM RETURN CODE = CM_OK
```

2.8.3.2.4 RTS

To return-to-service a line by DN:

```
> rts -d 7550505
DN = 7550505
CM RETURN CODE = CM_OK
```

To return-to-service a line by LEN:

```
> rts -l ss 0 0 0 5
LEN = ss 0 0 0 5
CM RETURN CODE = CM_OK
```

To return-to-service all lines on a GW:

```
> rts -gw rtp7-1104b.us.nortel.com
DN = 6136210010
CM RETURN CODE = CM_OK
DN = 6136210011
CM RETURN CODE = CM_OK
DN = 6136210012
CM RETURN CODE = CM_OK
DN = 6136210013
CM RETURN CODE = CM_OK
```

To Busy by the posted set:

```
> rts -set
DN = 6136210010
CM RETURN CODE = CM_OK
DN = 6136210011
CM RETURN CODE = CM_OK
DN = 6136210012
CM RETURN CODE = CM_OK
DN = 6136210013
CM RETURN CODE = CM_OK
```

2.8.3.2.5 TST

The TST performs a diag (where possible) depending upon the GW's ability to perform diagnostics on endpoints. Only GCP and MGCP GWs support the TST command.

To test by DN (SIP):

```
> tst -d 7550505
```

```
DN = 6137550505
LINE_STATE = PASSED
ENDPOINT_STATE = UNKNOWN
CLIENT = user5@47.142.166.65
TEST RESULT = PASSED
```

To test by DN (MGCP line):

```
> tst -d 6210010
```

```
DN = 6136210010
LINE_STATE = ON-HOOK
ENDPOINT_STATE = OK
```

To test using the LEN (SIP)

```
> tst -l ss 0 0 0 5
```

```
DN = 6137550505
LINE_STATE = PASSED
ENDPOINT_STATE = UNKNOWN
CLIENT = user5@47.142.166.65
TEST RESULT = PASSED
```

To test using the URI

```
> tst -u user5@rtp7ssa.com
```

```
URI = user5@rtp7ssa.com
LINE_STATE = PASSED
ENDPOINT_STATE = UNKNOWN
CLIENT = user5@47.142.166.65
TEST RESULT = PASSED
```

To test by GW (or VMG).

Note: Testing by VMG may take a long time and produce a large amount of information.

MGCP based GW:

```
> tst -gw rtp7-1104b.us.nortel.com
```

```
DN = 6136210010
LINE_STATE = ON-HOOK
ENDPOINT_STATE = OK
DN = 6136210011
LINE_STATE = ON-HOOK
ENDPOINT_STATE = OK
DN = 6136210012
LINE_STATE = ON-HOOK
ENDPOINT_STATE = OK
DN = 6136210013
LINE_STATE = ON-HOOK
```

ENDPOINT_STATE = OK

SIP GW

```
> tst -gw rtp7ssa
```

```
DN = 6137550500
LINE_STATE = FAILED
ENDPOINT_STATE = UNKNOWN
ERROR = Test Executed
```

```
DN = 6137550501
LINE_STATE = FAILED
ENDPOINT_STATE = UNKNOWN
ERROR = Test Executed
```

2.8.3.3 QUERY Commands

The query commands are used to perform various existing queries. These queries are the same as those from Servord.

Command format:

```
qdn <DN>
qlen <LEN>
qsip <DN, LEN>
```

Command usage:

To Query a DN

QDN 7201000

```
-----
DN: 7201000
TYPE: SINGLE PARTY LINE
SNPA: 619 SIG: DT LNATTIDX: N/A
LINE EQUIPMENT NUMBER: SS 00 2 00 00
END POINT: rtp2sesml SS/000/2/0000
LINE CLASS CODE: IBN
IBN TYPE: STATION
CUSTGRP: BNR SUBGRP: 0 NCOS: 0
CARD CODE: RDTLSG GND: N PADGRP: PKNIL BNV: NL MNO: N
PM NODE NUMBER : 142
PM TERMINAL NUMBER : 1
OPTIONS:
CWT DGT DPL Y 10
OFFICE OPTIONS:
SRA
```

```
END POINT DATA:
SIP_CLIENT_TYPE: ont
SIP_EP_NAME: SS/000/2/0000
SIP_VMG_NAME: rtp2sesml
SIP_DN: 6197201000
SIP_LOCATION: rtp2
SIP_PACKAGE: basic
SIP_URI: user0@rtp2.com
-----
```

To query by LEN


```
> qlen SS 0 2 0 0
```

```
-----
LEN:      SS      00 2 00 00
END POINT: rtp2sesm1  SS/000/2/0000
TYPE: SINGLE PARTY LINE
SNPA: 619
DIRECTORY NUMBER:      7201000
LINE CLASS CODE: IBN
IBN TYPE: STATION
CUSTGRP:      BNR      SUBGRP: 0  NCOS: 0
SIGNALLING TYPE: DIGITONE
CARDCODE: RDTLSG      GND: N  PADGRP: PKNIL  BNV: NL MNO: N
PM NODE NUMBER      :      142
PM TERMINAL NUMBER :      1
OPTIONS:
CWT DGT DPL Y 10
OFFICE OPTIONS:
SRA
END POINT DATA:
SIP_CLIENT_TYPE: ont
SIP_EP_NAME: SS/000/2/0000
SIP_VMG_NAME: rtp2sesm1
SIP_DN: 6197201000
SIP_LOCATION: rtp2
SIP_PACKAGE: basic
SIP_URI: user0@rtp2.com
-----
```

To query using the QSIP command. The parm can be either a DN or LEN.

```
> qsip 7550505
SS      00 0 00 05
SS/00/0/0005
```

```
-----
SIP USER DATA
=====
SIP URI: user5@rtp7ssa.com
ACCOUNT STATUS: ACTIVE
REGISTERED: Y
ALLOW POST BSY TERMINATIONS: Y
NUMBER OF CONTACTS: 1
CONTACTS: user5@47.142.166.65
SERVICE PACKAGE:
basic_package
SERVICES:
ALCLNT N IM SIPLN ADVSCR 3 3 N CLNTCO N N N N ADHOC 4 ADDRBK 50 PRES 10 Y
20 Y VIDEO N N NWLOG 50 50

SIP LINE DATA
=====
ENDPT ID: SS/000/0/0005
VMG: rtp7ssa
ZONE ID(s):
CLIENT TYPE: ONT
STATIC CLIENT: Y

SIP CALL DATA
=====
ACTIVE CALL APPEARANCES:
  NODENO  TERMNO
NUMBER OF ACTIVE SESSIONS IN CS2000 SESSION SERVER: 0
-----
>
```

2.8.3.4 MISC Commands

To quit from the LMM level - the user will remain in the MTC mode.

QUIT

2.8.3.5 Command Parsing

Multiple commands can be input on the same line - they must be separated by a “;”. Up to 4 lens, dns or uris can be specified with the POST, BSY, TST and RTS commands. Due to the potential volume of output, only one GW or VMG can be specified.

The commands are not case sensitive, but the parameters may be, i.e. GW name will be case sensitive.

Product = CS2K Management Tools

A00012310--Hunt, SCMP, and CWT variant support for SIP Lines

Functional Description

1: Applicable Solution(s)

CHS

1.1 Description

The purpose of this feature is to provide support for network based hunting, series completion and call waiting services for SIP user agents as part of the CS2K SIP Lines program.

In general, these services will behave in a manner consistent with their behavior in non-SIP configurations. Any exceptions are noted below.

1.1.1 Hunting

This feature provides support for the following hunt types on CS2K SIP Lines:

- DNH - Directory Number Hunt
- MLH - Multi-Line Hunt
- DLH - Distributed Line Hunt
- BNN - Bridged Night Number
- PRH - Preferential Hunt

In addition, the following hunt suboptions will be supported:

- CFGD/CFGDA - Call Forward Group Don't Answer
- LOD- Line Overflow to DN
- LOR - Line Overflow to Route
- CIR - Circular Hunt
- SHU - Stop Hunt
- RMB - Remote Make Busy

SIP lines can be used in the same hunt group as non-SIP lines. There will be no restrictions on using SIP lines in hunt configurations beyond the normal customer group and line class code restrictions imposed by standard hunt provisioning.

The functionality for SIP lines being in hunt groups has been defined to be:

- Termination on a SIP line for hunt purposes will only be considered if that line is involved in no other calls at the time. That is, the SIP line will be skipped in the hunt search algorithm if it is already involved in a call - even if it has the capability to engage in multiple call appearances.

Exceptions:

1.) CWT termination is allowed in DNH and PRH groups if the individual member has the CWT option. For SIP lines, if a DNH or PRH member has CWT, hunt calls will continue to be presented to the member until its maximum call appearances have been reached.

2.) In MLH configurations, if CWT is added to the pilot, extra call waiting calls are actually presented to the last member of the group. If that last member is a SIP line, calls will continue to be presented to that line until its maximum call appearances have been reached.

- If a hunt call terminates on a SIP line, and the SIP client declines the call (4XX or 6XX SIP response), the hunting search will continue to the next available hunt member. BNN groups are an exception to this rule. When a call terminates on a BNN and the SIP client declines the call, the call will receive busy treatment.
- If a hunt call terminates on a SIP line, and the SIP client redirects the call (3XX SIP response), the call will be forwarded to the redirection destination.
- Hunt suboptions CFGD/CFGDA, LOD, LOR, CIR, SHU, and RMB will function in the same manner as they do in non-SIP configurations.

It should also be noted that for query and maintenance commands performed on hunt members that do not have unique DNs (non-pilot MLH and DLH members), a LEN, gateway endpoint, or SIP URI must be used instead. For example:

- The CS2K core QSIP command - when given an MLH or DLH DN will return information on the pilot only. If information is desired for a particular member, the LEN of that member must be used as the QSIP argument.
- When posting lines on the CS2K LTP map level, only the MLH or DLH pilot can be posted using the DN. To post a group member, the LEN of that member must be used instead.
- When posting lines from the SSL system manager console, only the MLH or DLH pilot can be posted using the DN. To post a group member, the SIP URI of that member must be used.

1.1.2 Series Completion (SCMP)

This feature provides support for Series Completion on CS2K SIP Lines.

SIP lines can be in the same SCMP group as non-SIP lines. There will be no restrictions on using SIP lines in SCMP configurations beyond the normal restrictions imposed by standard SCMP provisioning.

In general, SCMP on a SIP line should function in exactly the same manner as it does for a non-SIP line. There are two items worth noting:

- SCMP takes precedence over CWT. Therefore, termination on a SIP line for SCMP purposes will only be considered if that line is involved in no other calls at the time, even if it has the capability to engage in multiple call appearances.
- SIP lines have the additional capability to decline calls after they have been presented to the line. If a SIP line with SCMP is idle but declines the call, the call will be directed to the SCMP DN rather than busy treatment.

1.1.3 Call Waiting Variants

This feature provides support for the following Call Waiting Variants on CS2K SIP Lines:

- CWI - Call Waiting Intragroup
- CWO - Call Waiting Originating
- CWD - Dial Call Waiting
- CWX - Call Waiting Exempt
- CWTACT - Call Waiting Activate
- SCWID - Spontaneous Call Waiting Identification

For SIP lines, a call waiting call is just a second call appearance being offered to the SIP client. The client is responsible for any tone application and the function of switching between the two calls via hold/restore. Therefore, for CS2K SIP lines, the presence of the above CWT options will be used to

determine when it is appropriate to offer multiple call appearances to the terminating SIP line.

In that context, the function of the above CWT variants is the same for SIP lines as it is for non-SIP lines.

1.2 Hardware Requirements or Dependencies

CWD requires PMA (Packet Media Anchor) insertion when the CWD originator is a SIP line. The PMA is required to provide subsequent digit collection after the CWD feature access code. Without the PMA, CWD cannot be initiated by a SIP line.

1.3 Software Requirements or Dependencies

In order to provision hunt groups on CS2K SIP lines, there is a dependency on feature A00012223: “SESM Additional Provisioning for SIP Lines”. This feature adds support for hunt group provisioning commands such as EST, ADD, DEL, ABNN, DBNN, and CHDN via SESM.

1.4 Limitations and restrictions

- MPH (Multi-Position Hunt) is not supported by this feature.
- Hunt group provisioning commands EST and ADD, when applied via SESM, will be limited to only one len or gateway endpoint per command. See feature A00012223 “SESM Additional Provisioning for SIP Lines” for more information.
- CWR (Call Waiting Ringback) and CWTC (Call Waiting Conference) are not supported by this feature.
- If a SIP line has max_call_appearances set to 1, then no call waiting calls can be presented to that line by any call wait variant, regardless of CWT variant provisioning.
- If a SIP line is using all of its available call appearances (example: max_call_appearances = 4, and 4 calls are active), then no further calls can be presented to that line by any call wait variant, regardless of CWT variant provisioning.
- Typically, core based features that impose call waiting on the terminating line (CWO, CWD) will override the use of Cancel Call Waiting (CCW) by the terminator. For SIP lines however, CCW is implemented in by the SIP client, so core based CWO and CWD cannot override it. This is a limitation of CWO and CWD for SIP lines.

1.5 Interactions

Not applicable.

1.6 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_

1.7 Glossary

Term	Description
New term	Definition

Product = CS2K Management Tools

A00012974--Correct Execdata mismatch between GWC EM and Core

Corrective CAF

1: Applicable Solution(s)

UA-AAL1, UA-IP

1.1 Purpose

Prior to SESM SN07 there is a TRUNK250 GWC profile which exec data include “ABTRK DTCEX” and “PRAB UTR250”. From SN07 the TRUNK250 profile is being changed to TRUNKNA, and “ABTRK DTCEX” becomes “ABTRK GWCEX”. Also, a valid TRUNKNA GWC has 3 pairs of

exec data. That is, “AB250 GWC250” is added by A89007187. Therefore, when both SESM and Core upgrade from SN6.2 or below to SN7.0 or above, both sides need to change the TRUNK250 profile to TRUNKNA profile.

This feature provides customers a function to change the execdata of a GWC from the GWCEM GUI. If the execdata of a GWC is changed, then both the SESM database table and Core table will be updated.

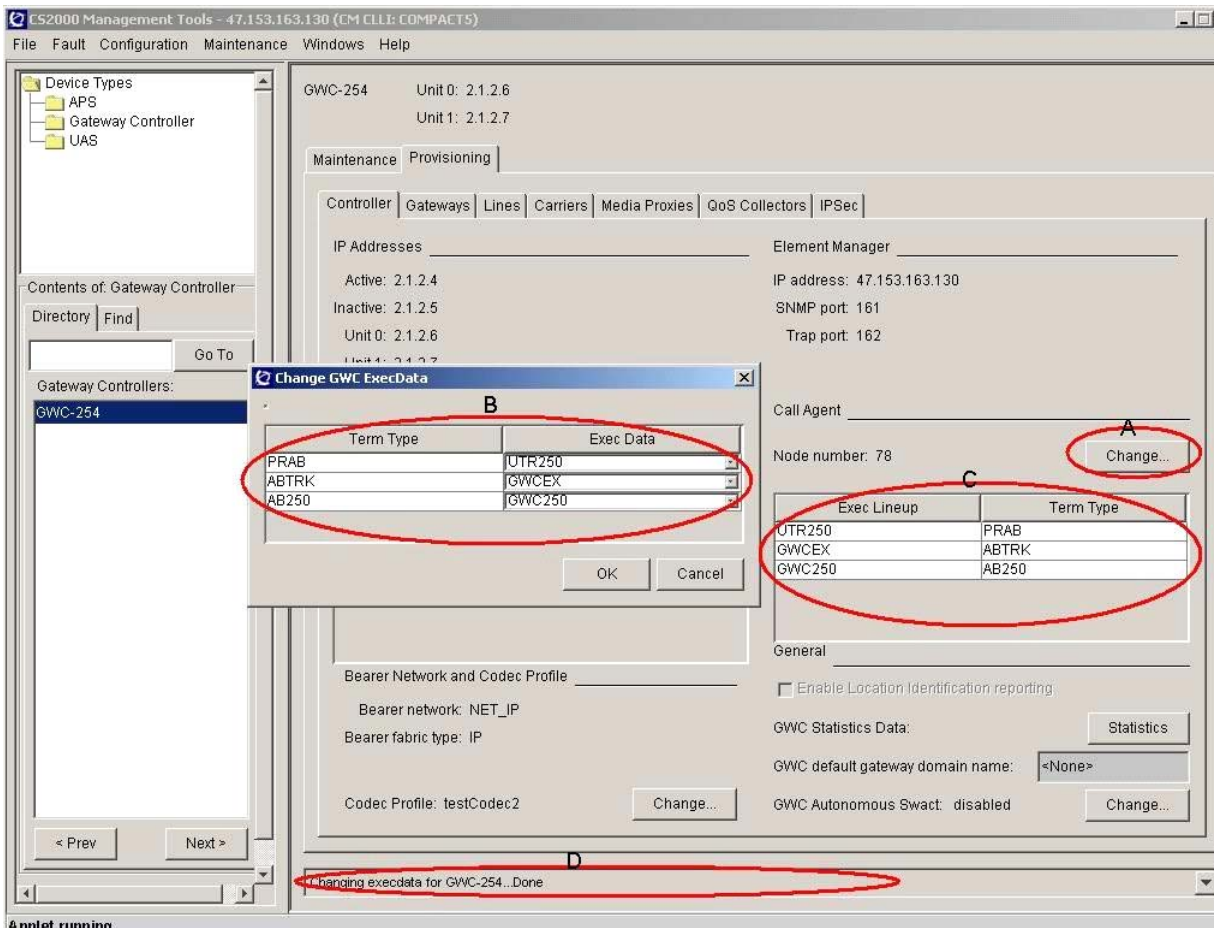
Since it is required for a GWC to have static data reloaded after a change of the exec data, a MN alarm will be generated to the IEMS for each GWC unit of a GWC pair until new static data is sent by locking and unlocking the cards.

1.2 Problem symptoms

Previously customers could choose execdata of a GWC profile for a GWC only when adding a new GWC. If the GWC has already been added into SESM the only way to change the GWC execdata is to delete the GWC and add it again. This is extremely service impacting.

This feature will introduce a new function which let customers change execdata of an existing GWC through the SESM GUI. After successful changing only a GWC, BSY/RTS operations are needed to make the new configuration valid on the GWC pair. Thus it is not necessary to delete and add a GWC in order to change the GWC execdata.

For example: Areas in red circles in the figure that follows show modification of this feature on the GUI.



A: Add a “Change...” button

B: Pop up a new dialogue when clicking the A button

C: The fields will be refreshed after successfully changing the ExecData

D: Messages will be prompted in the status bar during the operation

Nortel Networks - Alarm Manager - Connected to: 47.153.163.150

File Actions

Raw Alarm List

Network Element	Category	Alarm Time	Severity	Probable Cause
Audit	Processing Error	17:27:20 03-十一月-2005 GMT+...	Critical	Corrupt data
SNMP_NE_Poller	Communications	15:07:20 04-十一月-2005 GMT+...	Major	Communications subsystem failure
GWC-8-UNIT-1	Communications	16:22:33 04-十一月-2005 GMT+...	Major	Communications subsystem failure
GWC-11-UNIT-0	Quality of Service	14:54:29 04-十一月-2005 GMT+...	Critical	Underlying resource unavailable
GWC-11-UNIT-0	Communications	14:54:29 04-十一月-2005 GMT+...	Major	LAN error
GWC-8-UNIT-0	Communications	16:22:33 04-十一月-2005 GMT+...	Major	Communications subsystem failure
gwcem	Processing Error	14:55:41 04-十一月-2005 GMT+...	Critical	Corrupt data
GWC-11-UNIT-0	Communications	14:57:03 04-十一月-2005 GMT+...	Major	Communications subsystem failure

Show alarms: ☒ Critical ☒ Major ☒ minor ☐ warning

New Alarms:

11 alarms at: 16:22:56 04-十一月-2005 GMT+08:00

Advanced Filters

Refresh List

Details

Log Name: GWC 307

Component ID: GWC=GWC-8-UNIT-0;Version=GN091AS;Unit=unit_0;Software=NODEMTC

NE Name: GWC-8-UNIT-0

Alarm Level: Major

Category: Communications

Alarm Time: 16:22:33 04-十一月-2005 GMT+08:00

Probable Cause: Communications subsystem failure

System Uptime: 0 hours, 4 minutes, 12 seconds.

Alarm Description: Element Manager communication failure.

Specific Problem: EM indicates provisioned data mismatched in this unit

E: Alarm is raised after successful change of EXECDATA

F: The Alarm type is GWC 307, which means communication with the CS 2000 GWC Manager need to be restored. This alarm can be cleared by BSY/RTS of GWC unit.

1.3 Related documentation

N/A

Product = CS2K Management Tools

A00014049--GWC and SESM support for AAL2-G726-32 codec in IP Network

Corrective CAF

1: Applicable Solution(s)

PT-IP

1.1 Description

This Corrective CAF activity will enable the Gateway Controller and SESM to support the new codec AAL2-G726-32 in the SN09.1 Release. This activity also modifies SESM provisioning rules for IP network profiles.

The AAL2-G726-32 codec can be provisioned in the SESM GUI for IP network profiles only. To facilitate rapid deployment, the AAL2-G726-32 codec is replacing the iLBC codec in codec lists on SESM and GWC. iLBC codec is removed from codec lists from SN09FF onward.

From SN09.1 release onward, an IP network codec profile list will consist of 2 or 3 valid IP codecs, one of which **MUST** be PCMU or PCMA codec.

1.2 Hardware Requirements or Dependencies

VSP3 and VSP3-o cards support AAL2-G726-32 codec and the prior versions of VSP cards are not compatible with this SN09.1 functionality.

1.3 Software Requirements or Dependencies

For the integrated functionality in CS2K, the PVG image which supports AAL2-G726-32 codec is required.

1.4 Limitations and restrictions

This activity removes the existing iLBC codec and introduces AAL2-G726-32 codec in Gateway Controller and SESM. Hence in SN09.1 release, iLBC codec will not be available for network provisioning.

Note: The AAL2-G726-32 codec support will be patched back to SN08 and SN09 Gateway Controller releases. Till the Gateway Controller patches are available, the Gateway Controller will interpret AAL2-G726-32 codec provisioned in SESM as iLBC.

1.5 Interactions

None

1.6 Glossary

Term	Description
AAL2	ATM Adaptation Layer-2
ATM	Asynchronous Transfer Mode
CAF	Content Application Form
CS2K	Call Sever 2000
FN	Functional Description
GWC	Gateway Controller
iLBC	internet Low Bitrate Codec
PVG	Passport Voice Gateway
SAM21	Services Application Module (21 slots)
SESM	Succession Element and Sub-Element Manager

Product = IEMS

A00011281--MS2000 IPSec Configuration Via IEMS

Functional Description

1: Applicable Solution(s)

UA-IP

1.1 Description

This feature adds IPSec and IKE configuration capabilities to the MS2000 node configuration tool introduced in SN08. This will allow the craftsperson to enable IPSec for secure messaging between the IEMS and MS2000 as well as configure the IPSec and IKE parameters necessary for the MS2000 to securely send and receive messages to and from the GWC.

See the configuration section for full details on the new functionality.

1.2 Hardware Requirements or Dependencies

No specific requirements beyond what is necessary to support the SN09 software.

1.3 Software Requirements or Dependencies

SN09 IEMS and SSPFS.

SN08 or later MS2000 (?)

1.4 Limitations and restrictions

The MS2000 node does not support in-service updates to IPSec configuration data. Any changes to the IPSec data requires a reset of the MS2000 node.

1.5 Interactions

This feature extends the MS2000 configuration tool introduced in SN08 on the IEMS. It adds an additional tab to the tool that allows for the configuration of IPSec.

1.6 Glossary

Term	Description
IEMS	Integrated Element Management System

2: Configuration Management for A00011281

2.1 Hardware and Software Requirements

SN09 IEMS

SN08 or later MS2000

2.2 Initial Configuration

Standard SN09 IEMS deployment

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

Not applicable.

2.4 Upgrade Considerations

Not applicable.

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

Not applicable.

2.6 Service Orders (SO) (CM & SESM)

Not applicable.

2.7 Software optionality control (SOC)

Not applicable.

2.8 Element Management

2.8.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
IEMS - MS2000 Node Configuration	Changed

2.8.2 GUI information

2.8.2.1 GUI name: IEMS-MS2000 Node Configuration

2.8.2.1.1 Functional description

This GUI is used to configure the MS2000 node from the IEMS. This feature extends the existing GUI to include configuration of the IPSec and IKE parameters needed to allow for secure messaging between the IEMS and the MS2000 as well as between the MS2000 and the GWC.

2.8.2.1.2 GUI usage and implications

To configure IPSec and IKE parameters and enable them on the device, the following steps must be taken:

- set the IPSec and IKE parameters on the MS2000, including the initial key, via the new IEMS GUI tool.
- set IPSec as enabled on the MS2000 and reset the box
- set the IPSec and IKE parameters, including the initial key, on the SSPFS HTML servlet that currently exists. For documentation on the SSPFS configuration tool, see:
http://triweb/ja00/sloa/docs/howto_ipsec/howto_ipsec.html.
- return to the IEMS GUI and set the actual key.
- reset the MS2000
- return to the SSPFS HTML servlet and set the actual key.
- set the IPSec and IKE parameters for the GWC comms on the MS2000
- reset the MS2000

2.8.2.1.3 GUI size

Table 2 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
MS2000 Config	0	1	N/A

2.8.2.1.4 GUI fields

The following table lists fields for GUI MS2000 Config.

Table 3 IPSec GUI field descriptions

Field	New or Changed	Entry (examples)	Explanation and action	Associated MIB entry
IPSecPolicyRemotelPAddress	New	47.142.42.135	Destination IP address or a DNS name, this parameter is mandatory.note: if a DNS is given make sure the DNS server is also configured (DNSPriServerIP)	<see field name>
IPSecPolicySrcPort	New	161	Source port. 0 means all ports match.	
IPSecPolicyDstPort	New	9961	Destination port. 0 means all ports match.	

IPSecPolicyProtocol	New	0	Protocol type. 0 - all protocols match; 17- UDP, 6-TCP.
IPsecPolicyKeyExchangeMethodIndex	New	0-19 (see IKE table; matches with the IKE index)	The Index for the corresponding IKE entry, a few policies may be associated with a single IKE entry
IPsecPolicyLifeInSec	New	600	Lifetime in seconds for security association derived from this policy.
IPSecPolicyProposalEncryption_X	New	2	X – stands for the proposal number, up to 4 proposals are allowed [0-3].the valid encryption values are: 0 - NULL (no encryption) 1 - DES 2 - 3DES
IPSecPolicyProposalAuthentication_X	New	4	X – stands for the proposal number, up to 4 proposals are allowed [0-3].the valid authentication values are: 2 - SHA1 (SHA1_96)4 - MD5 (MD5_96)
IKEPolicySharedKey	New	020a04090e	The pre-shared key. The key is in text string format. Both peers need to register the same pre-shared key for the authentication process to succeed. The MS2000 will accept any key, however it is recommended that a hex character sequence is used.

IKEPolicyProposalEncryption_X	New	2	X – stands for the proposal number, up to 4 proposals are allowed [0-3].the valid encryption values are: 1 - DES 2 - 3DES
IKEPolicyProposalAuthentication_X	New	4	X – stands for the proposal number, up to 4 proposals are allowed [0-3].the valid authentication values are: 2 - SHA1 (SHA1_96) 4 - MD5 (MD5_96)
IKEPolicyProposalIDHGroup_X	New	1	X – stands for the proposal number, up to 4 proposals are allowed [0-3].the valid DH Group values are: 0 - 768 Bit 1 - 1024 Bit
IKEPolicyLifetimeSec	New	1200	Lifetime in seconds for security association derived from this policy.

2.8.2.1.5 Usage example

See walkthrough section at the end of this section for examples of using this code.

2.8.2.1.6 GUI release history update

SN08 - MS2000 GUI introduced.

SN09 - Updated to include IPSec configuration mechanism.

2.8.2.1.7 Context sensitive launching information

Launched from the IEMS - right click on the MS2000 node and choose configure MS2000 node option.

2.8.2.1.8 Supplementary information

None

2.8.3 CLUI Interface

Not applicable.

2.9 User interface changes

Not applicable.

2.10 OSSGate Interface Changes

Not applicable.

2.11 Security

Not applicable.

2.12 Configuration Walkthrough

2.12.1 Adding IPSec to the MS2000 node

2.12.1.1 Add IKE and IPSec parameters to the MS2000 for IEMS/MS2000 secure messaging

- 1 Launch the MS2000 Config and Maintenance Tool
- 2 Select the IPSec and IKE Config Tab
- 3 Select the IKE Configuration Tab
- 4 Select “Add Entry”
- 5 Enter the fields for the initial IKE configuration for the MS2000. These values will only be used to establish a temporary secure connection to allow the setting of the actual IKE fields. Essential: these fields should be selected based on the desired IPSec/IKE configuration for the lab. These fields will be needed for later configuration.
- 6 After all the fields are entered, the Add Entry button should be pressed.
- 7 Select the IPSec Configuration Tab.
- 8 Select “Add Entry”.
- 9 Enter the values for the IPSec temporary configuration. The index chosen for the IKE entry previously should be entered in the Exchange Method field here. Essential: these fields should be selected based on the desired IPSec/IKE configuration for the lab. These fields will be needed for later configuration.
- 10 Select “Add Entry”.
- 11 With both the IKE and IPSec tables configured, click the Enable IPSec check box.
- 12 In the new dialog box that appears, confirm the enabling of IPSec.

- 13** After receiving the message indicating successful enabling of IPSec, the MS2000 needs to be reset. This is done via the Reset button on the left side of the MS2000 config tool. Reset the MS2000 to enable the new parameters.
- 14** Once the MS2000 is reset, the IEMS will not be able to talk to the MS2000 until the IEMS server is configured for IPSec with the MS2000 IP. This is done via the configuration GUI at [http://\(ip address of server\)/ipsec/security.html](http://(ip address of server)/ipsec/security.html).
- 15** Adding IPSec support on SSPFS is described in detail in this document: http://iwebtrp.us.nortel.com/spvn/sloa/docs/howto_ipsec/howto_ipsec.html
- 16** Add the IPSec and then the IKE parameters via the GUI provided. Ensure that the selections made match the selections made during the MS2000 configuration. Do not close this window as it will be used again later.
- 17** At this point, communications between IEMS and the MS2000 have been secured. Configuration of the actual IPSec/IKE parameters can now begin.
- 18** Return the IPSec/IKE Configuration tab of the MS2000 Config tool.
- 19** Select the IKE Configuration tab.
- 20** Select the row in the table and click “Edit Entry”.
- 21** In the edit dialog, modify the desired fields. If the parameters previous entered are what is desired for the actual IKE parameters, only the shared key field needs to be modified. Click “Save”.
- 22** Select the IPSec table if any of the IPSec parameters need to be modified. If so, click “Edit Entry”, modify the values, and click “Save”.
- 23** At this point, the MS2000 needs to be reset again in order to enable the new preshared key (and any other modified values).
- 24** The IEMS server IPSec configuration for communications with the MS2000 needs to be modified to support the new parameters and shared key. Return the SSPFS configuration tool and delete the existing entries added earlier. Add new entries to match the new configuration of the MS2000, including the new preshared key.

2.12.1.2 Add IPSec and IKE parameters for MS2000/GWC communications

- 1** If secure messaging between the MS2000 and IEMS are desired before sending the preshared key to the AMS, complete the steps in section 12.12.1.
- 2** On the IEMS GUI, launch the MS2000 Config and Maintenance Tool.
- 3** Select the IPSec and IKE Config Tab.
- 4** Select the IKE Configuration Tab.
- 5** Select “Add Entry”.
- 6** Enter the IKE values needed to communicate with the GWC. These values should match the values provisioned on the GWC when appropriate. Essential: note which index is chosen as this field will be needed for later configuration.
- 7** After all the fields are entered, the Add Entry button should be pressed.
- 8** Select the IPSec Configuration Tab.
- 9** Select “Add Entry”.
- 10** Enter the IPSec values needed to communicate with the GWC. The index chosen for the IKE entry previously should be entered in the Exchange Method field here.
- 11** Select “Add Entry”.
- 12** If IPSec is not currently enabled, enable it following the steps 11 and 12 in section <cross-ref>“Adding IPSec to the MS2000 node” .
- 13** Reset the MS2000 box following step 13 in section <cross-ref>“Adding IPSec to the MS2000 node” . The MS2000 will now communicate securely with the GWC.

2.12.2 Disable IPSec on the MS2000

- 1** On the IEMS GUI, launch the MS2000 Config and Maintenance Tool.
- 2** Select the IPSec and IKE Config Tab.
- 3** If the Enable IPSec check box is selected, deselect it to disable IPSec.
- 4** A dialog will appear to confirm the desire to disable IPSec. Click “Yes”.
- 5** If desired, the data in the IPSec and IKE configuration tables can be deleted from the MS2000. Select the appropriate tab, select the row and click “Delete Entry”.

- 6 Reset the MS2000 following step 13 in section <cross-ref>“Adding IPSec to the MS2000 node” .
- 7 Once the MS2000 has reset, if IPSec was previously enabled between the IEMS and MS2000, the IEMS Server must disable IPSec to the MS2000 node in order to communicate.
- 8 Launch [http://\(ip address of server\)/ipsec/security.html](http://(ip address of server)/ipsec/security.html).
- 9 After logging in, select the entries corresponding to the MS2000 node and delete them. Once they are deleted, the IEMS will again be able to communicate with the MS2000.

2.12.3 Edit the preshared key on the MS2000

- 1 On the IEMS GUI, launch the MS2000 Config and Maintenance Tool.
- 2 Select the IPSec and IKE Config Tab.
- 3 Select the IKE Configuration Tab.
- 4 Select the row containing the key to update.
- 5 Click “Edit Entry”.
- 6 Update the preshared key.
- 7 Click “Save”.
- 8 Reset the MS2000 following step 13 in section 12.12.1.
- 9 Update the IEMS Server or GWC with the preshared key so that the MS2000 can communicate with that device.

Product = IEMS

A00012001--IEMS Call Server 2000 SIP Integration

Functional Description

1: Applicable Solution(s)

UA-IP

1.1 SN07/SN08 Background

In SN07&8, IEMS manages the Multimedia Communication Server Manager (MCS Manager). The MCS Manager when added can have as its managing type either an MCS/CSE MX NE or Media Proxy NE. When an MCS Manager

is added to they IEMS, the MCS/CSE MX NE or Media Proxy NE is added as a map symbol under the Network Elements. The MCS System Manager is added as an element in the Element Managers map.

Along with the configuration of the MCS device was the ability to associate Fault Performance Managers, FPM's, to an MCS device which would be another input for faults and performance data for IEMS.

There were provisions for fault, performance, and configuration management of MCS and FPM devices.

The current existing MCS device functionality along with the RTP Media Proxy and FPM will continue to be supported in SN09.

To see more information concerning the addition of the MCS device in SN08, please see document SN08 A00007346 - Backward Compatibility Functional Specification at
:http://livelink.us.nortel.com/livelink/livelink.exe?func=ll&objId=7485824&objAction=browse&sort=name

1.2 Main work Items

One of the first items is branding name changes for both the NGSS and MCS. The existing NGSS managed object to align with the Call Server 2000 Session Server. The Trunks version is relabelled to SStrunks. The MCS SIP lines which is now deployed on a Linux platform will be relabelled SSLines.

The MCS configuration and management remains the same from SN08 to SN09. The Icon for the MCS on the Solaris platform for the NE will be modified to MC52 and the tree name will be changed from MCS/CSE to MCS5200. Also, a change is made in the configuration of the MCS Mgr as an EM with a type from Media *Proxy* to Media *Portal*.

Integrating the management of the fault and performance interfaces of the new SSLines platform, Langley hardware running Linux OS. The SSLines system will also have the ability to configure the Session Manager platforms associated with the System Manager EM. There will also need to be configuration of the Provisioning Client servers. The configuration of the Session Managers will allow SSH launch to each Session Manager. The configuration of the Provisioning Client servers will allow the client to launch the MCS Provisioning Client.

Another work item consists of proxying all GUI/CLUI launches through the IEMS. The GUI/CLUIs that require proxying consist of:

- 1 MCS System Manager Console
- 2 Provisioning GUI

3 SSH to each platform associated with the SSLines deployment

The SSLines Element Manager and Network Element will provide and support all the existing functionality of the MCS/RTP Media Portal functionality pertaining to Fault Management, Performance collection, and device change management. There will however only be the option of being able to add the SSLines device as an SSLines Manager without the ability to configure the SSLines device as an RTP Media Portal. Also in SN09, the SSLines device will not be supporting FPM's.

To configure performance collection jobs, please refer to the SN08 document concerning MCS,

<http://livelink.us.nortel.com/livelink/livelink.exe?func=ll&objId=7485824&objAction=browse&sort=name>

1.3 Existing functionality

As specified previously this activity is for rebranding and proxying the MCS GUI's through the IEMS. The functionality of handling faults and provisioning data remains unchanged.

The change, and deletion of an SSLines type device has remained the same except for the type being deleted or changed.

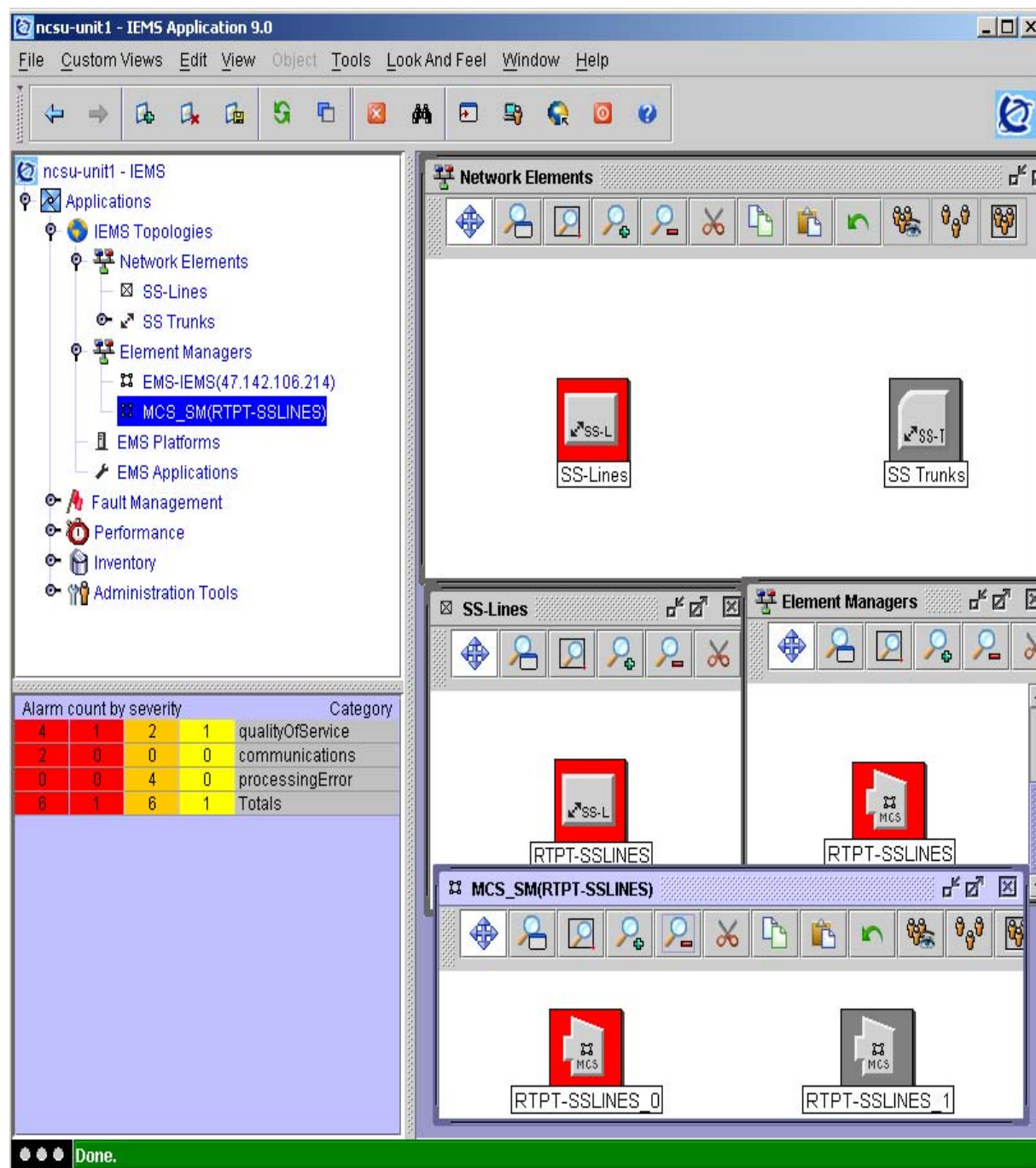
1.4 Changed Functionality

First and foremost is the branding change. When adding the SSLines device, an SSLines Mgr is added instead of an MCS Mgr or RTP Media Portal. The same information is entered concerning IP addresses, userid's, SNMP information, and performance data collection.

1.4.1 Topology

The topology of an SSLines as added into IEMS is displayed in the same hierarchy as the existing SN08 MCS. The following screen shot shows the new branding and topology for the SN09 SSLines.

Figure 1 Topology of SSLines EM and NE



The SS Trunks topology will be similar to that of the Session Server and will be displayed as follows in SN09.

command line is selected, a new frame will be displayed which will allow the user to select the platform to launch a command line to.

The launch of the command line for the System Manager and Session managers can be done from any of the maps in the GUI except from the Network Elements screen.

Figure 3 Launch of Command line From SSLines

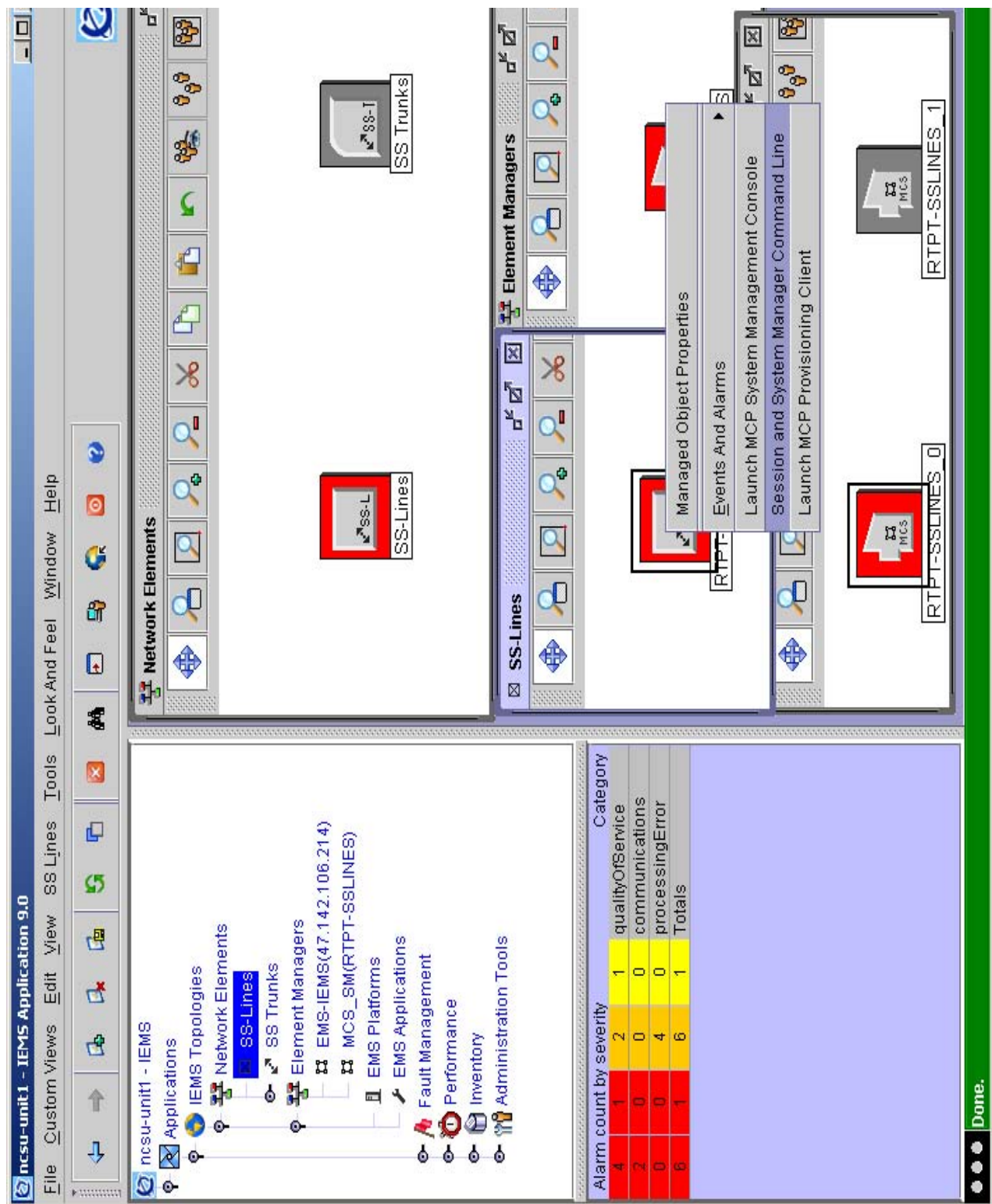


Figure 4 Launch of SSH command line to platform



The drop down box will allow the user to choose any of the platforms that SSH can be launched to. The SSH connections will be proxied via the IEMS server. There will be a new option against the EM to configure the platforms which will allow the user to configure these platforms.

1.5 New Functionality

1.5.1 GUI

For SN08, it was only possible to configure the platform(s) associated with the System Manager associated with an MCS or RTP Media Portal. In SN09, it is possible to configure all the platforms associated with an MCS/SSLines deployment including the IP addresses of

- 1 The Provisioning Clients (two IP addresses)
- 2 The Session Manager platform IP addresses (up to three pairs)

This configuration is done from the map reference of the SSLines EM.

From the EM or NE it is possible to launch the Provisioning client GUI.

Figure 5 Launch of Provisioning Client from EM Map

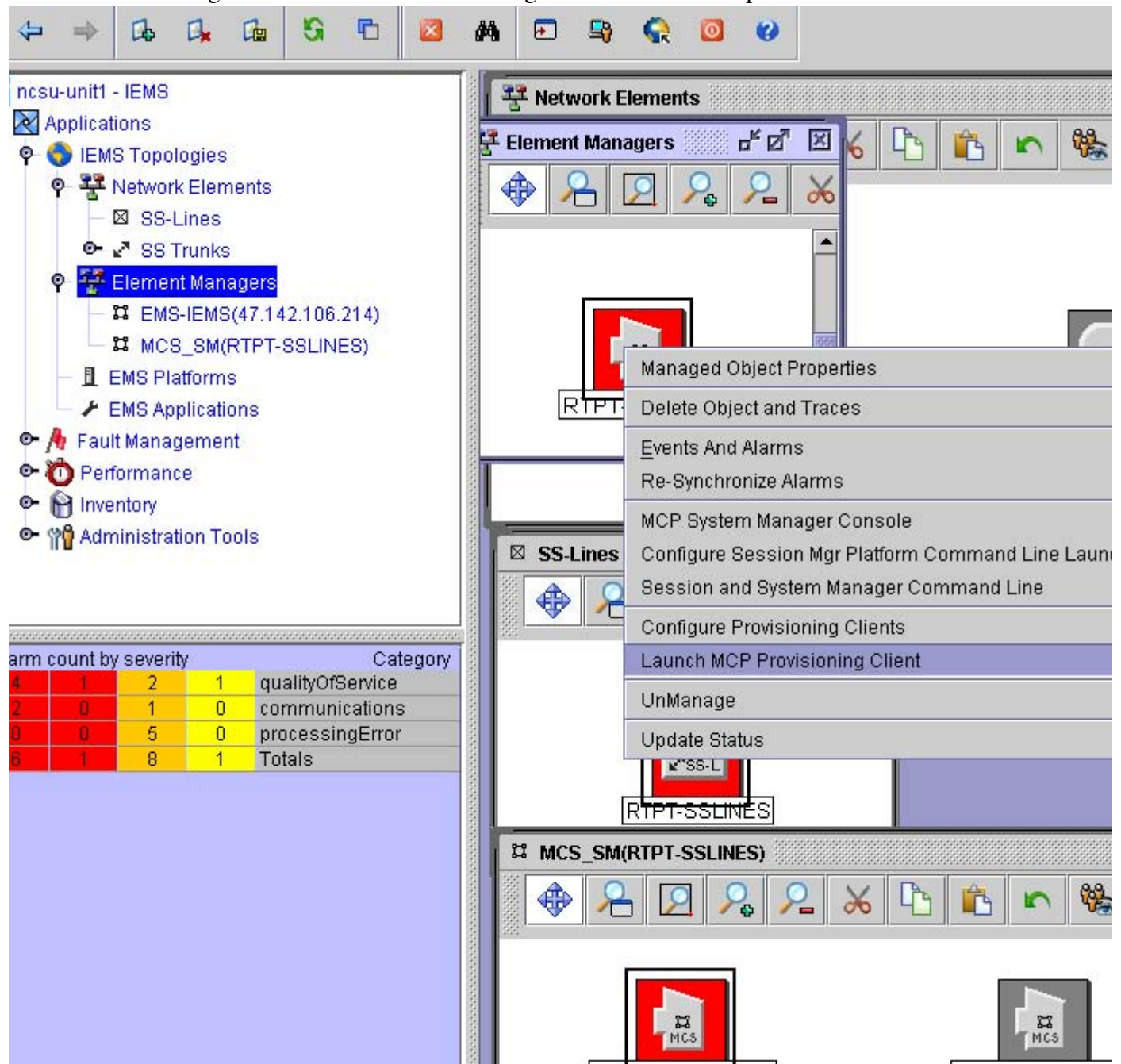


Figure 6 Launch from SSLines Element Manager Map

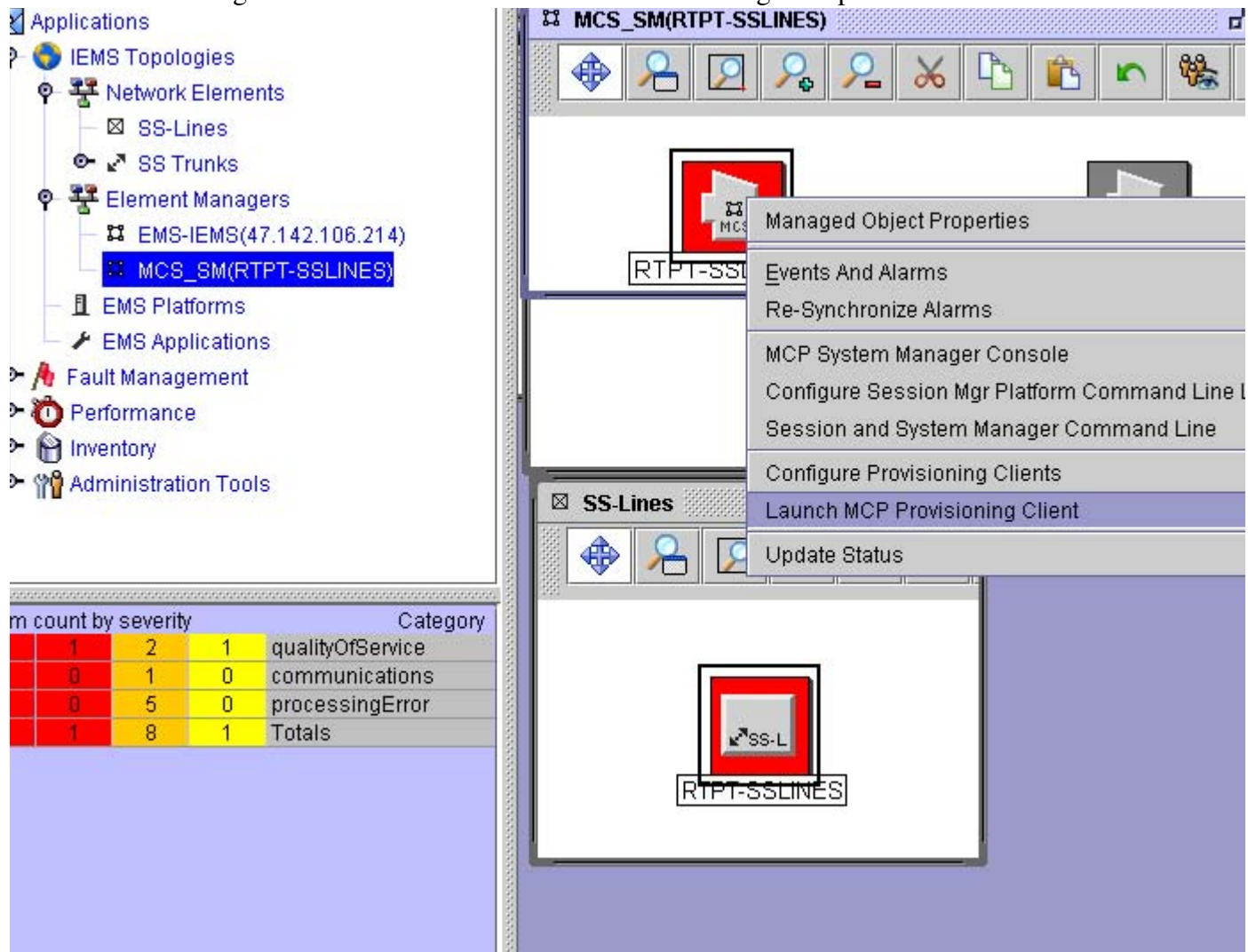
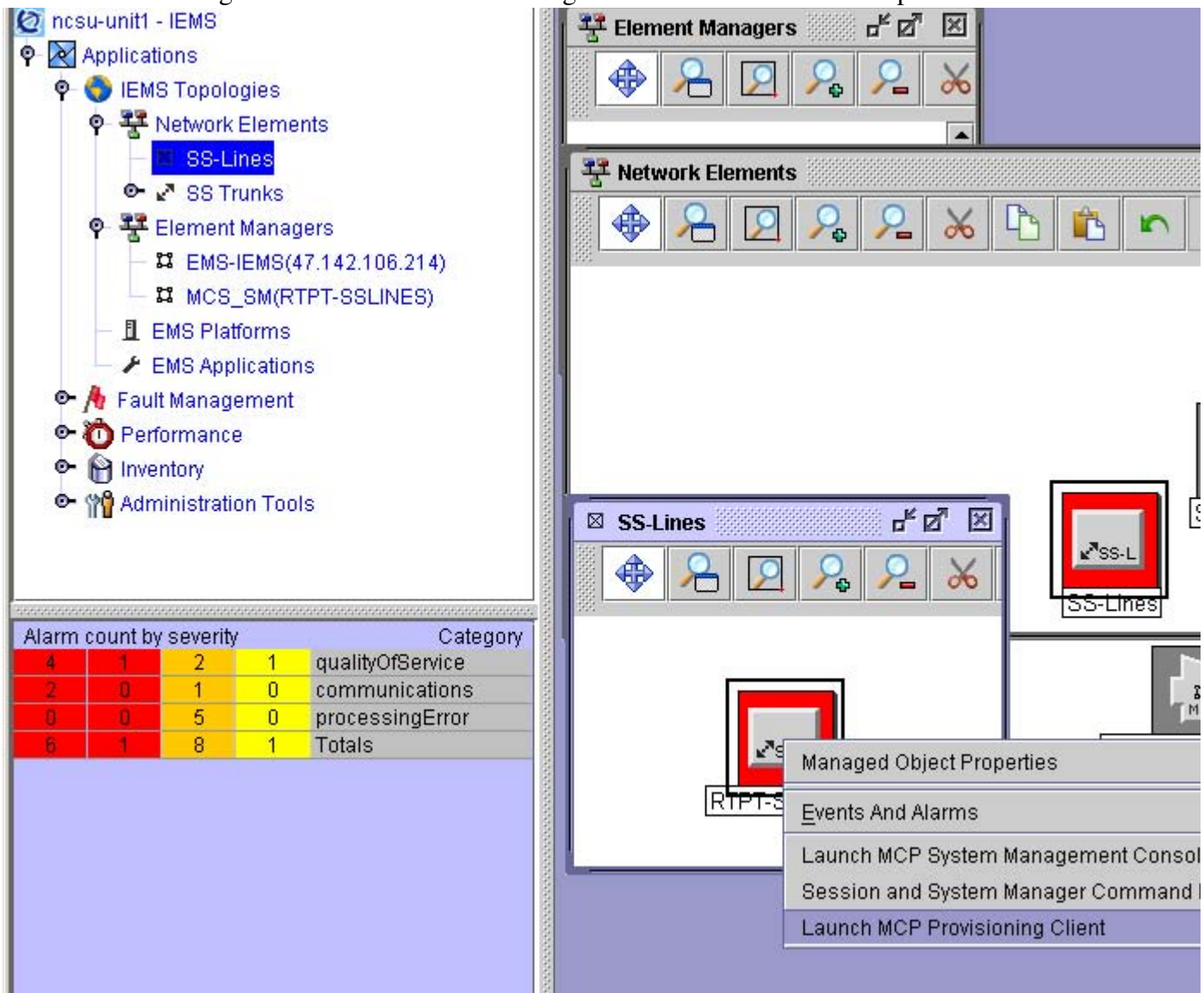
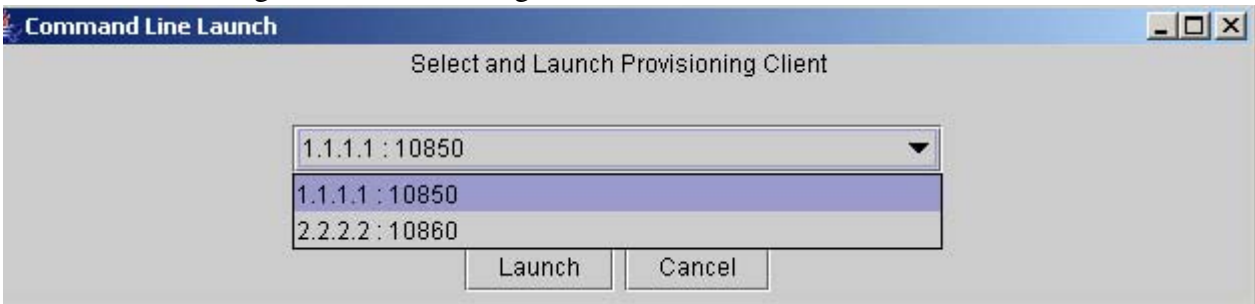


Figure 7 Launch of Provisioning Client from SSLines NE Map



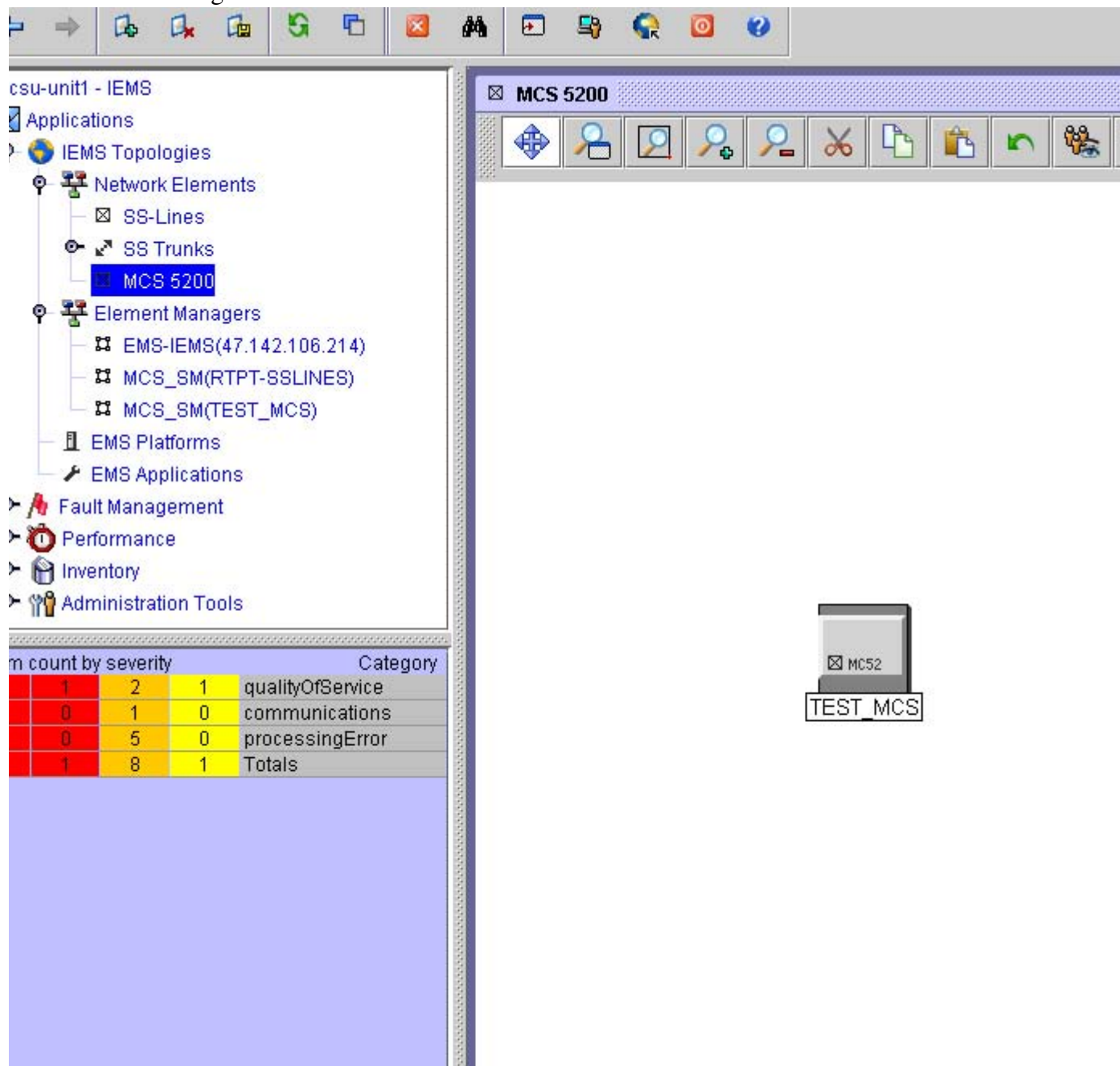
In all cases of launching the Provisioning Client, there will be a combo dialog displayed which will have the user choose which platform to launch the Provisioning Client to as following.

Figure 8 Provisioning Client Launch



The Topology is changed somewhat for the MCS as an MCS/CSE device in the tree display to the following.

Figure 9 MCS MCS/CSE rebranded to MCS 5200



1.5.2 Proxy of MCS system manager and Provisioning client

As mentioned earlier, the MCS system manager console and provisioning client will be launched via the HTTP proxy. Both GUIs communicate with their servers via HTTPS. The apache proxy must be configured using the SSPFS CLI command. These details will be specified in the CN section.

No new ports will need to be opened on the firewall for this component.

1.6 Upgrade Considerations

1.6.1 Upgrade

For an upgrade the SSLines and SStrunks configuration will be stored in the Oracle database as well as the faults and performance data and will be handled with the database upgrade.

1.6.2 Downgrade

For an upgrade the SSLines and SStrunks configuration will be stored in the Oracle database as well as the faults and performance data and will be handled with the database downgrade.

1.7 Security

1.7.1 Network configuration

1.7.2 Key management

1.7.3 Protocol

1.7.4 Authentication

1.8 Hardware Requirements or Dependencies

This feature requires the SIP Lines components to reside on the Langley Linux platform.

1.9 Software Requirements or Dependencies

This will require an SN09 or later version of SSPFS.

1.10 Limitations and restrictions

Log streaming and bulk import and export will not be supported for the proxied system manager launch (see Section 2.6.2).

1.11 Interactions

N/A.

1.12 Glossary

Term	Description
IEMS	Integrated Element Management System

2: Configuration Management for A00012001

All screen shots captured in this version are draft documents and this document will be updated when the official versions are complete.

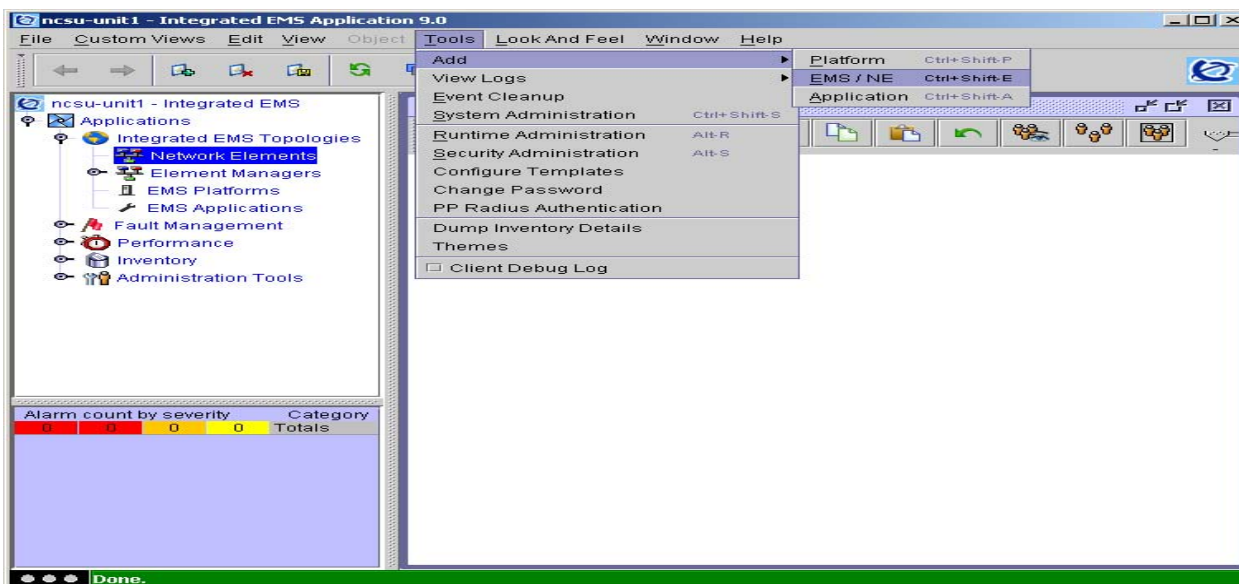
2.1 Hardware and Software Requirements

The feature requires IEMS to be installed on SN10 or later SSPFS loads.

2.2 Addition of an SSLines Mgr

The SSLines configuration is similar to that of the MCS Mgr device in SN08, only shown here is the configuration of the first panel as all the other components are the same.

Figure 1 Getting add panel



From this add panel, the SSLines option must be chosen.

Figure 2 Selecting SSLines Mgr

Add EMS,NE----ncsu-unit1

Add EMS,NE Details

Host Name / IP Address: comp5iems

Time Zone: America/New_York

Display Name: Test_SSLines

Type: EMS

Device Type: APS Mgr

Device Version:

Platform:

Device Type dropdown options:

- GWC Mgr
- MCS Mgr
- MG9K Mgr
- Preside MDM
- SAM21 Mgr
- UNEM Mgr
- UAS Mgr
- SSLines Mgr**

Buttons: Back, Next, Help, Cancel, Add

After this, the IP addresses for the System Manager platform and username are entered as follows. As shown below, the default is duplex for the SSLines or SIP lines on the Langley hardware.

Figure 3 Setting configuration data.

Add EMS,NE----ncsu-unit1

Add EMS,NE Details

Host Name / IP Address	47.142.91.165
Time Zone	America/New_York
Display Name	RTPT-SSLINES
Type	EMS
Device Type	SSLines Mgr
Device Version	9.0
Platform	None
	Duplex
Unit 0 IP Address/Host Name	47.142.91.163
Unit 1 IP Address/Host Name	47.142.91.150
User Name	nortel

Back Next Help Cancel

Add

The other configuration screens are configured like the MCS Mgr configuration in SN08. Please see the SN08 documentation for those references.

2.3 Addition of an SStrunks NE

The SStrunks is the SN10 rebranded name of the Session Server. Following is a screen shot of the add panel. All SN08 configuration parameters are present in the SN10 version.

After the add node is selected, select Type as NE

Figure 4 Selecting Type as NE

A screenshot of a configuration form with a light gray background. The form contains several fields with labels on the left and input controls on the right. The fields are: 'Type' with a dropdown menu showing 'NE'; 'Device Type' with a dropdown menu showing 'EMS' and 'NE' (highlighted); 'Device Version' with a dropdown menu showing '9.0'; 'Mode' with a dropdown menu showing 'Simplex'; and 'Card Location' with an empty text box. The form is titled 'Display Name' at the top left.

Then the Device Type of SS Trunks is chosen:

Figure 5 Select Device Type of SS Trunks

A screenshot of a configuration form with a light gray background. The form contains several fields with labels on the left and input controls on the right. The fields are: 'Time Zone' with a dropdown menu showing 'America/New_York'; 'Display Name' with an empty text box; 'Type' with a dropdown menu showing 'NE'; 'Device Type' with a dropdown menu showing 'CICM' and 'SS Trunks' (highlighted); 'Device Version' with a dropdown menu showing 'CICM', 'ERS 8600', 'MAS', 'MG 3200', 'MS 2000', 'SS Trunks', 'STORM', and 'USP'; 'Mode' with an empty text box; and 'Card Location' with an empty text box. The form is titled 'Display Name' at the top left.

All configuration after the Device Type is chose is the same as SN08, please see the SN08 documentation for details.

2.4 Change of configuration for Media Proxy to Media Portal

The Media Proxy NE type has been changed to Media Portal as shown below.

Figure 6 Addition of MCS with Media Portal as NE

The screenshot shows a Windows-style dialog box titled "Add EMS,NE----ncsu-unit 1". Inside the dialog, there is a section titled "Add EMS,NE Details" containing several fields and dropdown menus:

- Host Name / IP Address: Text input field.
- Time Zone: Dropdown menu showing "America/New_York".
- Display Name: Text input field.
- Type: Dropdown menu showing "EMS".
- Device Type: Dropdown menu showing "MCS Mgr".
- Device Version: Dropdown menu showing "9.0".
- Platform: Dropdown menu showing "None".
- Managing NE type: Dropdown menu showing "MCS/CSE MX".
- Mode: A list box showing "MCS/CSE MX" and "Media Portal" (which is highlighted).
- User Name: Text input field.

At the bottom of the dialog, there are four buttons: "Back", "Next", "Help", and "Cancel". Below these buttons is a green bar with the word "Add" in white text.

2.5 Configuring Session Managers for SSH launch

There is a requirement to be able to launch SSH directly to the Session Managers. To fulfill this requirement a new option needs to be added to allow the configuration of these Session Managers. This new option will be allowed from the EM in the MAP for SSLines.

Figure 7 Example launch of configure session manager

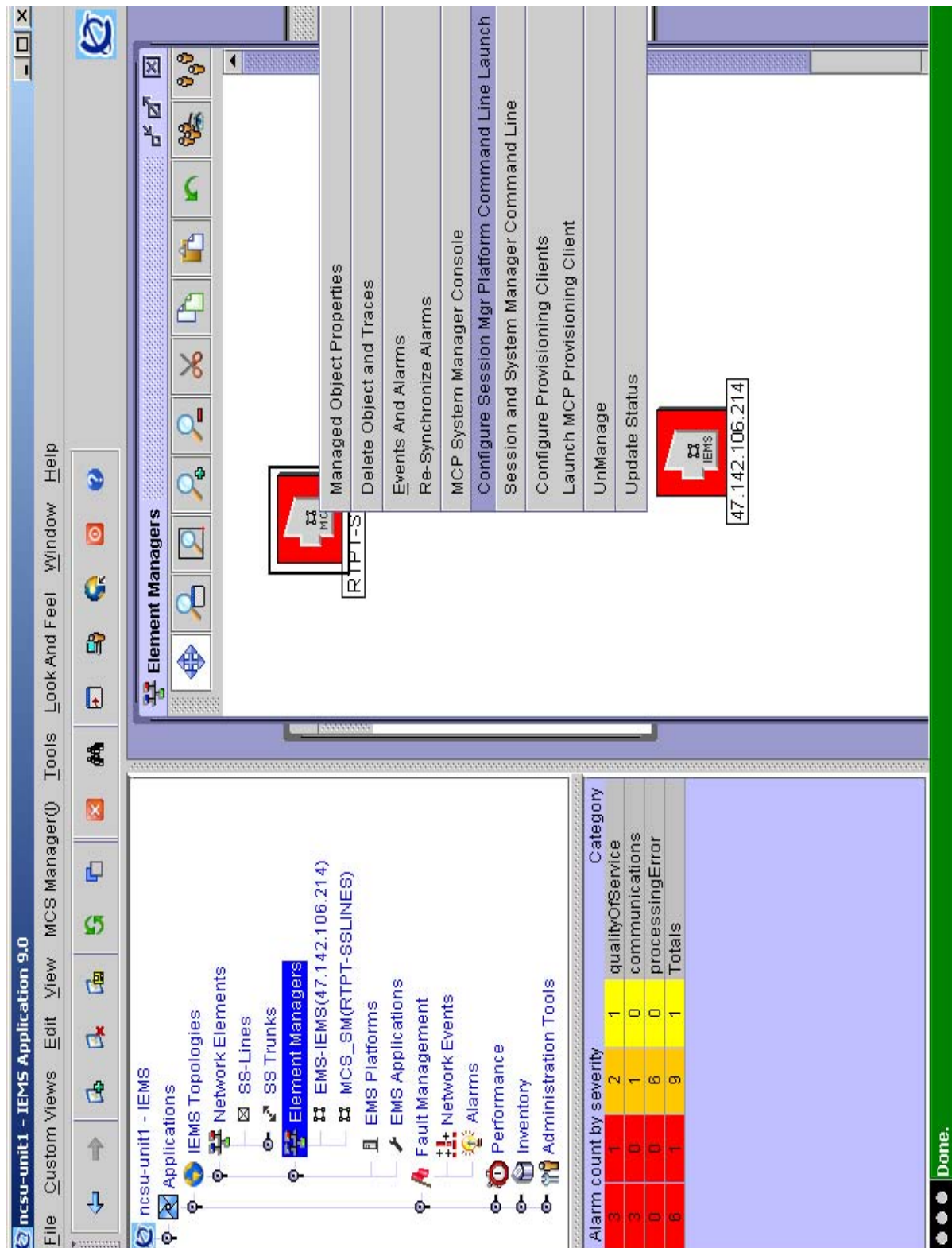


Figure 8 Or from MCS_SM map view

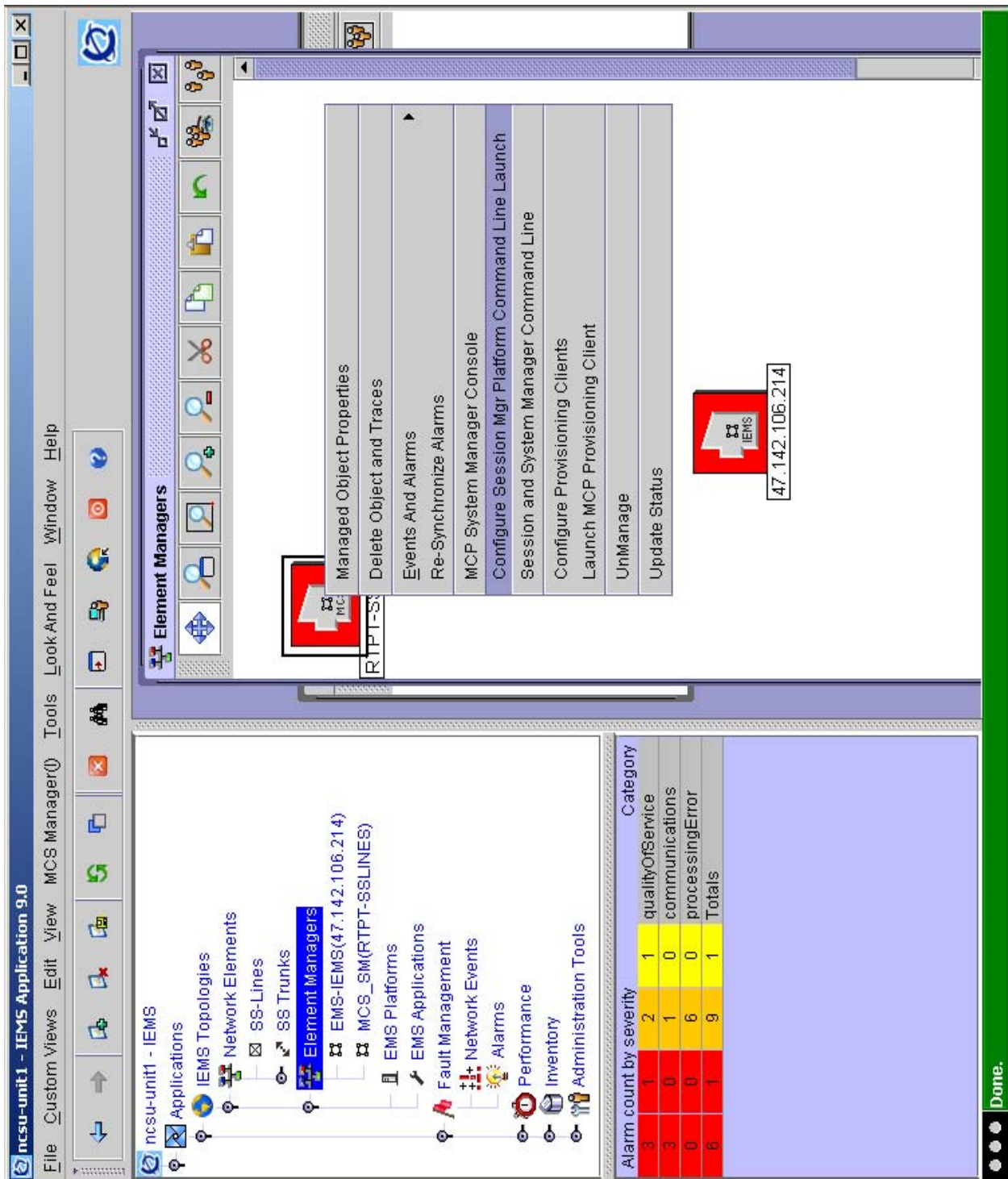


Figure 9 Configuring session managers that can have SSH launched to them

	Name	IP Address	User Name
Unit 0		1 . 1 . 1 . 1	
Unit 1		2 . 2 . 2 . 2	
Unit 0		3 . 3 . 3 . 3	
Unit 1		4 . 4 . 4 . 4	
Unit 0		5 . 5 . 5 . 5	
Unit 1		6 . 6 . 6 . 6	

OK Add Session Manager Remove Session Manager Cancel

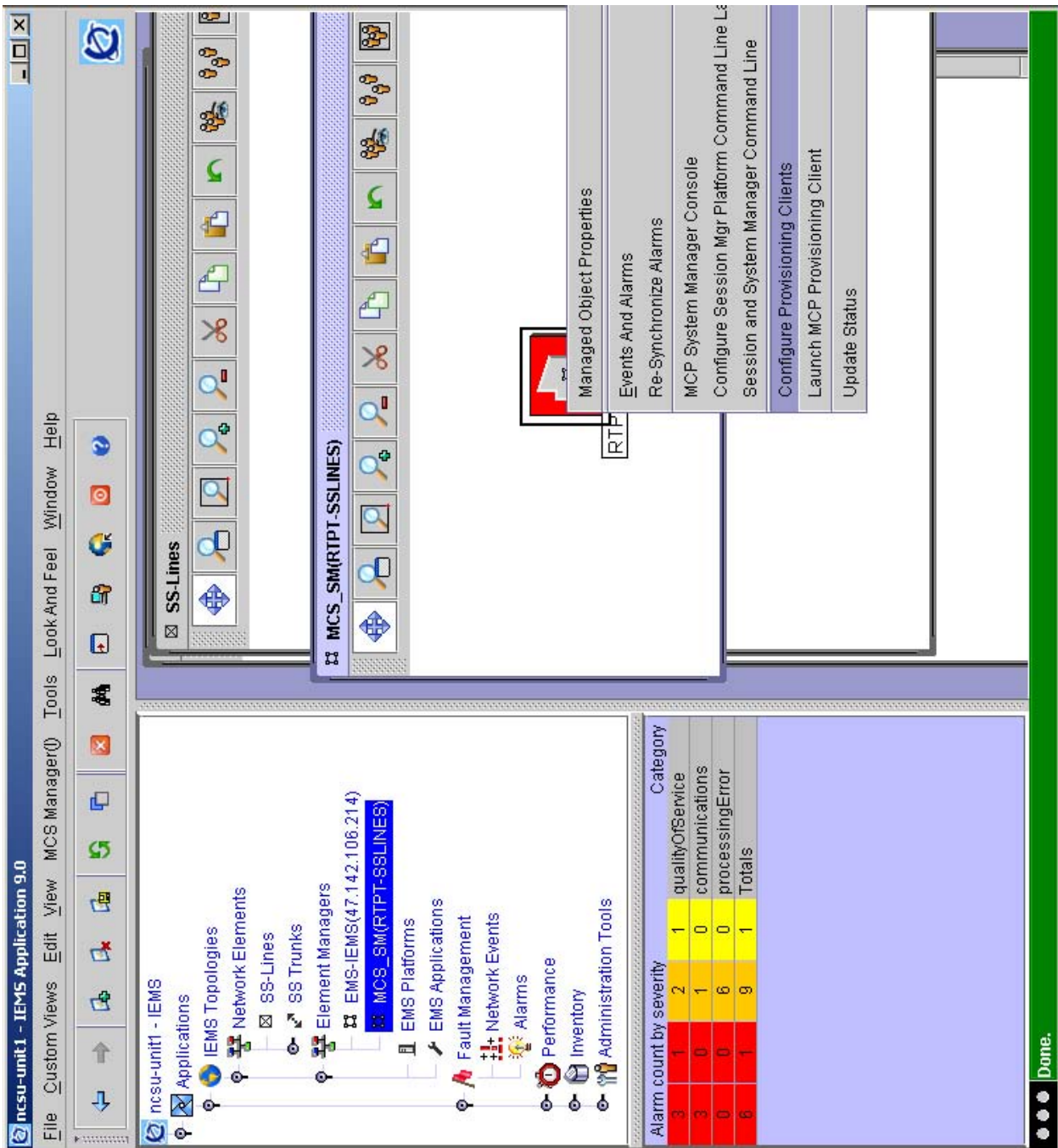
As noticed there can be 3 Session Manager pairs configured. This is a fully configured deployment.

The Add Session Manager and Remove Session Manager adds and removes a pair from the configuration screen. Only the Session Managers that are configured will be configured in the IEMS database.

2.6 Configuring Session Managers for SSH launch

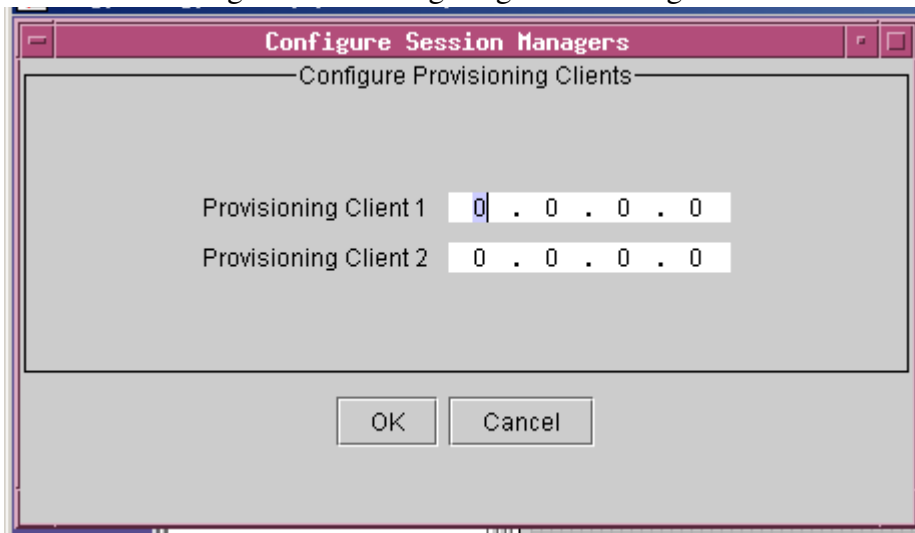
There is a requirement to be able to launch the Provisioning Client wherever they are running on the Sip lines deployment. To fulfill this requirement a new option needs to be added to allow the configuration of the IP addresses of where the provisioning servers are running. This new option will be allowed from the EM in the MAP for SSLines. These are not duplex or clustered.

Figure 10 Example launch of configuring Provisioning Client



The configuration of the provision clients can be done from either the MCS_SM map or from the Element Managers Map. Until the configuration is done, the provisioning clients cannot be launched.

Figure 11 Configuring Provisioning Clients for later launch



After the configuration the following dialog will be displayed. As the dialog indicates the WEBSERVER requires a restart prior to launching the provisioning client. The commands on the sspfs to restart the WEBSERVER is

servrestart WEBSERVER

Figure 12 Restart WEBSERVER dialog



2.7 Configuring the apache proxy using CLI

The apache webserver on the IEMS server machine must be configured to proxy https communication between the MCP management console and the system manager. The proxy is configured using the SSPFS cli tool.

The proxy configuration must be manually removed when the SSL lines platform is deprovisioned from IEMS.

MCP management console proxy configuration

An entry is required for each managed NE.

Procedure (adding an entry):

1. Login into the IEMS server box as root and invoke the “cli” command:

```
#cli
```

Select option 2 (Configuration), then option 2 (Apache Proxy Configuration), then option 1 (add_proxy_conf).

2. Configure the proxy as shown below:

When prompted for the proxy IP address enter the system manager IP address. (Use the virtual IP address for an HA system).

When prompted for the “hostname/tag associated the IP” again enter the address of the system manager followed by the tag “:12121”. For example for a system manager on IP address 47.142.77.88 you would enter 47.142.77.88:12121

When prompted for the optional remote hostname/tag, leave blank and hit “Enter”

When prompted for the port number enter the value “12121”

Answer “Y” when prompted to restart the Apache server.

Repeat the steps above for the other provisioning client IP address.

The session below shows the proxy configuration for a system manager at IP address 47.142.23.24:

```
# 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 - Security Services Configuration*
- 14 - Login Session*
- 15 - Location Configuration*
- 16 - Cluster Configuration*
- 17 - Succession Element Configuration*
- 18 - snmp_poller (SNMP Poller Configuration)*
- 19 - backup_config (Backup Configuration)*

X - exit

select - 2

Apache Proxy Configuration

- 1 - add_proxy_conf (Add an IP to the Apache Proxy Module configuration)*
- 2 - del_proxy_conf (Delete an IP from the Apache Proxy Module configuration)*
- 3 - list_proxy_conf (List the Apache Proxy Module configuration)*

X - exit

select - 1

=== Executing “add_proxy_conf”

Enter proxy IP address (X to exit): 47.142.23.24

Enter hostname/tag associated with IP 47.142.23.24: 47.142.23.24:12121

Optional, enter remote hostname/tag associated with IP 47.142.23.24:

Enter port number [443]: 12121

Accept the following values:

IP Address = 47.142.23.24

Hostname = 47.142.23.24:12121

Remote Tag =

Port Num = 12121

!!WARNING!! This will result in WEBSERVER going down (restarting) for a short time

Continue? [Y/N]:Y

Stopping group using servstop

Apache Web Service Stopping

WEBSERVER Stopped

Starting WEBSERVER through servstart

Updated alarm successfully.

Found valid security certificate, starting Web Services with SSL support...

Apache Web Service Starting

WEBSERVER Started

=== “add_proxy_conf” completed successfully

Apache Proxy Configuration

1 - add_proxy_conf (Add an IP to the Apache Proxy Module configuration)

2 - del_proxy_conf (Delete an IP from the Apache Proxy Module configuration)

3 - list_proxy_conf (List the Apache Proxy Module configuration)

X - exit

select - select - (X, 1-3) X

Procedure (removing an entry):

The procedure for removing a proxy entry is virtually identical to the procedure for adding an entry:

1. Login into the IEMS server box as root and invoke the “cli” command:

#cli

Select option 2 (Configuration), then option 2 (Apache Proxy Configuration), then option 1 (del_proxy_conf).

2. Delete the proxy entry by entering the provisioning IP address and port number when prompted.

The example session snippet below shows the IP address 47.142.24.23 being removed from the configuration:

Apache Proxy Configuration:

1 - add_proxy_conf (Add an IP to the Apache Proxy Module configuration)

2 - del_proxy_conf (Delete an IP from the Apache Proxy Module configuration)

3 - list_proxy_conf (List the Apache Proxy Module configuration)

X - exit

select - 2

=== Executing “del_proxy_conf”

Enter proxy IP address (X to exit): 47.142.23.24

Optional, enter remote hostname/tag associated with IP 47.142.23.24:

Enter port number [443]: 12121

Accept the following values:

IP Address = 47.142.23.24

Remote Tag =

Port Num = 12121

!!WARNING!! This will result in WEBSERVER going down (restarting) for a short time

Continue Removal? [Y/N]:Y

Stopping group using servstop

Apache Web Service Stopping

WEBSERVER Stopped

Starting WEBSERVER through servstart

Alarm exists, updating alarm...

ComponentID:

CLASS=SEC;CLASSTYPE=EXPIRED;SUBTYPE=HTTPSCERT;FILE=validcert.ksh

Updated alarm successfully.

Found valid security certificate, starting Web Services with SSL support...

Apache Web Service Starting

WEBSERVER Started

=== "del_proxy_conf" completed successfully

Product = IEMS

A00012843--IEMS Support for MDM Security Interface Changes

Functional Description

1: Applicable Solution(s)

UA-IP

1.1 Description

In SN09 MDM changes their security interface, MDM client is moving from a PAM Radius client to a PAM IS Client, so it will no longer require a Radius secret configuration in IEMS.

To support this change in MDM, IEMS requires the following design changes:

1. Remove the Radius Secret field from the MDM Mgr Addition wizard when adding a new SN09 or later MDM Element Manager. See Figure 1.

The screenshot shows a Windows-style dialog box titled "Add EMS,NE----zsups3f8". Inside, there's a section titled "Add EMS,NE Details". It contains several configuration fields: "Host Name / IP Address" (text input), "Time Zone" (dropdown menu showing "Etc/GMT+12"), "Display Name" (text input), "Type" (dropdown menu showing "EMS"), "Device Type" (dropdown menu showing "MDM"), "Device Version" (dropdown menu showing "9.0"), "Platform" (dropdown menu showing "MDM"), and "Mode" (dropdown menu showing "Simplex"). Below these is a checkbox labeled "Radius Secret" which is checked. The text input field next to it is circled in red. At the bottom of the dialog are four buttons: "Back", "Next", "Help", and "Cancel". Below these buttons is a green bar with the word "Add" in white text.

Figure 1 MDM Addition wizard

2. Disable the Update Radius Secret menu item from the MDM Element Manager's menu when it is a SN09 or later MDM Element Manager. See Figures 2 and 3.

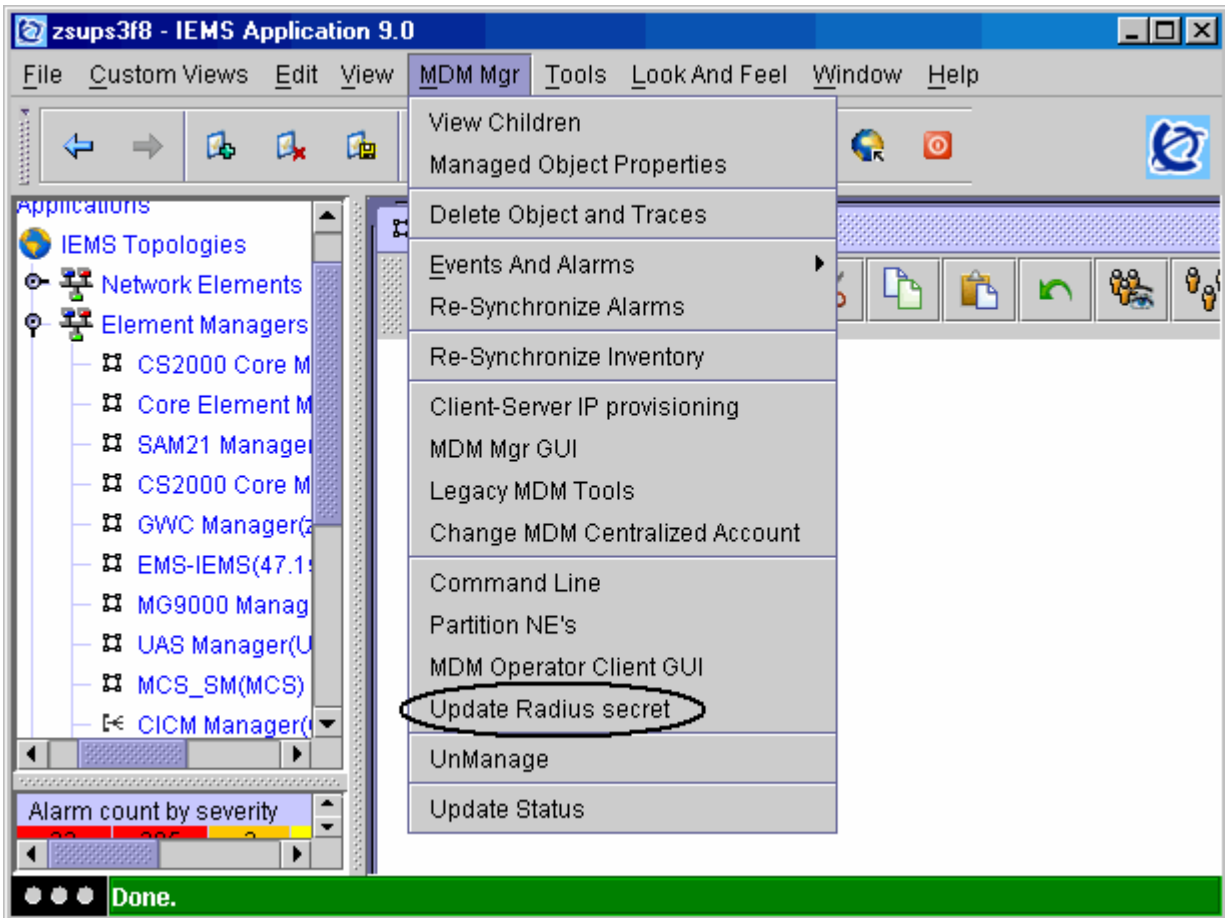


Figure 2 MDM Mgr Menu

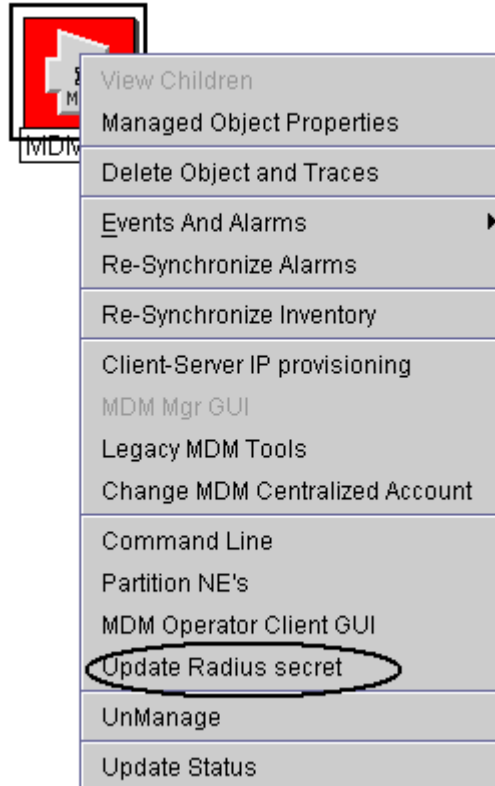


Figure 3 MDM Mgr Right Click Popup Menu

48.1 Hardware Requirements or Dependencies

N/A

48.2 Software Requirements or Dependencies

This Feature requires the following applications:

- IEMS Application Server SN09.1
- IEMS Security Server, MFT V1.1.0
- SN09 MDM Mgr R15.3
- SN08 MDM Mgr R15.2

48.3 Limitations and restrictions

N/A

48.4 Interactions

There are no interactions between this feature and existing features.

48.5 Glossary

RADIUS - Remote Authentication Dial-In User Service

IEMS - Integrated Element Management System

GUI - Graphical User Interface

EM - Element Manager

NE - Network Element

CLI - Command Line Interface

PAM - Pluggable Authentication Module

Product = IEMS

A00012905--ERS8600 Alarm Mapping Correction in IEMS *Corrective CAF*

1: Applicable Solution(s)

UA-IP

1.1 Description

This feature corrects ERS8600 alarm mappings defined in IEMS system. No user interfaces will be changed in this corrective CAF.

From SN08, some ERS8600 traps have an incorrect mapping relationship with IEMS fault code. This causes unknown and misunderstanding alarms or events in IEMS system. Refer to the FM section of this feature for the content changes of some alarms and events.

This feature will be delivered in SN09-FF release.

1.2 Hardware Requirements or Dependencies

N/A

1.3 Software Requirements or Dependencies

This Feature requires the following applications:

- IEMS Application Server SN09-FF

- SN09 ERS 8600 V3.7.2.2

1.4 Limitations and restrictions

N/A

1.5 Interactions

There are no interactions between this feature and existing features.

1.6 Glossary

IEMS - Integrated Element Management System

ERS 8600 – Ethernet Routing Switch 8600

2: Fault Management for A00012905

2.1 Fault management strategy

The ERS8600 faults descriptions in IEMS was outstanding until now. In SN09-FF feature A00012905, several ERS8600 faults severities were changed. This feature is intended to enhance the existing mapping of the ERS8600 events and provide the associated customer documentation in the “Carrier Voice over IP Fault Management Logs Reference manual (NN10275-909)” and the “Carrier VOIP OSS Guide Advanced Feature Guide” for ERS8600 faults.

In this document, all the ERS8600 faults will be described in the following.

2.2 Fault management tools and utilities

In a Carrier VOIP CS2000 central office the ERS8600s should be configured to forward their SNMP traps to the IEMS. The IEMS mediates these SNMP traps converting them into normalized customer log events. This normalization process provides the following:

- Converts the ERS8600 SNMP TRAPs into an alarm raise, alarm clear or an info customer log event.
- These normalized events are forwarded to the IEMS northbound interfaces (SCC2, NTstd, custlog, SNMP). Please refer to the “OSS Guide Advance Feature Guide” (PLN-i09-OSS) for a description of these northbound interfaces.
- Correlates these incoming SNMP TRAPs to a ERS8600 configured in the IEMS inventory.
- Persists these normalized events in the IEMS server allowing the craftperson to view them in the IEMS event browser (which provides both a real-time and

historical view of all ERS8600 normalized events) and alarm browser (which provides a real-time view of the incoming ERS8600 alarms).

2.3 ERS8600 alarm clearing policy

When working with the ERS8600 faults in the IEMS it is important to understand how these alarms are cleared. The ERS8600 does not support an interface that allows a northbound manager (i.e., the IEMS) the ability to resync with the ERS8600 alarm states. In addition, the ERS8600 does not support a direct mapping between all of its alarm raise events and clear events it sends. As a result the ERS8600 alarms can be cleared one of six ways from the IEMS alarm view (i.e., the IEMS alarm browser). These include:

- The ERS8600 sends a clear for an associated alarm that it previously raised. The IEMS performs the correlation between raise and clear and removes the associated alarm from the IEMS alarm view. It is important to note that the ERS8600 does not send an explicit clear event for all the ERS8600 alarms that are raised.
- Performing a manual clear in the IEMS alarm browser. This allows a craftperson to remove an alarm in the IEMS view that is no longer active in the ERS8600 (Note: This only clears the alarm in the IEMS).
- Performing a manual delete in the IEMS alarm browser. This allows a craftperson to remove an alarm in the IEMS view that is no longer active in the ERS8600 (Note: This only clears the alarm in the IEMS).
- IEMS Age based clearing Policy: This mechanism utilizes an automated alarm ageing clearing policy in the IEMS server. The alarm clearing job (refer to the 'administration tools | jobs | alarm clearing policy' in the IEMS JWS client) clears all alarms from the IEMS view for the configured device types based upon the alarms age. By default this policy is configured to clear all alarms that are older than 7 days. In addition, by default, the ERS8600 device type is included in this policy. This policy ensures that ERS8600 alarms do not continue to accumulate in the IEMS alarm view (Note: This only removes the alarm in the IEMS).
- IEMS NB SNMP Agent clear request. (Note: This only removes the alarm in the IEMS).
- Executing the `/opt/nortel/iems/current/bin/purgeTempData.sh` script on the IEMS server. Please note that this clears all alarm, event and performance data history for all devices on the IEMS server.

2.4 Alarms brief overview

This table contains all the ERS8600 alarms in the IEMS side. They will be described in the following sections.

Alarm Index	Alarm Name	Trap OID (v2c)	MDM Fault Code (Hex)	IEMS Event (severity)	SN09 IEMS log	Correction in IEMS SN09-FF
1	risingAlarm	1.3.6.1.2.1.16.0.1	S C1220008	minor	PP 310	
2	fallingAlarm	1.3.6.1.2.1.16.0.2	S C1220008	clear	PP 311	
3	Default Trap	DEFAULT	S C1229999	indeterminate	PP 312	
4	coldStart	1.3.6.1.6.3.1.1.5.1.0	S C0000000	clear	PP 313	info
5	warmStart	1.3.6.1.6.3.1.1.5.2.0	S C0000001	clear	PP 315	info
6	linkDown	1.3.6.1.6.3.1.1.5.3.0	S C0000002	major	PP 317	
7	linkUp	1.3.6.1.6.3.1.1.5.4.0	S C0000002	clear	PP 318	
8	authenticationFailure	1.3.6.1.6.3.1.1.5.5.0	S C0000004	warning	PP 319	
9	rcnChasPowerSupplyDown	1.3.6.1.4.1.2272.1.21.0.6	S C1220007	critical	PP 322	
10	rcnChasPowerSupplyUp	1.3.6.1.4.1.2272.1.21.0.14	S C1220007	clear	PP 323	
11	rcnChasFanDown	1.3.6.1.4.1.2272.1.21.0.7	S C1220006	critical	PP 324	
12	rcnChasFanUp	1.3.6.1.4.1.2272.1.21.0.21	S C1220006	clear	PP 325	
13	rcn2kCardDown	1.3.6.1.4.1.2272.1.21.0.11	S C1220001	major	PP 326	critical
14	rcn2kCardUp	1.3.6.1.4.1.2272.1.21.0.12	S C1220001	clear	PP 327	
15	rcn2kTemperature	1.3.6.1.4.1.2272.1.21.0.13	S C1220003	critical	PP 328	critical/ clear
16	rcnErrorNotification	1.3.6.1.4.1.2272.1.21.0.3	S C1220009	warning, major, critical	PP 329	
17	rcnLinkOscillation	1.3.6.1.4.1.2272.1.21.0.8	S C122000A	major	PP 330	
18	rcnMacViolation	1.3.6.1.4.1.2272.1.21.0.9	S C122000B	warning	PP 331	critical
19	rcnSonetTrap	1.3.6.1.4.1.2272.1.21.0.10	S C1220051	warning	PP 332	
20	rcnStpNewRoot	1.3.6.1.4.1.2272.1.21.0.4	S C122000C	warning	PP 333	
21	rcnStpTopologyChange	1.3.6.1.4.1.2272.1.21.0.5	S C122000D	warning	PP 334	
22	rcnStpTCN	1.3.6.1.4.1.2272.1.21.0.16	S C1220017	warning	PP 335	
23	rcn2kAtmPvcLinkStateChange	1.3.6.1.4.1.2272.1.21.0.15	S C1220012	info, minor, major/ clear	PP 336	
24	rcnSmlt1stLinkUp	1.3.6.1.4.1.2272.1.21.0.17	S C1220014	clear	PP 337	
25	rcnSmlt1stLinkDown	1.3.6.1.4.1.2272.1.21.0.18	S C1220014	major	PP 338	
26	rcnSmltLinkUp	1.3.6.1.4.1.2272.1.21.0.19	S C1220020	clear	PP 339	
27	rcnSmltLinkDown	1.3.6.1.4.1.2272.1.21.0.20	S C1220020	major	PP 340	
28	rcnPasswordChange	1.3.6.1.4.1.2272.1.21.0.22	S C1220022	warning	PP 341	

Alarm Index	Alarm Name	Trap OID (v2c)	MDM Fault Code (Hex)	IEMS Event (severity)	SN09 IEMS log	Correction in IEMS SN09-FF
29	rcnPcmciaCardRemoved	1.3.6.1.4.1.2272.1.21.0.25	S C1220049	warning	PP 342	critical
30	rcnSmartCpldTimerFired	1.3.6.1.4.1.2272.1.21.0.26	S C1220024	major	PP 343	
31	rcnCardCpldNotUpDate	1.3.6.1.4.1.2272.1.21.0.27	S C1220025	warning	PP 344	major
32	rcnlgapLogFileFull	1.3.6.1.4.1.2272.1.21.0.28	S C1220026	major	PP 345	
33	rcnCpLimitShutDown	1.3.6.1.4.1.2272.1.21.0.29	S C1220027	major	PP 346	
34	rcnSshServerEnabled	1.3.6.1.4.1.2272.1.21.0.30	S C1220028	clear	PP 347	
35	rcnSshServerDisabled	1.3.6.1.4.1.2272.1.21.0.31	S C1220028	major	PP 348	
36	rcnSshSessionLogin	1.3.6.1.4.1.2272.1.21.0.32	S C1220029	clear	PP 349	info
37	rcnSshSessionLogout	1.3.6.1.4.1.2272.1.21.0.33	S C1220029	major	PP 350	info
38	rcnSshUnauthorizedAccess	1.3.6.1.4.1.2272.1.21.0.34	S C1220030	major	PP 351	critical
39	rcnHaCpuState	1.3.6.1.4.1.2272.1.21.0.35	S C1220031	warning	PP 352	critical
40	rcnInsufficientMemory	1.3.6.1.4.1.2272.1.21.0.36	S C1220032	warning	PP 353	critical
41	rcnSaveConfigAction	1.3.6.1.4.1.2272.1.21.0.37	S C1220033	info	PP 354	
42	rcnLoopDetectOnPort	1.3.6.1.4.1.2272.1.21.0.38	S C1220034	warning	PP 355	critical
43	vrrpTrapStateTransition	1.3.6.1.2.1.46.1.3.0.3.0	S C1220048	warning	PP 356	critical
44	rcnEmError	1.3.6.1.4.1.2272.1.21.0.23	S C1220023	warning	PP 357	
45	ospfVirtIfStateChange	1.3.6.1.2.1.14.16.2.1	S C1220015	warning/clear	PP 358	
46	ospfNbrStateChange	1.3.6.1.2.1.14.16.2.2	S C1220011	warning/clear	PP 359	
47	ospfVirtNbrStateChange	1.3.6.1.2.1.14.16.2.3	S C1220016	minor/clear	PP 360	
48	ospfIfConfigError	1.3.6.1.2.1.14.16.2.4	S C122000F	major	PP 361	critical
49	ospfVirtIfConfigError	1.3.6.1.2.1.14.16.2.5	S C1220021	major	PP 362	critical
50	ospfIfAuthFailure	1.3.6.1.2.1.14.16.2.6	S C122000E	major	PP 363	critical
51	ospfVirtIfAuthFailure	1.3.6.1.2.1.14.16.2.7	S C1220013	major	PP 364	critical
52	ospfIfStateChange	1.3.6.1.2.1.14.16.2.16	S C1220010	warning/clear	PP 365	
53	rcnCardDown	1.3.6.1.4.1.2272.1.21.0.1		major	PP 366	critical
54	rcnCardUp	1.3.6.1.4.1.2272.1.21.0.2		clear	PP 367	
55	rcnbgpEstablished	1.3.6.1.4.1.2272.1.21.0.39	S C1220039	clear	PP 368	clear
56	rcnbgpBackwardTransition	1.3.6.1.4.1.2272.1.21.0.40	S C1220040	critical	PP 369	
57	rcnAggLinkUp	1.3.6.1.4.1.2272.1.21.0.41	S C1220041	clear	PP 370	
58	rcnAggLinkDown	1.3.6.1.4.1.2272.1.21.0.42	S C1220041	clear	PP 371	major

Alarm Index	Alarm Name	Trap OID (v2c)	MDM Fault Code (Hex)	IEMS Event (severity)	SN09 IEMS log	Correction in IEMS SN09-FF
59	rcnIcmpNewGroupMember	1.3.6.1.4.1.2272.1.21.0.43	S C1220042	clear	PP 372	info
60	rcnIcmpLossGroupMember	1.3.6.1.4.1.2272.1.21.0.44	S C1220042	clear	PP 373	info
61	rcnIcmpNewQuerier	1.3.6.1.4.1.2272.1.21.0.45	S C1220043	clear	PP 374	info
62	rcnIcmpQuerierChange	1.3.6.1.4.1.2272.1.21.0.46	S C1220044	clear	PP 375	info
63	rcnDvmrplfStateChange	1.3.6.1.4.1.2272.1.21.0.47	S C1220045	clear	PP 376	info
64	rcnDvmrpNewNbrChange	1.3.6.1.4.1.2272.1.21.0.48	S C1220046	clear	PP 377	info
65	rcnDvmrpNbrLossChange	1.3.6.1.4.1.2272.1.21.0.49	S C1220046	clear	PP 378	info
66	rcnFdbProtectViolation	1.3.6.1.4.1.2272.1.21.0.59	S C1220047	clear	PP 379	info
67	rcnLogMsgControl	1.3.6.1.4.1.2272.1.21.0.60	S C1220050	clear	PP 380	info
68	rcnSaveConfigFile	1.3.6.1.4.1.2272.1.21.0.61	S C1220052	clear	PP 381	info
69	rcnDNSRequestResponse	1.3.6.1.4.1.2272.1.21.0.62	S C1220057	clear	PP 382	info
70	pingProbeFailed	1.3.6.1.2.1.80.0.1.0	S C1220053	clear	PP 383	info
71	pingTestFailed	1.3.6.1.2.1.80.0.2.0	S C1220054	clear	PP 384	info
72	pingTestCompleted	1.3.6.1.2.1.80.0.3.0	S C1220054	clear	PP 385	info
73	traceRoutePathChange	1.3.6.1.2.1.81.0.1.0	S C1220055	clear	PP 386	info
74	traceRouteTestFailed	1.3.6.1.2.1.81.0.2.0	S C1220056	clear	PP 387	info
75	traceRouteTestComplete	1.3.6.1.2.1.81.0.3.0	S C1220056	clear	PP 388	info
76	UDPEapSessionEndTrap	1.3.6.1.4.1.562.42.5.1.3.2.2		clear	PP 389	info
77	UDPEapSessionStartTrap	1.3.6.1.4.1.562.42.5.1.3.2.1		clear	PP 390	info
78	rcnDuplicateIpAddress	1.3.6.1.4.1.2272.1.21.0.63		major	PP 391	critical
79	rcnLoopDetectPortDown	1.3.6.1.4.1.2272.1.21.0.64		major	PP 392	critical

Note: IEMS severity definition:

severity = 6|5|4|3|2|1

Critical = 1

Major = 2

Minor = 3

Warning = 4

Clear = 5

Info = 6

An Example entry of ERS8600TrapList.xml

```
<TRAP
  oid = ".1.3.6.1.4.1.2272.1.21.0.45"
  name = "rcnIgmppNewQuerier">
    <PROPERTIES>
      <eventprop name = "severity" value = "6"/>
      <eventprop name = "logName" value = "PP"/>
      <eventprop name = "logNumber" value = "374"/>
      <eventprop name = "eventType" value = "INFO"/>
      <eventprop name = "eventLabel" value = "PP Fault"/>
      <eventprop name = "category" value = "communications"/>
      <eventprop name = "entity" value = "$ip_Querier_$1"/>
      <eventprop name = "componentID" value = "ERS8600=$ip; igmpInterfaceIfIndex=$1"/>
      <eventprop name = "alarmClear" value = "3"/>
      <eventprop name = "probableCause" value = "New Querier in interface"/>
      <eventprop name = "description" value = "New Querier in interface: igmpInterfaceIfIndex = $1
(igmpInterfaceQuerier = $2 )"/>
      <eventprop name = "specificProblem" value = "New Querier in interface"/>
    </PROPERTIES>
    <VARBINDS>
      <varbind name = ".1.3.6.1.3.59.1.1.1.1.1" property = "$1"/>
      <varbind name = ".1.3.6.1.3.59.1.1.1.1.5" property = "$2"/>
    </VARBINDS>
  </TRAP>
```

This table is the ERS8600 raise-clear mappings.

ERS 8600 Trap Raise-Clear Mapping:

Index	Raise Alarm	Clear Alarm
1	RisingAlarm(PP310)	FallingAlarm(PP311)
2	LinkDown (PP317)	LinkUp(PP318)
3	RcnChasPowerSupplyDown / RcChasPowerSupplyDown (PP322)	RcnChasPowerSupplyUp / RcChasPowerSupplyUp (PP323)
4	RcnChasFanDown / RcChasFanDown (PP324)	RncChasFanUp / RnChasFanUp (PP325)
5	Rcn2kCardDown / Rc2kCardDown (PP326)	Rcn2kCardUp / Rc2kCardUp (PP327)
6	RcnSmlt1stLinkDown(PP338)	RcnSmlt1stLinkUp(PP337)
7	RcnSmltLinkDown / RcSmltLinkDown (PP340)	RcnSmltLinkUp / RcSmltLinkUp (PP339)
8	RcnSshServerDisabled(PP348)	RcnSshServerEnabled(PP347)
9	Rcn2kTemperature(PP328)	Rcn2kTemperature(PP328)
10	RcnCardDown / RcCardDown (PP366)	RcnCardUp / RcCardUp (PP367)
11	rcn2kAtmPvcLinkStateChange(PP336)	rcn2kAtmPvcLinkStateChange(PP336)
12	ospfVirtIfStateChange(PP358)	ospfVirtIfStateChange(PP358)

Index	Raise Alarm	Clear Alarm
13	ospfNbrStateChange(PP359)	ospfNbrStateChange(PP359)
14	ospfVirtNbrStateChange(PP360)	ospfVirtNbrStateChange(PP360)
15	ospflfStateChange(PP365)	ospflfStateChange(PP365)
16	rcnAggLinkDown (PP371)	rcnAggLinkUp (PP370)
17	rcnbgpBackwardTransition (PP369)	rcnbgpEstablished (PP368)

About the alarm clearing rule, IEMS judges it from the severity level. If the severity level is 5, IEMS considers it is a clear alarm. For those alarms without explicit corresponding clear alarm, IEMS will clear them when it reaches the age time or the alarms are cleared manually.

2.5 Alarm (PP310)

risingAlarm, Trap OID is 1.3.6.1.2.1.16.0.1

2.5.1 Explanation

The PP310 alarm signifies that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps.

This alarm is set when an alarm threshold is crossed. The text of the alarm message identifies the alarm value that triggered the alarm, the item that was being monitored, and the threshold level.

A rising alarm indicates that the alarm is triggered when the alarm value rises above the threshold value.

A falling alarm indicates that the alarm is triggered when the alarm value falls below the threshold value.

The falling alarm clears the rising alarm.

2.5.2 Action

Please refer to ERS8600 Fault Management document.

2.5.3 Corresponding Clear Log

PP311.

2.5.3.1 Format

2.5.3.2 NTSTD

Not available.

2.5.4 Field descriptions

This alarm has no selected fields.

2.5.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.5.6 Additional information

This alarm requires no additional information.

2.6 Alarm (PP311)

fallingAlarm, Trap OID is 1.3.6.1.2.1.16.0.2

2.6.1 Explanation

The PP311 alarm signifies that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.

2.6.2 Action

Please refer to ERS8600 Fault Management document.

2.6.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.6.3.1 Format

2.6.3.2 NTSTD

Not available.

2.6.4 Field descriptions

This alarm has no selected fields.

2.6.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.6.6 Additional information

This alarm requires no additional information.

2.7 Alarm (PP313)

coldStart, Trap OID is 1.3.6.1.6.3.1.1.5.1.0

2.7.1 Explanation

The PP313 alarm signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.

2.7.2 Action

Please refer to ERS8600 Fault Management document.

2.7.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.7.3.1 Format

2.7.3.2 NTSTD

zsups3f8 PP313 OCT26 01:28:48 0009 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: operator
Cause: Agent reinitialized itself with default settings
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Agent reinitialized itself with default settings
Description: A coldStart trap signifies that the snmp agent is reinitializing itself with default settings.
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.1.0
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.7.4 Field descriptions

Table 1: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

2.7.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.7.6 Additional information

This alarm requires no additional information.

2.8 Alarm (PP315)

warmStart, Trap OID is 1.3.6.1.6.3.1.1.5.2.0

2.8.1 Explanation

The PP315 alarm signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.

2.8.2 Action

Please refer to ERS8600 Fault Management document.

2.8.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.8.3.1 Format

2.8.3.2 NTSTD

zsup3f8 PP315 OCT26 01:28:48 0011 INFO PP Fault

Location: ERS8600_RTP;47.142.106.1

State: None

Category: operator

Cause: Agent reinitialized itself with its configuration unaltered.

Time: Oct 26 01:28:48 2005

Component ID: ERS8600=47.142.106.1

Specific Problem: Agent reinitialized itself with its configuration unaltered.

Description: A warmStart trap signifies that the SNMPv2 agent is reinitializing itself such that its configuration is unaltered.

.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.2.0

.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.8.4 Field descriptions

Table 2: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

2.8.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.8.6 Additional information

This alarm requires no additional information.

2.9 Alarm (PP317)

linkDown, Trap OID is 1.3.6.1.6.3.1.1.5.3.0

2.9.1 Explanation

The PP317 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to transition into the down state.

2.9.2 Action

Please refer to ERS8600 Fault Management document.

2.9.3 Corresponding Clear Log

PP318.

2.9.3.1 Format

2.9.3.2 NTSTD

```
zsups3f8 ** PP317 OCT26 01:28:48 0013 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: communications
Cause: loss of communication
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; ifIndex=100
Specific Problem: Generic Link Status
Description: Link Down: ifIndex = 100(AdminStatus = up OperationStatus
= down Port = 37 Slot = 1)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.3.0
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
```

2.9.4 Field descriptions

Table 3: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, ifIndex and node ID of the device.
OperationStatus	character string	Can be one of {up (1), down (2), testing (3)}
PhysicalInfo	character string	Indicates the physical information appended to OperationStatus. The actual physical information is determined by ifIndex. ifIndex >= 64 and ifIndex <= 703 the information is: Port = '(ifIndex & 0x3f) + 1' Slot = 'ifIndex >>6' ifIndex >= 832 and ifIndex <= 863 the information is: Circuitless IP = 'ifIndex - 832 + 1' ifIndex >= 2048 and ifIndex <= 4095 the information is: VLAN = 'ifIndex - 2048 + 1' ifIndex >= 4096 and ifIndex <= 4127 the information is: MLT = 'ifIndex - 4096 + 1' ifIndex >= 4352 and ifIndex <= 5351 the information is: Tunnel = 'ifIndex - 4352 + 1' An ifIndex not within the above ranges, the information is: unknown of ifIndex meaning Note: The content in “ ” part will be calculated out.

2.9.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.9.6 Additional information

This alarm requires no additional information.

2.10 Alarm (PP318)

linkUp, Trap OID is 1.3.6.1.6.3.1.1.5.4.0

2.10.1 Explanation

The PP318 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links has transitioned out of the down state.

2.10.2 Action

Please refer to ERS8600 Fault Management document.

2.10.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.10.3.1 Format

2.10.3.2 NTSTD

```
zsups3f8    PP318 OCT26 01:28:48 0016 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: communications
Cause: communication regained
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; ifIndex=100
Specific Problem: Generic Link Status
Description: Link Up: ifIndex = 100(AdminStatus = up OperationStatus =
up Port = 37 Slot = 1)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.4.0
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
```

2.10.4 Field descriptions

Table 4: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, ifIndex and node ID of the device.
OperationStatus	character string	Can be one of {up (1), down (2), testing (3)}

Table 4: Field descriptions

Field	Value	Description
PhysicalInfo	character string	Indicates the physical information appended to OperationStatus. The actual physical information is determined by ifIndex. ifIndex ≥ 64 and ifIndex ≤ 703 the information is: Port = '(ifIndex & 0x3f) + 1' Slot = 'ifIndex $\gg 6$' ifIndex ≥ 832 and ifIndex ≤ 863 the information is: Circuitless IP = 'ifIndex - 832 + 1' ifIndex ≥ 2048 and ifIndex ≤ 4095 the information is: VLAN = 'ifIndex - 2048 + 1' ifIndex ≥ 4096 and ifIndex ≤ 4127 the information is: MLT = 'ifIndex - 4096 + 1' ifIndex ≥ 4352 and ifIndex ≤ 5351 the information is: Tunnel = 'ifIndex - 4352 + 1' An ifIndex not within the above ranges, the information is: unknown of ifIndex meaning Note: The content in “ ” part will be calculated out.

2.10.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.10.6 Additional information

This alarm requires no additional information.

2.11 Alarm (PP319)

authenticationFailure, Trap OID is 1.3.6.1.6.3.1.1.5.5.0

2.11.1 Explanation

The PP319 alarm signifies an authenticationFailure on the device.

2.11.2 Action

Please refer to ERS8600 Fault Management document.

2.11.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.11.3.1 Format

2.11.3.2 NTSTD

zsups3f8 PP319 OCT26 01:28:48 0017 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: security
Cause: Authentication failure
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Authentication failure
Description: Authentication failure occurred
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.5.0
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.11.4 Field descriptions

Table 5: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

2.11.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.11.6 Additional information

This alarm requires no additional information.

2.12 Alarm (PP322)

rcnChasPowerSupplyDown, Trap OID is 1.3.6.1.4.1.2272.1.21.0.6

2.12.1 Explanation

The PP322 alarm signifies that 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 down state.

This alarm is set when the power supply unit goes down. The alarm is cleared when the power supply comes up again.

2.12.2 Action

Please refer to ERS8600 Fault Management document.

2.12.3 Corresponding Clear Log

PP323.

2.12.3.1 Format

2.12.3.2 NTSTD

```
zsups3f8 *** PP322 OCT26 01:28:49 0045 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: Power Supply down
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; SupplyId=1
Specific Problem: Power Supply Status
Description: Power Supply Status: SupplyId = 1(OperationStatus = down)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.6
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
```

2.12.4 Field descriptions

Table 6: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.

Table 6: Field descriptions

Field	Value	Description
Component Id	character string	Indicates the IP address, supplyId and node ID of the device.
OperationStatus	character string	Can be one of {unknown (1), empty (2), up (3), down (4)}

2.12.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.12.6 Additional information

This alarm requires no additional information.

2.13 Alarm (PP323)

rcnChasPowerSupplyUp, Trap OID is 1.3.6.1.4.1.2272.1.21.0.14

2.13.1 Explanation

The PP323 alarm signifies that 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.

2.13.2 Action

Please refer to ERS8600 Fault Management document.

2.13.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.13.3.1 Format

2.13.3.2 NTSTD

```

zsup3f8      PP323 OCT26 01:28:49 0057 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: equipment
Cause: Power supply up
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; SupplyId=1
Specific Problem: Power Supply Status
Description: Power Supply Status: SupplyId = 1(OperationStatus = up)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.14
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
```

2.13.4 Field descriptions

Table 7: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, supplyId and node ID of the device.
OperationStatus	character string	Can be one of {unknown (1), empty (2), up (3), down (4)}

2.13.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.13.6 Additional information

This alarm requires no additional information.

2.14 Alarm (PP324)

rcnChasFanDown, Trap OID is 1.3.6.1.4.1.2272.1.21.0.7

2.14.1 Explanation

The PP324 alarm signifies that 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 down state.

This trap is set when the fan goes down. The alarm is cleared when the fan comes up again.

For 3 slot and 6 slot chassis, there is a single fan.

A 10 slot chassis has two fans; one that cools the top 5 slots and the other that cools the bottom 5 slots.

The chassis will overheat even if a single fan goes down. So both the fans are needed for the chassis to be operational.

2.14.2 Action

Please refer to ERS8600 Fault Management document.

2.14.3 Corresponding Clear Log

PP325.

2.14.3.1 Format

2.14.3.2 NTSTD

```
zsups3f8 *** PP324 OCT26 01:28:49 0047 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: Fan status down
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; fanId=1
Specific Problem: Fan down
Description: Fan Down: fanId= 1(OperationStatus = down)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.7
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
```

2.14.4 Field descriptions

Table 8: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, fanId and node ID of the device.
OperationStatus	character string	Can be one of {unknown (1), up (2), down (3)}

2.14.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.14.6 Additional information

This alarm requires no additional information.

2.15 Alarm (PP325)

rcnChasFanUp, Trap OID is 1.3.6.1.4.1.2272.1.21.0.21

2.15.1 Explanation

The PP325 alarm signifies that 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.

2.15.2 Action

Please refer to ERS8600 Fault Management document.

2.15.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.15.3.1 Format

2.15.3.2 NTSTD

zsups3f8 PP325 OCT26 01:28:49 0077 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: equipment
Cause: Fan Status Up
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; fanId=1
Specific Problem: Fan Up
Description: Fan Up: fanId= 1(OperationalStatus = up)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.21
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.15.4 Field descriptions

Table 9: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, fanId and node ID of the device.

Table 9: Field descriptions

Field	Value	Description
OperationStatus	character string	Can be one of {unknown (1), up (2), down (3)}

2.15.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.15.6 Additional information

This alarm requires no additional information.

2.16 Alarm (PP326)

rcn2kCardDown, Trap OID is 1.3.6.1.4.1.2272.1.21.0.11

2.16.1 Explanation

The PP326 alarm signifies that 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.

2.16.2 Action

Please refer to ERS8600 Fault Management document.

2.16.3 Corresponding Clear Log

PP327.

2.16.3.1 Format

2.16.3.2 NTSTD

```
zsups3f8 *** PP326 OCT26 01:28:49 0051 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: Rc 2k Card Down
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; cardIndex=1
Specific Problem: RC 2k Card Status
Description: Card Down: cardIndex = 1(AdminStatus = down
OperationStatus = down)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.11
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
```

2.16.4 Field descriptions

Table 10: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, cardIndex and node ID of the device.
AdminStatus	character string	Can be one of {up (1), down (2), testing (3)}
OperationStatus	character string	Can be one of {up (1), down (2), testing (3), unknown (4), dormant (5)}

2.16.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.16.6 Additional information

This alarm requires no additional information.

2.17 Alarm (PP327)

rcn2kCardUp, Trap OID is 1.3.6.1.4.1.2272.1.21.0.12

2.17.1 Explanation

The PP327 alarm signifies that 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.

2.17.2 Action

Please refer to ERS8600 Fault Management document.

2.17.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.17.3.1 Format

2.17.3.2 NTSTD

zsups3f8 PP327 OCT26 01:28:49 0053 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: equipment
Cause: Card status Up
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; cardIndex=1
Specific Problem: RC 2k Card Status
Description: Card Up: cardIndex = 1(AdminStatus = up OperationStatus = up)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.12
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.17.4 Field descriptions

Table 11: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, cardIndex and node ID of the device.
AdminStatus	character string	Can be one of {up (1), down (2), testing (3)}
OperationStatus	character string	Can be one of {up (1), down (2), testing (3), unknown (4), dormant (5)}

2.17.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.17.6 Additional information

This alarm requires no additional information.

2.18 Alarm (PP328)

rcn2kTemperature, Trap OID is 1.3.6.1.4.1.2272.1.21.0.13

2.18.1 Explanation

The PP328 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected the chassis is over-heating.

The chassis is overheating. This trap is generated at a threshold temperature of 48 degrees centigrade.

2.18.2 Action

Please refer to ERS8600 Fault Management document.

2.18.3 Corresponding Clear Log

PP328.

2.18.3.1 Format

2.18.3.2 NTSTD

```
zsups3f8 *** PP328 OCT26 01:28:49 0055 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: Over-heating of the chassis detected
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: RC 2K Chassis Temperature
Description: Chassis over-heating: rc2kChassisTemperature = 50
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.13
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
```

2.18.4 Field descriptions

Table 12: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.
Status	Raised/Cleared	Indicated the alarm severity. It is determined by the temperature.

Table 12: Field descriptions

Field	Value	Description
rc2kChassisTemperature	character string	Indicates the temperature of the chassis. When the temperature is ≥ 48 degree, a critical alarm will be raised. Once the temperature is < 48 degree, raise a corresponding clear alarm.

2.18.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.18.6 Additional information

This alarm requires no additional information.

2.19 Alarm (PP329)

rcnErrorNotification, Trap OID is 1.3.6.1.4.1.2272.1.21.0.13

2.19.1 Explanation

The PP329 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected that an error condition has occurred.

2.19.2 Action

Please refer to ERS8600 Fault Management document.

2.19.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.19.3.1 Format

2.19.3.2 NTSTD

```

zsup3f8      PP329 OCT26 01:28:48 0023 TBL  PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: other
Cause: Error condition occurred
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: RC 2K Error
Description: Error occurred: Error Level = 0(Error Code = 1 Error Text =)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.3
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
```

2.19.4 Field descriptions

Table 13: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.
Severity	warning/major/critical	Indicates the alarm severity. It is determined by the Error level.
Error Level	character string	Error level = 0 or 1, indicates warning alarm. Error level = 2 or 3, indicates major alarm. Error level = 4, indicates critical alarm.

2.19.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.19.6 Additional information

This alarm requires no additional information.

2.20 Alarm (PP330)

rcnLinkOscillation, Trap OID is 1.3.6.1.4.1.2272.1.21.0.8

2.20.1 Explanation

The PP330 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected an excessive number of link state transitions on the specified port.

2.20.2 Action

Please refer to ERS8600 Fault Management document.

2.20.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.20.3.1 Format

2.20.3.2 NTSTD

zsups3f8 ** PP330 OCT26 01:28:49 0049 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: Link Oscillation detected
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; portIndex=1
Specific Problem: RC Link Oscillation
Description: LinkOscillation: portIndex = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.8
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.20.4 Field descriptions

Table 14: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, portIndex and node ID of the device.

2.20.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.20.6 Additional information

This alarm requires no additional information.

2.21 Alarm (PP331)

rcnMacViolation, Trap OID is 1.3.6.1.4.1.2272.1.21.0.9

2.21.1 Explanation

The PP331 alarm signifies that the SNMPv2 entity, acting in an agent role, has received a PDU with an invalid source MAC address.

2.21.2 Action

Please refer to ERS8600 Fault Management document.

2.21.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.21.3.1 Format

2.21.3.2 NTSTD

```
zsups3f8 *** PP331 OCT26 01:28:49 0061 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: other
Cause: RC Mac Violation
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; portIndex=1
Specific Problem: RC Mac violation
Description: RC Mac Violation: portIndex= 1(rcErrorText =)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.9
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
.1.3.6.1.2.1.2.2.1.1.0: 0
```

2.21.4 Field descriptions

Table 15: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, portIndex and node ID of the device.

2.21.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.21.6 Additional information

This alarm requires no additional information.

2.22 Alarm (PP332)

rcnSonetTrap, Trap OID is 1.3.6.1.4.1.2272.1.21.0.10

2.22.1 Explanation

The PP332 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected a change of status on a Sonet port.

2.22.2 Action

Please refer to ERS8600 Fault Management document.

2.22.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.22.3.1 Format

2.22.3.2 NTSTD

zsups3f8 PP332 OCT26 01:28:49 0059 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: other
Cause: Sonet port status change
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; portIndex=1
Specific Problem: Sonet port status change
Description: Sonet Trap: portIndex = 1(TrapType = sectionAlarm Trap
Indication = sectionLossOfSignal)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.10
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.22.4 Field descriptions

Table 16: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, portIndex and node ID of the device.

Table 16: Field descriptions

Field	Value	Description
TrapType	character string	Can be one of {sectionAlarm (1), lineAlarm (2), pathAlarm (3)}
Trap Indication	character string	Can be one of {noDefect (1), sectionLossOfSignal (2), sectionLossOfFrame (3), lineAlarmIndication (4), lineRemoteDefectIndication (5), pathLossOfPointer (6), pathAlarmIndication (7), pathRemoteDefectIndication (8), pathUnequipped (9), pathSignalLabelMismatch (10), pathTraceMismatch (11)}

2.22.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.22.6 Additional information

This alarm requires no additional information.

2.23 Alarm (PP333)

rcnStpNewRoot, Trap OID is 1.3.6.1.4.1.2272.1.21.0.4

2.23.1 Explanation

The PP333 alarm signifies that 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.

2.23.2 Action

Please refer to ERS8600 Fault Management document.

2.23.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.23.3.1 Format

2.23.3.2 NTSTD

```

zsups3f8    PP333 OCT26 01:28:48 0025 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: other

```

Cause: Stp New Root
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; stgId=1
Specific Problem: Stp New Root
Description: Stp New Root: stgId = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.4
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.23.4 Field descriptions

Table 17: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, stgId and node ID of the device.

2.23.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.23.6 Additional information

This alarm requires no additional information.

2.24 Alarm (PP334)

rcnStpTopologyChange, Trap OID is 1.3.6.1.4.1.2272.1.21.0.5

2.24.1 Explanation

The PP334 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected the Spanning Tree Protocol has gone due to a topology change event.

2.24.2 Action

Please refer to ERS8600 Fault Management document.

2.24.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.24.3.1 Format

2.24.3.2 NTSTD

zsups3f8 PP334 OCT26 01:28:48 0027 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: other
Cause: Stp Topology change
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; stgId=1
Specific Problem: Stp Topology change
Description: Stp Topology change: stgId= 1(portIndex = 1)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.5
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.24.4 Field descriptions

Table 18: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, stgId and node ID of the device.

2.24.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.24.6 Additional information

This alarm requires no additional information.

2.25 Alarm (PP335)

rcnStpTCN, Trap OID is 1.3.6.1.4.1.2272.1.21.0.16

2.25.1 Explanation

The PP335 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected the Spanning Tree Protocol has gone due a topology change event.

2.25.2 Action

Please refer to ERS8600 Fault Management document.

2.25.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.25.3.1 Format

2.25.3.2 NTSTD

zsups3f8 PP335 OCT26 01:28:49 0067 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: other
Cause: Stp TCN
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; portIndex=1
Specific Problem: Stp TCN
Description: Stp TCN: portIndex= 1(stgId= 1 BridgeAddress=
00-08-74-F0-3C-EC)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.16
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.25.4 Field descriptions

Table 19: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, portIndex and node ID of the device.

2.25.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.25.6 Additional information

This alarm requires no additional information.

2.26 Alarm (PP336)

rcn2kAtmPvcLinkStateChange, Trap OID is 1.3.6.1.4.1.2272.1.21.0.15

2.26.1 Explanation

The PP336 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected that the rc2kAtmPvcOamVcStatus object for one of PVC is about to transition into different state, either from up to down or from down to up.

2.26.2 Action

Please refer to ERS8600 Fault Management document.

2.26.3 Corresponding Clear Log

PP336.

2.26.3.1 Format

2.26.3.2 NTSTD

zsups3f8 PP336 OCT26 01:28:49 0065 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: environmental
Cause: PVC link status change
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; rc2kAtmPvcIfIndex=0
Specific Problem: PVC link status change
Description: Atm Pvc Link State Change: AtmPvcIfIndex = 0(AtmPvcVpi
= 0 AtmPvcVci = 0 AtmPvcOamVcStatus = notManaged)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.15
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.26.4 Field descriptions

Table 20: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, rc2kAtmPvcIfIndex and node ID of the device.

Table 20: Field descriptions

Field	Value	Description
Severity	info/minor/major/clear	Indicated the alarm severity. It is determined by the AtmPvcOamVcStatus.
AtmPvcOamVcStatus	character string	AtmPvcOamVcStatus = "notManaged", indicates info alarm. AtmPvcOamVcStatus = "downVerify" or "upVerify", indicates minor alarm. AtmPvcOamVcStatus = "down", indicates major alarm. AtmPvcOamVcStatus = "up", indicates clear alarm.

2.26.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.26.6 Additional information

This alarm requires no additional information.

2.27 Alarm (PP337)

rcnSmltIstLinkUp, Trap OID is 1.3.6.1.4.1.2272.1.21.0.17

2.27.1 Explanation

The PP337 alarm signifies that the split MLT link is from down to up.

2.27.2 Action

Please refer to ERS8600 Fault Management document.

2.27.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.27.3.1 Format

2.27.3.2 NTSTD

zsup3f8 PP337 OCT26 01:28:49 0069 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: other

Cause: Split MLT link status up
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Split MLT link status up
Description: Split MLT link status up
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.17
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.27.4 Field descriptions

Table 21: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

2.27.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.27.6 Additional information

This alarm requires no additional information.

2.28 Alarm (PP338)

rcnSmltIstLinkDown, Trap OID is 1.3.6.1.4.1.2272.1.21.0.18

2.28.1 Explanation

The PP338 alarm signifies that the split MLT link is from up to down.

2.28.2 Action

Please refer to ERS8600 Fault Management document.

2.28.3 Corresponding Clear Log

PP337.

2.28.3.1 Format

2.28.3.2 NTSTD

zsups3f8 ** PP338 OCT26 01:28:49 0071 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: other
Cause: Split MLT Link Status Down
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Split MLT Link Status Down
Description: Split MLT Link Status Down
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.18
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.28.4 Field descriptions

Table 22: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

2.28.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.28.6 Additional information

This alarm requires no additional information.

2.29 Alarm (PP339)

rcnSmltLinkUp, Trap OID is 1.3.6.1.4.1.2272.1.21.0.19

2.29.1 Explanation

The PP339 alarm signifies that the split SMLT link is up.

2.29.2 Action

Please refer to ERS8600 Fault Management document.

2.29.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.29.3.1 Format

2.29.3.2 NTSTD

zsups3f8 PP339 OCT26 01:28:49 0073 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: other
Cause: Split SMLT link up
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; rcMltSmltId=1
Specific Problem: Split SMLT Link status
Description: Split SMLT link up: rcMltSmltId = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.19
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.29.4 Field descriptions

Table 23: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, rcMltSmltId and node ID of the device.

2.29.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.29.6 Additional information

This alarm requires no additional information.

2.30 Alarm (PP340)

rcnSmltLinkDown, Trap OID is 1.3.6.1.4.1.2272.1.21.0.20

2.30.1 Explanation

The PP340 alarm signifies that the split SMLT link is down.

2.30.2 Action

Please refer to ERS8600 Fault Management document.

2.30.3 Corresponding Clear Log

PP339.

2.30.3.1 Format

2.30.3.2 NTSTD

```
zsups3f8 ** PP340 OCT26 01:28:49 0075 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: other
Cause: Split SMLT Link down
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; rcMltSmltId=1
Specific Problem: Split SMLT link status
Description: Split SMLT link down: rcMltSmltId = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.20
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
```

2.30.4 Field descriptions

Table 24: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, rcMltSmltId and node ID of the device.

2.30.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.30.6 Additional information

This alarm requires no additional information.

2.31 Alarm (PP341)

rcnPasswordChange, Trap OID is 1.3.6.1.4.1.2272.1.21.0.22

2.31.1 Explanation

The PP341 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected that the one of the cli password is changed.

2.31.2 Action

Please refer to ERS8600 Fault Management document.

2.31.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.31.3.1 Format

2.31.3.2 NTSTD

zsups3f8 PP341 OCT26 01:28:49 0081 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: security
Cause: CLI password changed
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: CLI password has been changed
Description: CLI password changed (PasswordChange = ssladmin
PassChangeResult = success)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.22
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.31.4 Field descriptions

Table 25: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.

Table 25: Field descriptions

Field	Value	Description
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.
PasswordChange	character string	Can be one of {ro (1), l1 (2), l2 (3), l3 (4), rw (5), rwa (6), slboper (7), l4oper (8), oper (9), slbadmin (10), l4admin (11), ssladmin (12), commStrRo (13), commStrRw (14), commStrl3 (15), commStrl2 (16), commStrl1 (17), webPassWdRo (18)}
PassChangeResult	character string	Can be one of {success (1), fail (2)}

2.31.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.31.6 Additional information

This alarm requires no additional information.

2.32 Alarm (PP342)

rcnPcmciaCardRemoved, Trap OID is 1.3.6.1.4.1.2272.1.21.0.25

2.32.1 Explanation

The PP342 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected that the PCMCIA card is being removed.

2.32.2 Action

Please refer to ERS8600 Fault Management document.

2.32.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.32.3.1 Format

2.32.3.2 NTSTD

zsups3f8 *** PP342 OCT26 01:28:49 0085 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: PCMCIA card is being removed.
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: PCMCIA card removed.
Description: PCMCIA card is being removed.
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.25
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.32.4 Field descriptions

Table 26: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

2.32.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.32.6 Additional information

This alarm requires no additional information.

2.33 Alarm (PP343)

rcnSmartCpldTimerFired, Trap OID is 1.3.6.1.4.1.2272.1.21.0.26

2.33.1 Explanation

The PP343 alarm signifies that the cpld timer fired.

2.33.2 Action

Please refer to ERS8600 Fault Management document.

2.33.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.33.3.1 Format

2.33.3.2 NTSTD

zsups3f8 ** PP343 OCT26 01:28:49 0087 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: cpld timer fired
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; CardIndex=1
Specific Problem: cpld timer fired
Description: cpld timer fired: CardIndex = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.26
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.33.4 Field descriptions

Table 27: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, CardIndex and node ID of the device.

2.33.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.33.6 Additional information

This alarm requires no additional information.

2.34 Alarm (PP344)

rcnCardCpldNotUpDate, Trap OID is 1.3.6.1.4.1.2272.1.21.0.27

2.34.1 Explanation

The PP344 alarm signifies that the cpld is not up to date.

2.34.2 Action

Please refer to ERS8600 Fault Management document.

2.34.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.34.3.1 Format

2.34.3.2 NTSTD

```
zsups3f8 ** PP344 OCT26 01:28:49 0089 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: cpld is not up to date
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; CardIndex=1
Specific Problem: cpld not up to date
Description: cpld is not up to date: CardIndex = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.27
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
```

2.34.4 Field descriptions

Table 28: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, CardIndex and node ID of the device.

2.34.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.34.6 Additional information

This alarm requires no additional information.

2.35 Alarm (PP345)

rcnIgapLogFileFull, Trap OID is 1.3.6.1.4.1.2272.1.21.0.28

2.35.1 Explanation

The PP345 alarm signifies that the Igap accounting time-out Log File reached the maximum.

2.35.2 Action

Please refer to ERS8600 Fault Management document.

2.35.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.35.3.1 Format

2.35.3.2 NTSTD

```
zsups3f8 ** PP345 OCT26 01:28:49 0091 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: processingError
Cause: Igap Log file full
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Igap Log file full
Description: Igap accounting time-out Log File reach the maximum.
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.28
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
```

2.35.4 Field descriptions

Table 29: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.

Table 29: Field descriptions

Field	Value	Description
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

2.35.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.35.6 Additional information

This alarm requires no additional information.

2.36 Alarm (PP346)

rcnCpLimitShutDown, Trap OID is 1.3.6.1.4.1.2272.1.21.0.29

2.36.1 Explanation

The PP346 alarm signifies that the cp limit for the port is shutting down.

2.36.2 Action

Please refer to ERS8600 Fault Management document.

2.36.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.36.3.1 Format

2.36.3.2 NTSTD

```

zsups3f8 ** PP346 OCT26 01:28:50 0093 TBL PP Fault
  Location: ERS8600_RTP;47.142.106.1
  State: Raised
  Category: equipment
  Cause: cp limit for the port is shutting down
  Time: Oct 26 01:28:50 2005
  Component ID: ERS8600=47.142.106.1; PortIndex=1
  Specific Problem: cp limit for the port is shutting down
  Description: Cp limit for port is shutting down: PortIndex= 1(AdminStatus
    = up OperStatus = down CpLimitShutDown = true)
    .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.29
    .1.3.6.1.4.1.2272.1.21.0.29: 0
    .1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

```

2.36.4 Field descriptions

Table 30: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, PortIndex and node ID of the device.
AdminStatus	character string	Can be one of {up (1), down (2), testing (3)}
OperationStatus	character string	Can be one of {up (1), down (2), testing (3), unknown (4), dormant (5)}
CpLimitShutDown	character string	Can be one of {true (1), false (2)}

2.36.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.36.6 Additional information

This alarm requires no additional information.

2.37 Alarm (PP347)

rcnSshServerEnabled, Trap OID is 1.3.6.1.4.1.2272.1.21.0.30

2.37.1 Explanation

The PP347 alarm signifies that the SSH server is enabled.

2.37.2 Action

Please refer to ERS8600 Fault Management document.

2.37.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.37.3.1 Format

2.37.3.2 NTSTD

zsups3f8 PP347 OCT26 01:28:50 0097 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: communications
Cause: SSH server is enabled
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; SshGlobalPort=1
Specific Problem: SSH server enabled
Description: SSH server is enabled: SshGlobalPort = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.30
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.37.4 Field descriptions

Table 31: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, SshGlobalPort and node ID of the device.

2.37.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.37.6 Additional information

This alarm requires no additional information.

2.38 Alarm (PP348)

rcnSshServerDisabled, Trap OID is 1.3.6.1.4.1.2272.1.21.0.31

2.38.1 Explanation

The PP348 alarm signifies that the SSH server is disabled.

2.38.2 Action

Please refer to ERS8600 Fault Management document.

2.38.3 Corresponding Clear Log

PP347.

2.38.3.1 Format

2.38.3.2 NTSTD

```
zsups3f8 ** PP348 OCT26 01:28:50 0095 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: communications
Cause: SSH server is disabled
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; SshGlobalPort=1
Specific Problem: SSH server disabled
Description: SSH server is disabled: SshGlobalPort = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.31
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
```

2.38.4 Field descriptions

Table 32: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, SshGlobalPort and node ID of the device.

2.38.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.38.6 Additional information

This alarm requires no additional information.

2.39 Alarm (PP349)

rcnSshSessionLogin, Trap OID is 1.3.6.1.4.1.2272.1.21.0.32

2.39.1 Explanation

The PP349 alarm signifies that there is a SSH session login.

2.39.2 Action

Please refer to ERS8600 Fault Management document.

2.39.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.39.3.1 Format

2.39.3.2 NTSTD

zsups3f8 PP349 OCT26 01:28:50 0099 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: SSH Session login
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1;
SshGlobalHostIpAddr=47.142.106.60
Specific Problem: SSH Session login
Description: SSH session login occurred: SshGlobalHostIpAddr =
47.142.106.60
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.32
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.39.4 Field descriptions

Table 33: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, SshGlobalHostIpAddr and node ID of the device.

2.39.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.39.6 Additional information

This alarm requires no additional information.

2.40 Alarm (PP350)

rcnSshSessionLogout, Trap OID is 1.3.6.1.4.1.2272.1.21.0.33

2.40.1 Explanation

The PP350 alarm signifies that there is a SSH session logout.

2.40.2 Action

Please refer to ERS8600 Fault Management document.

2.40.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.40.3.1 Format

2.40.3.2 NTSTD

zsup3f8 PP350 OCT26 01:28:50 0101 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: SSH session logout
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1;
SshGlobalHostIpAddr=47.142.106.60
Specific Problem: SSH session logout
Description: SSH session logout occurred: SshGlobalHostIpAddr =
47.142.106.60
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.33
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.40.4 Field descriptions

Table 34: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.

Table 34: Field descriptions

Field	Value	Description
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, SshGlobalHostIpAddr and node ID of the device.

2.40.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.40.6 Additional information

This alarm requires no additional information.

2.41 Alarm (PP351)

rcnSshUnauthorizedAccess, Trap OID is 1.3.6.1.4.1.2272.1.21.0.34

2.41.1 Explanation

The PP351 alarm signifies that an unauthorized access has occurred.

2.41.2 Action

Please refer to ERS8600 Fault Management document.

2.41.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.41.3.1 Format

2.41.3.2 NTSTD

```
zsup3f8 *** PP351 OCT26 01:28:50 0103 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: security
Cause: Unauthorized access
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1;
SshGlobalHostIpAddr=47.142.106.60
Specific Problem: Unauthorized access
Description: Unauthorized access occurred: SshGlobalHostIpAddr =
47.142.106.60
```


.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.34
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.41.4 Field descriptions

Table 35: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, SshGlobalHostIpAddr and node ID of the device.

2.41.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.41.6 Additional information

This alarm requires no additional information.

2.42 Alarm (PP352)

rcnHaCpuState, Trap OID is 1.3.6.1.4.1.2272.1.21.0.35

2.42.1 Explanation

The PP352 alarm signifies that the state of the HA-CPU.

2.42.2 Action

Please refer to ERS8600 Fault Management document.

2.42.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.42.3.1 Format

2.42.3.2 NTSTD

zsup3f8 *** PP352 OCT26 01:28:50 0105 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised

Category: equipment
Cause: State of the HA-CPU
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; CardIndex=1
Specific Problem: State of the HA-CPU
Description: State of the HA-CPU: CardIndex = 1 (HaCpuState = initialization)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.35
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.42.4 Field descriptions

Table 36: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, CardIndex and node ID of the device.
HaCpuState	character string	Can be one of {initialization (0), oneWayActive (1), twoWayActive (2), synchronized (3), remoteIncompatible (4), error (5), disabled (6), peerNotConnected (7), peerConnected (8), lostPeerConnection (9), notSynchronized (10)}

2.42.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.42.6 Additional information

This alarm requires no additional information.

2.43 Alarm (PP353)

rcnInsufficientMemory, Trap OID is 1.3.6.1.4.1.2272.1.21.0.36

2.43.1 Explanation

The PP353 alarm signifies that insufficient memory on CPU blade for proper operation. Recommended memory = 256 MB available through Nortel Networks upgrade kit.

2.43.2 Action

Please refer to ERS8600 Fault Management document.

2.43.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.43.3.1 Format

2.43.3.2 NTSTD

zsups3f8 *** PP353 OCT26 01:28:50 0107 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: environmental
Cause: Insufficient memory on CPU blade for proper operation
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; CardIndex=1
Specific Problem: Insufficient memory on CPU
Description: Insufficient memory: CardIndex = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.36
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.43.4 Field descriptions

Table 37: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, CardIndex and node ID of the device.

2.43.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.43.6 Additional information

This alarm requires no additional information.

2.44 Alarm (PP354)

rcnSaveConfigAction, Trap OID is 1.3.6.1.4.1.2272.1.21.0.37

2.44.1 Explanation

The PP354 alarm signifies that the switch run time or boot configuration is being saved.

2.44.2 Action

Please refer to ERS8600 Fault Management document.

2.44.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.44.3.1 Format

2.44.3.2 NTSTD

zsups3f8 PP354 OCT26 01:28:50 0109 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: processingError
Cause: Switch run time or boot configuration is saved
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Switch configuration saved
Description: Switch configuration saved: SysAction = none
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.37
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.44.4 Field descriptions

Table 38: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.

Table 38: Field descriptions

Field	Value	Description
Component Id	character string	Indicates the IP address and node ID of the device.
SysAction	character string	Can be one of {none (1), hardReset (2), softReset (3), saveToNVRAM (4), resetCounters (5), saveToStandbyNVRAM (6), cpuSwitchOver (7), checkSwInFlash (8), checkSwInPcmcia (9), resetConsole (10), resetModem (11), flushIpRouteTbl (12), saveRuntimeConfig (13), saveRuntimeConfigToSlave (14), saveBootConfig (15), saveSlaveBootConfig (16), reset1stStatCounters (17)}

2.44.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.44.6 Additional information

This alarm requires no additional information.

2.45 Alarm (PP355)

rcnLoopDetectOnPort, Trap OID is 1.3.6.1.4.1.2272.1.21.0.38

2.45.1 Explanation

The PP355 alarm signifies that a loop has been detected on a port. The vlan on that port will be disabled.

2.45.2 Action

Please refer to ERS8600 Fault Management document.

2.45.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.45.3.1 Format

2.45.3.2 NTSTD

```
zsups3f8 *** PP355 OCT26 01:28:50 0111 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
```

Category: communications
Cause: Loop detected on port. The vlan on that port will be disabled
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; PortIndex=1
Specific Problem: Loop detected on port.
Description: Loop detected on port: PortIndex = 1 (rcVlanId = 1)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.38
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.45.4 Field descriptions

Table 39: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, PortIndex and node ID of the device.

2.45.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.45.6 Additional information

This alarm requires no additional information.

2.46 Alarm (PP356)

vrrpTrapStateTransition, Trap OID is 1.3.6.1.2.1.46.1.3.0.3.0

2.46.1 Explanation

The PP356 alarm signifies that a state transition has occurred on a particular vrrp interface. Implementation of this trap is optional. 'vrrpOperIpAddr' contains the IP address of the vrrp interface while 'ipAdEntAddr' contains the IP address assigned to physical interface.

2.46.2 Action

Please refer to ERS8600 Fault Management document.

2.46.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.46.3.1 Format

2.46.3.2 NTSTD

```

zsups3f8 *** PP356 OCT26 01:28:49 0063 TBL PP Fault
  Location: ERS8600_RTP;47.142.106.1
  State: Raised
  Category: communications
  Cause: State transition has occurred on vrrp interface
  Time: Oct 26 01:28:49 2005
  Component ID: ERS8600=47.142.106.1; ifIndex=100
  Specific Problem: Trap state transition
  Description: State Transition: ifIndex = 100 (TransitionType =
masterToBackup TransitionCause = shutdownReceived Port = 37 Slot = 1)
.1.3.6.1.2.1.4.20.1.1.0: 0.0.0.0
.1.3.6.1.2.1.46.1.1.10.1.3.0: 0.0.0.0
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.46.1.3.0.3.0
.1.3.6.1.2.1.46.1.1.10.1.2.0: 0
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

```

2.46.4 Field descriptions

Table 40: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, ifIndex and node ID of the device.
TransitionType	character string	Can be one of {none (1), masterToBackup (2), backupToMaster (3), initializeToMaster (4), masterToInitialize (5), initializeToBackup (6), backupToInitialize (7), backupToBackUpMaster (8), backUpMasterToBackup (9)}

Table 40: Field descriptions

Field	Value	Description
TransitionCause	character string	Can be one of {none (1), higherPriorityAdvertiseReceived (2), shutdownReceived (3), vrrpAddrAndPhysicalAddrMatch (4), masterDownInterval (5), preempted (6), criticalIPFail (7), usrConfig (8), syncFromPrimary (9), iPlInterfaceDown (10), lowerPrioAdvReceived (11), higherSrcIPEqualPrioAdvReceived (12), lowerSrcIPEqualPrioAdvReceived (13), startVR (14), other (15)}
PhysicalInfo	character string	Indicates the physical information appended to TransitionCause. The actual physical information is determined by ifIndex. ifIndex ≥ 64 and ifIndex ≤ 703 the information is: Port = '(ifIndex & 0x3f) + 1' Slot = 'ifIndex >>6' ifIndex ≥ 832 and ifIndex ≤ 863 the information is: Circuitless IP = 'ifIndex - 832 + 1' ifIndex ≥ 2048 and ifIndex ≤ 4095 the information is: VLAN = 'ifIndex - 2048 + 1' ifIndex ≥ 4096 and ifIndex ≤ 4127 the information is: MLT = 'ifIndex - 4096 + 1' ifIndex ≥ 4352 and ifIndex ≤ 5351 the information is: Tunnel = 'ifIndex - 4352 + 1' An ifIndex not within the above ranges, the information is: unknown of ifIndex meaning Note: The content in “ ” part will be calculated out.

2.46.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.46.6 Additional information

This alarm requires no additional information.

2.47 Alarm (PP357)

rcnEmError, Trap OID is 1.3.6.1.4.1.2272.1.21.0.23

2.47.1 Explanation

The PP357 alarm signifies that the SNMPv2 entity, acting in an agent role, has detected Em error.

2.47.2 Action

Please refer to ERS8600 Fault Management document.

2.47.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.47.3.1 Format

2.47.3.2 NTSTD

zsups3f8 PP357 OCT26 01:28:49 0079 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: Em error detected
Time: Oct 26 01:28:49 2005
Component ID: ERS8600=47.142.106.1; CardIndex=1
Specific Problem: Em error detected
Description: Em error: CardIndex = 1 (Em Error = none)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.23
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.47.4 Field descriptions

Table 41: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, CardIndex and node ID of the device.

Table 41: Field descriptions

Field	Value	Description
Em Error	character string	Can be one of {none (1), non128KCardOffLine (2), checkSlaveConfigNResetForEmMMMode (3), mismatchResetForEmMode (4), mismatchEmModeMasterSlave (5), incompatMasterResetForEmMode (6), putSlaveOffEmImcompat (7), slave8690EmIncompatGoingOffline (8), cpu8690DisableEm (9)}

2.47.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.47.6 Additional information

This alarm requires no additional information.

2.48 Alarm (PP358)

ospfVirtIfStateChange, Trap OID is 1.3.6.1.2.1.14.16.2.1

2.48.1 Explanation

The PP358 alarm signifies that there has been a change in the state of an OSPF virtual interface. This trap should be generated when the interface state regresses (e.g., goes from Point-to-Point to Down) or progresses to a terminal state (i.e., Point-to-Point).

2.48.2 Action

Please refer to ERS8600 Fault Management document.

2.48.3 Corresponding Clear Log

PP358.

2.48.3.1 Format

2.48.3.2 NTSTD

```

zsups3f8    PP358 OCT26 01:28:48 0043 TBL  PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: environmental
Cause: OSPF virtual interface state change
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; ospfRouterId=47.142.106.70

```

Specific Problem: OSPF virtual interface state change
Description: OSPF virtual interface state change: ospfRouterId = 47.142.106.70 (AreaId = 0.0.0.0 Neighbor = 0.0.0.0 State = pointToPoint)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.14.16.2.1
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.48.4 Field descriptions

Table 42: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, ospfRouterId and node ID of the device.
Severity	warning/clear	Indicated the alarm severity. It is determined by the State value.
State (In the Description)	character string	State = "down", indicates warning alarm. State = "pointToPoint", indicates clear alarm.

2.48.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.48.6 Additional information

This alarm requires no additional information.

2.49 Alarm (PP359)

ospfNbrStateChange, Trap OID is 1.3.6.1.2.1.14.16.2.2

2.49.1 Explanation

The PP359 alarm signifies that there has been a change in the state of a non-virtual OSPF neighbor. This trap should be generated when the neighbor

state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., 2-Way or Full). When an neighbor transitions from or to Full on non-broadcast multi-access and broadcast networks, the trap should be generated by the designated router. A designated router transitioning to Down will be noted by ospfIfStateChange.

2.49.2 Action

Please refer to ERS8600 Fault Management document.

2.49.3 Corresponding Clear Log

PP359.

2.49.3.1 Format

2.49.3.2 NTSTD

```
zsups3f8    PP359 OCT26 01:28:48 0029 TBL  PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: Non-virtual neighbor state change
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; ospfRouterId=47.142.106.70
Specific Problem: Non-virtual OSPF neighbor state change
Description: Non-virtual neighbor state change: RouterId = 47.142.106.70
(NbrIpAddr = 47.154.182.56 NbrRouter = 47.154.182.1 State = loading)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.14.16.2.2
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
.1.3.6.1.2.1.14.10.1.2: 0
```

2.49.4 Field descriptions

Table 43: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, ospfRouterId and node ID of the device.

Table 43: Field descriptions

Field	Value	Description
Severity	warning/clear	Indicated the alarm severity. It is determined by the State value.
State (In the Description)	character string	State = "down", "attempt", "init", "twoWay", "exchangeStart", "exchange", "loading", indicates warning alarm. State = "full", indicates clear alarm.

2.49.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.49.6 Additional information

This alarm requires no additional information.

2.50 Alarm (PP360)

ospfVirtNbrStateChange, Trap OID is 1.3.6.1.2.1.14.16.2.3

2.50.1 Explanation

The PP360 alarm signifies that there has been a change in the state of an OSPF virtual neighbor. This trap should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., Full).

2.50.2 Action

Please refer to ERS8600 Fault Management document.

2.50.3 Corresponding Clear Log

PP360.

2.50.3.1 Format

2.50.3.2 NTSTD

zsup3f8 * PP360 OCT26 01:28:48 0037 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1

State: Raised
 Category: environmental
 Cause: Virtual OSPF neighbor state change
 Time: Oct 26 01:28:48 2005
 Component ID: ERS8600=47.142.106.1; ospfRouterId=47.142.106.70
 Specific Problem: Virtual OSPF neighbor state change
 Description: Virtual neighbor state change: RouterId = 47.142.106.70
 (NbrArea = 47.154.182.56 NbrRouter = 47.154.182.1 State = loading)
 .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.14.16.2.3
 .1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.50.4 Field descriptions

Table 44: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, ospfRouterId and node ID of the device.
Severity	minor/clear	Indicated the alarm severity. It is determined by the State value.
State (In the Description)	character string	State = "down", "attempt", "init", "twoWay", "exchangeStart", "exchange", "loading", indicates warning alarm. State = "full", indicates clear alarm.

2.50.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.50.6 Additional information

This alarm requires no additional information.

2.51 Alarm (PP361)

ospfIfConfigError, Trap OID is 1.3.6.1.2.1.14.16.2.4

2.51.1 Explanation

The PP361 alarm signifies that a packet has been received on a non-virtual interface from a router whose configuration parameters conflict with this router's configuration parameters. Note that the event option Mismatch should cause a trap only if it prevents an adjacency from forming.

2.51.2 Action

Please refer to ERS8600 Fault Management document.

2.51.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.51.3.1 Format

2.51.3.2 NTSTD

```
zsups3f8 *** PP361 OCT26 01:28:48 0031 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: Configuration error
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; ospfRouterId=47.142.106.70
Specific Problem: configuration error
Description: IfConfig Error: ospfRouterId = 47.142.106.70 (IpAddress =
47.154.182.56)
.1.3.6.1.2.1.14.7.1.2: 0
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.14.16.2.4
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
```

2.51.4 Field descriptions

Table 45: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.

Table 45: Field descriptions

Field	Value	Description
Component Id	character string	Indicates the IP address, ospfRouterId and node ID of the device.

2.51.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.51.6 Additional information

This alarm requires no additional information.

2.52 Alarm (PP362)

ospfVirtIfConfigError, Trap OID is 1.3.6.1.2.1.14.16.2.5

2.52.1 Explanation

The PP362 alarm signifies that a packet has been received on a virtual interface from a router whose configuration parameters conflict with this router's configuration parameters. Note that the event optionMismatch should cause a trap only if it prevents an adjacency from forming.

2.52.2 Action

Please refer to ERS8600 Fault Management document.

2.52.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.52.3.1 Format

2.52.3.2 NTSTD

```
zsups3f8 *** PP362 OCT26 01:28:48 0039 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: Virtual interface configuration error
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; ospfRouterId=47.142.106.70
Specific Problem: Virtual interface configuration error
Description: VirtIfConfigError: ospfRouterId = 47.142.106.70 (AreaId =
47.154.182.1 Neighbor = 47.154.182.56 ErrorType =badVersion)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.14.16.2.5
```


.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.52.4 Field descriptions

Table 46: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, ospfRouterId and node ID of the device.
ErrorType	character string	Can be one of {badVersion (1), areaMismatch (2), unknownNbmaNbr (3), unknownVirtualNbr (4), authTypeMismatch (5), authFailure (6), netMaskMismatch (7), helloIntervalMismatch (8), deadIntervalMismatch (9), optionMismatch (10), crcCheckFailed (11)}

2.52.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.52.6 Additional information

This alarm requires no additional information.

2.53 Alarm (PP363)

ospfIfAuthFailure, Trap OID is 1.3.6.1.2.1.14.16.2.6

2.53.1 Explanation

The PP363 alarm signifies that a packet has been received on a non-virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.

2.53.2 Action

Please refer to ERS8600 Fault Management document.

2.53.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.53.3.1 Format**2.53.3.2 NTSTD**

```

zsups3f8 *** PP363 OCT26 01:28:48 0033 TBL PP Fault
  Location: ERS8600_RTP;47.142.106.1
  State: Raised
  Category: security
  Cause: ospf If authentication failure
  Time: Oct 26 01:28:48 2005
  Component ID: ERS8600=47.142.106.1; ospfRouterId=47.142.106.70
  Specific Problem: ospf If authentication failure
  Description: ospf If authentication failure: ospfRouterId = 47.142.106.70
  (ConfigErrorType =authTypeMismatch)
  .1.3.6.1.2.1.14.7.1.2: 0
  .1.3.6.1.2.1.14.7.1.1: 0.0.0.0
  .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.14.16.2.6
  .1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

```

2.53.4 Field descriptions**Table 47: Field descriptions**

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, ospfRouterId and node ID of the device.
ConfigErrorType	character string	Can be one of {badVersion (1), areaMismatch (2), unknownNbmaNbr (3), unknownVirtualNbr (4), authTypeMismatch (5), authFailure (6), netMaskMismatch (7), helloIntervalMismatch (8), deadIntervalMismatch (9), optionMismatch (10), crcCheckFailed (11)}

2.53.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.53.6 Additional information

This alarm requires no additional information.

2.54 Alarm (PP364)

ospfVirtIfAuthFailure, Trap OID is 1.3.6.1.2.1.14.16.2.7

2.54.1 Explanation

The PP364 alarm signifies that a packet has been received on a virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.

2.54.2 Action

Please refer to ERS8600 Fault Management document.

2.54.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.54.3.1 Format

2.54.3.2 NTSTD

```
zsups3f8 *** PP364 OCT26 01:28:48 0041 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: security
Cause: ospf virtual interface authentication failure
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; ospfRouterId=47.142.106.70
Specific Problem:
Description: ospfVirtIfAuthFailure: ospfRouterId = 47.142.106.70 (AreaId
= 47.154.182.1 Neighbor = 47.154.182.56 ErrorType =authTypeMismatch)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.14.16.2.7
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
```

2.54.4 Field descriptions

Table 48: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, ospfRouterId and node ID of the device.

Table 48: Field descriptions

Field	Value	Description
ErrorType	character string	Can be one of {badVersion (1), areaMismatch (2), unknownNbmaNbr (3), unknownVirtualNbr (4), authTypeMismatch (5), authFailure (6), netMaskMismatch (7), helloIntervalMismatch (8), deadIntervalMismatch (9), optionMismatch (10), crcCheckFailed (11)}

2.54.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.54.6 Additional information

This alarm requires no additional information.

2.55 Alarm (PP365)

ospfIfStateChange, Trap OID is 1.3.6.1.2.1.14.16.2.16

2.55.1 Explanation

The PP365 alarm signifies that there has been a change in the state of a non-virtual OSPF interface. This trap should be generated when the interface state regresses (e.g., goes from Dr to Down) or progresses to a terminal state (i.e., Point-to-Point, DR Other, Dr, or Backup).

2.55.2 Action

Please refer to ERS8600 Fault Management document.

2.55.3 Corresponding Clear Log

PP365.

2.55.3.1 Format

2.55.3.2 NTSTD

zsup3f8 PP365 OCT26 01:28:48 0036 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: equipment
Cause: Non-virtual OSPF interface state change
Time: Oct 26 01:28:48 2005

Component ID: ERS8600=47.142.106.1; ospfRouterId=47.142.106.70
 Specific Problem: Non-virtual OSPF interface state change
 Description: Non-virtual OSPF interface state change: ospfRouterId =
 47.142.106.70 (IpAddress = 47.154.182.56 State =pointToPoint)
 .1.3.6.1.2.1.14.7.1.2: 0
 .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.14.16.2.16
 .1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.55.4 Field descriptions

Table 49: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, ospfRouterId and node ID of the device.
Severity	warning/clear	Indicated the alarm severity. It is determined by the State value.
State (In the Description)	character string	State = "down", "loopback", "waiting", indicates warning alarm. State = "pointToPoint", "designedRouter", "backupDesignatedRouter", "otherDesignatedRouter", indicates clear alarm.

2.55.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.55.6 Additional information

This alarm requires no additional information.

2.56 Alarm (PP366)

rcnCardDown, Trap OID is 1.3.6.1.4.1.2272.1.21.0.1

2.56.1 Explanation

The PP366 alarm signifies that 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.

2.56.2 Action

Please refer to ERS8600 Fault Management document.

2.56.3 Corresponding Clear Log

PP367.

2.56.3.1 Format

2.56.3.2 NTSTD

```
zsup3f8 *** PP366 OCT26 01:28:48 0019 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: equipment
Cause: RC Card status down
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; rcCardIndex=1
Specific Problem: RC Card status
Description: RC card status down: CardIndex = 1 (AdminStatus = up
OperStatus = down)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.1
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
```

2.56.4 Field descriptions

Table 50: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, rcCardIndex and node ID of the device.

Table 50: Field descriptions

Field	Value	Description
AdminStatus	character string	Can be one of {up (1), down (2), testing (3)}
OperStatus	character string	Can be one of {up (1), down (2), testing (3), unknown (4), dormant (5)}

2.56.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.56.6 Additional information

This alarm requires no additional information.

2.57 Alarm (PP367)

rcnCardUp, Trap OID is 1.3.6.1.4.1.2272.1.21.0.2

2.57.1 Explanation

The PP367 alarm signifies that 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.

2.57.2 Action

Please refer to ERS8600 Fault Management document.

2.57.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.57.3.1 Format

2.57.3.2 NTSTD

```
zsups3f8    PP367 OCT26 01:28:48 0021 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: equipment
Cause: RC card status up
Time: Oct 26 01:28:48 2005
Component ID: ERS8600=47.142.106.1; rcCardIndex=0
Specific Problem: RC Card Status
Description: RC card status up: CardIndex = 0 (AdminStatus = up
OperStatus = up)
```

.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.2
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.57.4 Field descriptions

Table 51: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, rcCardIndex and node ID of the device.
AdminStatus	character string	Can be one of {up (1), down (2), testing (3)}
OperStatus	character string	Can be one of {up (1), down (2), testing (3), unknown (4), dormant (5)}

2.57.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.57.6 Additional information

This alarm requires no additional information.

2.58 Alarm (PP368)

rcnbgpEstablished, Trap OID is 1.3.6.1.4.1.2272.1.21.0.39

2.58.1 Explanation

The PP368 alarm is generated when the BGP FSM enters the ESTABLISHED state.

2.58.2 Action

Please refer to ERS8600 Fault Management document.

2.58.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.58.3.1 Format

2.58.3.2 NTSTD

```

zsups3f8    PP368 OCT26 01:28:50 0113 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: communications
Cause: BGP FSM entered the ESTABLISHED state
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1;
rcIpBgpPeerIpAddress=47.142.106.70
Specific Problem: BGP FSM entered the ESTABLISHED state
Description: BGP FSM entered ESTABLISHED state: PeerIpAddress =
47.142.106.70 (PeerLastError = 1 PeerState =active)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.39
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

```

2.58.4 Field descriptions

Table 52: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, rcIpBgpPeerIpAddress and node ID of the device.
PeerState	character string	Can be one of {idle (1), connect (2), active (3), opensent (4), openconfirm (5), established (6)}

2.58.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.58.6 Additional information

This alarm requires no additional information.

2.59 Alarm (PP369)

rcnbgpBackwardTransition, Trap OID is 1.3.6.1.4.1.2272.1.21.0.40

2.59.1 Explanation

The PP369 alarm is generated when the BGP FSM moves from a higher numbered state to a lower numbered state.

2.59.2 Action

Please refer to ERS8600 Fault Management document.

2.59.3 Corresponding Clear Log

PP368.

2.59.3.1 Format

2.59.3.2 NTSTD

```
zsup3f8 *** PP369 OCT26 01:28:50 0115 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: communications
Cause: BGP FSM backward transition
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1;
rcIpBgpPeerIpAddress=47.142.106.70
Specific Problem: BGP FSM backward transition
Description: BGP FSM backward transition: PeerIpAddress =
47.142.106.70 (PeerLastError = 1 PeerState = active)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.40
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
```

2.59.4 Field descriptions

Table 53: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.

Table 53: Field descriptions

Field	Value	Description
Component Id	character string	Indicates the IP address, rcIpBgpPeerIpAddress and node ID of the device.
PeerState	character string	Can be one of {idle (1), connect (2), active (3), opensent (4), openconfirm (5), established (6)}

2.59.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.59.6 Additional information

This alarm requires no additional information.

2.60 Alarm (PP370)

rcnAggLinkUp, Trap OID is 1.3.6.1.4.1.2272.1.21.0.41

2.60.1 Explanation

The PP370 alarm is generated when the operational state of the aggregator changes from down to up.

2.60.2 Action

Please refer to ERS8600 Fault Management document.

2.60.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.60.3.1 Format

2.60.3.2 NTSTD

zsup3f8 PP370 OCT26 01:28:50 0117 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Cleared
Category: communications
Cause: Aggregator up
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; rcMltId=1
Specific Problem: Aggregator status

Description: Aggregator up: rcMltId = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.41
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.60.4 Field descriptions

Table 54: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, rcMltId and node ID of the device.

2.60.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.60.6 Additional information

This alarm requires no additional information.

2.61 Alarm (PP371)

rcnAggLinkDown, Trap OID is 1.3.6.1.4.1.2272.1.21.0.42

2.61.1 Explanation

The PP371 alarm is generated when the operational state of the aggregator changes from up to down.

2.61.2 Action

Please refer to ERS8600 Fault Management document.

2.61.3 Corresponding Clear Log

PP370.

2.61.3.1 Format

2.61.3.2 NTSTD

zsup3f8 ** PP371 OCT26 01:28:50 0119 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1

State: Raised
Category: communications
Cause: Aggregator Down
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; rcMltId=1
Specific Problem: Aggregator status
Description: Aggregator Down: rcMltId = 1
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.42
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.61.4 Field descriptions

Table 55: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, rcMltId and node ID of the device.

2.61.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.61.6 Additional information

This alarm requires no additional information.

2.62 Alarm (PP372)

rcnIgmPNewGroupMember, Trap OID is 1.3.6.1.4.1.2272.1.21.0.43

2.62.1 Explanation

The PP372 alarm signifies that a new member has come on an interface.

2.62.2 Action

Please refer to ERS8600 Fault Management document.

2.62.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.62.3.1 Format

2.62.3.2 NTSTD

zsups3f8 PP372 OCT26 01:28:50 0127 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: New Group member in interface
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; rcIgmpGroupIfIndex=0
Specific Problem: New Group member in interface
Description: New Group member in interface: rcIgmpGroupIfIndex = 0
(GroupIpAddress = 47.142.106.70 Port = 0 Members 47.142.106.71)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.43
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.62.4 Field descriptions

Table 56: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, rcIgmpGroupIfIndex and node ID of the device.

2.62.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.62.6 Additional information

This alarm requires no additional information.

2.63 Alarm (PP373)

rcnIgmpLossGroupMember, Trap OID is 1.3.6.1.4.1.2272.1.21.0.44

2.63.1 Explanation

The PP373 alarm signifies that a group member has been lost on an interface.

2.63.2 Action

Please refer to ERS8600 Fault Management document.

2.63.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.63.3.1 Format

2.63.3.2 NTSTD

```
zsup3f8    PP373 OCT26 01:28:50 0129 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: Group member lost on interface
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; rcIgmpGroupIfIndex=0
Specific Problem: Group member lost on interface
Description: Group member lost on interface: rcIgmpGroupIfIndex = 0
(GroupIpAddress = 47.142.106.70 Port = 0 Members 47.142.106.71)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.44
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
```

2.63.4 Field descriptions

Table 57: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, rcIgmpGroupIfIndex and node ID of the device.

2.63.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.63.6 Additional information

This alarm requires no additional information.

2.64 Alarm (PP374)

rcnIgmppNewQuerier, Trap OID is 1.3.6.1.4.1.2272.1.21.0.45

2.64.1 Explanation

The PP374 alarm signifies that a new querier has come up on an interface.

2.64.2 Action

Please refer to ERS8600 Fault Management document.

2.64.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.64.3.1 Format

2.64.3.2 NTSTD

zsups3f8 PP374 OCT26 01:28:50 0131 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: New Querier in interface
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; igmpInterfaceIfIndex=0
Specific Problem: New Querier in interface
Description: New Querier in interface: igmpInterfaceIfIndex = 0
(igmpInterfaceQuerier = 47.142.106.70)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.45
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.64.4 Field descriptions

Table 58: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.

Table 58: Field descriptions

Field	Value	Description
Component Id	character string	Indicates the IP address, igmpInterfaceIfIndex and node ID of the device.

2.64.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.64.6 Additional information

This alarm requires no additional information.

2.65 Alarm (PP375)

rcnIgmpQuerierChange, Trap OID is 1.3.6.1.4.1.2272.1.21.0.46

2.65.1 Explanation

The PP375 alarm signifies that the querier has changed.

2.65.2 Action

Please refer to ERS8600 Fault Management document.

2.65.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.65.3.1 Format

2.65.3.2 NTSTD

```

zsups3f8    PP375 OCT26 01:28:50 0133 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: Querier changed
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; igmpInterfaceIfIndex=0
Specific Problem: Querier changed
Description: Querier changed: igmpInterfaceIfIndex = 0 (NewQuerier =
47.142.106.70 igmpInterfaceQuerier = 47.142.106.71)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.46
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
```

2.65.4 Field descriptions

Table 59: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, igmpInterfaceIfIndex and node ID of the device.

2.65.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.65.6 Additional information

This alarm requires no additional information.

2.66 Alarm (PP376)

rcnDvmrpIfStateChange, Trap OID is 1.3.6.1.4.1.2272.1.21.0.47

2.66.1 Explanation

The PP376 alarm signifies that there has been a change in the state of a DVMRP interface.

2.66.2 Action

Please refer to ERS8600 Fault Management document.

2.66.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.66.3.1 Format

2.66.3.2 NTSTD

zsup3f8 PP376 OCT26 01:28:50 0121 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications

Cause: DVMRP interface state change
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; dvmrpInterfaceIfIndex=0
Specific Problem: DVMRP interface state change
Description: DVMRP interface state change: dvmrpInterfaceIfIndex = 0
(OperState = up)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.47
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.66.4 Field descriptions

Table 60: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, dvmrpInterfaceIfIndex and node ID of the device.
OperState	character string	Can be one of {up (1), down (2)}

2.66.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.66.6 Additional information

This alarm requires no additional information.

2.67 Alarm (PP377)

rcnDvmrpNewNbrChange, Trap OID is 1.3.6.1.4.1.2272.1.21.0.48

2.67.1 Explanation

The PP377 alarm signifies that a new neighbor has come up on a DVMRP interface.

2.67.2 Action

Please refer to ERS8600 Fault Management document.

2.67.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.67.3.1 Format

2.67.3.2 NTSTD

zsups3f8 PP377 OCT26 01:28:50 0123 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: New neighbor is up on DVMRP interface
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; dvmrpNeighborIfIndex=0
Specific Problem: New neighbor is up on DVMRP interface
Description: New neighbor is up on DVMRP interface:
dvmrpNeighborIfIndex= 0 (NeighborAddress = 47.142.106.70)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.48
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.67.4 Field descriptions

Table 61: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, dvmrpNeighborIfIndex and node ID of the device.

2.67.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.67.6 Additional information

This alarm requires no additional information.

2.68 Alarm (PP378)

rcnDvmrpNbrLossChange, Trap OID is 1.3.6.1.4.1.2272.1.21.0.49

2.68.1 Explanation

The PP378 alarm signifies that a new neighbor has gone down on a DVMRP interface.

2.68.2 Action

Please refer to ERS8600 Fault Management document.

2.68.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.68.3.1 Format

2.68.3.2 NTSTD

zsup3f8 PP378 OCT26 01:28:50 0125 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: Neighbor gone down on DVMRP interface
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; dvmrpNeighborIfIndex=0
Specific Problem: Neighbor gone down on DVMRP interface
Description: Neighbor gone down on DVMRP interface:
dvmrpNeighborIfIndex= 0 (NeighborAddress = 47.142.106.70)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.49
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.68.4 Field descriptions

Table 62: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, dvmrpNeighborIfIndex and node ID of the device.

2.68.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.68.6 Additional information

This alarm requires no additional information.

2.69 Alarm (PP379)

rcnFdbProtectViolation, Trap OID is 1.3.6.1.4.1.2272.1.21.0.59

2.69.1 Explanation

The PP379 alarm signifies that the system has violated the user configured limit for total number of fdb-entries learned on that port.

2.69.2 Action

Please refer to ERS8600 Fault Management document.

2.69.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.69.3.1 Format

2.69.3.2 NTSTD

zsups3f8 PP379 OCT26 01:28:50 0151 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: fdb-entries limit violation
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; PortIndex=1
Specific Problem: fdb-entries limit violation
Description: fdb-entries limit violation: PortIndex = 1 (VlanId = 1)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.59
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.69.4 Field descriptions

Table 63: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.

Table 63: Field descriptions

Field	Value	Description
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, PortIndex and node ID of the device.

2.69.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.69.6 Additional information

This alarm requires no additional information.

2.70 Alarm (PP380)

rcnLogMsgControl, Trap OID is 1.3.6.1.4.1.2272.1.21.0.60

2.70.1 Explanation

The PP380 alarm signifies whether or not the number of repetitions of the particular Log message has exceeded the particular frequency/count or not.

2.70.2 Action

Please refer to ERS8600 Fault Management document.

2.70.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.70.3.1 Format

2.70.3.2 NTSTD

```
zsup3f8      PP380 OCT26 01:28:50 0157 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: equipment
Cause: Log Message control trap
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Log Message control trap
Description: rcnLogMsgControl: SysMsgLogFrequency = 2
(SysMsgLogText = )
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.60
```

.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.70.4 Field descriptions

Table 64: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

2.70.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.70.6 Additional information

This alarm requires no additional information.

2.71 Alarm (PP381)

rcnSaveConfigFile, Trap OID is 1.3.6.1.4.1.2272.1.21.0.61

2.71.1 Explanation

The PP381 alarm signifies that either the runtime config or the boot config has been saved on the switch.

2.71.2 Action

Please refer to ERS8600 Fault Management document.

2.71.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.71.3.1 Format

2.71.3.2 NTSTD

zsup3f8 PP381 OCT26 01:28:50 0153 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: equipment

Cause: Run time / boot config saved on switch
 Time: Oct 26 01:28:50 2005
 Component ID: ERS8600=47.142.106.1
 Specific Problem: Run time / boot config saved on switch
 Description: Config saved on switch: SysAction = none
 (SysConfigFileName = boot.conf)
 .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.61
 .1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.71.4 Field descriptions

Table 65: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.
SysAction	character string	Can be one of {none (1), hardReset (2), softReset (3), saveToNVRAM (4), resetCounters (5), saveToStandbyNVRAM (6), cpuSwitchOver (7), checkSwInFlash (8), checkSwInPcmcia (9), resetConsole (10), resetModem (11), flushIpRouteTbl (12), saveRuntimeConfig (13), saveRuntimeConfigToSlave (14), saveBootConfig (15), saveSlaveBootConfig (16), reset1stStatCounters (17)}

2.71.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.71.6 Additional information

This alarm requires no additional information.

2.72 Alarm (PP382)

rcnDNSRequestResponse, Trap OID is 1.3.6.1.4.1.2272.1.21.0.62

2.72.1 Explanation

The PP382 alarm signifies that the switch had sent a query to the DNS server or it had received a successful response from the DNS Server.

2.72.2 Action

Please refer to ERS8600 Fault Management document.

2.72.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.72.3.1 Format

2.72.3.2 NTSTD

zsups3f8 PP382 OCT26 01:28:50 0155 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: Request/Response from DNS server
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Request/Response from DNS server
Description: Request sent to or response got from DNS server:
DnsServerLastIpAddr = 47.154.182.1 (DnsRequestType = request)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.62
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.72.4 Field descriptions

Table 66: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.
DnsRequestType	character string	Can be one of {request (0), response (1)}

2.72.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.72.6 Additional information

This alarm requires no additional information.

2.73 Alarm (PP383)

pingProbeFailed, Trap OID is 1.3.6.1.2.1.80.0.1.0

2.73.1 Explanation

The PP383 alarm is generated when a probe failure is detected when the corresponding pingCtlTrapGeneration object is set to probeFailure(0) subject to the value of pingCtlTrapProbeFailureFilter. The object pingCtlTrapProbeFailureFilter can be used to specify the number of successive probe failures that are required before this notification can be generated.

2.73.2 Action

Please refer to ERS8600 Fault Management document.

2.73.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.73.3.1 Format

2.73.3.2 NTSTD

```
zsups3f8    PP383 OCT26 01:28:50 0135 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: Probe failure is detected
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Probe failure is detected
Description: Probe failure is detected: (ping TargetAddress =
47.154.182.56)
.1.3.6.1.2.1.80.1.3.1.8.0: 0
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.80.0.1.0
.1.3.6.1.2.1.80.1.3.1.4.0: 2485256176
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
.1.3.6.1.2.1.80.1.3.1.9.0: 0
.1.3.6.1.2.1.80.1.3.1.5.0: 1208611943
.1.3.6.1.2.1.80.1.3.1.10.0:
.1.3.6.1.2.1.80.1.3.1.6.0: 941686800
.1.3.6.1.2.1.80.1.3.1.7.0: 1208902023
.1.3.6.1.2.1.80.1.3.1.3.0: 8a
```

2.73.4 Field descriptions

Table 67: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

2.73.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.73.6 Additional information

This alarm requires no additional information.

2.74 Alarm (PP384)

pingTestFailed, Trap OID is 1.3.6.1.2.1.80.0.2.0

2.74.1 Explanation

The PP384 alarm is generated when a ping test is determined to have failed when the corresponding pingCtlTrapGeneration object is set to testFailure(1). In this instance pingCtlTrapTestFailureFilter should specify the number of probes in a test required to have failed in order to consider the test as failed.

2.74.2 Action

Please refer to ERS8600 Fault Management document.

2.74.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.74.3.1 Format

2.74.3.2 NTSTD

```
zsup3f8    PP384 OCT26 01:28:50 0137 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
```

Cause: Ping test failed
 Time: Oct 26 01:28:50 2005
 Component ID: ERS8600=47.142.106.1
 Specific Problem: Ping test failed
 Description: Ping test failed: (ping TargetAddress = 47.154.182.56)
 .1.3.6.1.2.1.80.1.3.1.8.0: 0
 .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.80.0.2.0
 .1.3.6.1.2.1.80.1.3.1.4.0: 2485256176
 .1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
 .1.3.6.1.2.1.80.1.3.1.9.0: 0
 .1.3.6.1.2.1.80.1.3.1.5.0: 1208611943
 .1.3.6.1.2.1.80.1.3.1.10.0:
 .1.3.6.1.2.1.80.1.3.1.6.0: 941686800
 .1.3.6.1.2.1.80.1.3.1.7.0: 1208902023
 .1.3.6.1.2.1.80.1.3.1.3.0: 8a

2.74.4 Field descriptions

Table 68: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

2.74.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.74.6 Additional information

This alarm requires no additional information.

2.75 Alarm (PP385)

pingTestCompleted, Trap OID is 1.3.6.1.2.1.80.0.3.0

2.75.1 Explanation

The PP385 alarm is generated at the completion of a ping test when the corresponding pingCtlTrapGeneration object is set to testCompletion(4).

2.75.2 Action

Please refer to ERS8600 Fault Management document.

2.75.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.75.3.1 Format

2.75.3.2 NTSTD

```

zsups3f8    PP385 OCT26 01:28:50 0139 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: Ping test completed
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Ping test completed.
Description: Ping test completed: (ping TargetAddress = 47.154.182.56)
.1.3.6.1.2.1.80.1.3.1.8.0: 0
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.80.0.3.0
.1.3.6.1.2.1.80.1.3.1.4.0: 2485256176
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
.1.3.6.1.2.1.80.1.3.1.9.0: 0
.1.3.6.1.2.1.80.1.3.1.5.0: 1208611943
.1.3.6.1.2.1.80.1.3.1.10.0:
.1.3.6.1.2.1.80.1.3.1.6.0: 941686800
.1.3.6.1.2.1.80.1.3.1.7.0: 1208902023
.1.3.6.1.2.1.80.1.3.1.3.0: 8a

```

2.75.4 Field descriptions

Table 69: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

2.75.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.75.6 Additional information

This alarm requires no additional information.

2.76 Alarm (PP386)

traceRoutePathChange, Trap OID is 1.3.6.1.2.1.81.0.1.0

2.76.1 Explanation

The PP386 alarm signifies that the path to a target has changed.

2.76.2 Action

Please refer to ERS8600 Fault Management document.

2.76.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.76.3.1 Format

2.76.3.2 NTSTD

```
zsup3f8      PP386 OCT26 01:28:50 0141 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: The path to a target has changed
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: The path to a target has changed
Description: The path to a target has changed: (TargetAddress =
47.154.182.56)
.1.3.6.1.2.1.81.1.3.1.4.0: unknown
.1.3.6.1.2.1.81.1.2.1.3.0: unknown
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.81.0.1.0
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
.1.3.6.1.2.1.81.1.3.1.5.0: 0.0.0.0
```

2.76.4 Field descriptions

Table 70: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

2.76.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.76.6 Additional information

This alarm requires no additional information.

2.77 Alarm (PP387)

traceRouteTestFailed, Trap OID is 1.3.6.1.2.1.81.0.2.0

2.77.1 Explanation

The PP387 alarm signifies that the system could not determine the path to a target.

2.77.2 Action

Please refer to ERS8600 Fault Management document.

2.77.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.77.3.1 Format

2.77.3.2 NTSTD

```
zsups3f8    PP387 OCT26 01:28:50 0143 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: Could not determine the path to a target
Time: Oct 26 01:28:50 2005
```


Component ID: ERS8600=47.142.106.1
Specific Problem: Could not determine the path to a target
Description: Could not determine the path to a target: (TargetAddress = 47.154.182.56)
.1.3.6.1.2.1.81.1.3.1.4.0: unknown
.1.3.6.1.2.1.81.1.2.1.3.0: unknown
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.81.0.2.0
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
.1.3.6.1.2.1.81.1.3.1.5.0: 0.0.0.0

2.77.4 Field descriptions

Table 71: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

2.77.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.77.6 Additional information

This alarm requires no additional information.

2.78 Alarm (PP388)

traceRouteTestComplete, Trap OID is 1.3.6.1.2.1.81.0.3.0

2.78.1 Explanation

The PP388 alarm signifies that the path to a target has just been determined.

2.78.2 Action

Please refer to ERS8600 Fault Management document.

2.78.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.78.3.1 Format

2.78.3.2 NTSTD

zsups3f8 PP388 OCT26 01:28:50 0145 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: communications
Cause: The path to a target has just been determined.
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: The path to a target has just been determined.
Description: The path to a target has just been determined: (TargetAddress = 47.154.182.56)
.1.3.6.1.2.1.81.1.3.1.4.0: unknown
.1.3.6.1.2.1.81.1.2.1.3.0: unknown
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.2.1.81.0.3.0
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
.1.3.6.1.2.1.81.1.3.1.5.0: 0.0.0.0

2.78.4 Field descriptions

Table 72: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

2.78.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.78.6 Additional information

This alarm requires no additional information.

2.79 Alarm (PP389)

UDPEapSessionEndTrap, Trap OID is 1.3.6.1.4.1.562.42.5.1.3.2.2

2.79.1 Explanation

The PP389 alarm signifies that the UDPEap session has ended.

2.79.2 Action

Please refer to ERS8600 Fault Management document.

2.79.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.79.3.1 Format

2.79.3.2 NTSTD

```
zsup3f8    PP389 OCT26 01:28:50 0149 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: other
Cause: Session end trap
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Session end trap
Description: UDPEapSession end trap
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.562.42.5.1.3.2.2
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
.1.3.6.1.4.1.562.42.5.1.3.1.1.9: 0
.1.3.6.1.4.1.562.42.5.1.3.1.1.8: 0
.1.3.6.1.4.1.562.42.5.1.3.1.1.7: 0
.1.3.6.1.4.1.562.42.5.1.3.1.1.4:
.1.3.6.1.4.1.562.42.5.1.3.1.1.3:
.1.3.6.1.4.1.562.42.5.1.3.1.1.2:
.1.3.6.1.4.1.562.42.5.1.3.1.1.1: 0
```

2.79.4 Field descriptions

Table 73: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

2.79.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.79.6 Additional information

This alarm requires no additional information.

2.80 Alarm (PP390)

UDPEapSessionStartTrap, Trap OID is 1.3.6.1.4.1.562.42.5.1.3.2.1

2.80.1 Explanation

The PP390 alarm signifies that the UDPEap session has started.

2.80.2 Action

Please refer to ERS8600 Fault Management document.

2.80.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.80.3.1 Format

2.80.3.2 NTSTD

```
zsup3f8      PP390 OCT26 01:28:50 0147 INFO PP Fault
Location: ERS8600_RTP;47.142.106.1
State: None
Category: other
Cause: Session start trap
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1
Specific Problem: Session start trap
Description: UDPEapSession start trap
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.562.42.5.1.3.2.1
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.
.1.3.6.1.4.1.562.42.5.1.3.1.1.7: 0
.1.3.6.1.4.1.562.42.5.1.3.1.1.6:
.1.3.6.1.4.1.562.42.5.1.3.1.1.5:
.1.3.6.1.4.1.562.42.5.1.3.1.1.10: 0
.1.3.6.1.4.1.562.42.5.1.3.1.1.4:
.1.3.6.1.4.1.562.42.5.1.3.1.1.3:
.1.3.6.1.4.1.562.42.5.1.3.1.1.2:
.1.3.6.1.4.1.562.42.5.1.3.1.1.1: 0
```

2.80.4 Field descriptions

Table 74: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

2.80.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.80.6 Additional information

This alarm requires no additional information.

2.81 Alarm (PP391)

rcnDuplicateIpAddress, Trap OID is 1.3.6.1.4.1.2272.1.21.0.63

2.81.1 Explanation

The PP391 alarm signifies that a duplicate IP address is detected on the subnet.

2.81.2 Action

Please refer to ERS8600 Fault Management document.

2.81.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.81.3.1 Format

2.81.3.2 NTSTD

```
zsup3f8 *** PP391 OCT26 01:28:50 0159 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: communications
Cause: More than one host with the same IP address have been detected
on a subnet.
Time: Oct 26 01:28:50 2005
```

Component ID: ERS8600=47.142.106.1
Specific Problem: Duplicate IP address detected on the subnet.
Description: Duplicate IP address detected on subnet:
NetAddress=47.154.182.56 (PhysicalAddress= 00-08-74-F0-3C-EC)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.63
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.81.4 Field descriptions

Table 75: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address and node ID of the device.

2.81.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.81.6 Additional information

This alarm requires no additional information.

2.82 Alarm (PP392)

rcnLoopDetectPortDown, Trap OID is 1.3.6.1.4.1.2272.1.21.0.64

2.82.1 Explanation

The PP392 alarm signifies that a loop has been detected on a port and the port is going to shut down.

2.82.2 Action

Please refer to ERS8600 Fault Management document.

2.82.3 Corresponding Clear Log

This alarm has no corresponding clear alarm.

2.82.3.1 Format

2.82.3.2 NTSTD

zsup3f8 *** PP392 OCT26 01:28:50 0161 TBL PP Fault
Location: ERS8600_RTP;47.142.106.1
State: Raised
Category: communications
Cause: A network configuration error is creating a loop between ports in a vlan
Time: Oct 26 01:28:50 2005
Component ID: ERS8600=47.142.106.1; portIndex=1
Specific Problem: Loop detected on a port and port is going to shut down
Description: Loop detected on port: PortIndex=1 (AdminStatus=up OperStatus=down)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.64
.1.3.6.1.2.1.1.3.0: 40 days, 16 hours, 52 minutes, 18 seconds.

2.82.4 Field descriptions

Table 76: Field descriptions

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the alarm.
Component Id	character string	Indicates the IP address, portIndex and node ID of the device.
AdminStatus	character string	Can be one of {up (1), down (2), testing (3)}
OperationStatus	character string	Can be one of {up (1), down (2), testing (3), unknown (4), dormant (5)}

2.82.5 Associated Operational Measurements or Performance Measurements

This alarm has no associated OM registers.

2.82.6 Additional information

This alarm requires no additional information.

Product = IEMS

A00013508--System Manager Auto-failover Support

Functional Description

1: Applicable Solution(s)

UA-IP

1.1 Introduction

This document gives the overall design level changes required in the IEMS Software to integrate the System Manager Auto-Failover Support functionality in to IEMS. System Manager is already being managed by the IEMS, but due to a requirement, System Manager is going to include the Auto-Failover functionality on it, which will lead to certain changes in the Data Exchange between the IEMS and the System Manager. This document captures all such changes and the necessary IEMS side modifications required to perform the System Manager Management as expected.

1.2 Scope

This document only covers the IEMS software related design changes to support the System Manager Auto-Failover functionality. Details that are not discussed on this document remain the same.

1.3 Existing IEMS-System Manager Interface

IEMS manages the following devices under the System Manager umbrella,

- MCS Manager and
- FPM Manager

All these share a similar type of Inventory, Fault and Performance handling in IEMS. These devices can be provisioned in to the IEMS either in a Simplex or Duplex mode. If the device is added in the Simplex mode, a parent logical Folder will be added to the IEMS topology and the physical unit (_0) will be added as a child object to the Logical Folder. In the case of a duplex provisioning, two physical unit objects (_0 and _1) will be added under the Logical folder. Each of these physical unit objects will have its own Fault Connector to receive the faults from the System Manager.

All the incoming faults will be associated against the physical unit objects and the parent will be given the status of the active unit. At any point of time only

one of the units will be active and the other one will be shown as in-active in the IEMS system. A swact will be identified whenever a trap comes from the current in-active node or during the status poll cycle. The status polling will be happening on the physical units by sending SNMP requests.

The Performance Collection on the System Manager in IEMS happens by a SFTP PULL Mechanism. IEMS will be pulling the performance files from the System Manager device using SFTP connection. A concern was raised on this mechanism as this might lead to processing older data initially or processing already processed files after a double swact on the device side.

1.4 Requirements & Design Changes

1.4.1 Auto-Failover Functionality

The System Manager is going to provide the Auto-Failover ability from the upcoming SN09FF release. This in turn will introduce the following changes in the way the data's are forwarded or sent to the OSS (IEMS in this case). IEMS being the Management software of System Manager has to make sure that the changes will not affect the Fault, Performance and other Management activities due to this. The major changes with respect to the IEMS data exposure due to the Auto-Failover support will be,

- SNMP Traps (Faults from the System Manager) will have the Logical IP Address as their source address instead of the physical unit IP address.
- SNMP Requests should be coming to the Logical IP Address of the System Manager to retrieve any fault or performance data.
- No Stranded data should be passed on to the OSS from the System Manager via IEMS

IEMS will undergo the following design changes to get integrated with the above changes:

- Inventory and status poll handling
- Fault handling
- Performance handling
- Ensuring backwards compatibility of system manager devices

Each of these aspects is discussed in order in the following paragraphs.

1.4.2 Inventory & Status poll Handling:

The IEMS Inventory or Topology Handling will remain the same, as it exists now. There will be a Logical Folder representing the System Manager and the Physical units will be shown under the Logical Folder as their children based on the mode of the device.

The status of the child units will be shown based on a status poll made on the physical unit IP Address. Meaning the status of the physical units will be determined by sending SNMP requests to the System Manager physical unit address instead of the Logical IP Address. This will help us to identify the active and in-active units if the device is a duplex device. This is possible only if the System Manager is able to respond to SNMP requests sent to the physical unit address on the active and should not respond on the inactive side.

Whenever a Simplex System Manager is provisioned in to IEMS, it will do the status polling with the IP Address that is specified while adding the device.

Whenever a Duplex System Manager is added to the IEMS, it will try to communicate with the device using the physical unit 0 address, If this is successful, IEMS will show the unit 0 in the active state and the other unit in the inactive state. If the query fails, IEMS will try to send a request to unit 1, if that succeeds; unit 1 will be shown active. If both the units fail to respond, IEMS will raise a loss of communication alarm and show the device as down. In the next poll cycle, the polling will happen to the current active unit and the status will be determined. If that fails, IEMS will request the other unit and if the request succeeds, IEMS will consider that a swact has happened on the device side. And the swact related processing would be triggered.

1.4.3 Fault Handling:

IEMS will only be registering for Traps from the System Manager's Logical IP Address instead of the physical unit address. There will be a single Fault Adaptor for a System Manager irrespective of the mode in which it is provisioned in the IEMS. This Adaptor will be listening for Traps from the System Manager and will be parsing them based on the NMI Trap definition. No new traps or no format changes were introduced as a part of this feature. The traps/faults will be associated against the physical unit (unit 0 or unit 1) which ever is active. The parent logical folder will be replicating the status of the active unit.

IEMS will also be processing the coldStart and warmStart generic traps from the Logical address. The coldStart will be considered as an indication of the device reset, on receiving this,

- IEMS will initiate a status poll to identify the active unit instance and
- IEMS will clear all the existing alarms against the System Manager and will resync them from the device.

Upon receiving a warmStart trap, IEMS will consider that a swact has happened on the device side.

- IEMS will simply do a swact in its Inventory information. Note that IEMS will not try to verify the state of the units on receiving a warmStart trap, it will just swap the active and in-active state of the units and

- IEMS will clear all the existing alarms against the System Manager and will resync them from the device.

The other entire fault handling techniques like automatically resynchronizing the missed alarms remains unchanged. Note that when a swact happens the Trap Sequence Number is not being maintained on the System Manager, hence a resync will always happen after a swact. The resynchronization SNMP requests will be sent to the Logical IP Address.

In addition to the processing of incoming traps, the Fault Adaptor will also take care of the Swact handling based on the status polling as mentioned in the Inventory and Status poll Handling Topic.

1.4.4 Performance Handling:

The Performance collection from the System Manager will be happening using the same SFTP PULL Mechanism. Additional changes will be made

- To avoid processing an already processed file and
- To avoid processing older data from the System Manager.

To achieve the above-mentioned requirements, IEMS will rename the files that were collected from the System Manager so that it will know if the same file is collected again in the next cycle. The supported file extensions in the System Manager are:

.active(.gz) – refers to the file which is currently being written

.closed(.gz) – refers to the file which has the data completely written to it

.reading(.gz) – refers to the files which are currently being read by an external application

.processed(.gz) – refers to the files which are processed by the external system

.err – refers to an erred condition file (due to sudden death of the unit)

The .gz refers to the compressed version of files if compression is enabled on the device side. The system can either write the files compressed or plain files.

IEMS will be collecting the files with the extension “**.closed**” and it will be renaming that to “**.processed**” and hence will know that the file has been already collected.

Whenever a System Manager is provisioned and a collection Job is provisioned, IEMS will establish the SFTP session with the device and will modify the .closed files to .processed files to avoid processing the older data. This file-resetting algorithm will happen during,

- Initial System Manager and Collection Job provisioning.
- After a swact identification on the device side.
- After an IEMS restart, if the collection job is available.
- When the device is unmanaged and re-managed.
- User name problems.

It has to be noted that renaming the files on the device side will require essential user permissions for the user that is specified while data filling the performance parameters at the time of provisioning the device. If the user specified does not have the required privileges to change the file name, a log will be generated by the IEMS to the OSS indicating the problem. This log will be generated even if the privilege gets changed down the time period. The same log will be used with a different description if IEMS is not able to login to the System Manager with the configured Username and the password details.

The log details will be as follows,

```
source - IEMS Mgr (associated against the IEMS object)
logname - EMJS
lognumber - 351
logkey - combination of logname and lognumber
severity - Major/Clear (raise/clear)
description -
Unable to login to the Device: <Device Name> with the
specified Username and password to collect PM data (If
login fails)
Insufficient privileges for the specified Username and
password to rename the PM files on the Device: <Device
Name> (If file renaming fails)
category - other
eventType - TBL/INFO (raise/clear)
eventLabel - IEMS OM Collection Job Failure
probableCause - communicationsSubsystemFailure
```

Note: The Username and password strings in the above log will not be replaced with the actual username and password information.

This alarm will be generated only once and will be cleared once the log situation is rectified. One important thing to note is that, if the above log situation arises, IEMS will not collect any data from the System Manager to avoid processing the same files again and again.

IEMS will not maintain the list of files processed in the earlier cycle for the System Manager since it is going to reset the file names after collection. IEMS will continue to collect the files using the physical unit addresses to avoid any loss of data during a swact. All the other performance collection aspects remain the same.

It has to be noted that the above design assumes that the Customer or the OSS will be retrieving the System Manager OM data only via IEMS. If the customer is going to use FTP PUSH directly from the SM/FPM, it will lead to loss of data on both the feeds (data being sent from IEMS and the data directly being pushed by the SM/FPM). This is due to the fact the file extension will be changed from .closed to .processed by the FTP PUSH configuration. This requires a special Note in the customer documentation to avoid wrong configurations.

All the above-mentioned changes are applicable to all the devices falling under the System Manager category that are provisioned as SN09FF devices in the IEMS.

1.4.5 Ensuring Backwards Compatibility of System Manager Devices:

IEMS has to maintain backwards compatibility for the System Manager devices. It has to be made possible for having N-2 Backward Compatible System Manager Management in IEMS. This means users will be able to provision or modify the existing System Managers to lower versions based on the N-2 requirement. Note that System Manager will not have a N-3 backwards compatibility, as there exists a major design change from SN07 -> SN08 MCS device Management. Hence if there is a SN07 MCS Mgr Configured in IEMS, this has to be removed and re-added as SN09FF MCS Mgr.

This N-2 support is not applicable for SSLines Mgr as that is a new device that is going to be supported from SN09FF IEMS releases.

1.5 Customer Visible Changes in IEMS due to this Activity

- 1 While Provisioning the System Manager in to IEMS, the user will have to specify the Logical IP of the System Manager in the Hostname/IP Address text field of the initial Add Node screen. In the existing scenario, this can be either the Logical IP or the Physical Unit IP.
- 2 Traps received from the Physical Unit address will not be considered as Traps from the System Manager; with this feature introduction IEMS will be listening for Traps from the Logical IP only.
- 3 The Resync Alarms Menu will be enabled in the Parent System Manager Object and the same will be disabled in the Physical Unit Objects, which is the opposite of what exists now.

- 4 The OSS will see a new Performance alarm EMJS351 if there are problems with the login details specified for collecting the PM Files from the System Manager and the same will be cleared if the problem is resolved.
- 5 A Note should be added to the customer documentation to avoid configuring a direct FTP PUSH OM Collection directly from the SM/FPM to Performance data collection.

Product = MCS

A00012242--TME-CD with GSM Wireless Client, Ph-1: “Mobility for Converged Desktop - MCD”

Functional Description

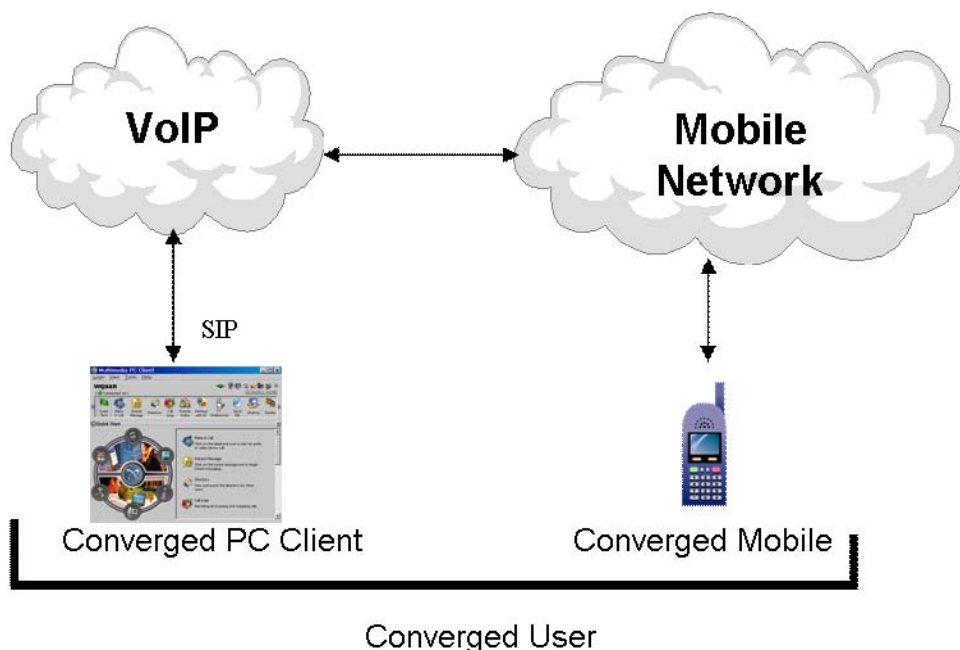
1: Applicable Solution(s)

MCS

1.1 Description

The Converged Desktop feature was introduced in previous versions of MCS and enabled subscribers to use their SIP PC Client for the multi-media portion of their communication, while using their existing telephony system for voice.

Figure 1 Mobile Converged Network



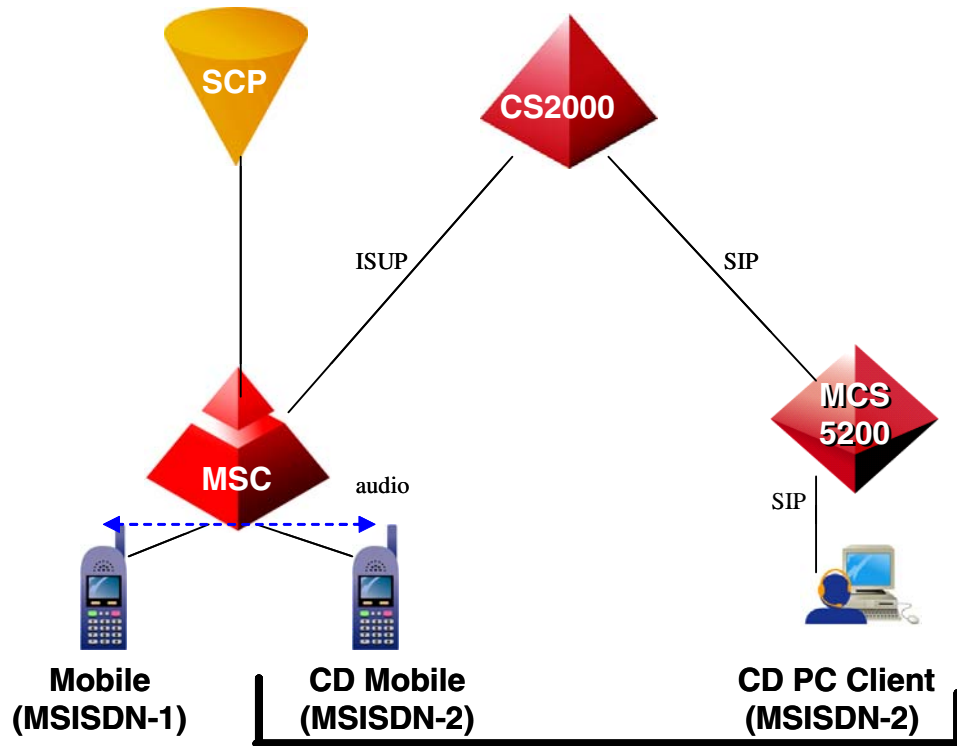
This feature provides a new Centrex service on the MCS application server that enables limited call control of wireless calls from the terminating Converged PC Client, while the audio streams to a preferred audio device in an existing wireless network. In this phase, the services are limited to terminating services without video.

Generally, the feature sets offered by each network are independent such that mobile features are not integrated with the MCS network. Only within the context of this feature are the networks ‘converged’. Features provided on the

mobile network are in no way limited by this feature. The operator should consider feature interactions, as they may intersect on the converged networks. Voicemail is an example of this interaction, as either / both networks can provide a network based voice mail service.

The network component view of the converged networks and the connectivity between the CD Mobile and the CD PC Client is shown in Figure 2.

Figure 2 Network Component Diagram



The mobile network is typically comprised of several MSC (and peripherals for the radio interface) so the illustration is simplified in this regard. The mobile converged phone is illustrated as 'CD Mobile' and is also referred to as the preferred audio device throughout this document. The established voice path (audio stream) is between the mobile terminals. The CD PC Client is used to manage calls terminating to CD Mobile.

The only Intelligent Network (IN) node illustrated on the mobile network is the SCP. This is clearly a simplification of the Intelligent Network, and the figure illustrates only the nodes relevant to this feature. The SCP serves as a central point of service logic, which includes the necessary digit manipulation and logic enabling the MCS to later supervise the call. Generally, the IN nodes are not assumed to be Nortel switching nodes.

The MSC is expected to possess SSP functionality to interact with the SCP. In general terms, the terminating mobile will subscribe to a trigger in the AIN terminating call model. Thereafter when a termination attempt is processed, the trigger will be hit, and call processing will suspend on the MSC to query the SCP for service processing. Service logic in the SCP will execute to prefix digits and respond to the query with an analyze_route message to the MSC. The MSC (SSP) will continue processing the call and terminate the call to the CS2000. The MSC (SSP) nodes of the network need not be Nortel switching nodes.

The Nortel CS2000 is a key network component employed to tandem calls between the MCS IP network and the mobile TDM network, and is a required component for this feature. The CS2000 serves as a gateway between the mobile network and the MCS IP network. When this feature is enabled, calls destined for CD Mobile will be routed through the CS2000 and down to the MCS5200 for supervision before being presented to the CD Mobile.

This converged network topology requires overflow route engineering on the CS2000 to ensure mobile calls are properly routed during an IP network outage. The CS2000 is able to detect the SIP trunk status by sending periodic heart-beat messages on the SIP trunk connecting it with the MCS5200. The SIP trunk status could be out-of-service if the MCS5200 becomes network isolated on the IP network or is simply offline for any reason. The CS2000 must be configured to route traffic to an alternate overflow route if the SIP trunk status is detected as out-of-service. The operator should engineer overflow routes on the CS2000 to accommodate the mobile traffic in such an outage on the MCS IP network. The operator should refer to CS2000 documentation for detailed discussions of provisioning this functionality.

This feature is only designed to interact with the clients shown in Figure 2. That is, the CS2000 and the MCS5200 may be hosting other lines and user agents, yet these call-types fall outside the scope of this feature.

Based on PC Client, this feature has been designed for Small to Medium Enterprises with limited access bandwidth, so that audio streams are never exchanged between the PC Client and the network. Once the terminating CD Mobile voice path is established, this feature allows the MCS 5200 to supervise all calls terminating to that CD Mobile via the MCD Client. Thus, the subscriber can use the MCD PC Client to modify the audio stream to the CD Mobile. This is made possible in the MCS IP network because the audio session can be updated (third party call control) without modifying the audio connection on the mobile network. The functionality provided by the MPC Client will be especially useful in scenarios with several concurrent calls, since the GUI of the MCD PC Client can be more intuitive in managing multiple calls and initiating multi-call features such as conference or transfer.

Provisioning this Centrex service requires configuration on the Mobile Network and the MCS network. As part of the PSTN configuration, a required dial-plan must be established (section 1.2.2 Dial Plans), and a prefix numbering scheme is provisioned by the operator across the network. Mobile CD subscribers will be provisioned on the SCP as fixed extensions of the company they belong to in the Corporate Service, linked to the company's new "non-existent" PBX (MCS). Unless otherwise stated, mobile features enabled on the PSTN are not coordinated with those provided by this service and therefore mobile subscribers can continue to invoke features from the mobile without the MCS5200 knowledge or supervision. This document will later consider only one such feature- voice mail.

On the MCS system, the operator must provision the following prefixes to use this mobility converged service. These can be provisioned on the sub-domain or the subscriber. If both the sub-domain and subscriber have a prefix provisioned, the subscriber prefix will be used. Provisioning is discussed in more detail in section 1.1.12.1 Service Prefix Provisioning.

- Destination Call Leg Return Code (CRD): This is the sum of navigational digits that will be placed in front of the (non CD) destination mobile number for outgoing calls from the MCD client to the mobile network.
- Associated Call Leg Return Code (CRA): This is the sum of navigational digits that will be placed in front of the CD destination mobile number (PAD). This prefix can be used to identify this call leg on the GSM network as a non-chargeable call.

On the MCS network, the operator can assign services and create service packages that expose features to the 'Personal Agent' and enable the feature set at the client. Some services are not compatible with this feature. Logic in the provisioning server will prevent incompatible services from being packaged together in the same service package. Section 20.7.1 Service Compatibility covers these service interactions in more detail.

The services that are supported in the MCD PC Client generally fall into two categories: multimedia services and voice services. Generally, multimedia services are available only to MCS clients. For example, the 'whiteboard collaboration' feature of the PC Client requires both parties to use the MCS PC Client. Multimedia services have no interaction with the mobile network. Multimedia services are supported only between MCS Clients, and can be enabled (and disabled) via the existing service assignment and packaging mechanism by the administrator. The existing behavior of the client is to render service related buttons only when that service is exposed to the subscriber. That is, the PC Client GUI has dynamic behavior based on the subscriber service package contents. This document assumes these services are enabled.

The following optional services are the only multimedia services supported in this feature. Services not listed will not be supported in this release.

- Collaboration: File Transfer
- Collaboration: Clipboard Transfer
- Collaboration: Web Push
- Collaboration: White Board
- SIP based Instant Messaging

The voice services in the MCD PC Client allow the subscriber to manage calls and invoke call related features. Some voice services will require service assignment and packaging. For example, conferencing requires the service 'Ad Hoc Conferencing' and the service package parameter for the 'maximum number of conference ports' is enforced in the MCS application server.

The MCD subscriber can perform the following services from the MCD PC Client. Services not listed will not be supported in this release.

- Originate new calls
- Receive incoming calls
- Hold and Retrieve calls
- Switch between several connected calls
- Direct transfer an existing call to another party
- Request a new conference
- Join all calls into a single conference

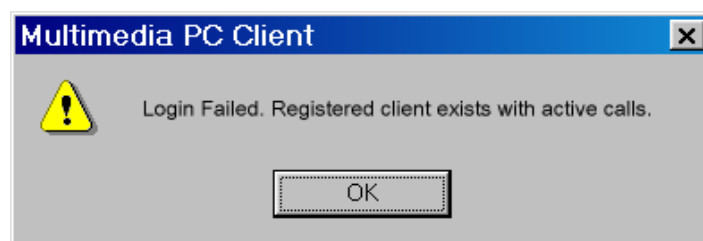
1.1.1 SIP Client Registration

All features of the MCD PC Client are enabled after successful login to a MCS Application Server. The authenticated login process essentially employs a SIP REGISER transaction to associate the users contact on the application server. Additionally, the client retrieves a service package which itemizes all services and capabilities available to the subscriber and the parameters associated with those services. This section details the registration behavior the subscriber can expect for various client configurations.

1.1.1.1 MCD Client Login

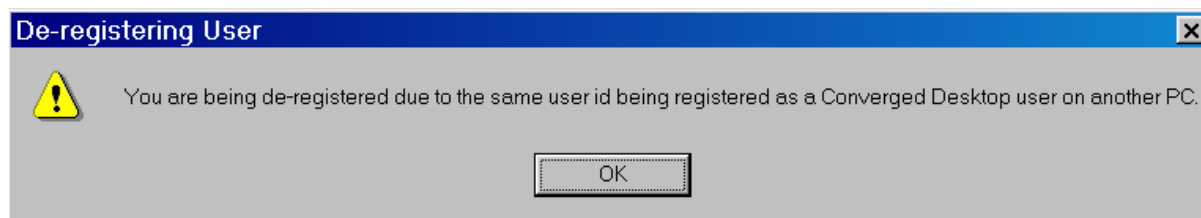
The mobile converged PC client logic is automatically activated in the Multimedia PC Client if the service package contains the Mobile Converged Desktop service. Unlike the previous converged-desktop client, once activated the PC Client may not be manually un-converged via the 'preference' GUI. The PC Client in the mobile converged mode of operation will be referred to as MCD PC Client within this document.

A subscriber should only login a single instance of the MCD PC Client. If the subscriber attempts to register a second instance of the MCD PC Client while calls are in progress, the second registration will be rejected by the MCS application server and the client will indicate to the user that active calls are still in progress.



If there are no calls in progress when the second instance registers, the first instance will be de-registered. The deregistered client will display a notification to the user as shown in Figure 3.

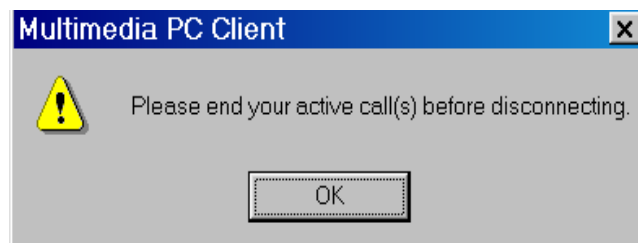
Figure 3 Deregistered on client



1.1.1.2 MCD Client Logout (or Exit)

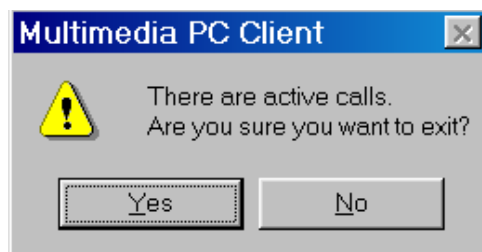
The subscriber may attempt to logout or exit the client at any time. The client logout process involves the typical SIP REGISTER (with a subscriber contact and expires of zero). During a 'Logout' attempt with active calls, the MCD PC Client will prompt the user to end active calls before disconnecting (Figure 4). The user can only click 'OK' and should manually release any active calls before proceeding with the logout.

Figure 4 Logout attempt with active calls



During an 'Exit' attempt with active calls, the MCD PC Client will warn the user that calls are still in progress. The user can either click 'Yes' to release all active calls and shutdown the client or 'No' to cancel the attempt.

Figure 5 Exit attempt with active calls



In the event the MCD PC Client becomes network isolated with active calls, the mobile subscriber will lose the ability to manage the existing calls. The best way to cleanup the existing calls is to release the PAD leg on the CD Mobile. The application server will automatically release all calls for the MCD subscriber when the CD Mobile (PAD) leg is released. Additionally, the MCS application server executes periodic call audits to release calls that are apparently stranded. The situation where the MCD client is network isolated or unavailable is discussed in more detail in 1.1.11 Client Unavailable / Calls of Grace.

1.1.1.3 Standard Client Registration

Non converged clients perform a 'standard' client registration upon subscriber login. If a subscriber with the MCD service assigned in the service package utilizes a non-converged client (e.g. I200x device), then call terminations to them will be presented to the clients using the existing call forking mechanism at the Application Server and no mobile converged client control functionality (as described in this document) will be provided.

1.1.2 Supported Releases of the Multimedia PC Client

The MCD PC Client functionality is only supported in the 4.1 release of the PC Client.

1.1.3 Call Origination Behavior

This section assumes the MCD PC Client is registered and the corresponding CD Mobile is actively available on the mobile network for originating calls. The subscriber can originate calls either from the CD Mobile or the MCD PC Client. The following sections consider the behavior for both scenarios. Detailed call processing (signaling) details are deferred to a later section.

1.1.3.1 MCD PC Client Origination / Click-to-call

Even though the MCD PC Client is not used for voice, the subscriber can use the MCD PC Client to originate calls. This call scenario is also referred to as 'click-to-call' and behaves much like a direct transfer. In the click-to-call

scenario, a call leg to CD Mobile is first established and immediately followed by the PAD being transferred to the destination mobile (MSISDN-2). All calls originated from the MCD PC Client employ the click-to-call mechanism.

The basic origination initiated on the MCD Client is performed by clicking 'New Call' and providing the address of the terminating mobile (MSISDN-2). The client will establish a secure HTTP connection (via SSL) to the Personal Agent to initiate the call to the MCS application server. Upon initiating the click-to-call, the MCD PC Client displays a call window similar to that shown in Figure 6. Call originations may be abandoned on the MCD Client.

Figure 6 Click-to-call Outgoing call window



Additionally, the click-to-call origination can be initiated directly from the Personal Agent web application. However in this case, the subscriber cannot cancel (abandon) the call attempt like on the MCD PC Client.

The mobile converged service suspends the MCD subscriber from making or receiving additional calls while a click to call outgoing call attempt is 'In Progress'. The MCS Session Manager will reject subsequent outgoing call attempts indicating that active calls are still in progress, and, likewise, the MCS Session Manager will also reject any incoming calls by responding with a 600 Busy Everywhere SIP response. Thus, once call is originated on the MCD PC Client, it will not be possible to originate another call from the client or terminate another call to the client until the initial call is either answered or terminated

1.1.3.2 CD Mobile

When the PAD originates a new call, the wireless network (MSC) will route the call without interaction with MCS application server. The MCD PC Client will not be supervised from the wireless network for originating call scenarios from the PAD.

1.1.4 Call Termination Behavior

This section assumes the MCD PC Client is registered and the corresponding CD Mobile is available on the mobile network for receiving calls. When a call attempt is made to the CD Mobile, the MCS application server will present the call to the registered MCD PC Client. The PC Client will display a call dialog GUI indicating a call is being received at the same time the CD Mobile starts ringing. This section discusses the MCD PC Client behavior for various terminating scenarios. Detailed call processing (signaling) details are deferred to section 1.2.4 PAD Terminated Scenarios.

MCD PC Client behavior depends on the subscriber assigned services. Thus, the MCD PC Client GUI may display icons that enable various features such as Reply with Instant Messaging, Transfer, or Conference. Recall, it is possible to limit the features exposed on the client by provisioning a service package without collaboration features, conferencing, etc. The following sections illustrate the client GUI behavior in the standard theme with all supported services enabled.

1.1.4.1 Call Window Before Answer

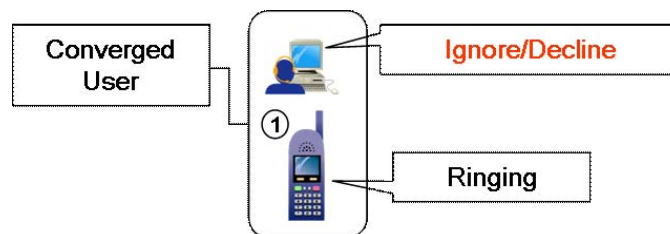
Before a call is answered on the CD Mobile, the MCD PC Client displays a call window similar to that shown in Figure 7. When the call is presented, a Picture-ID and the calling party number are provided. A custom Picture-ID is only available if the other end is an MCP user and has assigned such a picture in Preferences section of the Personal Agent. Otherwise a default Picture-ID¹ will be used. Additionally, the subscriber may have the option to initiate multimedia services such as SIP Instant Messaging². Recall, these services may not be exposed to all subscribers.

¹ The default Picture-ID can be modified in a custom PC Client theme.

² SIP Instant Messaging is not integrated with mobile network SMS messaging in this release.

Figure 7 Initial Inbound Call to MCD PC Client

Note the 'Answer' button is inactive. Thus, the audio options available for this pending call simply allow the subscriber to immediately ignore or decline the call.



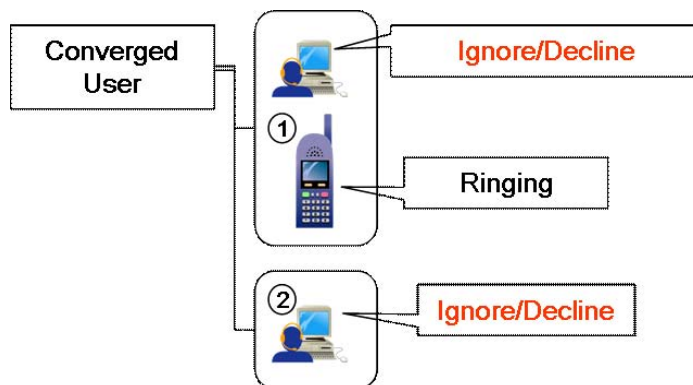
When the 'Ignore' button is pressed it would stop the client from ringing while the application server would continue executing any terminating services for the call. That is, terminating service logic is executed to route advance to another destination or voice mail. After all terminating services completed on the application server, it would release the call with cause and the mobile network could execute terminating services. Within the context of this feature, the Ignore button affects all user network contacts. This behavior, while typically customizable from the "Users Preference GUI -> Miscellaneous -> Ignore Buttons" menu, will not be customizable for the MCD PC Client.

The decline option results in releasing the call such that terminating services on the application server would cease for the call. The MCS application server would release the call with cause and the mobile network could execute terminating services.

The 'Answer' button remains disabled on the MCD PC Client until the CD Mobile has answered. That is, the initial call attempt to the CD Mobile can not be answered from the MCD PC Client. Subsequent calls can be answered from the MCD PC Client.

In the case of two or more simultaneous incoming calls prior to answering the CD Mobile, the 'Answer' buttons on all incoming call windows is disabled as shown in Figure 7. The first incoming call will be answered upon answering the CD Mobile, and the call window for that call will appear as shown in the following section. Additionally, the 'Answer' buttons on any remaining call windows will be enabled, and these remaining calls will be handled as subsequent incoming calls in the multiple call scenario described in section 1.1.5.1 Call Waiting.

Aside from the behavior of the 'Answer' button, multiple incoming pending calls will exhibit behavior similar to the initial call.



1.1.4.2 Call Window After Answer

An initial call can only be answered on the CD mobile. Thus, to accept this initial call the CD mobile answers the call. Once the call is answered on the mobile, the PAD leg is established. Subsequent calls may be answered from the PC client.

The MCD PC client call window updates after the CD mobile answers similar to the illustration in Figure 8. The MCS application server signals the client by means of a SIP message to update the GUI with new audio options

Figure 8 Initial call is answered on MCD PC client

The only supported audio options for answered calls are listed below.

Audio options available on answered call	
New Call	Used to place a new call. Clicking 'New Call' will implicitly (local) Hold any existing established calls.
Hold / Retrieve	The user can hold and retrieve the call from the MCD PC Client (local hold). However, the user cannot initiate a local hold if the call is already in remotely held. This scenario is referred to as dual-hold, and is not supported.
Conference	Initiates an audio conference. Established calls will be placed on local hold until conference is joined.
Transfer	Initiates a direct transfer of the established call to another destination.
Hang Up	Releases the established call. The CD Mobile call leg will remain established if other calls are on Hold by the MCD PC Client.

Assuming the originator is an MCS SIP subscriber, the following multimedia capabilities must be provisioned by the administrator to be utilized from the terminating MCD PC Client.

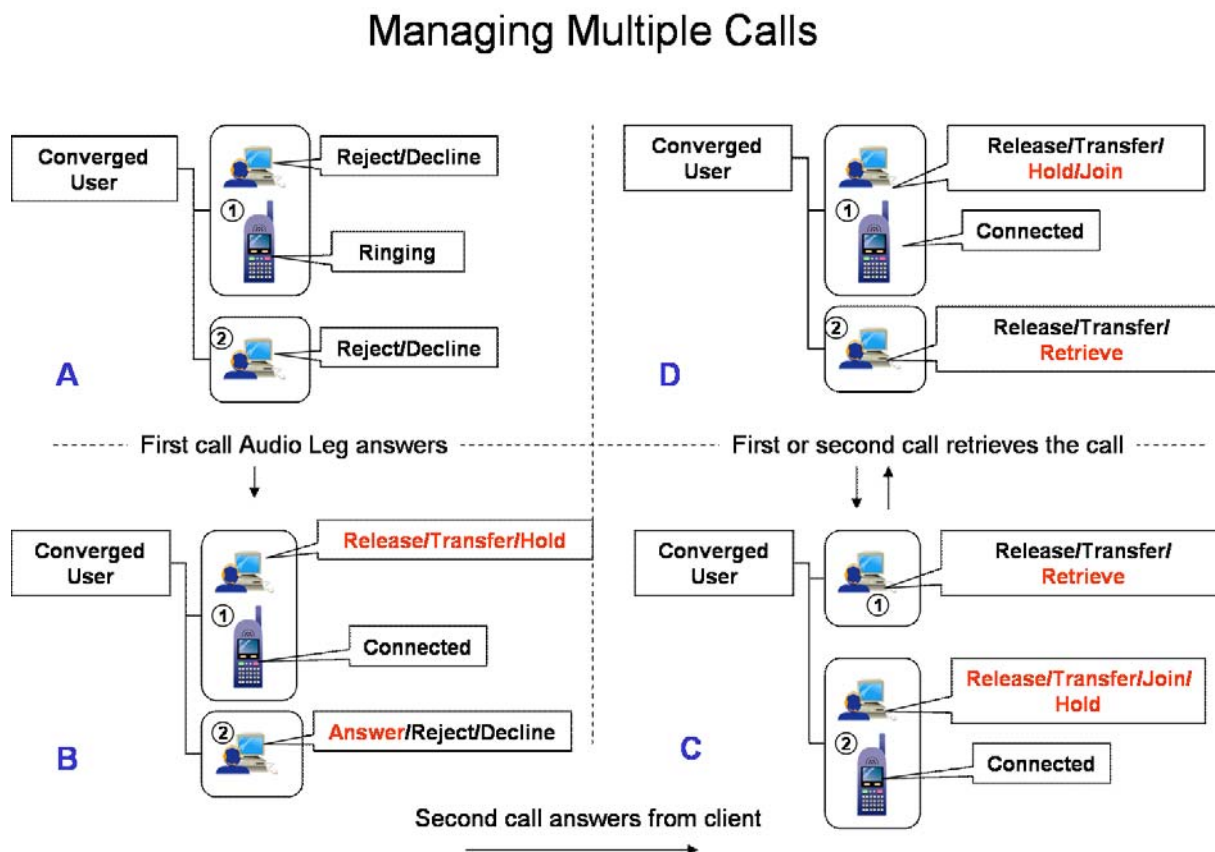
Multimedia capabilities available between MCS SIP clients	
Picture Calling Line Id	Shows a picture of the other party involved in the call
File Transfer	Allows the user to transfer files between MCS PC Client
White Board sharing	Allows the user to establish a White board collaboration session between MCS PC Client
Clip Board Transfer	Allows the user to send the 'clipboard' to another MCS PC Client
Web Co-browsing	Allows the user to push a web page to another MCS PC Client
Instant Messaging	Allows the user to establish SIP Instant Message session between MCS PC Clients
Presence state indications	The presence state of the MCD PC Client is monitored, while the state of the MCD Mobile (PAD) is not. On-the-phone presence is not supported.

1.1.5 MCD Multimedia PC Client with Multiple Calls

This feature introduces new behavior in the MCD PC Client to assist managing multiple established calls and call waiting scenarios. The MCD PC Client uses the PAD as the only audio device and therefore can only support one active voice conversation while the remaining established calls are placed on hold. Thus, the MCD PC Client now provides an interface to juggle several calls on behalf of the PAD.

An illustration summarizing multi-call PC Client behavior is shown in Figure 9. Each quadrant represents a scenario with two calls. The PAD is indicated by the mobile phone icon, and the features available to each call leg are shown in a box next to each.

Figure 9 Managing Multiple Calls



The quadrant labeled 'A' illustrates two incoming calls coming into the MCD PC Client, and the PAD has not yet answered. The PAD is ringing for the first inbound call attempt, and is therefore grouped together with the first call leg.

Just as the PAD answers, the transition to quadrant 'B' occurs. With the audio stream now established to the PAD, the MCD PC Client GUI is updated to reflect the functionality available to the converged user. The first call leg is associated to the PAD, and can now Hold, Release or Transfer the call from the MCD PC Client. The second call continues to ring, but the call can now be answered from the MCD PC Client. These new options are indicated in the figure with an orange color.

Assuming the second call leg is answered from the MCD PC Client, the transition to quadrant 'C' occurs. If the first call leg is not already on hold, upon answer the MCD PC Client will automatically place the first call leg on local hold. The MCS Session Manager will then exchange the audio stream to establish voice-path on the second call leg. Since the audio stream at the PAD is now established on the second call leg, the PAD is re-grouped to the second call leg in the figure. With multiple calls now active, the PC Client offers the

ability to establish a conference by introducing the 'Join' button on the established (PAD) call leg. If the user creates such a conference, all active call legs will reduce to a single call leg to the conference server (not shown). Additionally, the user may (direct) transfer this call from MCD PC Client to an alternate address.

The user can alternate between locally held calls from the MCD PC Client. The transition to quadrant 'D' indicates this behavior at the client. The MCS Session Manager will exchange the audio stream to the PAD to associate the single established call, while the remaining calls will be placed on local hold. At any time the converged user can 'Join' the calls into a single conference.

1.1.5.1 Call Waiting

Call waiting is the ability to present incoming calls while already engaged in a conversation. This section discusses how the subscriber can handle these subsequent calls. When a subsequent call is presented to the PC client, the available options are 'Answer', 'Ignore', 'Decline' or 'Reply with IM'. These options are similar to those presented on the initial call with the exception of the ability to answer the new call. The screenshot in Figure 10 illustrates these options.

Figure 10 Second inbound call to MCD PC Client



Audio options are similar to the pending call behavior as described in 1.1.4.1 Call Window Before Answer. There is no modification of the active CD Mobile (PAD) call leg.

If the subscriber chooses to answer the new call, the initial call is automatically placed on local hold by the MCD PC Client, and the audio will be established between the CD mobile and the new caller.

1.1.5.2 Joining Multiple Established Calls into Conference

When a subscriber already has an active call in progress and multiple calls on local hold, the converged PC client offers the ability to join these calls into conference. That is, the 'Conference' button will transition to a 'Join' button when multiple simultaneous calls are present. Note the 'Join' button in the active call GUI as shown in Figure 11.

Figure 11 Active Call



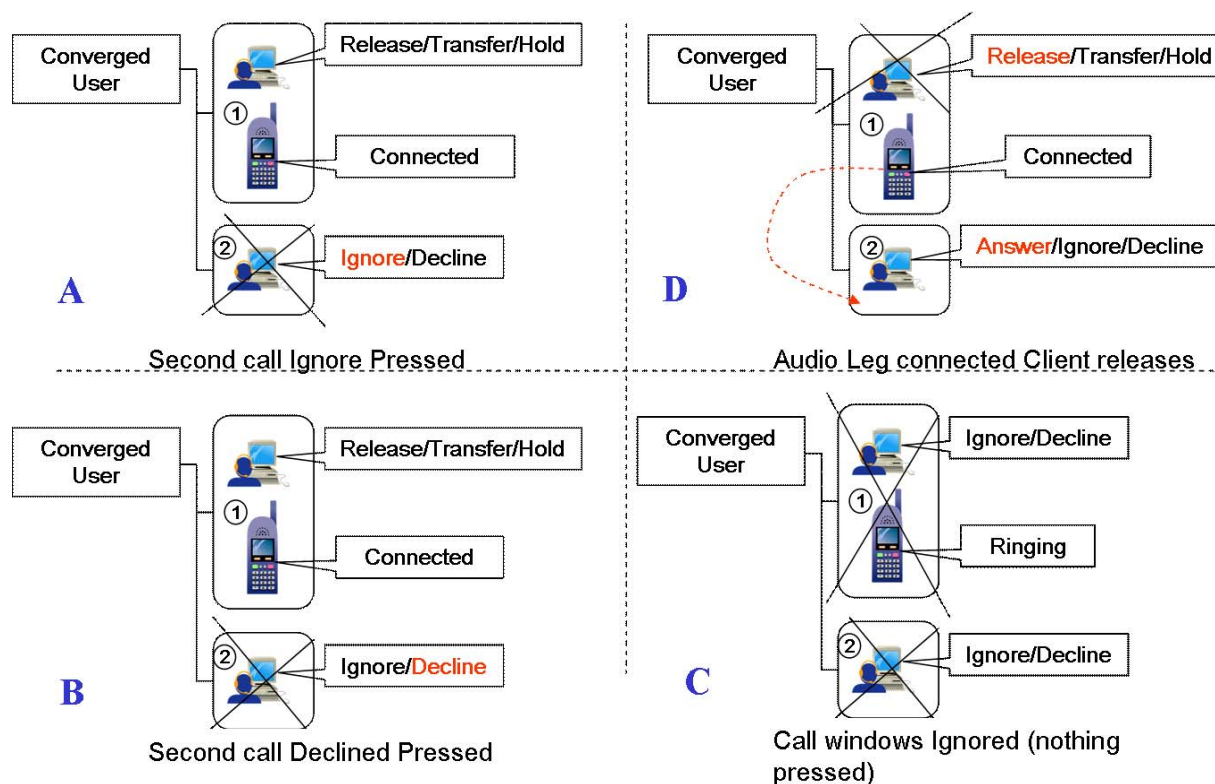
If the subscriber joins the calls into an audio conference, all the call dialogs will reduce to a single call dialog to 'Conference'. A maximum number of simultaneous calls are enforced on the MCS application server during call processing with the exception that the conference leg does not count against the maximum call limit while joining calls into a conference.

1.1.6 MCD Multimedia PC Client Release

This section considers the MPC Client behavior when calls are released. An illustration summarizing multi-call MPC Client release behavior is shown in Figure 12. Each quadrant represents a scenario with two calls. The PAD is indicated by the mobile phone icon, and the features available to each call leg are shown in a box next to each.

Figure 12 Release scenarios

Release Scenarios



The quadrant 'A' illustrates the scenario when a call is already established on the PAD and a subsequent call attempt is pending. The subscriber then chooses to ignore the second incoming call by clicking the 'Ignore' button. The Ignore function on the application server allows remaining terminating services to be executed, such as CPL. However, in the absence of CPL, the ignore will result in releasing the call attempt on the mobile network. The call released may not be forwarded to voice mail on the mobile network. For signaling details of this call processing scenario please refer to 20.3.4.2 Call Ignore from MCD PC Client.

Similarly, quadrant 'B' illustrates a subsequent pending call attempt. However, in this scenario the subscriber chooses to decline the call by clicking the 'Decline' button on the call window. The decline function on the application server does not allow remaining terminating services to run, and the call is immediately released. The call released may be forwarded to voice mail on the mobile network. For signaling details of this call processing scenario please refer to 20.3.4.2 Call Ignore from MCD PC Client.

The scenario shown in quadrant 'C' is a simple one, yet its significance can not be overlooked. The scenario involves two pending call attempts where the subscriber chooses to not press any buttons. Perhaps the subscriber is not physically at the PC Client at the time these call attempts are being made. Regardless, a couple of important topics to consider here are call timers and forwarding to voice mail. Typically a call attempt timer would expire (e.g. ISUP timer T9) and release the call with cause. The MCS application server will implement a timer to release these ignored call attempts with a cause. The mobile network may execute additional terminating services to handle the release with cause. For example, forward these unanswered calls to a voice mail system in the mobile network.

The release scenario in quadrant 'D' illustrates PC client behavior when the PAD leg is released while another pending call attempt is presented. When the user clicks the 'Hang Up' or 'Stop' button on the active call window the first call will be released, and the PAD would then be associated to the second call. However, the voice path would not be established until the 'Answer' button is pressed on the second pending call window

1.1.7 Direct Call Transfer

The MCD PC Client can perform a direct call transfer once the call is answered on the CD mobile. As part of the call transfer operation the PC client will automatically put the callers on local hold before transferring to the target party. The consult transfer functionality is not supported in this release.

1.1.8 Conference Calls

Only after an initial call is established can the MCD PC Client initiate a conference call and join multiple calls into a conference. Pending calls can not be joined into conference.

1.1.9 Hold / Retrieve

The MCD PC client control window provides the ability to initiate a hold for the call should that call be active, conversely a retrieve option (same button) is available should the call already be on hold.

The client will instigate the holding of the active call leg by means of a SIP INVITE to the Application Server with an SDP containing the following headers:

`c=0.0.0.0`, specifying 0.0.0.0 as the IP address for the audio connection

`m= audio 50010 RTP/AVP 0 8 18 110 111`, specifying 0 as the port for the audio connection

A held leg can then be subsequently retrieved by the client again sending a SIP INVITE but with a valid c= line. This will cause the Application Server to re-bridge the media via use of re-INVITES.

If the MCD subscriber has 'music on hold' in their service package then this feature will apply as appropriate in call hold scenarios.

1.1.10 Call Logs

Call logs provide the subscriber with a record of all incoming and outgoing calls. The PC Client will locally manage these call logs, as opposed to Network Call Logs (NCL) feature which resides on the Personal Agent. Calls may be originated from the call logs and will behave as described in 1.1.3.1 MCD PC Client Origination / Click-to-call.

1.1.10.1 Inbox

Inbound call attempts are recorded in the Inbox. The ability to successfully re-dial a caller from this call log depends on the calling line id provided by the adjacent switch (CS2K). The prefix (CRD) introduced in this feature will automatically be prefixed to the outgoing address to assist in routing.

1.1.10.2 Outbox

Only outbound call attempts made from the MCD PC Client are recorded in this Outbox. Outbound call originations from the PAD will not be recorded in this log (or the NCL).

1.1.11 Client Unavailable / Calls of Grace

Previous sections have described the PC Client behavior when both the converged PC Client and the converged Mobile are actively available and how the feature is then utilized. This section will focus on the feature behavior when the client is unavailable or transitions between available and unavailable. In this context 'unavailable' would mean the client is non-accessible due to network isolation or simply unregistered. In addition, the concept of the 'call of grace' will be presented, along with how these calls are handled on the application server.

Let us begin with a couple of simple scenarios. One simple scenario occurs when the subscriber is not logged in on a PC Client and the CD Mobile is available. Then mobile calls will continue to be routed back to the mobile network, where mobile terminating services may execute. Another simple scenario is when the CD Mobile is unavailable (maybe out-of-area or turned off) and the PC Client is registered. The PC Client does not have audio capabilities, and the PAD leg will not be established. These are the trivial cases not only because they involve only an initial call, but also because part of the converged client was unavailable.

More complicated scenarios can be constructed when the client transitions between active and inactive. Recall, for this feature the mobile network is configured to route calls to the MCS5200 by triggering service logic in the SCP. Thus, terminating services will be executed at the application server before being processed in the mobile network. This introduces the possibility of latency during call setup. To address this, the application server implements

a mechanism of detecting the PC client network connectivity and minimizing call latency. That is, all calls will be presented to the converged PC client via a SIP INVITE. In order to provide a consistent interface between the application server and the PC Client, irrespective of whether this is a new call or a subsequent call in a multi-call scenario, the client will auto-answer all initial INVITE requests received. This does not mean that the client has indicated that call should be answered; it simply means that the client has initiated a control window for this session and is ready for further instruction from the Application Server. The auto-answer approach simplifies the notification of the client when an initial call has been answered at the MCD mobile, and makes the detection of an isolated client far faster. The detection of an isolated client is faster since the Application Server will shorten the number of re-transmissions of the INVITE to four attempts (equaling 4 seconds) as the client should be auto-generating a 100 Trying provisional response followed by a final 200 OK response if available. The 100 Trying is the first response received by the Application Server to the INVITE and, in effect, indicates the client active and triggers the Application to cease retransmission of the INVITE request. The following examples discuss this behavior.

For example, it is possible for the PC Client to login after a non-CD call has already been established on the CD Mobile. Further assume subsequent call attempts to the converged subscriber occur. When the application server executes this feature as part of its terminating services, it will now present these subsequent calls to the newly registered PC client and create a new PAD leg. Thus, when the client is unregistered all call attempts will be directly presented to the CD Mobile. However, once the client is registered the application server must assume the client is available and attempt to present the call to the client (expecting the auto answer 200 OK from the client). The application server will process this as an initial call described in section 1.1.4 Call Termination Behavior.

Similarly, it is possible for the PC Client to become isolated after calls were established on the CD mobile. Further assume a subsequent call attempt to the converged mobile occurs. Since the MCS application server is aware of the initial established call, the application server does not modify the voice path until after the user clicks 'Answer' on the PC Client. The application server assumes the client is accessible and will transmit an INVITE expecting an auto-answer from the client. However, in this case the timer expires after four seconds, and only then does the application server route the call back to the mobile network. Once the application server detects the client is isolated (with established calls), an internal flag is set to store this isolated status. This flag is later observed when subsequent call attempts occur. When subsequent calls attempts occur and the client has previously been detected as isolated, most of these subsequent calls will be directly routed back to the mobile network to avoid the extra four second latency.

For the scenario when the application server has already detected an isolated client, the application server can be engineered to present one of every N subsequent call attempts to the PC client. These calls-of-grace will be presented to the PC client to test the client network connectivity. If the client network connectivity is restored, the multi-call behavior will resume as described in section 1.1.5 MCD Multimedia PC Client with Multiple Calls. The term call-of-grace refers to the scenario when the MCS application server presents a call to the PC Client even when the status of the MCD PC Client is assumed to be isolated. In this context, that one call attempt of N is considered a call-of-grace. The call-of-grace may involve longer call setup latency when the client remains isolated. The value of N is configured through the System Management Console as shown in section 1.1.12.7.1 CallOfGraceInterval. It must be a positive number (default=5), where N=0 deactivates these call-of-grace attempts.

When the MCD PC Client is registered and used to terminate mobile calls, limitations may apply that enforce a maximum number of simultaneous calls supervised at the MCS application server. This limits the number of simultaneous calls that are placed on local hold, or joined into a single conference. The calls routed directly to the mobile network do not count against this maximum number of calls as they are being handled by the CD mobile directly. Incoming call attempts from the mobile network that exceed this threshold will be rejected on the MCS application server (SIP 486 Busy Here).

Call audits occur on the MCS application server to verify established calls are still valid and to provide a mechanism to detect and release network resources that appear stranded. If the call has a Mobile call leg associated to it, the call audit will be forwarded on to the CS2000. If the call does not have a mobile call leg associated and fails the call audit, the application server will release the call to free network resources.

1.1.12 System Configuration and Provisioning

1.1.12.1 Service Prefix Provisioning

As part of the proposed prefix numbering scheme, the operator has to provision the following numbers for each domain to be used by the wireless converged service.

Destination Prefix (CRD): This is the prefix that will be placed in front of the destination number for outgoing calls from the MCD client.

Audio Device Prefix (CRA): This is the prefix that will be placed in front of the destination number for click to call scenarios from the MCD client.

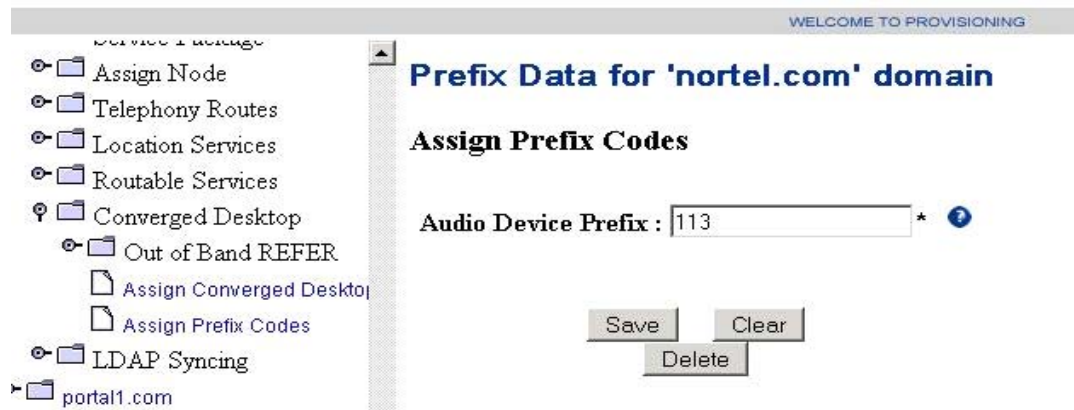
These numbers will be provisioned for each domain/sub-domain that will provide this service. The service on the MCS application server will

automatically insert these prefixes before translations are executed. Thus, it is important that the domain administrator has verified that translations do not exist that may conflict with this dial plan. If translations exist that match the CRA/CRD prefixed destination, calls may be misrouted.

1.1.12.1.1 Audio Device Prefix

A new option called “Assign Prefix Codes” will be added to the Converged Desktop Menu in the provisioning client to provision the audio device prefix.

Figure 13 Provisioning prefix codes



The following new methods will be added to the OPI interface to provision these prefixes. These methods will be added to the existing ConvergedDesktopServiceMgr interface.

```
/**
 * Adds the Prefix data for the mobile converged Service using the
 * Domain as the key
 * @param String domain, the domain to which the service data belong.
 * @param String domPrefixData, the new service data
 * @throws ProvisionException: This exception is thrown when an input
 * parameter is invalid,
 * a duplicate object exists in the data store, a dependency exists
 * in the data store or the data
 * store is not available.
 */
public void assignDomainMCPrefixData(String domain, String
domPrefixData) throws ProvisionException;

/**
```

* Returns the domain prefix data for the mobile converged Service using the Domain as the key

* @param String domainID, the domain to which the service data belong.

* @param String domPrefixData, the new service data

* @throws ProvisionException: This exception is thrown when an input parameter is invalid,

* a duplicate object exists in the data store, a dependency exists in the data store or the data

* store is not available.

*/

public String getDomainMCPrefixData(String domain) throws ProvisionException;

/**

* This method is used for removing prefix data associated with a domain for the mobile converged service

* @param String domain, domain from which the service data needs to be removed.

* @throws ProvisionException: This exception is thrown when an input parameter is invalid,

* a duplicate object exists in the data store, a dependency exists in the data store or the data

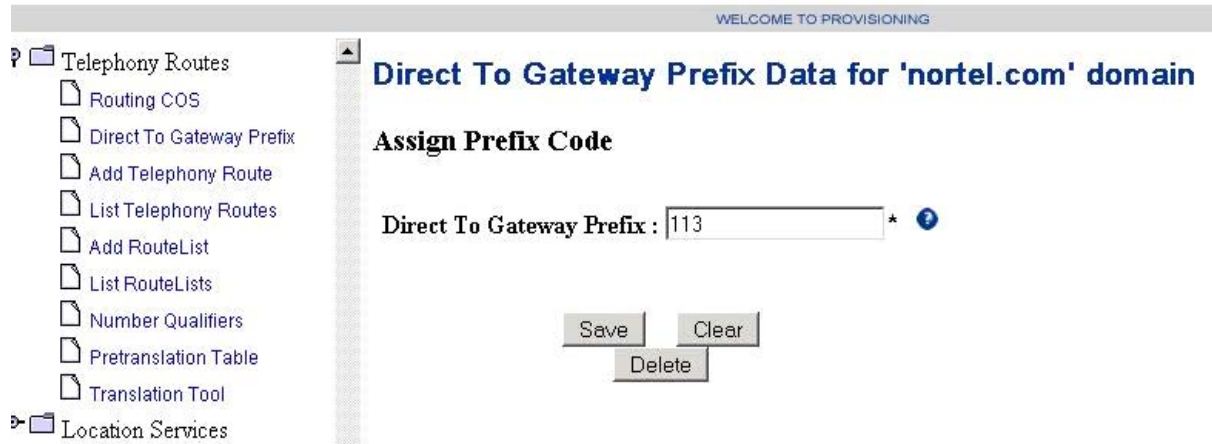
* store is not available.

*/

public void removeDomainMCPrefixData(String domain) throws ProvisionException;

1.1.12.1.2 Destination Prefix

A new option called “Direct To Gateway Prefix” will be added to the Telephony Routes menu in the provisioning client to provision the destination prefix or the direct to gateway prefix.



The following new methods will be added to the OPI interface to provision the direct to gateway or the destination prefix. These methods will be added to the existing TelephonyRouteMgr interface.

```
/**
```

```
 * This method is used to assign the DirectToGW service prefix data
to the domain
```

```
 * @param String domain, the domain name
```

```
 * @param String domPrefixData, the prefix data
```

```
 * @throws ProvisionException, if there was any problem retrieving
the
```

```
 * telephony Route information due to the data
```

```
 * store not being available or invalid data
```

```
 * being passed in
```

```
 **/
```

```
public void assignDirectToGatewayPrefixData (String domain, String
domPrefixData) throws ProvisionException;
```

```
/**
```

```
 * This method is used to get the DirectToGW service prefix data of
the domain
```

```
 * @param String domain, the domain name
```

```
 * @returns String domPrefixData, the prefix data
```



```
* @throws ProvisionException, if there was any problem retrieving
the
*
*         telephony Route information due to the data
*
*         store not being available or invalid data
*
*         being passed in
**/

public String getDirectToGWPrefixData (String domain) throws
ProvisionException;

/**
* This method is used to remove the DirectToGW service prefix data
of the domain
* @param String domain, the domain name
* @throws ProvisionException, if there was any problem retrieving
the
*
*         telephony Route information due to the data
*
*         store not being available or invalid data
*
*         being passed in
**/
```

1.1.12.2 Outbound Translations

This section provides an overview of the basic provisioning required on the MCS to route an outbound MCD PC Client originated call to the wireless network. Essentially two routes will need to be defined:

- Private route to the CS2000 – Used when signaling the destination mobile.
- Public route to the CS2000 – Used when signaling the CD Mobile (PAD).

The Mobile CD service will insert the prefixes automatically for the call. The routes are necessary for delivering the correct charge id (public/private) to the CS2000. The routes have to be based on the CRA/CRD values for each domain. A private route based on the CRD is required to send the private chargeid of the user i.e. CC+Ext as the calling party. A public route based on the CRA of the domain is required to send the public charge id of the user, i.e. MSISDN as the calling party.

The private and public charge ids for a user can be provisioned from the user details page in the provisioning client. From the above figure, the private charge id will be used when signaling the destination mobile and the public charge id will be used when signaling the CD mobile.

Provisioning screen shot of the user details page. The user's MSISDN should be provisioned as the public charge id and CC+Ext should be provisioned as the private charge id.

Figure 14 Provisioning subscriber charge IDs

The screenshot shows the 'Users' section of a provisioning interface. The left sidebar lists various configuration options, with 'Users' expanded. The main panel displays the details for a user named 'Test User'. The 'Private Charge ID' field is highlighted with a red box and contains the value 'CC+EXT'. The 'Public Charge ID' field contains the value 'MSISDN'. Other fields include 'First Name', 'Last Name', 'Service package' (set to 'gold'), 'Aliases', 'Status Reason' (set to 'ACTIVE'), 'email', 'Business Phone', 'Home Phone', 'Cell Phone', 'Pager', 'Fax', 'Directory Number', 'Location' (set to 'Use Domain Default Location 'Other''), 'Class of Service' (set to '--None Selected--'), 'Redirection Class of Service' (set to '--None Selected--'), 'Time Zone' (set to 'Pacific Standard Time'), and 'Locale' (set to 'English'). A 'Save' button is at the bottom right.

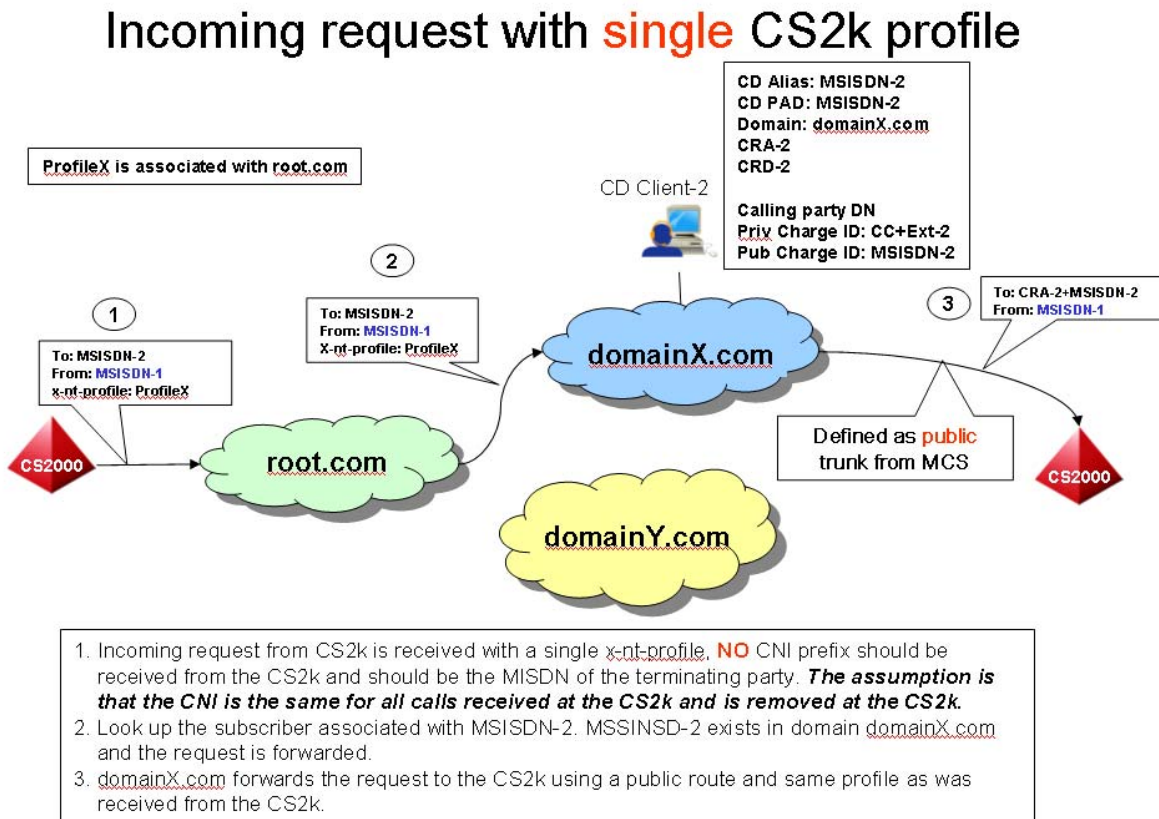
1.1.12.3 Inbound Translations

This section provides an overview of the basic provisioning required on the MCS to route an inbound call to a MCD subscriber.

1.1.12.3.1 Incoming Request with Single CS2K Profile

The following figure illustrates a call flow when there is only one CS2000 profile for all incoming requests. No translations are required in this case since the CNi is removed by the CS2K.

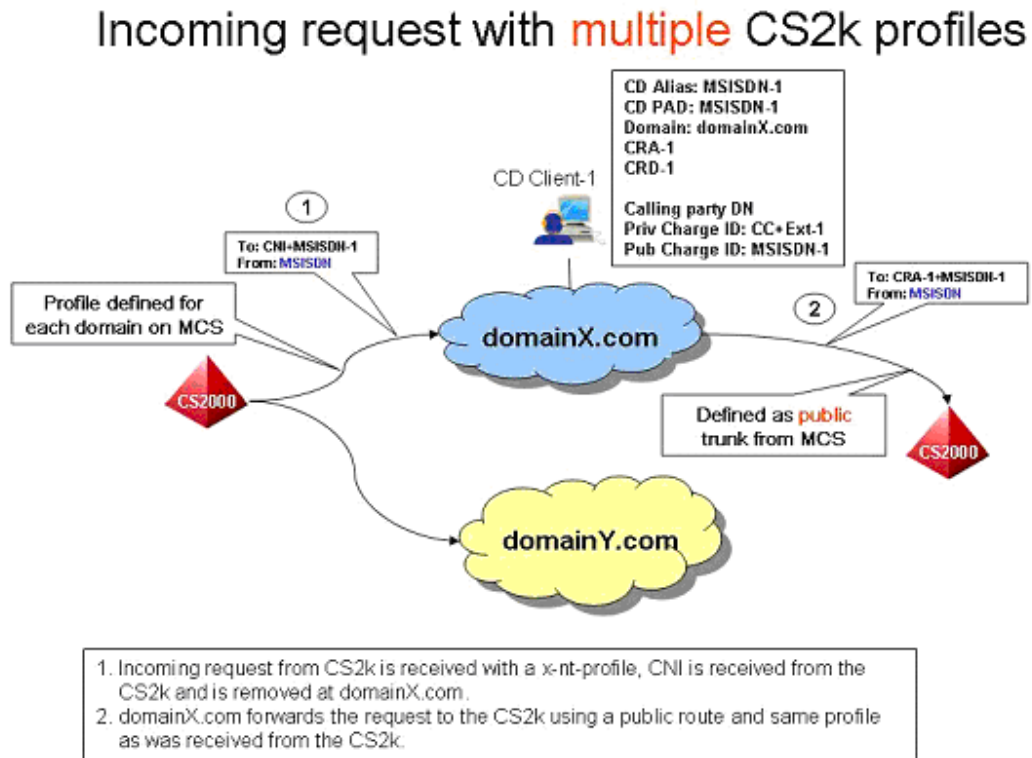
Figure 15 Incoming request with single CS2000 profile



1.1.12.3.2 Incoming Request with Multiple CS2K Profiles

The following figure illustrates the call flow when the incoming requests have multiple CS2k profiles.

Figure 16 Incoming request with multiple CS2000 profiles



The administrator has to set up translations for each domain /sub-domain to strip the incoming prefix. For example, Figure 17 shows a route 'CD3' provisioned to remove the digits '222'.

Figure 17 Telephony route to strip CNI prefix

Modify Telephony Route

Name:

Description:

From Digits:

To Digits:

Min Number of Digits:

Max Number of Digits:

Route Type:

Remove:

Prefix:

Recursive:

Route List:

The following figure is the “List Telephony Routes” page from the provisioning client showing the route that was created to remove the incoming prefix (CNI).

Figure 18 Listing of the telephony route

Telephony Route Listing for - dpl.com

Name	From Digits	To Digits	Min Digits	Max Digits	Route Type	Remove	Prefix	Recursive	Delete
CD3	222	222	12	12	Private	3		No	Delete
Change Parameters									

1.1.12.4 Service Package

A new option called “Mobile Converged” will be added to the Setup parameter of the Converged Desktop service. This option will be used to identify the users that will have this Mobile Converged service. In addition to that a new service called “Direct to Gateway” is introduced by this feature. This service defines if the calls have to be directed to a predefined gateway or not.

Figure 19 Provisioning the mobile converged desktop service

☐ Banned Users	☐ Converged Desktop	Setup	MobileConverged
☐ Status Reasons		Converged Desktop Enabled	Yes
☐ Service Package	☐ Direct to Gateway		
Create Package	☐ IM Chatroom		
List Packages	☐ Instant Messaging		
List Services	☐ Multiple Call Restriction	Number of Simultaneous Calls	10
Assign Service:			
Assign Package:			
View Resource			

A new service called “Multiple Call Restriction” will be created. This service defines if the multiple call restriction should be enforced on the user or not. If enabled, the number of simultaneous calls that a user can have will be defined by the new parameter labeled “Maximum Number of Calls Allowed” that will be added to the “Multiple Calls Restriction” service. This will indicate the number of calls that the user can answer/hold. Min=1, Max=20, Default=10.

Figure 20 Provisioning Client screen shot for the new service parameter

Provisioning	☐ Multiple Call Restriction	Maximum Number of Calls Allowed	10
Admins	☐ Music On Hold		
Domains	☐ Net6 Support on 2004	Net6 Server IP	
Devices	☒ Network Call Logs	Maximum Number of Inbox Call Logs	50
Service Nodes		Maximum Number of Outbox Call Logs	50
IPCM Clusters	☒ Presence	Maximum size of client friend list	10
Voice Mail			
Services			
Define Service Parameters			
Assign Services			
View Resources			

Note: Refer to the Feature Interactions section for the list of supported and mutually exclusive services

1.1.12.5 Subscriber Provisioning

For users to be able to use this new service, the following information has to be provisioned. The user should be assigned to a service package that has the Converged Service which has the setup parameter of the service set to “Mobile Converged”.

The directory number (DN) field of the user is used to provision the user's MSISDN. The directory number of the user should be unique in the whole system. The directory number should be unique in the whole system. Provisioning rules will be in place which will make sure that the DN is unique in the whole system. Identifying a converged user without knowing the domain is necessary because converged calls that are routed from an existing switch to the MCP will always contain the same domain. This domain may or may not be the user's real domain. The following figure explains the page wherein the directory number can be provisioned for a user.

The screenshot displays the Nortel user provisioning interface. On the left, a sidebar shows a tree view of domains and user management options. The 'Users' option is selected, showing sub-options: 'Add User', 'List Users', 'List Aliases', 'List Converged', and 'Move Users'. The main area on the right contains a form for user details. The form fields are as follows:

First Name:	TME	?
Last Name:	4220	?
Service package:	CD3	
Aliases:		
Status Reason:	ACTIVE	
email:		
Business Phone:		
Home Phone:		
Cell Phone:		
Pager:		
Fax:		
Directory Number:	2146854220	?
Private Charge ID:	6854220	
Public Charge ID:	2146854220	

The audio device prefix (CRA) and the direct to gateway prefix (CRD) can optionally be provisioned at the user level to override the (sub) domain prefixes.

1.1.12.5.1 Audio Device Prefix

The audio device prefix can also be provisioned at the user level. This can be provisioned from the Converged Desktop Properties tab in the user details page. This will only be available to Mobile Converged users.

The screenshot shows a web-based user management interface. On the left is a sidebar with a tree view containing domains like kash.com, ldapsync1.com, ldapsync2.com, lk1.com, lk2.com, nobranding.com, and nortel.com. Under nortel.com, there are sub-items like Set Profile, Domain Locales, Domain Bulletins, Domain Params, Sub-Domains, Users, Add User, and List Users. The top navigation bar has tabs: Main, Change Password, Voicemail, MeetMe properties, Converged Desktop properties, SIP Line Data, Routes, Customize service package, Unified Communications Properties, and Prefix Data. The main content area is titled 'Prefix Data for user s2146854220@nortel.com'. It contains a form with a label 'Audio Device Prefix :', a text input field with the value '113', and a help icon. Below the input field are 'Save', 'Clear', and 'Delete' buttons.

The following methods will be added to the existing ConvDesktopUserMgr OPI interface to be able provision this value from OPI.

```
/**
 * Adds the Prefix data for the mobile converged Service using the
 * user as the key
 * @param String username, the user to which the service data belong.
 * @param String userPrefixData, the new service data
 * @throws ProvisionException: This exception is thrown when an input
 * parameter is invalid,
 * a duplicate object exists in the data store, a dependency exists
 * in the data store or the data
 * store is not available.
 */

public void assignUserMCPrefixData (String username, String
userPrefixData) throws ProvisionException;

/**
 * Returns the user prefix data for the mobile converged Service
 * using the username as the key
 * @param String username, the user to which the service data belong.
 * @param String userPrefixData, the user service data
 * @throws ProvisionException: This exception is thrown when an input
 * parameter is invalid,
```

* a duplicate object exists in the data store, a dependency exists in the data store or the data

* store is not available.

*/

```
public String getUserMCPrefixData (String username) throws  
ProvisionException;
```

```
/**
```

* This method is used for removing prefix data associated with a user for the mobile converged service

* @param String username, user from which the service data needs to be removed.

* @throws ProvisionException: This exception is thrown when an input parameter is invalid,

* a duplicate object exists in the data store, a dependency exists in the data store or the data

* store is not available.

*/

```
public void removeUserMCPrefixData (String username) throws  
ProvisionException;
```

1.1.12.5.2 Direct to Gateway Prefix

The direct to gateway prefix can also be provisioned at the user level. This can be provisioned from the new “Prefix Data” tab in the user details page. This will only be available to Mobile Converged users who have the “Direct to Gateway” service.

The screenshot shows a web-based user management interface. On the left is a tree view of domains and users. The main area displays a tabbed interface for user 's2146854220@nortel.com'. The 'Prefix Data' tab is active, showing a text input field for 'Direct To Gateway Prefix', a 'Save' button, a 'Clear' button, and a 'Delete' button. Above the input field is a table with navigation links.

Main	Change Password	Voicemail	MeetMe properties	Converged Desktop properties
SIP Line Data	Routes	Customize service package	Unified Communications Properties	<u>Prefix Data</u>

Direct To Gateway Prefix Data for user s2146854220@nortel.com

Direct To Gateway Prefix : * ⓘ

Save Clear

Delete

A new interface called “UserPrefixDataMgr” will be created to have the methods required to provision this value from OPI.

```
/**
 * Adds the Prefix data for the user using the username as the key
 * @param String username, the user to which the data belongs.
 * @param String userPrefixData, the new prefix data
 * @throws ProvisionException: This exception is thrown when an input
parameter is invalid,
 * a duplicate object exists in the data store, a dependency exists
in the data store or the data
 * store is not available.
 */
public void assignUserDirectToGWPrefixData (String username, String
userPrefixData) throws ProvisionException;

/**
 * Returns the prefix data for the user using the username as the key
 * @param String usernameD, the user to which the prefix data belongs
to.
 * @param String domPrefixData, the new service data
 * @throws ProvisionException: This exception is thrown when an input
parameter is invalid,
 * a duplicate object exists in the data store, a dependency exists
in the data store or the data
 * store is not available.
 */
public String getUserDirectToGWPrefixData (String username) throws
ProvisionException;

/**
 * This method is used for removing prefix data associated with a user
 * @param String username, the user for which the data needs to be
removed.
 * @throws ProvisionException: This exception is thrown when an input
parameter is invalid,
 * a duplicate object exists in the data store, a dependency exists
in the data store or the data
```

```

* store is not available.
*/

public void removeUserDirectToGWPrefixData (String username) throws
ProvisionException;

```

1.1.12.6 Open Provisioning Interface (OPI)

The following summarizes the OPI methods that will be exposed as part of this feature.

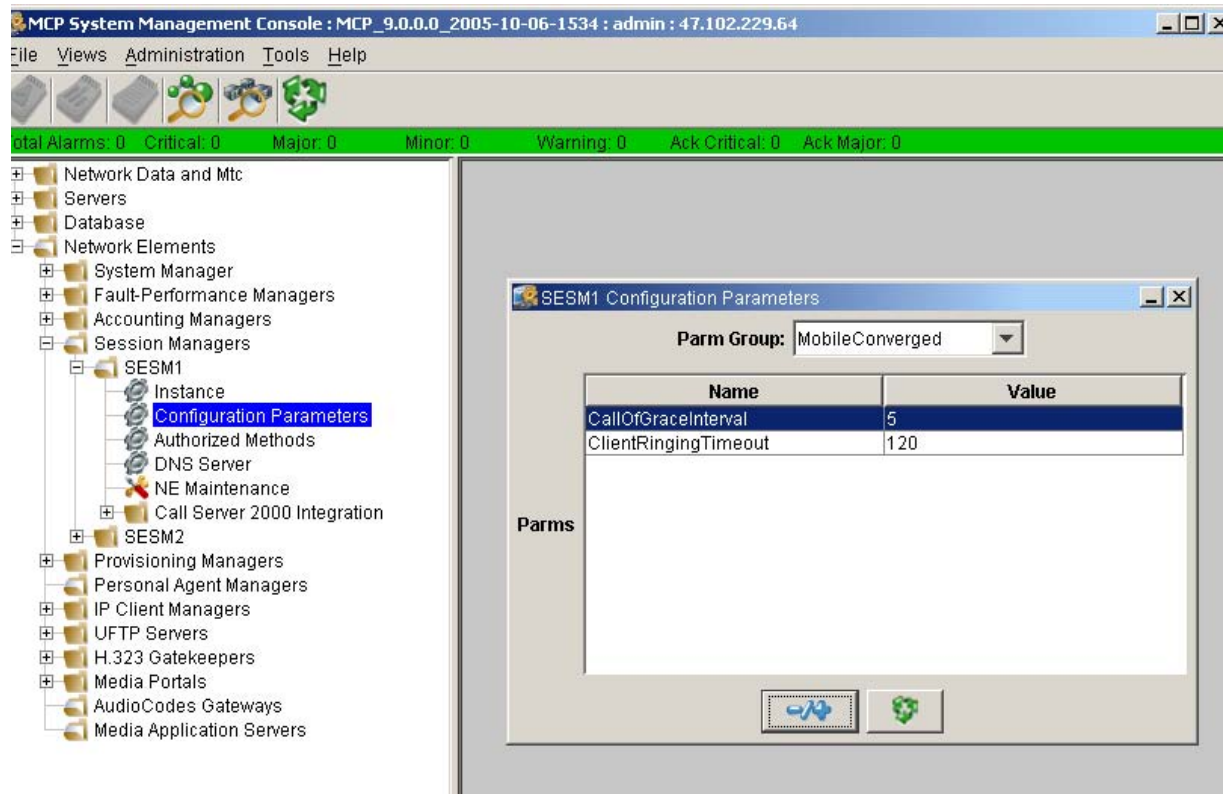
These commands will also be available from the BPT command line tool.

	Command	Parameter List
User Prefix	addMobileConvDesktopUserData	String username, MobileConvDesktopUserData userData
	getMobileConvDesktopUserData	String username
	removeMobileConvDesktopUserData	String username
Domain Prefix	addMobileConvDesktopDomainData	String domain, MobileConvDesktopDomainData domPrefixData
	getMobileConvDesktopDomainPrefixData	String domain
	removeMobileConvDesktopDomainPrefixData	String domain

1.1.12.7 System Configuration Parameters

Two new system parameters are available through the System Management Console GUI, the CallOfGraceInterval and ClientRingingTimeout. These parameters are both accessible through the System Management Console GUI and are provisioned for each Session Manager individually.

To access these parameters, click on the Configuration Parameters for a Session Manager and selecting the “Mobile Converged” Parm Group in the Configuration Parameters panel shown in the following figure.

Figure 21 Configuration Parameters Panel**1.1.12.7.1 CallOfGraceInterval**

This parameter sets the call number interval the session manager will wait before attempting to present a subsequent call attempt to an MCD client after it has become “unavailable” as described in section “Client Unavailable / Calls of Grace” on page 1341.

1.1.12.7.2 RingingTimeout

This is a timer setting the number of seconds the session manager will allow an incoming call to a user currently registered on an MCD Client to remain ringing before bringing the call down. When this timer expires, a SIP BYE message is sent to the client to terminate the call leg to the MCD Client and a 480 Temporarily Unavailable sent to the originator to terminate the call and the call leg to the PAD is dropped.

1.2 Call Processing

This section details the call flow and supervision from the MCS network perspective.

1.2.1 Interfaces supported

The supported interface between the MCP and the existing switching system is Session Initiation Protocol (SIP).

1.2.2 Dial Plans

Two prefixes must be provisioned on the system for this feature. The CRD and CRA are defined again as follows:

- Destination Call Leg Return Code (CRD): This is an E.164 number that will prefix the (non CD) destination mobile number for outgoing calls from the MCD client to the mobile network.
- Associated Call Leg Return Code (CRA): This is an E.164 number that will prefix the CD mobile number (PAD). This prefix can be used to identify this call leg on the GSM network as a non-chargeable call.

The following sections discuss the usage of these prefixes for both terminating to a CD Mobile and originating from an MCD PC Client. Note that there is no section addressing conference calls since conference calls do not require establishing a new PSTN connection; thus, CDR and CDA prefixes are not required for joining the previously established calls into a conference.

1.2.2.1 Prefix usage for CD Mobile Terminations

The following table describes when the CRA is prefixed to a CD Mobile termination. The two scenarios considered are:

1. Call is received from another CD Mobile (row 1)
2. Call is received by non CD Mobile (row 2)

These rules also apply to 'Advanced Routing' (if provisioned) where the terminator has multiple destinations. For example, MSISDN-2 rings another CD mobile and then a non CD mobile. For both destinations the CRA needs to be added as described.

Figure 22 Prefix on CD Mobile Terminations

CD Mobile Terminations			
Originator	Terminator	Called Number	Description
CD Mobile (MSISDN-1) (CRA-1)	CD Mobile (MSISDN-2) (CRA-2)	CRA-2+MSISDN-2	CRA of the terminator is used in the called number here because the originator could be known, but not looked up at the MCS for CD Mobile to Mobile call.
Non - CD Mobile (MSISDN)	CD Mobile (MSISDN-2) (CRA-2)	CRA-2+MSISDN-2	CRA of the terminator is used here because the originator is unknown at the MCS.

1.2.2.2 Prefix usage for MCD PC Client Originations

The following table describes when the CRA and CRD are used when a client origination takes place to a

1. CD Mobile
2. Non CD Mobile
3. PSTN number

These rules also apply to 'Advanced Routing' (if provisioned) where the terminator has multiple destinations. For example, MSISDN-2 rings another CD mobile and then a non CD mobile. For both destinations the CRA/CRD needs to be added as described.

Figure 23 Prefix for Client Originations

MCD Client Origination / click-to-call				
Originator	Terminator	CRA (Owner) First Leg (orig)	CRD (Owner) Second Leg (term)	Description
CD Mobile (MSISDN-1) (CRA-1) (CRD-1)	CD Mobile (MSISDN-2) (CRA-2) (CRD-2)	CRA-1+MSISDN-1	CRD-1+MSISDN-2	CRA of the originator is used for the first and CRD of the originator is used in the terminating leg because it is a client origination.
CD Mobile (MSISDN-1) (CRA-1) (CRD-1)	CD Mobile (user ID) (MSISDN-2) (CRA-2) (CRD-2)	CRA-1+MSISDN-1	CRD-1+MSISDN-2	CRA of the originator is used for the first and CRD of the originator is used in the terminating leg because it is a client origination.
CD Mobile (MSISDN-1) (CRA-1) (CRD-1)	Non-CD Mobile (MSISDN)	CRA-1+MSISDN-1	CRD-1+MSISDN	CRA of the originator is used for the first and CRD of the originator is used in the terminating leg because it is a client origination.

1.2.2.3 Prefix Usage for Call Transfer

The following table describes when the CRA and CRD are used when a client transfers a call. The table below has a call setup between party A and B, then party B transfers the call to party C.

The rules need to also apply to 'Advance Routing' where the terminator has multiple destinations. For example, MSISDN-3 rings another CD mobile and

then a non CD mobile. For both destinations the CRD needs to be added as described. The same rules will apply if Party B forwards the request to Party C.

Figure 24 Prefix used for call transfer

Call transfer					
Party A	Party B (transferring party)	Party C (transfer party)	Calling Number sent to Party C	Called Number sent to Party C	Description
CD Mobile (MSISDN-1) (CRA-1) (CRD-1)	CD Mobile (MSISDN-2) (CRA-2) (CRD-2)	CD Mobile (MSISDN-3) (CRA-3) (CRD-3)	(TBD)	CRD-2+MSISDN-3	CRD of the transferring party is used because party C is a known MCS user. This is similar to party B just originating a call to party C.
CD Mobile (MSISDN-1) (CRA-1) (CRD-1)	CD Mobile (user ID) (MSISDN-2) (CRA-2) (CRD-2)	Non-CD Mobile (MSISDN)	(TBD)	CRD-2+MSISDN	CRD of the transferring party is used because party C is a known MCS user. This is similar to party B just originating a call to party C.

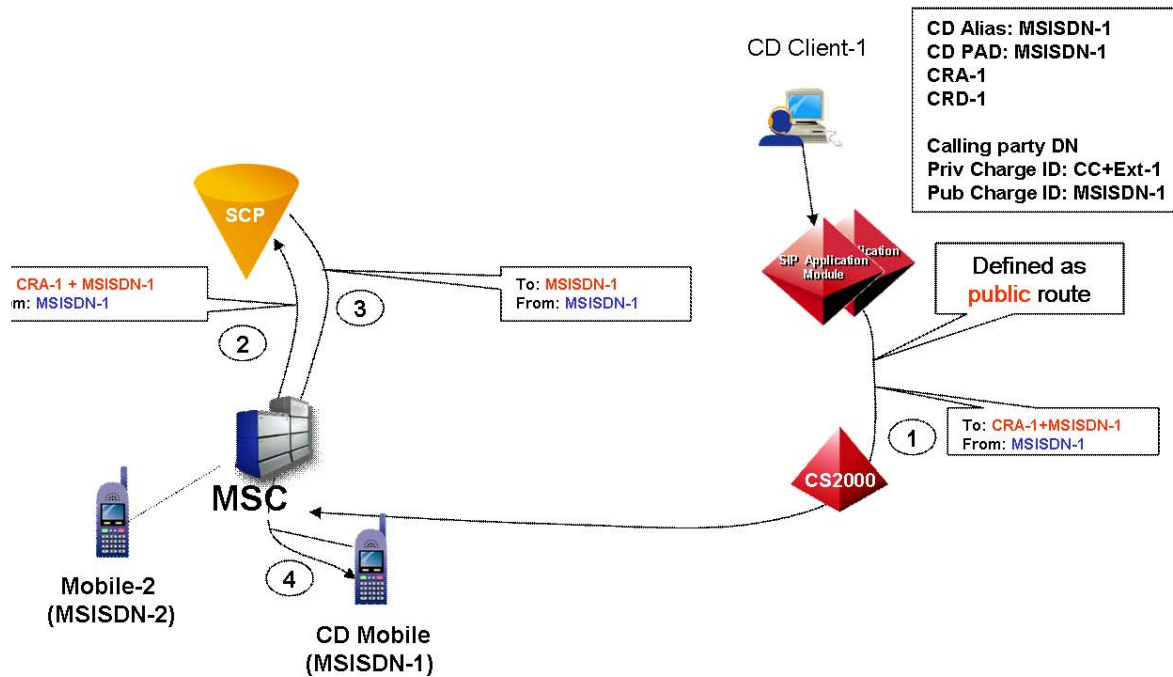
1.2.3 MCD PC Client Originated Scenarios

The situation in which a converged user (MCD Client-1) makes a call to a mobile user (Mobile-2) from the MCD PC Client is discussed. Since the MCD PC Client does not provide the audio for the call, all originations from the PC client are click-to-call scenarios.

The Click-to-call scenario always involves two call legs. The first call is to the CD Mobile (MSISDN-1), and is illustrated in Figure 25.

Figure 25 Call origination from MCD PC Client (part 1)

MCD Client Origination to (non CD) mobile destination (part 1)



Step 1: MCS Application Server attempts to establish the audio call with the MSISDN-1 by first prefixing with the originators CRA and routing to the CS2000. The CS2000 translates and sends ISUP IAM to the MSC of the mobile network.

Step 2: The CRA+MSISDN-1 is presented to SCP for the originating leg.

Step 3: SCP removes CRA and sends the call to the CD Mobile (MSISDN-1). Note that the request is not sent back to MCS.

Step 4: The originator's mobile rings and originator answers the call.

The second half of the call attempts to establish the audio call with the non CD terminating Mobile-2. This scenario is illustrated below in Figure 26.

Figure 27 MCD PC Client origination with ringback from far end

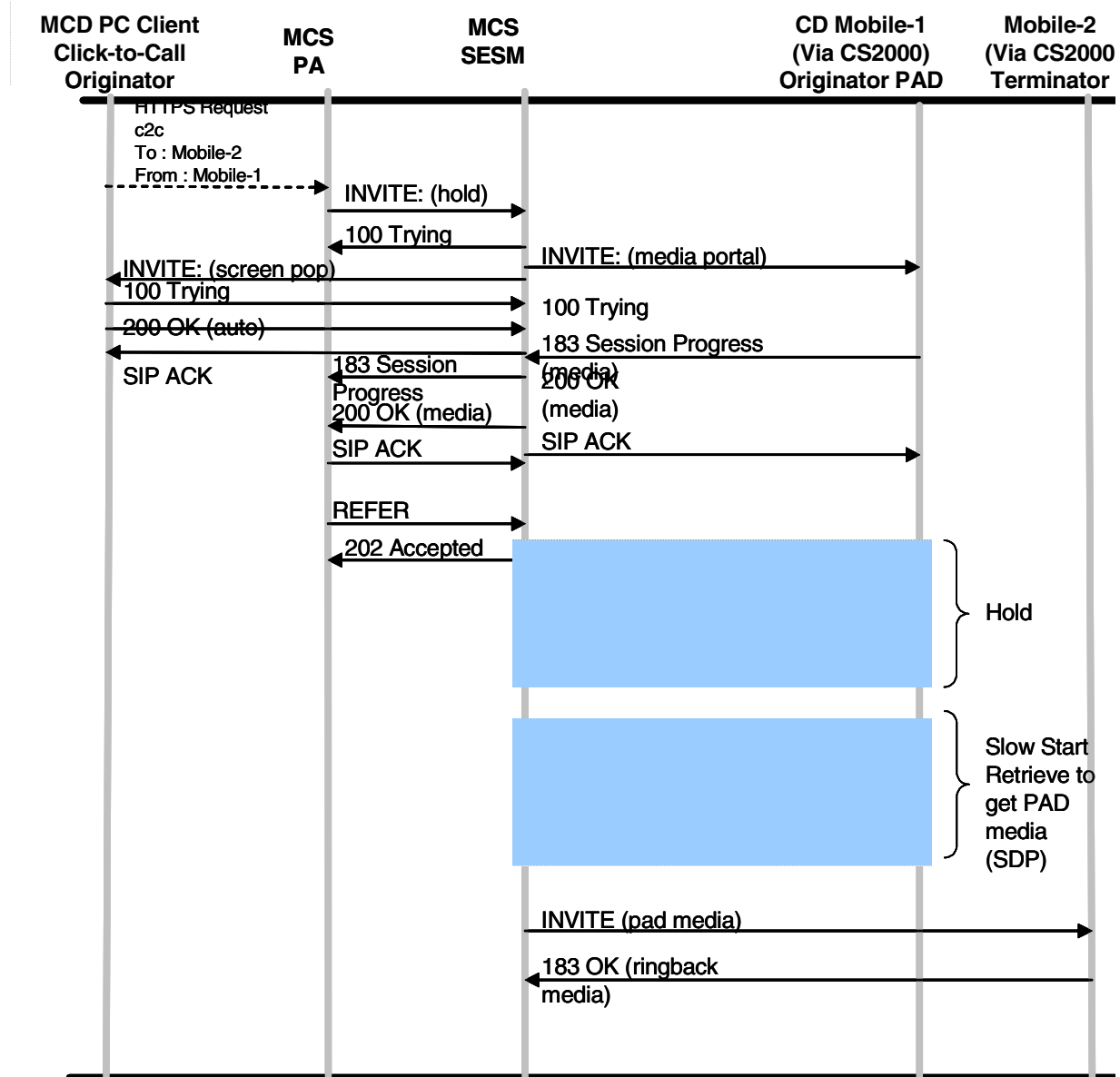
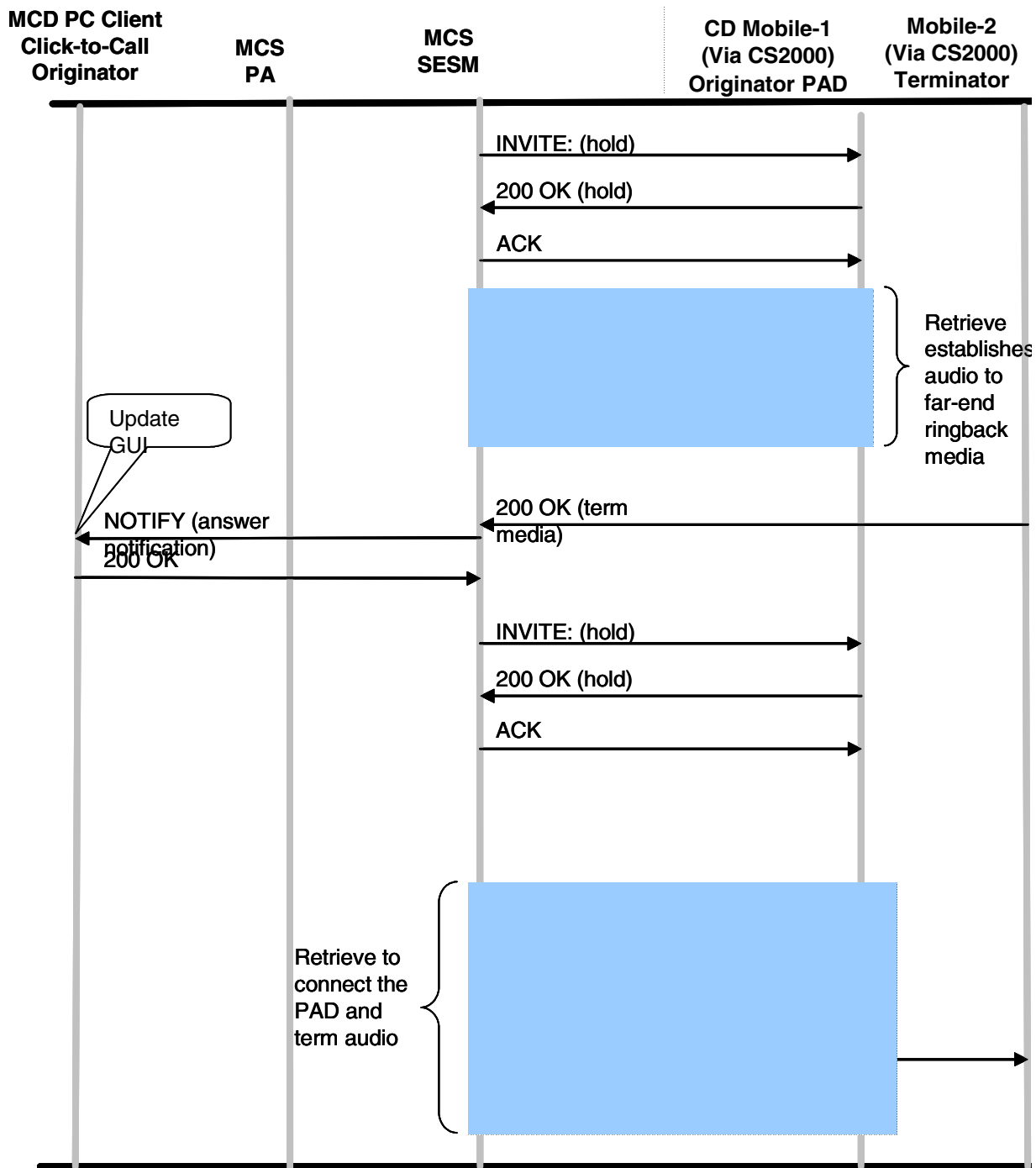


Figure 28 MCD PC Client origination with ringback from far end (cont.)



1.2.4 PAD Terminated Scenarios

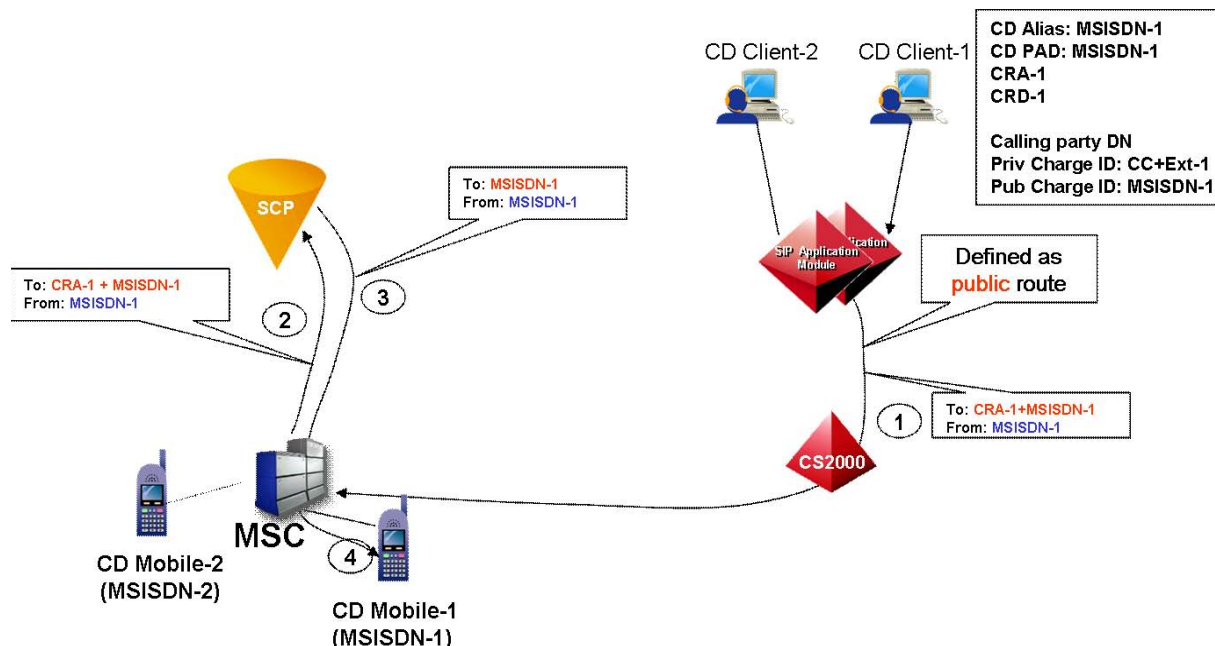
This section covers the termination scenario in which a converged subscriber (CD mobile-1) makes a call to a CD User (CD mobile-2). It also deals with

situations in which the inbound call is Ignored and Rejected from the MCD PC Client.

1.2.4.1 Call Answer on PAD

The basic termination to the converged users PAD is shown in Figure 28. In this scenario a converged wireless subscriber (CD Mobile-1) calls another converged wireless subscriber (CD Mobile-2).

Figure 29 CD call termination (part 1)



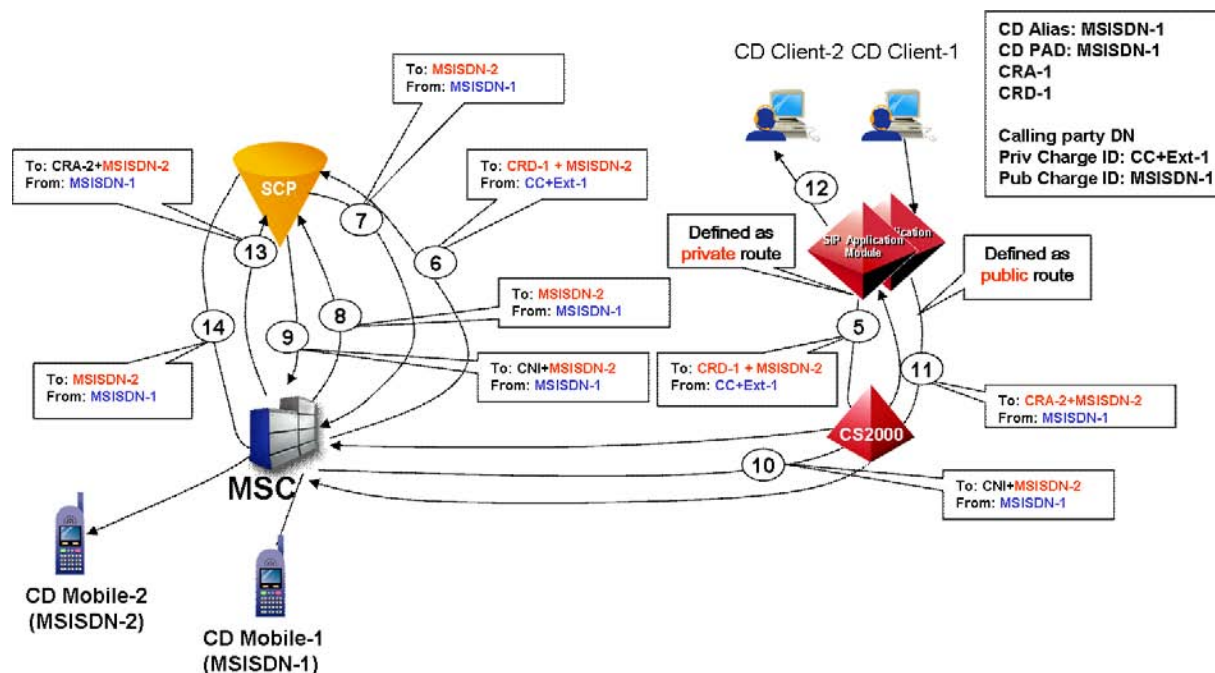
Step 1: First leg terminates to the CD mobile's own mobile device. Owner's CRA+MSISDN is the called and MSISDN-1 is the calling party. CRA routing needs to use a public telephony route so public charge ID (MSISDN-1) is presented as the calling number.

Step 2: CRA+MSISDN-1 is presented to SCP for the originating leg

Step 3: SCP removes CRA and sends the call to the Mobile-1 which answers the call.

Step 4: The originator's mobile rings and the originator answers the call.

Figure 30 Call Termination (part 2)



Step 5: CRD of the originator is prefixed to the terminator's MSISDN and from party is changed to CC+Ext of the originator.

Step 6: The MSC sends the request to SCP.

Step 7: SCP modifies the called and calling party to the actual MSISDN involved.

Step 8: The MCS sends the request to the SCP again to add the CNI.

Step 9: SCP prefixes the CNI to the terminating call

Step 10: Request received at the MCS with CNI (or without if CS2k removes it).

Step 11: MCS adds the CRA of the terminating party and routes the request to the MSC

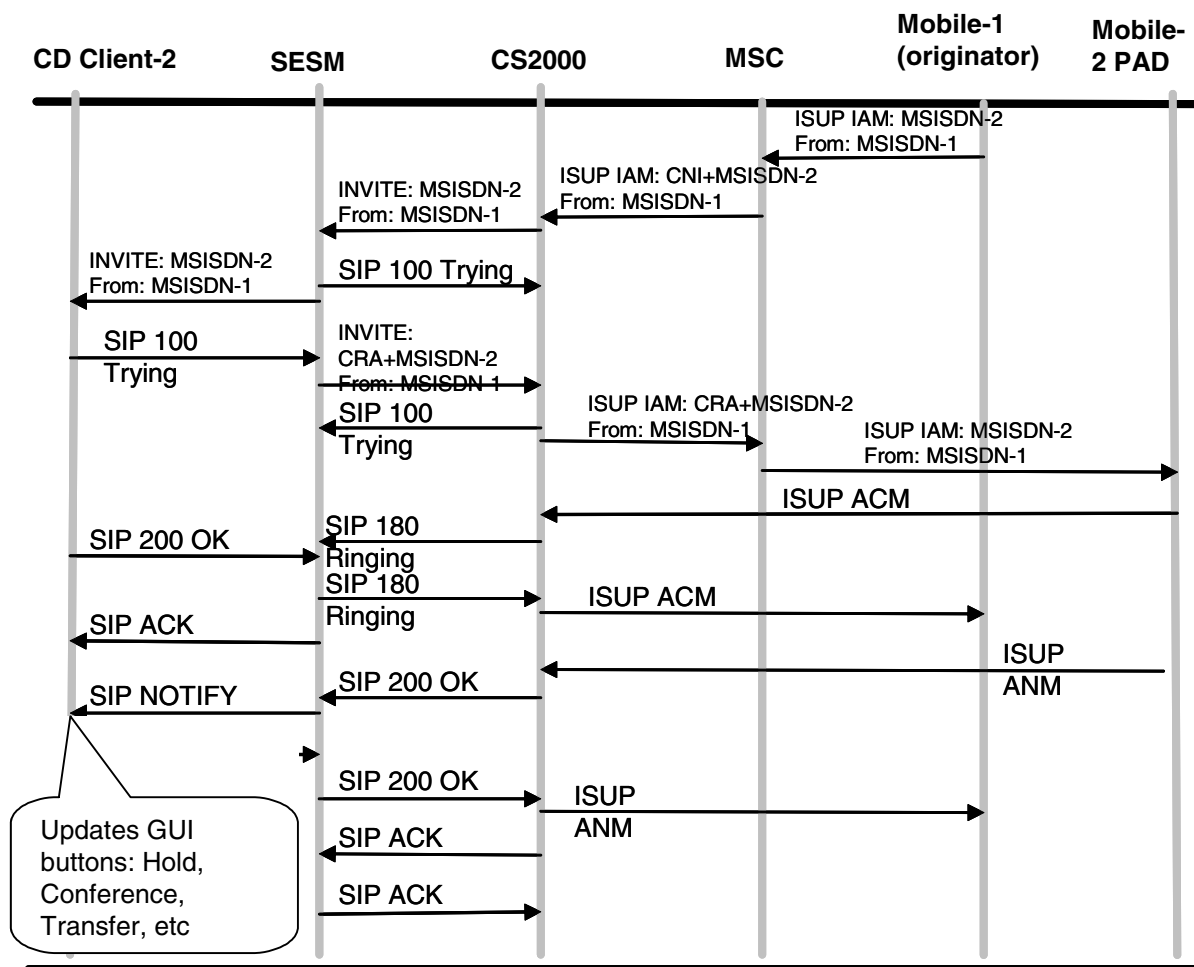
Step 12: CD Client-2 is presented with call.

Step 13: MSC sends the request to the SCP to remove the CRA.

Step 14: Request to MSC is sent to ring the terminating mobile.

The call flow from the perspective of the MCS Session Manager is shown below.

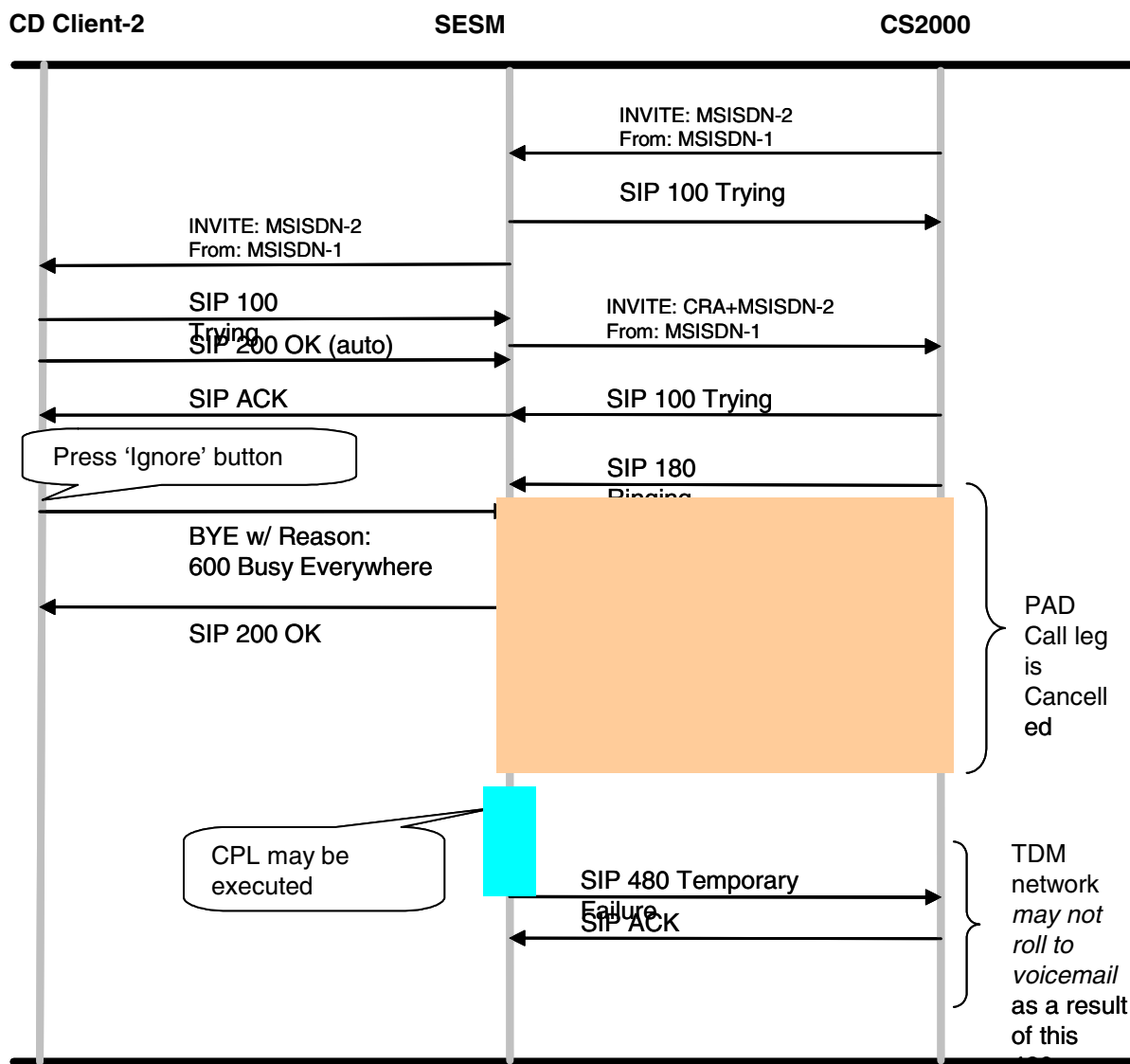
Figure 31 MCD PC Client termination



20.3.4.2 Call Ignore from MCD PC Client

Incoming calls to the MCD PC Client call be ignored. This will allow the SESM to execute any MCS CPL scripts (advanced routing) and/or roll to MCS voice mail. The call flow from the perspective of the MCS Session Manager is shown below.

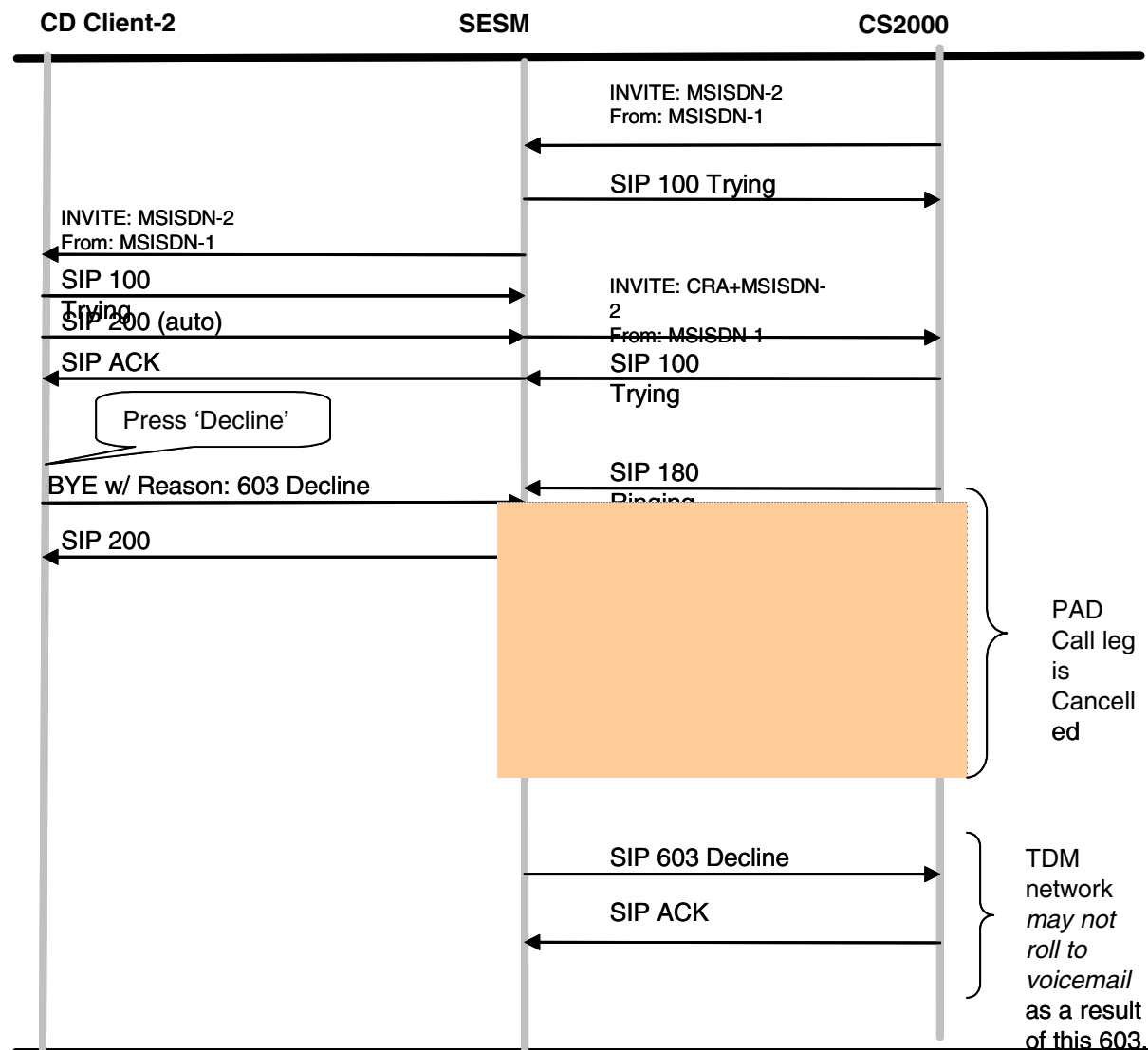
Figure 32 MCD PC Client Ignores inbound call (no CPL)



20.3.4.3 Call Decline (reject) from MCD PC Client

Incoming calls to the MCD PC Client call be rejected. The call flow from the perspective of the MCS Session Manager is shown below.

Figure 33 MCD PC Client Declines inbound call



20.3.5 Established Call Behavior

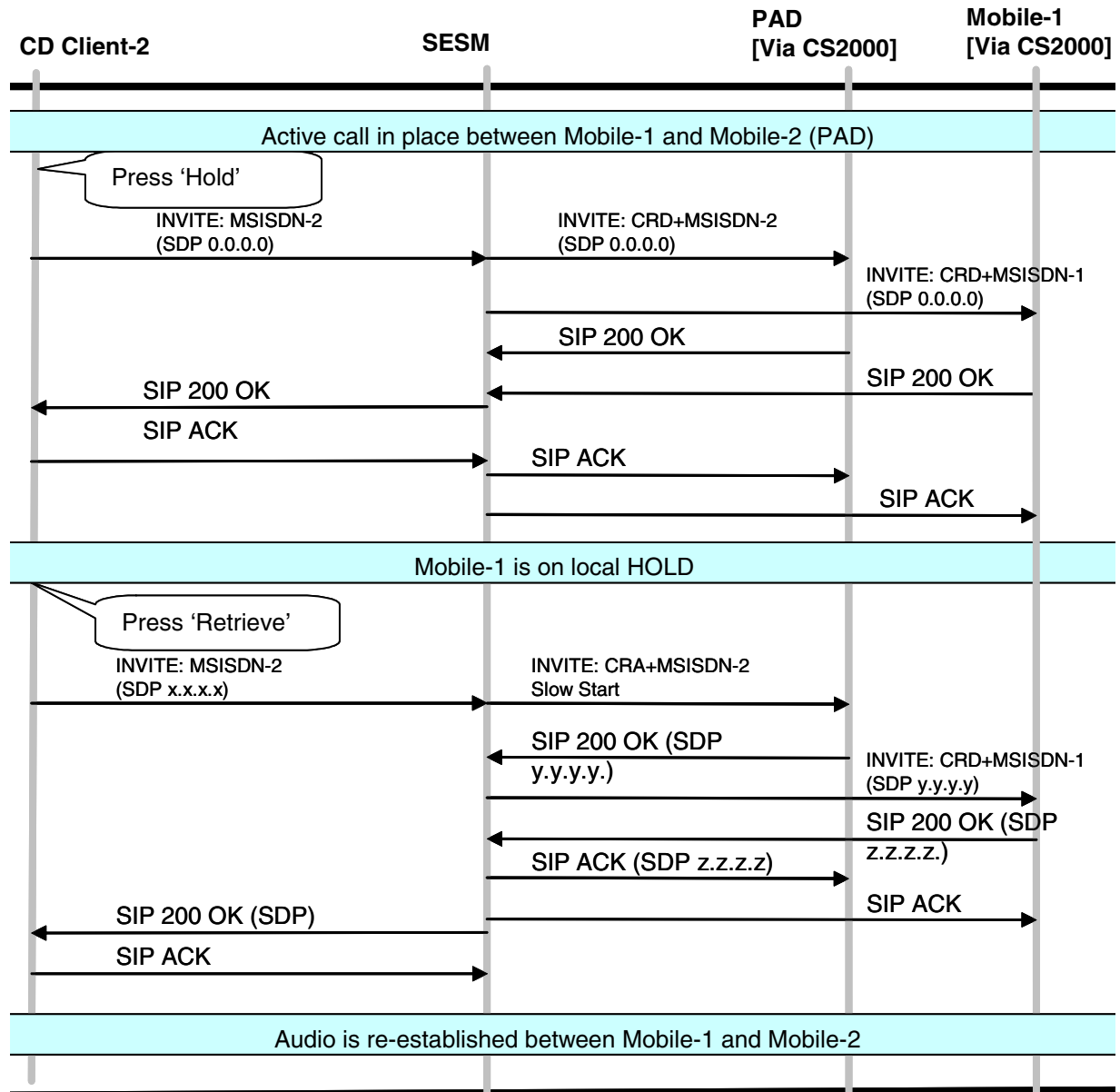
This section covers the situations in which a converged subscriber (mobile-1) already has an established call and additional mid-call features are being requested from the terminating MCD PC Client. Specifically, the scenarios presented are Hold / Retrieve, Conference, and Direct Transfer from the MCD PC Client.

20.3.5.1 Hold/Retrieve from MCD PC Client

The PC Client allows active calls to be placed on local hold by pressing the Hold button. This behavior is also invoked automatically if the client answers subsequent incoming calls. The call flow for the PC Client invoking local hold

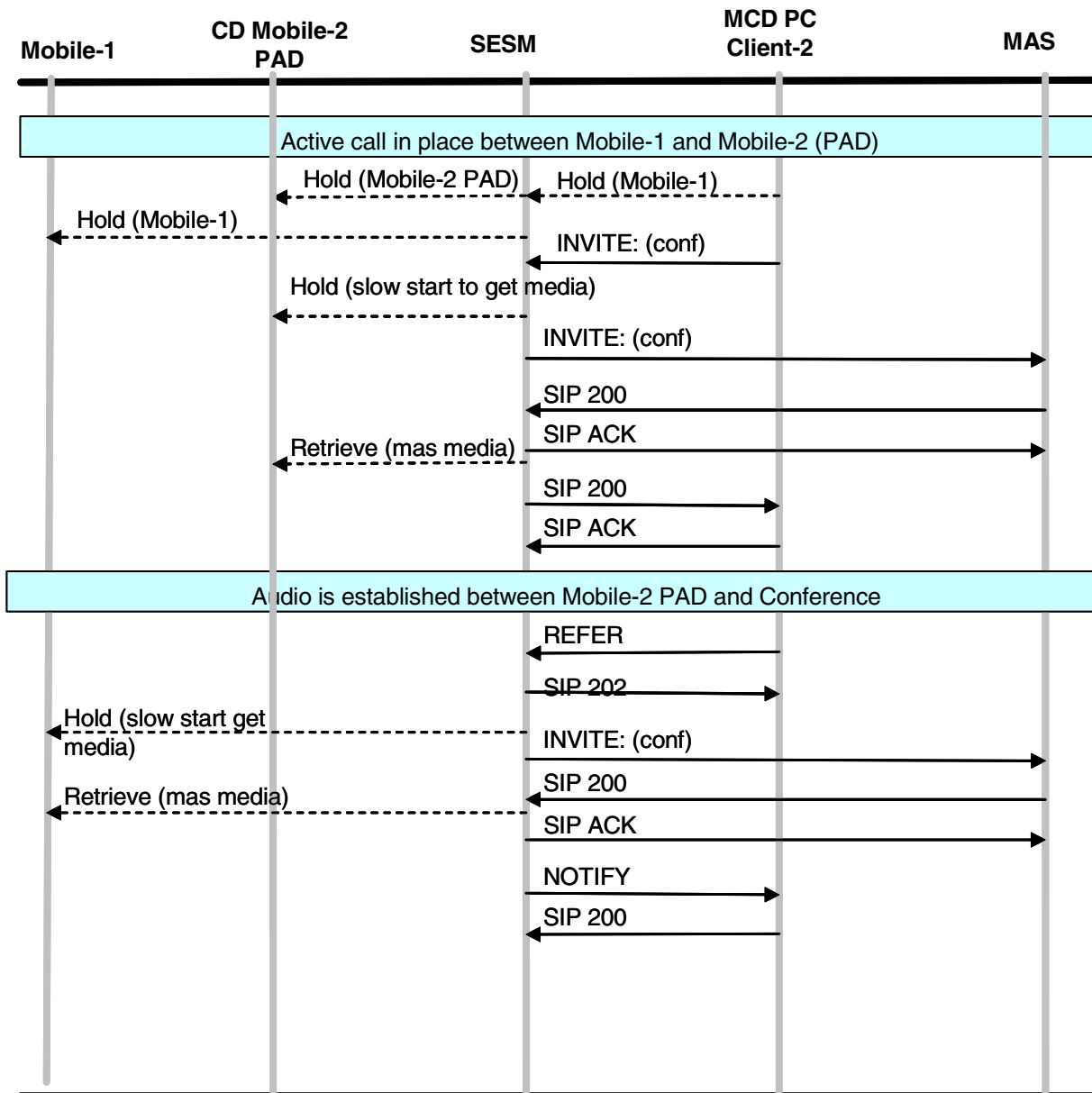
is as follows. (Note that call flows for hold and retrieve may be abbreviated in subsequent sections for simplicity.)

Figure 34 MCD PC Client Hold/Retrieve call



20.3.5.2 Conference from MCD PC Client

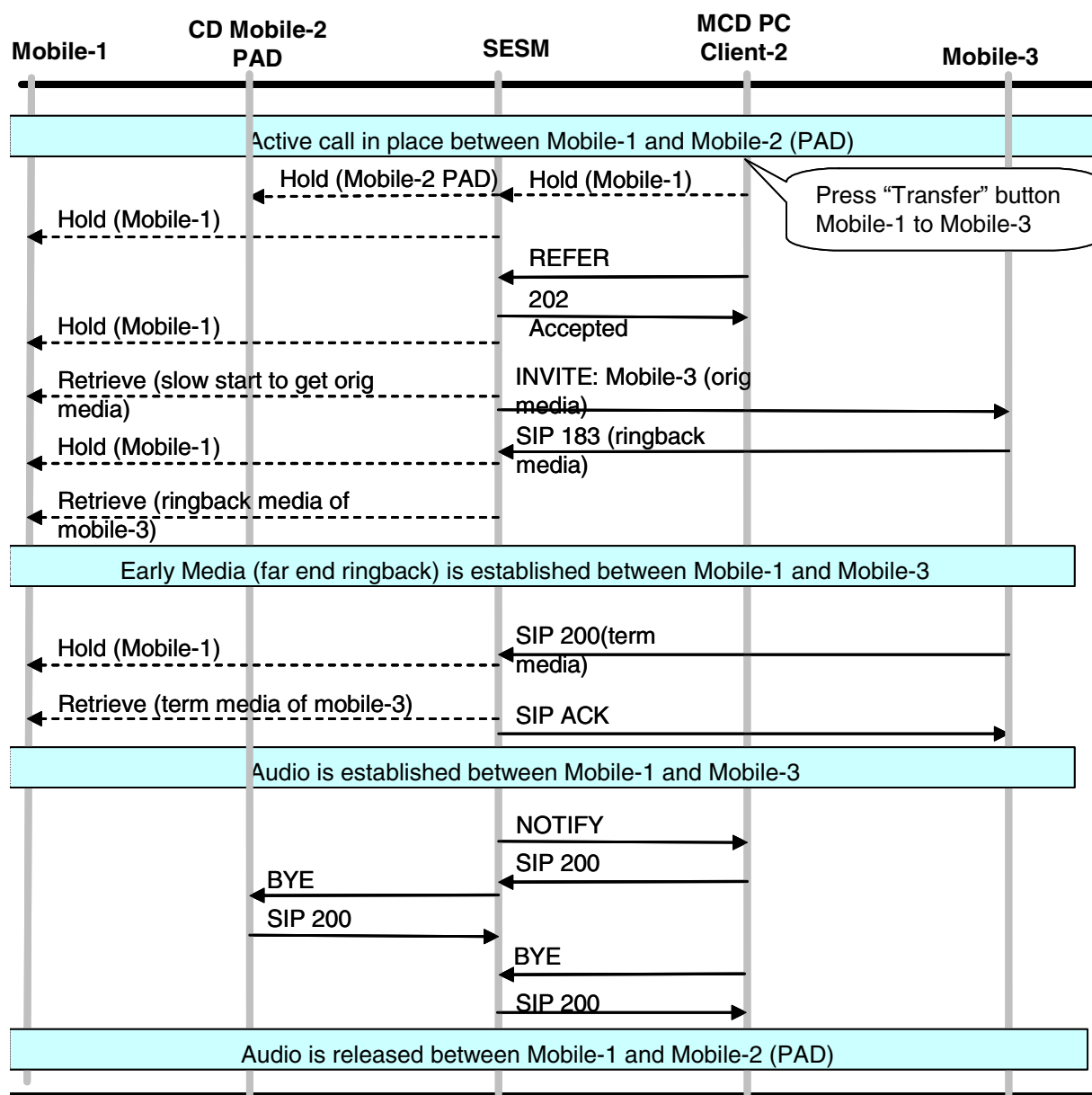
The call flow for the PC Client joining users into a conference is as follows.



20.3.5.3 Transfer from MCD PC Client

An established call exists between Mobile-1 and CD Mobile-2 (PAD). The MCD PC Client-2 invokes a direct transfer of this established call to Mobile-3. An abbreviated call flow for the direct transfer to is shown in Figure 35. Only Mobile-2 is a converged user. Most SIP signaling must go through the CS2000, thus the SESM executes internal REFER logic using Hold/Retrieve.

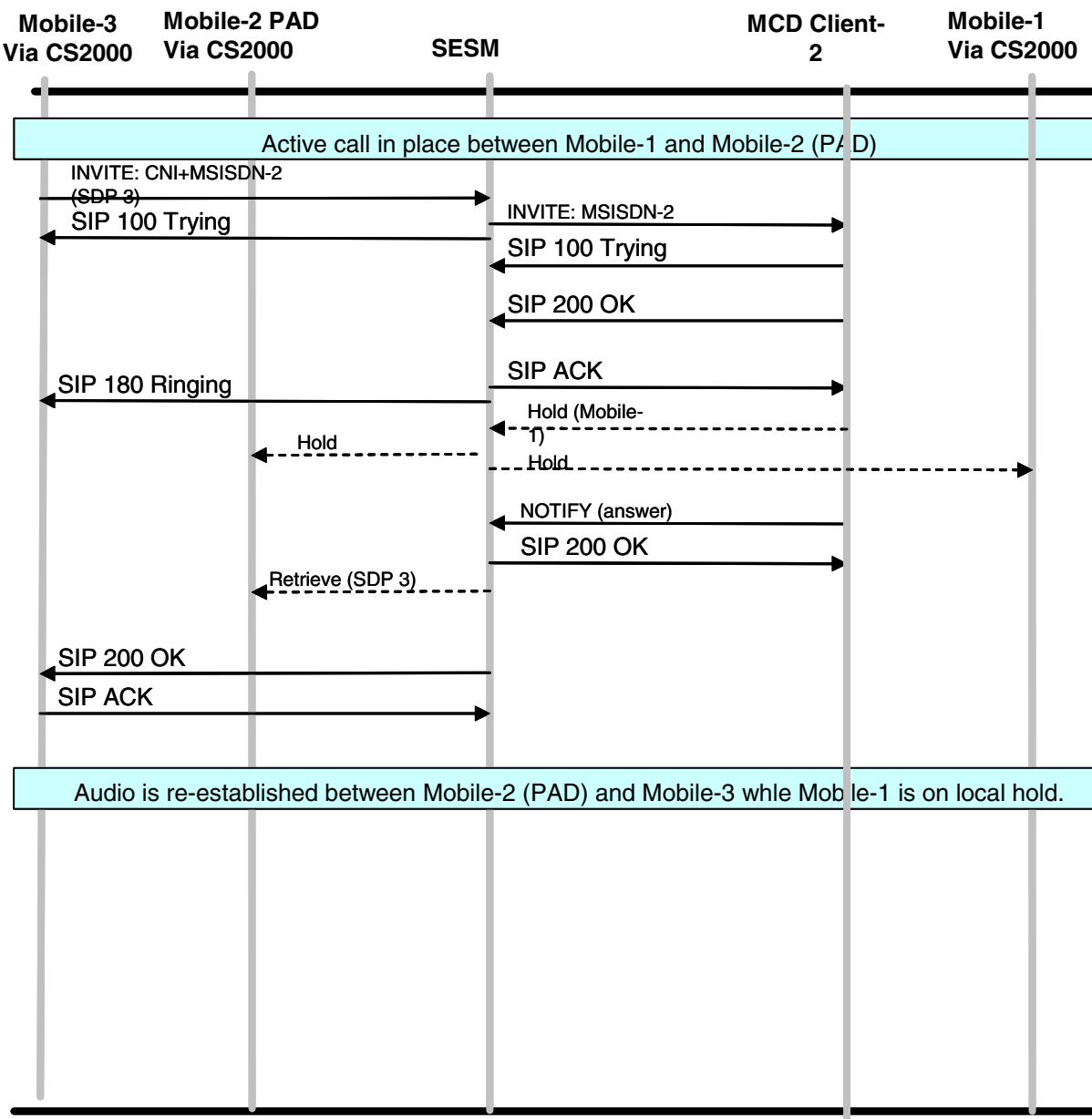
Figure 35 MCD PC Client Transfers call



20.3.5.4 New Inbound Call to PAD (multi-call)

The call flow for the PC Client new call is as follows.

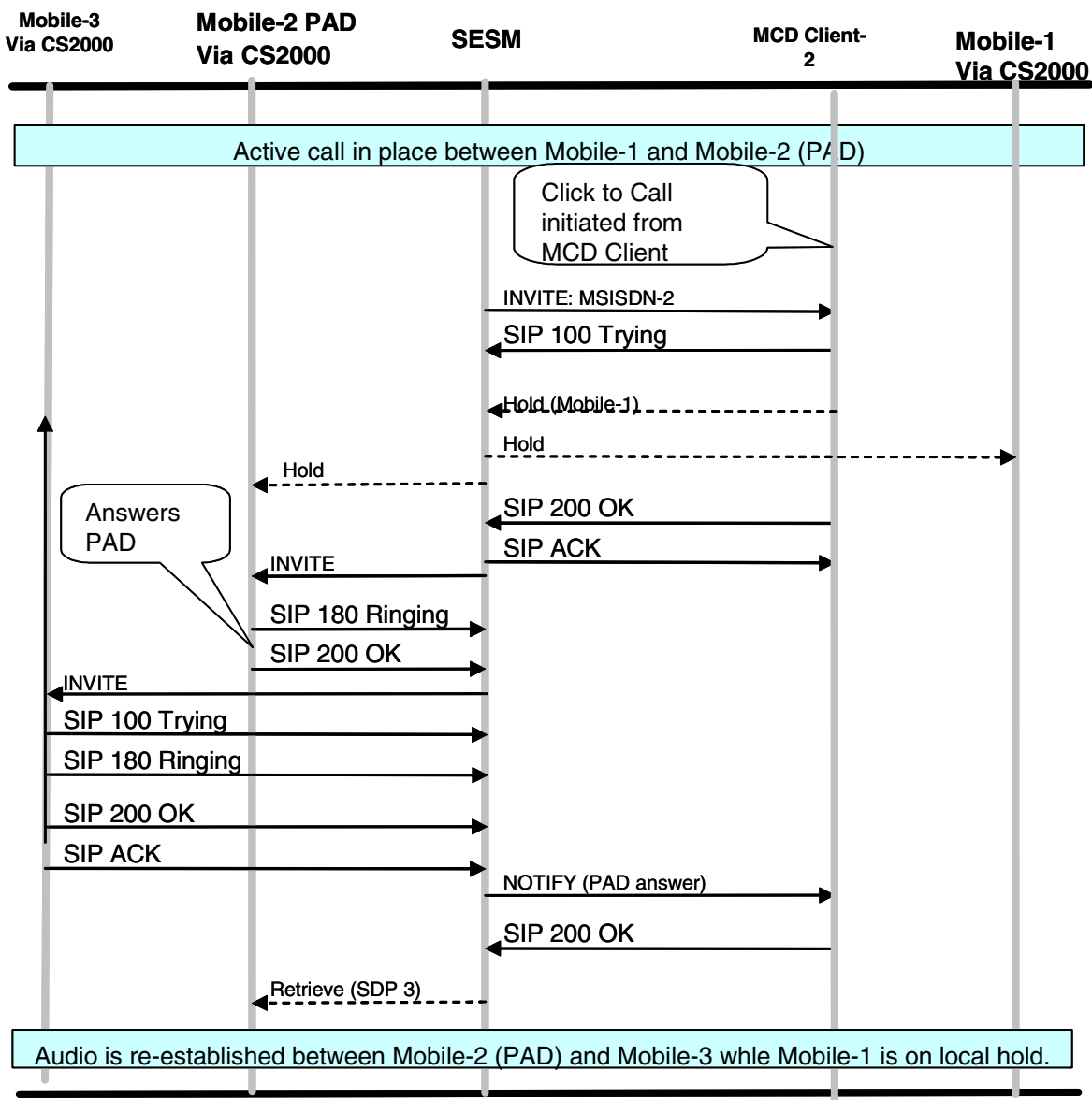
Figure 36 MCD PC Client Receives new multi-call



20.3.5.5 New Outbound Call to PAD (multi-call)

The call flow for the PC Client new call is as follows.

Figure 37 MCD PC Client Receives new multi-call



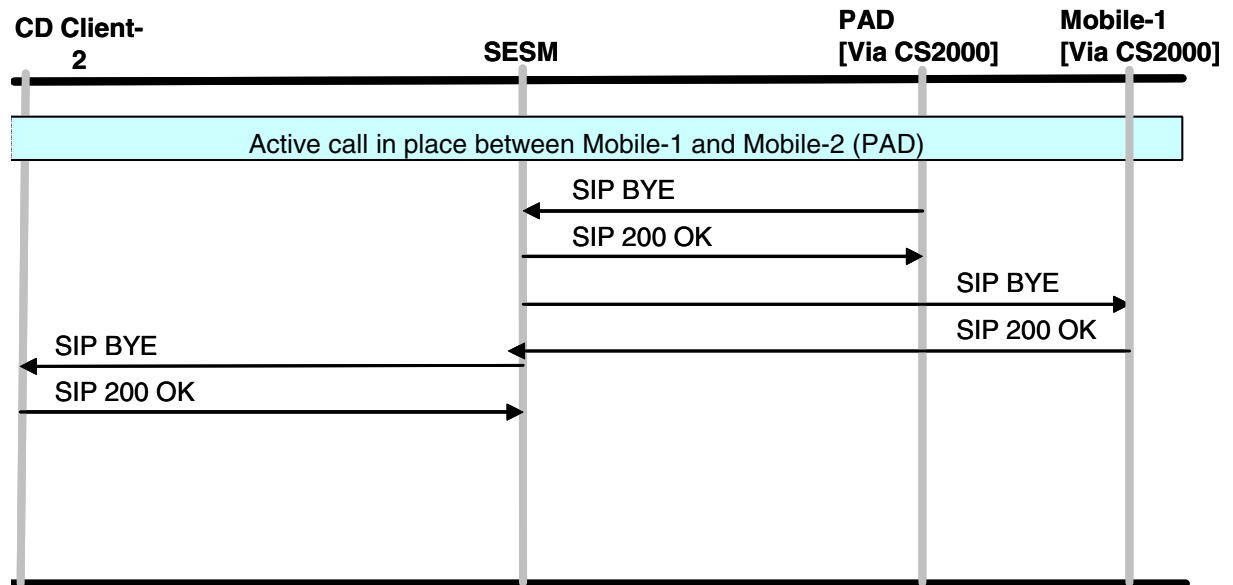
20.3.6 Release Scenarios

This section covers the situations in which a subscriber (mobile-1) disconnects established calls. Specifically, the scenarios presented are PAD Release, Network Release and Release from the MCD PC Client

20.3.6.1 PAD Release

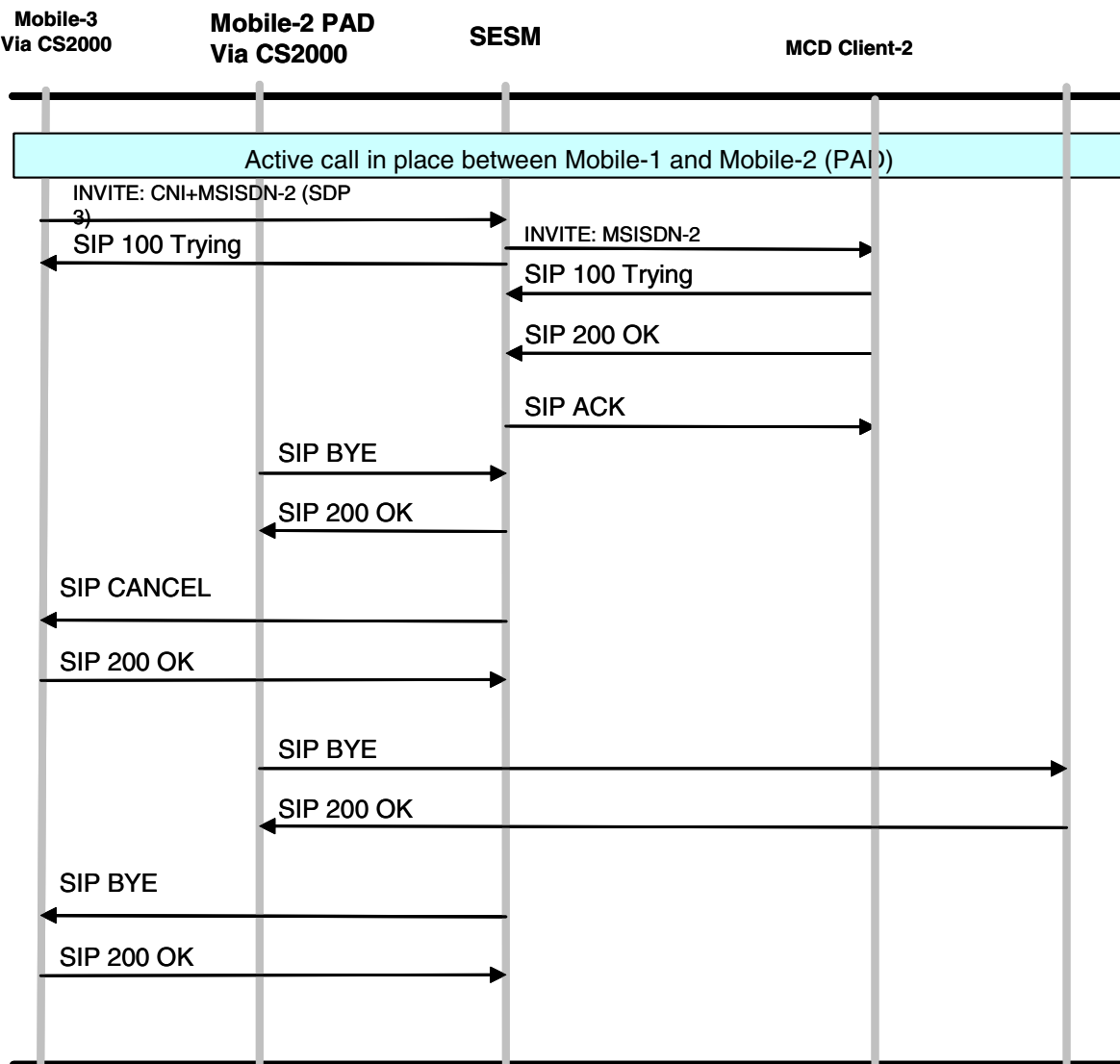
The PAD release and the TDM network release appear identical from the MCS perspective. The call flow is shown below.

Figure 38 PAD Release



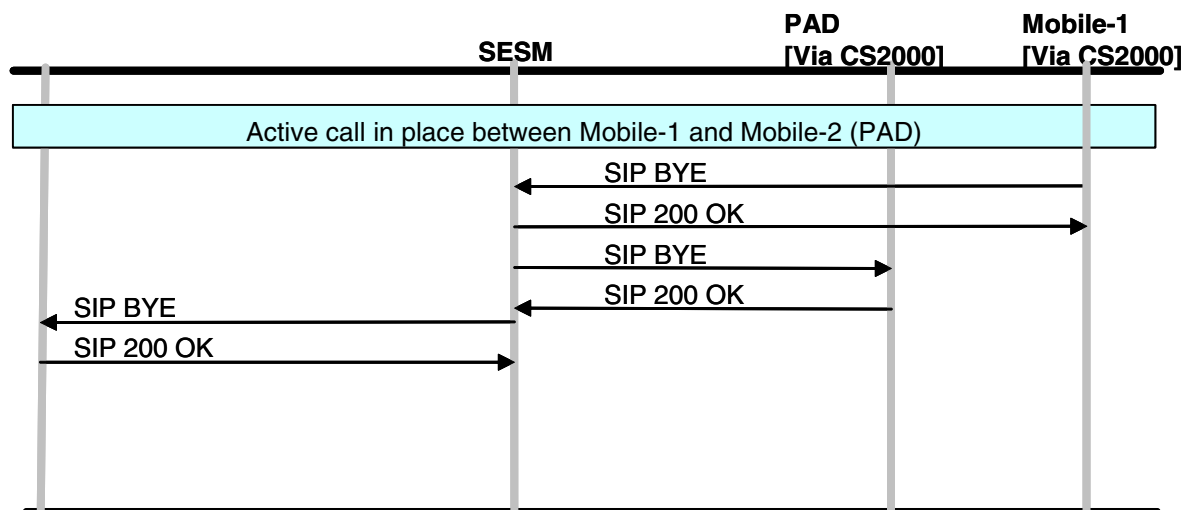
20.3.6.2 PAD Release for Inbound Call (multi-call)

The call flow for the PC Client new call is as follows.

Figure 39 PAD Release for Inbound Call (multi-call)**20.3.6.3 Remote Party Release**

The call flow for the PC Client new call is as follows.

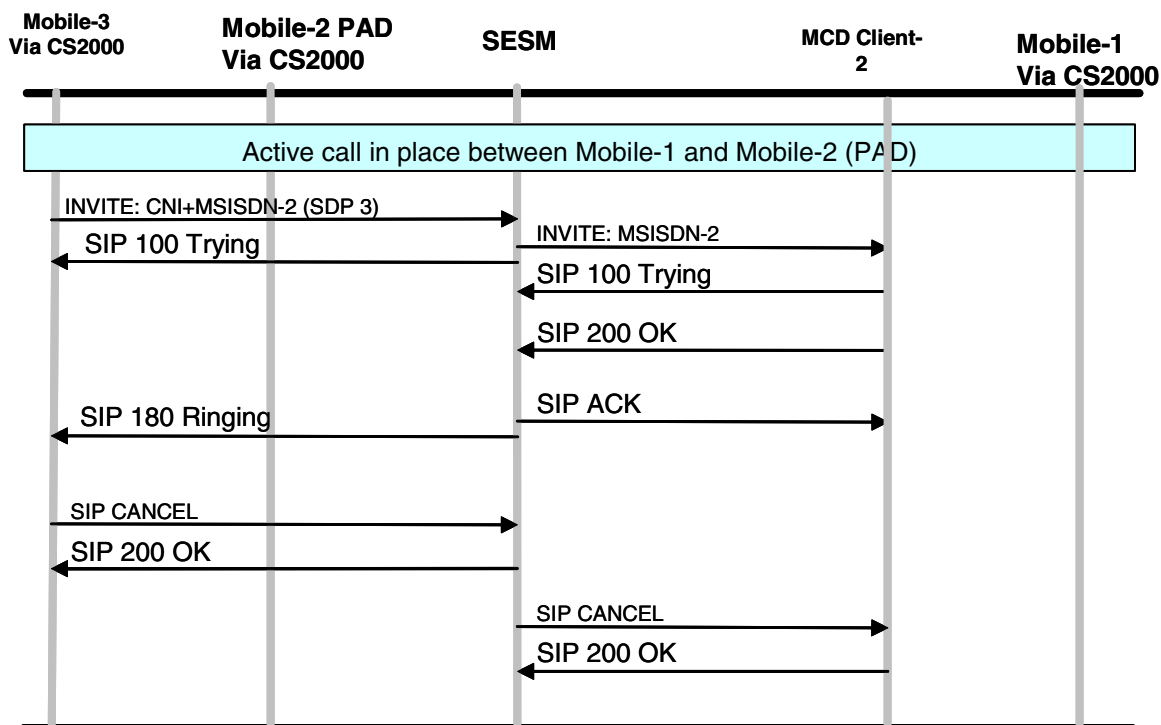
Figure 40 Remote Party Release



20.3.6.4 Remote Party Cancel

The call flow for the PC Client new call is as follows.

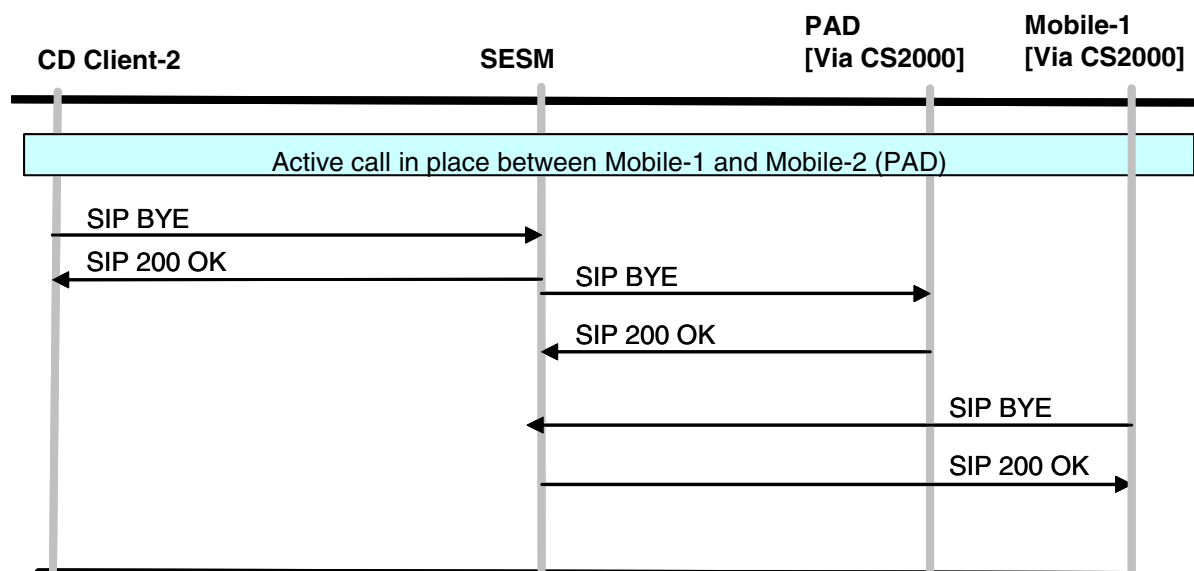
Figure 41 Remote Party Cancel



20.3.6.5 MCD PC Client Release

The PC Client release can occur for any active call leg. The call flow below illustrates the scenario where the establish call is released from the PC Client.

Figure 42 PAD Release



20.4 Hardware Requirements or Dependencies

The Nortel Communication Server 2000 (CS2000) is required to perform the features described.

20.5 Software Requirements or Dependencies

The following software is required to perform this feature.

MCS Component	MCS External Dependency	Description
Sip Application Module	Nortel CS2K or DMS Release ISN08 (or later)	The Wireless Converged Desktop service provides multimedia functionality to existing Mobile TDM switching systems. This entry lists the switch releases that the service supports.

20.6 Limitations and Restrictions

The following restrictions apply to this feature:

1. Video Calls are not supported in this release.

2. Functionality initiated by the PAD does not interact with the MCD feature, and call stated reflecting such services functionality will not be reflected by the MCD PC Client. For example, if a call is put on hold via the PAD, it will not appear to be put on hold as observed on the MCD PC Client, or a call originated by the PAD will have no call control window presented by the MCD PC Client.
3. Dual Hold is not supported on the MCD PC Client in this release. This scenario is when the client attempts to put a call on hold when the call has already been placed on hold by the far end. When the MCD Client has been put on hold (remote hold) and the hold button is blinking to indicate the call is on hold, clicking the hold button will have no effect and will not cause the client to attempt to hold the call again from the client's near end (local hold). Note that this restriction is only applicable when the far end is a SIP or MCD Client user; thus, if the far end is a mobile user and holds the call, as described in restriction 2, the MCD PC Client nor the MCD Service running on the Application Server will be unaware the call is on hold and will not prevent this dual hold scenario.
4. On-call-presence is not supported for PAD originations in this release.
5. The Converged Multimedia PC Client presence works only when the client is registered. If the user logs out of the MCD PC Client, or disconnects from the network, presence will not be correct until the PC Client re-registers.
6. Call Logs (including network call logs) will not be generated for PAD originations.
7. Call logs for MCD PC Client terminated calls contain the CLI provided by the CS2K. Prefixes may be required for call log originations to complete.
8. Call redirection (before answer) is not available in this release.
9. Consult transfer of established calls is not available in this release.
10. Call Park is not available on the Converged Multimedia Client.
11. CS2K overflow routing must be considered and engineered as part of the provisioning of this feature. This is because an MCS SESM outage can impact TDM call completion of converged users on the wireless (e.g. GSM) network. Overflow routing at the CS2K will allow an alternate route to ensure the GSM calls complete in the event the SIPT trunk connecting the MCS is detected as faulty.
12. The Converged Multimedia PC Client does not support Audio; must use the PAD.
13. A Converged User can only have one Multimedia PC Client active at any one time.
14. The MCS must interface a DMS based TDM switching system (CS2K).
15. A single Converged Phone Number can be assigned to a subscriber.

16. The Converged Multimedia PC Client is not aware of Service provided by the Switching System (e.g. Call Forward, Roll Over to Voice Mail).
17. Voicemail – A user should have one VM provisioned. For example, a user should not have VM provisioned on MCP and TDM switch. This can introduce unexpected behavior with the user's PA rules and VM pickup timing. For example, if a user has VM off of GSM network (for their mobile) and provisions a rule on their PA to ring their client (Mobile) 3 times, along with other destinations in their ring-list and their GSM VM is set for 3 rings, then their GSM VM could pick up and the remainder of the PA rules will not be run. The user may expect the PA rules to finish before their GSM VM picking up. Care must be taken on how ring-lists and VM are setup, so the desired behavior is seen.
18. Whenever Voicemail is hosted off TDM switch, MWI is not provided to converged users MCD PC Client.
19. When a MCD user appears in a Personal Agent ring-list the MCD user's redirect COS is not used when a call is extended to the user's converged phone. Instead, the MCD user's primary COS is used. This guarantees that a call to a MCD user will always be able to terminate to their converged phone. Because a MCD user's Preferred Audio Device (the number used to reach their converged phone) is provisioned by the administrator, fraud via redirect should not be a problem.
20. The mobile subscriber (PAD) cannot be part of a centrex group.
21. The mobile subscriber (PAD) can only have single line appearance. Either public or private but not both.
22. Client and network services provided on the wireless TDM network are not coordinated with those provided by the MCS 5200. Each network provides its services independently such that wireless features invoked on the CD Mobile (PAD) will not supervise the MCS Session Manager or its clients.
23. The only originating service supported in this release is click-to-call.
24. If Branding is provisioned, the mobile subscriber may hear branding multiple times during call setup on the PAD. Specifically, branding media files will be played for each call leg into the MCS application server.
25. Telephony translations that involve the prefixes CRD or CRA should be avoided. The CD service will prefix the destination accordingly.
26. Personal Agent routes can not be used to screen converged users PAD number or SIP user ID.
27. This feature does not support MCD PADs accessed from the MCS via a PRI gateway.
28. The Picture ID functionality will ONLY work if a call is made from an MCD PC Client SIP client using SIP addressing. If the call is routed through the GSM network then the picture ID information will be lost.

20.7 Feature Interaction

20.7.1 Service Compatibility

This feature is not compatible with various other MCS services. A summary of service compatibility is provided in the following Table. Service packages that contain the Converged Desktop feature can not be provisioned with any service indicated as 'Not Compatible' in the following table.

Table 21 Service Compatibility

MCS Service	Interaction with Converged Desktop Service
Ad Hoc Conference	Compatible - Subscribers can invoke MCS Conferencing by Joining established calls.
Advance Address book	Compatible - This is used by the "Converged" client to save other subscribers calling information. The address book can be used to originate calls.
Advance Screening	Compatible - This provides the advanced routing and screening capabilities from the MCS Personal Agent.
Allowed Clients – PCClient Set Control	Not Compatible
Assistant Console	Not Compatible - not used by MCD users
Assistant Support	Not Compatible - not used by MCD users
Call Park	Not Compatible - MCD users cannot park or retrieve calls while converged, but the call from a MCD user can be parked
CS2000 SIP Line	Not Compatible - not used by MCD users
Calling Line ID Restriction	Compatible - This service is applied when using the C2C in the "Converged Mode" or using another MCS client for origination of calls from the MCS system. If Calling line restriction is required from a TDM phone then this service would need to be provisioned on the TDM switch providing the service to the phone.
Call Waiting Disable	Not Compatible
Client Collaboration	Compatible – However, all forms of client collaboration are applicable to only MCS subscribers.
Colorful Ringback Tones	Not Compatible
Converged Desktop	Compatible - Set to the following for MCD service "Mobile converged"
Device Access Restrictions	Not Compatible
Hot Line	Not Compatible
Multiple Login Restriction	Not Compatible
Net6 Support on 2004	Not Compatible
IM Chatroom Meet Me conferencing	Compatible - can be assigned to a MCD user to access conferencing bridge and MCS chat room.

Table 21 Service Compatibility

MCS Service	Interaction with Converged Desktop Service
Music On Hold	Compatible – Can be used in most call scenarios where the call traverses the MCS system.
Network Call Logs	Compatible – However, call logs originated from the PAD will not be logged in the ‘outbox’. However calls originated from the MCD PC Client (via click-to-call) will be logged to the call log ‘outbox’.
Presence	Compatible – However, presence of a MCD user is based on the MCD Client registration. If the MCD Client is not registered, presence of the MCD user is not updated.
Qos	Not Compatible
Subscriber OPI	Compatible
Unified Communication	Compatible – MCS / MAS hosted voice mail
Video	Not Compatible
Voice Mail	Compatible - TDM based voice mail.
Wireless Client	Not Compatible
Wireless Gateway	Not Compatible

The following sections describe the interactions of Wireless Converged Desktop service with other supported features that may exist on a converged call. Services not listed are not supported in this release.

1.7.2 Advanced Routing

No special handling is required for sequential or simultaneous calls that include a Converged User.

1.7.3 Voice Mail

Calls that terminate to a MCD PC Client can forward to a Voice Mail system. There are two approaches that can be taken to accomplish this.

The first approach is to have the user continue to use their mobile based voice mail. In this configuration the MCS application server will release these call attempts and the CS2000 must map this release to an ISUP message REL w/ cause. The call can then be further processed on the mobile network to forward the call to a voice mail system.

The second approach is to transition users to an MCP based voice mail system. If an MCP based messaging system is used, then both call legs of the dual leg call to a MCD User are cancelled, and the call is rolled over to the voice messaging system.

1.7.3.1 Voice Mail Hosting

It is recommended that the MCP handle Voice Mail roll over instead of the mobile switching system. This will allow the Personal Agent to search the subscriber's other terminating devices before rolling over to Voice Mail. Doing this may take additional resources because the switching system will have to send all calls to the MCP so that voice mail can be handled.

1.7.3.2 Voice Mail Waiting Indicator (MWI)

If the voice messaging system is hosted off of the MCP the MCD Multimedia PC Client provides a voice mail indicator. The voice mail icon at the top will flash when a new unread message is in your inbox and will stay flashing until the message has been retrieved. VM MWI is not provided if VM is hosted on the TDM system.

1.7.3.3 Voice Mail Access

The MCD user can access their voice mail box by making a call to the voice mail number on the MCD Multimedia Client (which is through the click to call mechanism) or dialing the number on the Converged phone directly. After the call is established, the user can then navigate the voice mail system and retrieve their Voicemail using their Converged Phone keypad. The MCD Multimedia Client cannot be used to do this (unlike the non-converged Multimedia PC Client which can). Double-clicking on the voice mail icon does not call the voice mail server on the mobile network.

1.7.4 Interaction with IM and Web push

Instant Messages or Web pushes received by a SIP user are directed to the MCD Multimedia PC Client only.

1.7.5 Multiple Call Restriction

The maximum number of simultaneous calls is enforced on the MCS Session Manager during call processing.

1.7.6 Presence

Presence is available only on the MCD Multimedia PC when registered. The enhancement called "On the Phone" presence (automatically changes state if the client is engaged in an active call) is not available in this release. For example, if a call originates from the CD Mobile the presence state will not change to "On the Phone" at the PC Client. However, presence states can be manually changed on the MCD PC Client. The standard list of presence states are supported along with any user defined states. Please refer to the "SIP Multimedia PC Client Fundamentals" user documentation for information on Presence for the Multimedia PC Client.

1.7.7 Call Redirect (before answer)

Redirect before answer is not available to a MCD PC Client, but the MCD PC Client and its Converged Phone (PAD) can be redirected by another MCP client before answer.

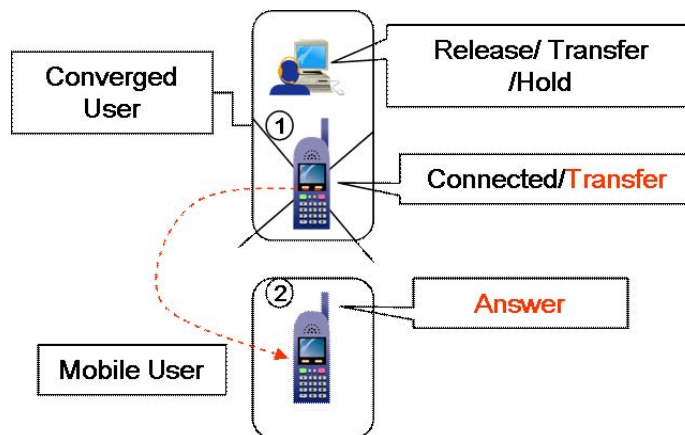
1.7.8 Call Transfer

Direct Transfer after answer is available to the MCD PC Client. When the 'transfer' button is clicked, the subscriber will be shown a window for entering the destination the call should be transferred to and only offers the option to perform a direct transfer. If a direct transfer is invoked, the client will send a SIP REFER message to direct the call to the transfer destination and the call on the PC client is released once the transfer is complete.

Consult Transfer is not available to the MCD PC Client. However the MCD PC Client and its Converged Phone (PAD) can be transferred by another MCP client.

The call-transfer features on the mobile phone may have undesirable side effects when used in conjunction with the MCD feature offered by MCS. Generally, the MCS will not have knowledge of the mobile invoked features. Consider the following scenario which may occur as these features intersect. Figure 43 shows Converged User already engaged in a conversation with a party B (not shown). However, when a transfer is invoked from Converged User's mobile phone to Mobile-2, the voice path will be modified on the mobile network without knowledge of this transition on the MCS network. Thus, resulting in a scenario where the MCD PC Client can control the audio stream of the transferred call even when the audio is changed over to Mobile-2.

Figure 43 Call Transfer from Mobile



1.7.9 Conference Calls

Conference calls are supported on the MCD PC Client.

1.7.10 Meet Me Conferencing

Meet me conference calls are supported on the MCD PC Client.

1.7.11 Caller Line ID (Privacy)

Caller Line ID Privacy is supported on the MCD PC Client and the MCS network. However, the feature must also be enabled on the TDM network at the same time to be effective.

1.7.12 Network Call Logs

1.7.12.1 Inbox

Inbound call attempts are recorded in the Inbox. The ability to successfully re-dial a caller from this call log depends on the calling line id provided by the adjacent switch (CS2K). The prefixing introduced in this feature will be automatically pre-pended by the application server during call routing.

1.7.12.2 Outbox

Only outbound call attempts made from the MCD PC Client are recorded in this Outbox. Outbound call originations from the PAD will not be recorded in this log.

1.7.13 Interaction with RTP Portal

RTP media portal will not be inserted even when the MCD PC Client is behind a firewall.

1.7.14 Interaction with Long Call Audit

Call audits that involve the PAD leg (CD mobile) will simply be forwarded to the CS2000. The MCS Session Manager will not release these call legs directly.

1.7.15 Interaction with Other Media Services

The following services depend on the MAS for providing media.

1.7.15.1 Branding

MAS hosted branding is supported on the MCD PC Client.

1.7.15.2 Colorful Ring-back Tones

CRBT is not supported the MCD PC Client.

1.7.15.3 Music On Hold

MAS hosted music-on-hold is played to all parties on hold (when provisioned).

1.7.15.4 Announcements and Treatments

MAS hosted announcements are not played to a gateway subscribers. Thus, mobile subscribers will not be able to hear these media files on the mobile.

1.7.16 Class of Service considerations for MCD Terminations

When a call terminates to a Converged User, a call leg is extended to the user's converged phone over a gateway route using the Preferred Audio Device DN

that is provisioned for that user. The rules for determining the class of service and dial-plan for processing of the Preferred Audio Device DN are as follows.

When calling within the same domain or across different domains, translations uses the dial-plan of the domain that is being terminated to and the class of service of the Converged Desktop User that is being terminated to.

1.8 Accounting

1.8.1 Converged Desktop Supplementary Service

This feature introduces a new supplementary service to the IPDR. The serviceType field will be labeled “mobileConverged” if this service is running on the call leg that the record is generated on.

```
<ipdr:UE xsi:type="UE-VoIP-Type">
  <recTime>2005-08-04T21:43:51.361Z</recTime>
  <protocol>sip</protocol>
  <uID>058372efe9135810c17e69f7d9e71275f5d13b4@47.104.23.220</uID>

<corrID>058372e6b11c90d3117e69f303e6ff078956bd7@47.104.23.220</corrID>
>

  <connSubscriberID>u2149971915@nortel.com</connSubscriberID>
  <startTime>2005-08-04T21:43:32.079Z</startTime>
  <connParty>sip:2149971915 @nortel.com</connParty>
  <outputPulsedDigits>sip:2149971915 @nortel.com</outputPulsedDigits>
  <tMG>47.104.17.146</tMG>
  <ansInd>>true</ansInd>
  <ansTime>2005-08-04T21:43:51.314Z</ansTime>
  <aband>>false</aband>
  <supplementaryService>
    <sdpService>
      <sessionName>Phone-Call</sessionName>
      <media>
        <mediaName>audio</mediaName>
        <sdpProtocol>RTP/AVP</sdpProtocol>
        <origSdpPort>50082</origSdpPort>
        <origConnAddr>47.102.245.76</origConnAddr>
```



```
<termSdpPort>45040</termSdpPort>
<termConnAddr>47.104.17.146</termConnAddr>
<dir>1</dir>
<codecList>
  <codec>0 PCMU/8000</codec>
  <codec>110 telephone-event/8000</codec>
</codecList>
</media>
</sdpService>
</supplementaryService>
<supplementaryService>
  <mobileConverged>
    <directoryNumber>2149971915</directoryNumber>
    <subscriberID>u2149971915@nortel.com</subscriberID>
  </mobileConverged>
</supplementaryService>
```

1.8.2 IPDR (Internet Protocol Detail Record)

There are some important aspects of the IPDR records generated by the Converged Desktop feature that need to be understood to ensure proper billing can be provided. The following sections describe how accounting for this service is different than normal MCP based calls.

1.8.2.1 Number of Billing records on a Converged Call

The general accounting rules for generating IPDRs apply to Mobile Converged Desktop. The only scenario where the MCD service deviates from the normal policy is when the MCP creates two separate legs for a 'converged' call (one for Mobile and one for PC Client). In that case, the two legs are treated as one and only one record set (i.e. CI/DI or CE/DE) is created to represent both legs of the call.

1.8.2.2 Mid-call (event based) SDP IPDR

On a converged call, when mid-call audio changes occur, each leg on a Dual Leg will generate an SDP IPDR for the stream type it handles. The audio leg will generate an SDP IPDR containing only audio SDP if the audio stream has changed. Additionally, when the PAD audio is modified through the CS2000 the MCS will generate SDP IPDR records.

1.8.2.3 MCP / TDM billing record correlation

All IPDR records generated by a converged call, including the extra IPDRs generated on a Dual Leg call, will have the "corrID" IPDR field set to the same

value so that they can be records. This field can be used to correlate records from converged calls on the MCP and the TDM switch.

If a correlation ID is passed to the MCP via the “x-nt-corr-id” header in an SIP INVITE from a TDM switch, then all IPDRs generated on that call will have the “corrID” field set to the value of the received correlation ID. In addition, if the call is extended back to a TDM switch (same switch or another), the same correlation ID is passed in the SIP INVITE to that switch via the “x-nt-corr-id” header.

1.9 Fault Management

1.9.1 Logs

N/A

1.9.2 Operational Measurements

The following Operational Measurements are added:

1. Each time a CD call is originated by click-to-call

Component: Session Manager

OM group: CONVERGEDDESKTOP3_SERVICE

Tuple Name: ConvergedDesktop_Service

Register Name: CDC2C

Range: Integer

Definition: Counts the number click-to-call originations that were placed from a MCD PC Client.

2. Number of call attempts answered on the CD Mobile (PAD)

Component: Session Manager

OM group: CONVERGEDDESKTOP3_SERVICE

Tuple Name: ConvergedDesktop_Service

Register Name: CDANSPAD

Range: Integer

Definition: Counts the number call attempts that were answered on the CD Mobile (PAD). This scenario occurs when the subscriber is registered on the MCD PC Client and the CD Mobile answers the initial call. Thus, can also be considered the number of 'initial calls answered'. The counter is incremented on the successful SIP Notify transaction sent to the PC

client. This register will not peg if the subscriber is not registered on the MCD PC client.

3. Each time a call attempt is answered on the MCD PC Client

Component: Session Manager

OM group: CONVERGEDDESKTOP3_SERVICE

Tuple Name: ConvergedDesktop_Service

Register Name: CDANSPCC

Range: Integer

Definition: Counts the number call attempts that were answered on the MCD PC Client. This scenario occurs when the MCD Client answers the initial call. Thus, can also be considered the number of 'subsequent calls answered'.

4. Number of call attempts to MCD PC Client when client becomes network isolated

Component: Session Manager

OM group: CONVERGEDDESKTOP3_SERVICE

Tuple Name: ConvergedDesktop_Service

Register Name: CDCOG

Range: Integer

Definition: Counts the number call-of-grace terminations that were attempted on a MCD PC Client. This scenario occurs when a MCD PC Client has a registered contact on the MCS application server, yet fails to auto-answer an incoming call attempt. The behavior at the application server is to attempt this call-of-grace 1 of N call attempts.

5. Number of call attempts redirected to PSTN when MCD PC Client is not registered

Component: Session Manager

OM group: CONVERGEDDESKTOP3_SERVICE

Tuple Name: ConvergedDesktop_Service

Register Name: CDPXYCALL

Range: Integer

Definition: Counts the number call attempts that were proxied back to the CS2000. This scenario occurs when a MCD PC Client has not registered on the MCS application server. All call attempts should be proxied back to the mobile network.

6. Each time a call attempt timer expires on the application server for a CD3 subscriber.

Component: Session Manager

OM group: CONVERGEDDESKTOP3_SERVICE

Tuple Name: ConvergedDesktop_Service

Register Name: CDCATTEXP

Range: Integer

Definition: Counts the number of termination attempts presented to MCD PC Client, where the call attempt timer expired. The call was presented to the subscriber but no action was taken. The application server releases the call upon expiry.

7. Each time a call termination attempt is Rejected / Declined by a CD3 subscriber

Component: Session Manager

OM group: CONVERGEDDESKTOP3_SERVICE

Tuple Name: ConvergedDesktop_Service

Register Name: CDDECLINE

Range: Integer

Definition: Counts the number of declined termination attempts that were presented to MCD PC Client. The subscriber must press 'Decline' for this register to increment.

8. Each time a call termination attempt is Ignored by a CD3 subscriber

Component: Session Manager

OM group: CONVERGEDDESKTOP3_SERVICE

Tuple Name: ConvergedDesktop_Service

Register Name: CDIGNORE

Range: Integer

Definition: Counts the number of ignored termination attempts presented to MCD PC Client. The subscriber must press 'Ignore' for this to register to increment.

9. Each time a call hold / retrieve is attempted by a CD3 subscriber

Component: Session Manager

OM group: CONVERGEDDESKTOP3_SERVICE

Tuple Name: ConvergedDesktop_Service

Register Name: CDHLDRT

Range: Integer

Definition: Counts the number of hold/retrieve attempts managed by the CD3 service.

10. Each time a call transfer is initiated by a CD3 subscriber

Component: Session Manager

OM group: CONVERGEDDESKTOP3_SERVICE

Tuple Name: ConvergedDesktop_Service

Register Name: CDXFER

Range: Integer

Definition: Counts the number of call transfers managed by the CD3 service.

11. Each time a conference call is initiated by a CD3 subscriber

Component: Session Manager

OM group: CONVERGEDDESKTOP3_SERVICE

Tuple Name: ConvergedDesktop_Service

Register Name: CDCONF

Range: Integer

Definition: Counts the number of conference calls managed by the CD3 service.

12. Each time MCD PC Client Register message is received

Component: Session Manager

OM group: CONVERGEDDESKTOP3_SERVICE

Tuple Name: ConvergedDesktop_Service

Register Name: CDREG

Range: Integer

Definition: Counts the number of register messages that are sent by the MCD PC Client during Login, updates, and Presence state changes.

1.10 Glossary

Term	Description
SME	Small to Medium Enterprise
CD	Converged Desktop
GUI	Graphical User Interface
RTP	Real-time Transport Protocol
SIP	Session Initiation Protocol
PBX	Private Branch Exchange
IP	Internet Protocol
STP	SS7 Signal Transfer Point
SCP	SS7 Service Control Point
HLR	Home Location Register
ISUP	Signaling System 7 ISDN User Part
ISDN	Integrated Services Digital Network
SS7	Common Channel Signaling System No. 7
MAP	Mobile Application Part
MSC	Mobile Switching Center
CRD	Destination Call Leg Return Code – preferred audio device prefix
CRA	Associated Call Leg Return Code – click to call prefix
PAD	Preferred Audio Device

Product = MCS

A00012273--SIP Lines: Call Forwarding Indication

Functional Description

1: Applicable Solution(s)

CHS

1.1 Description

This activity provides the CS2K support for Call Forwarding Indicator and Call Forwarding Reminder for SIP agents that interface to the CS2K.

Note that this functionality also requires SIP Client development in the SIP messaging arena, which is not covered by this activity.

Call Forwarding Indicator is provisioned using option CFIND. The SIP client provides a special dialtone (sometimes called “stuttered dialtone”) to a subscriber who goes offhook when the subscriber has had call forwarding activated.

Call Forwarding Reminder provides a brief one-time ringing (sometimes called “ring splash”) to a subscriber who is onhook when call forwarding is active and a call was attempted to the subscriber and forwarded.

Enabling/Disabling of Call Forwarding Reminder is not provisioned as a separate option, but is dependent upon the type of call forwarding and also possibly feature data for some call forwarding types. For example, Call Forward Busy (CFB) never has Call Forwarding Reminder, while Call Forward Universal (CFU) always does, and Selective Call Forwarding (SCF) has feature data indicating if it does.

1.2 Hardware Requirements or Dependencies

None

1.3 Software Requirements or Dependencies

None

1.4 SIP User Agent Interactions & Requirements

If the SIP User Agent (UA) is not registered, calls attempting to terminating to it are unaffected by this feature.

If the UA does not respond to an INVITE, calls attempting to terminating to it are unaffected by this feature.

If the UA rejects an INVITE, calls attempting to terminating to it are unaffected by this feature.

In order to support this feature, the UA must be compliant to draft-ietf-sipping-config-framework-07 (ua-profile event package). The ua-profile event package deals with the call forwarding indicator. Additionally, there is a new event package defined by this feature for the call forwarding reminder.

1.4.1 Call Forwarding Indicator

The syntax used for the call forwarding indicator:

SUBSCRIBE

Event: ua-profile

Accept: application/server-call-feature-status+xml

NOTIFY

Event: ua-profile

Content type: application/server-call-feature-status+xml

Content:

<ua-profile>

<feature>call-forward-indicator</feature>

<status>on | off</status>

</ua-profile>

When call forward is activated, every subsequent origination attempt should get a distinctive dial tone (stutter dialtone).

1.4.2 Call Forwarding Reminder

The new event package deals with the call forwarding reminder. The syntax:

SUBSCRIBE

Event: network-redirection-reminder

Accept: application/network-redirection

NOTIFY

Event: network-redirection-reminder

Content type: application/network-redirection

Content:

call-redirected | subscription-active | subscription-expired

When the call forwarding reminder is activated, if the UA has no calls, there should be a short alerting tone or message presented at the user interface.

1.5 Limitations and restrictions

Option CFIND (in SERVORD) for DPL lines must have feature data STN_TONE set to “CFT”. This is an existing limitation for all types of LGRP lines, which includes DPL lines.

1.6 Interactions

None.

1.7 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_

1.8 Glossary

Term	Description
New term	Definition

1.9 Sample Datafill & Usage

For both call forwarding indicator and call forwarding reminder, it is necessary to have call forwarding datafilled on the line. A sample SERVORD command for call forwarding on DN 5200001 (assuming a RES line):

```
ADO $ 5200001 CFW C NSCR 1 $
```

For call forwarding indicator, it is also necessary to have the CFIND option datafilled. CFIND is a RES option. A sample SERVORD command for CFIND on DN 5200001 is:

```
ADO $ 5200001 CFIND CFT 1000 $
```

With the above datafill, after the subscriber activates call forwarding:

- A stuttered dial tone is given to the subscriber when going off-hook
- When a call is placed to 5200001 and is forwarded, the SIP device will generate a ring splash.

Product = MCS

A00012385--SIP Lines MADN Support

Functional Description

1: Applicable Solution(s)

MCS

1.1 Description

The purpose of this feature is to interwork a specific set of Session Initiation Protocol (SIP) clients into IBN/RES network-based Multiple Appearance Directory Number (MADN) Single Call Arrangement (SCA) features.

SIP Line support is providing the following MDN line options, suboptions, and subfeatures:

- SCA - single call arrangement
- SCA Bridging
- PRL - MADN Privacy Release, PRLA and PRLC activation code
- SCA MREL - MADN Release of Bridging

1.2 Hardware Requirements or Dependencies

Madn Bridging requires that MTM ports be available.

There are no hardware dependencies required to execute this feature.

1.3 Software Requirements or Dependencies

1.3.1 Feature Activity Dependencies

- A00012223 “SESM: Additional Provisioning for SIP Lines

- A00009528 “Call Pickup on Multimedia Communications Platform MCP 9.0”
- A00012273 “SIP Lines: Call Forward Indication”

1.3.2 Software Dependencies

- Succession release SN09 with drop 2 service set patches.
- GWC load GC091
- Session Server / Manager software load MCP_9.1.0.0

1.3.3 Firmware Dependencies

None

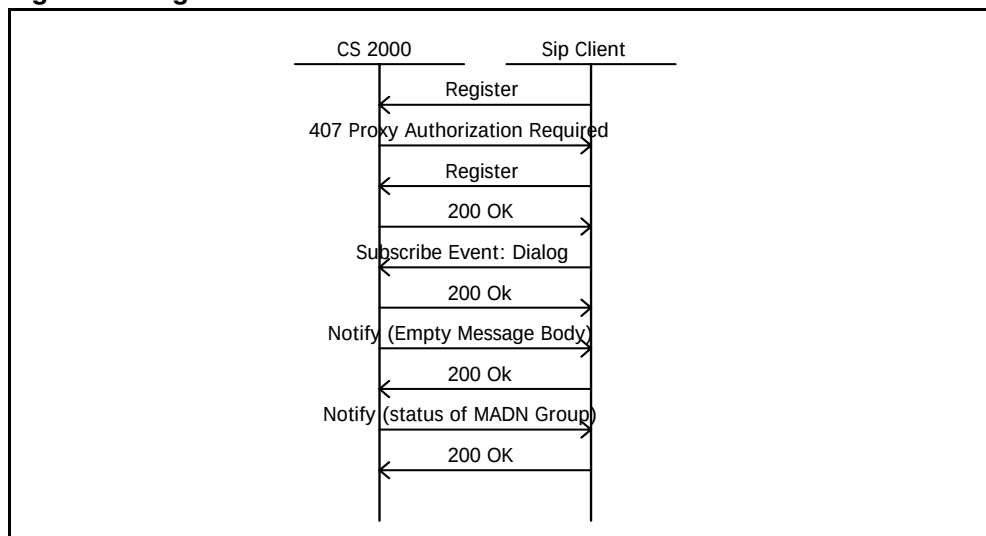
1.3.4 SIP Client Requirements

SIP Clients wishing to supply CS 2000 Network-Based MADN SCA Bridging functionality are expected to be compliant to RFC 3261, RFC 3265 and draft-ietf-sipping-dialog-package-06. The following information is provided so Client vendors will understand the message sequences of special importance.

1.3.4.1 Client Registration/Subscription and the Dialog Event Package

The ONT SIP clients must be provisioned with the MADN Dialog Event Package such that the client will properly register for the events. When a client supporting MADN registers, in addition to sending a SIP Registration to register the contact, it also needs to Subscribe to the Dialog event package. The message sequence is shown below. All of the Register and Subscribe messages should be authenticated by the SS. In the flow below the expectation is that the client is reusing the Proxy Authentication header.

Figure 1 Registration Call Flow



The Subscription to the dialog event should be subscribing to the user's own dialog status. The first Notify sent back will just contain the time out information for the subscription. The ONT should not treat an empty message body as anything other than a Notification of the status of the subscription. It should not cause a state change for the MADN group status. In order to change the group status the client must receive a message body in the Notify. Only two of the states are expected to be reported for the MADN group. If the group is busy the state of Confirmed will be sent. If the group is idle the state will be terminated.

The content type of the message body is that defined in the draft which is: application/dialog-info+xml. The message body for the active state will look like the following:

```
<?xml version="1.0"?>
  <dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info"
    version="0" state="full"
    entity="sip:MADNDN@example.com">
    <dialog id="as7d900as8">
      <state>confirmed</state>
    </dialog>
  </dialog-info>
```

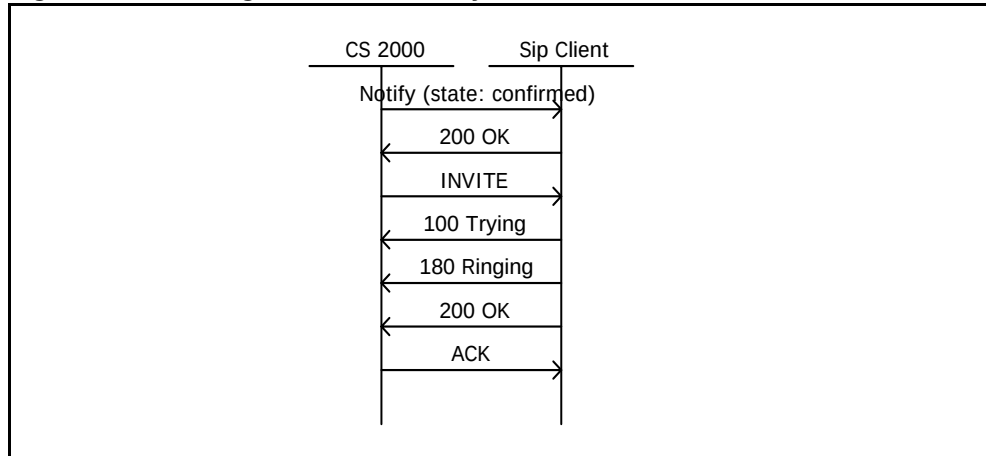
The MADNDN in the above message body example will be replaced with the actual MADN.

For the idle state the confirmed will be replaced with terminated. If the client has not received any indication of a state change it should assume that the state of the group is idle.

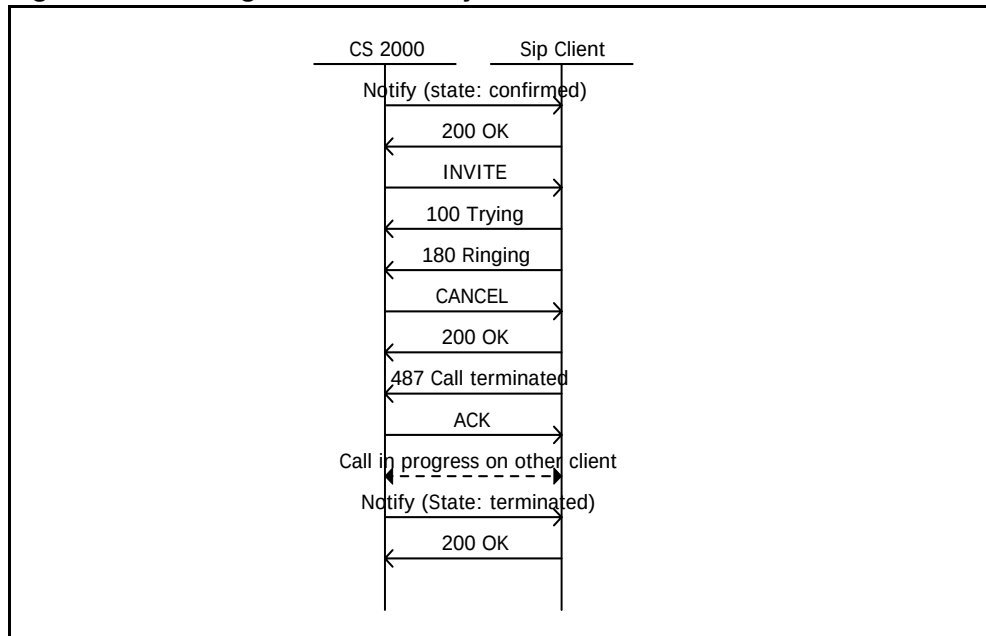
The reason that the state of the group is important is that any member of a MADN SCA group needs to treat an off-hook while the group is active as a bridging request unless a client is currently processing an inbound invite. The bridging request is discussed in section "1.3.4.3 Bridging Requests"

1.3.4.2 Incoming Call Processing

An inbound call to a client should be processed as any normal SIP invite inbound to the client. The state of the MADN group should not cause an inbound INVITE to be treated any differently. The Group will transition to the confirmed state either shortly before the Invite is received or shortly afterwards.

Figure 2 Incoming Call Answered by Client

If the call is answered by another member of the MADN group the call flow will look like any other abandoned call. The group will stay active until the call is released by all members of the MADN group.

Figure 3 Incoming call answered by another client

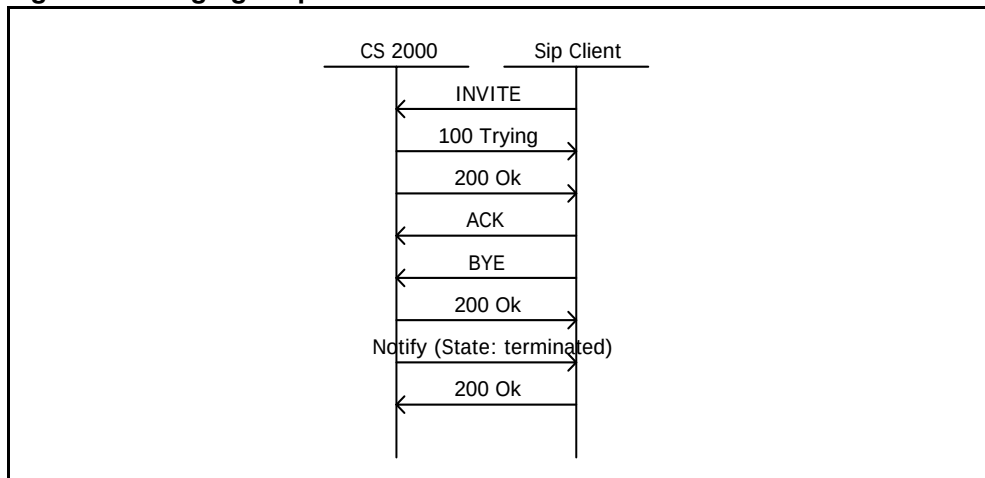
1.3.4.3 Bridging Requests

When a client is Idle but the group is busy and the user takes the handset off-hook the client should initiate an invite immediately without providing dial tone or letting the user input dtmf digits. This invite will be treated as a request to bridge the call into the active call. For this invite request it is recommended that the Invite look like the user is calling themselves. For example if the MADN dn is 555-1212 and the domain for the user is example.com the status line, to and from headers for the call would look like the following:

INVITE sip:5551212@example.com SIP/2.0
To: sip:5551212@example.com
From: sip:5551212@example.com;tag=3149adf0987

The rest of the INVITE would be formatted as any other initial INVITE request from the client. The call will be fast answered, meaning the client will receive a 200 Ok to the INVITE without any other provisional responses with the exception of the 100 trying.

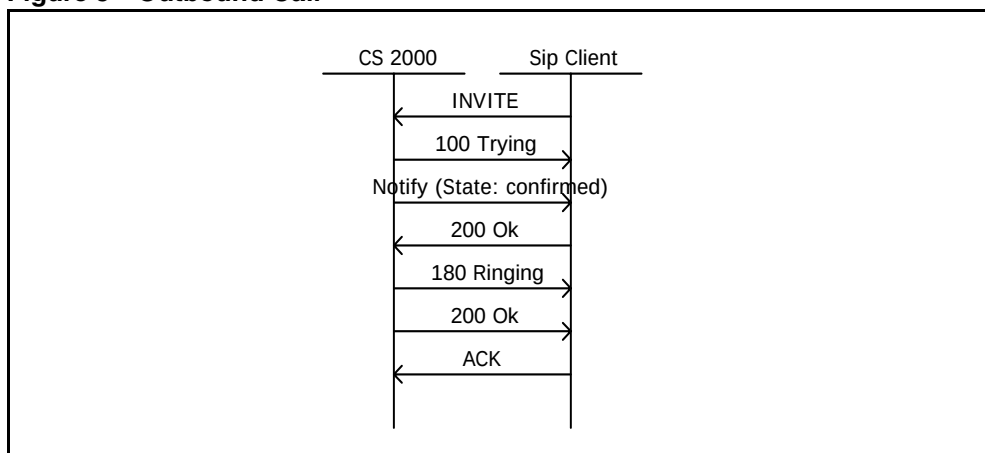
Figure 4 Bridging Request



1.3.4.4 Outbound Call

The normal outbound call case is when an idle client in an idle group sends an INVITE out. In this case the client will collect digits from the user and then send the INVITE. Shortly after sending the Invite a NOTIFY will be received marking the group as active.

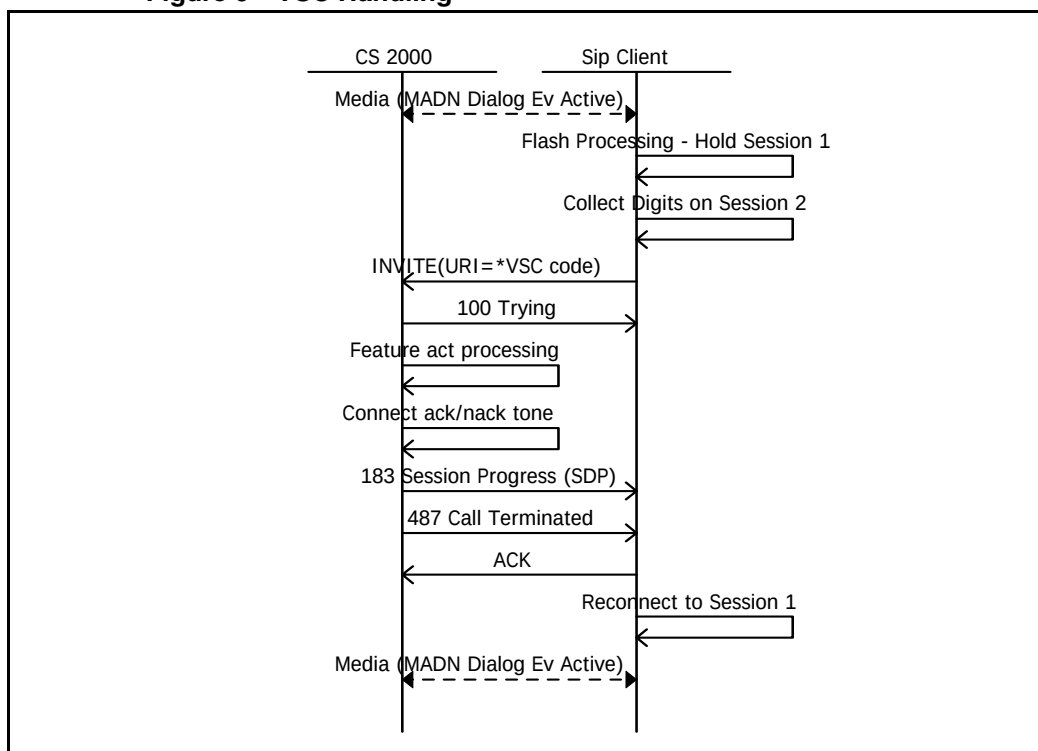
Figure 5 Outbound Call



1.3.5 VSC Call

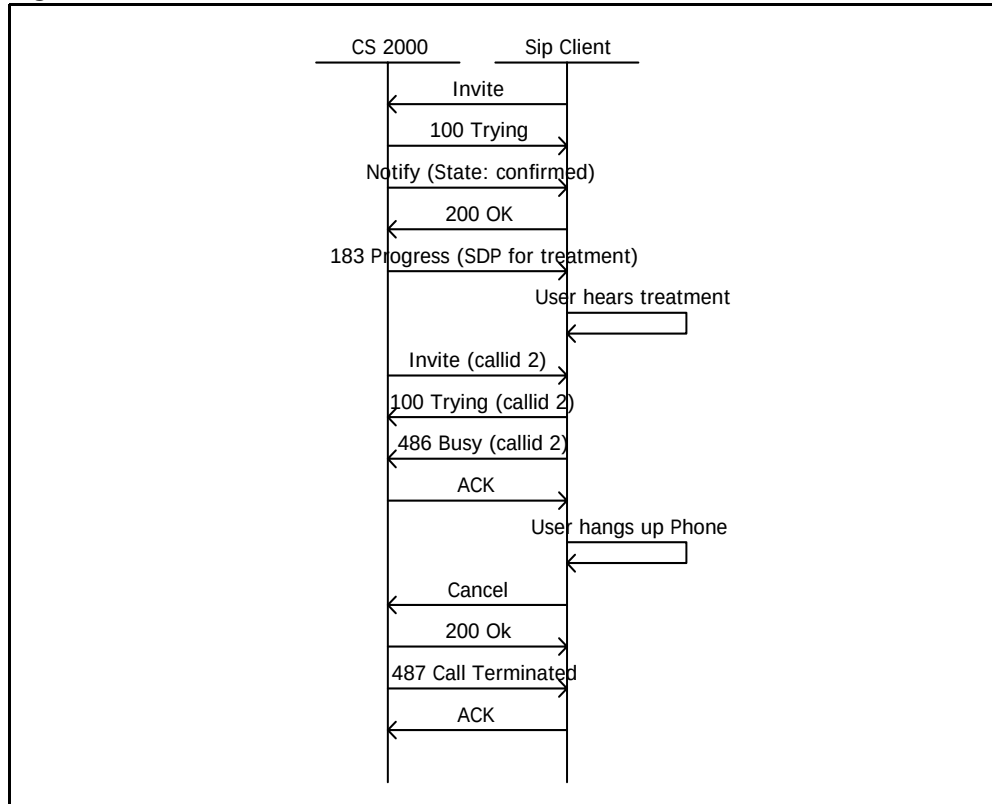
MADN has imbedded features MHOLD and PRL which must be handled via Vertical Service Codes (VSCs) during active calls in the MADN group. For a MADN member participating in the MADN call (active media stream), the client is expected to handle Flash + digits processing, and send those digits to the CS 2000 for processing. The CS 2000 will evaluate the digits and process accordingly, connecting the VSC session to Ack or Nack tone, and then providing instruction to collapse the VSC call. The client is then expected to reconnect the media path to the original session.

Figure 6 VSC Handling

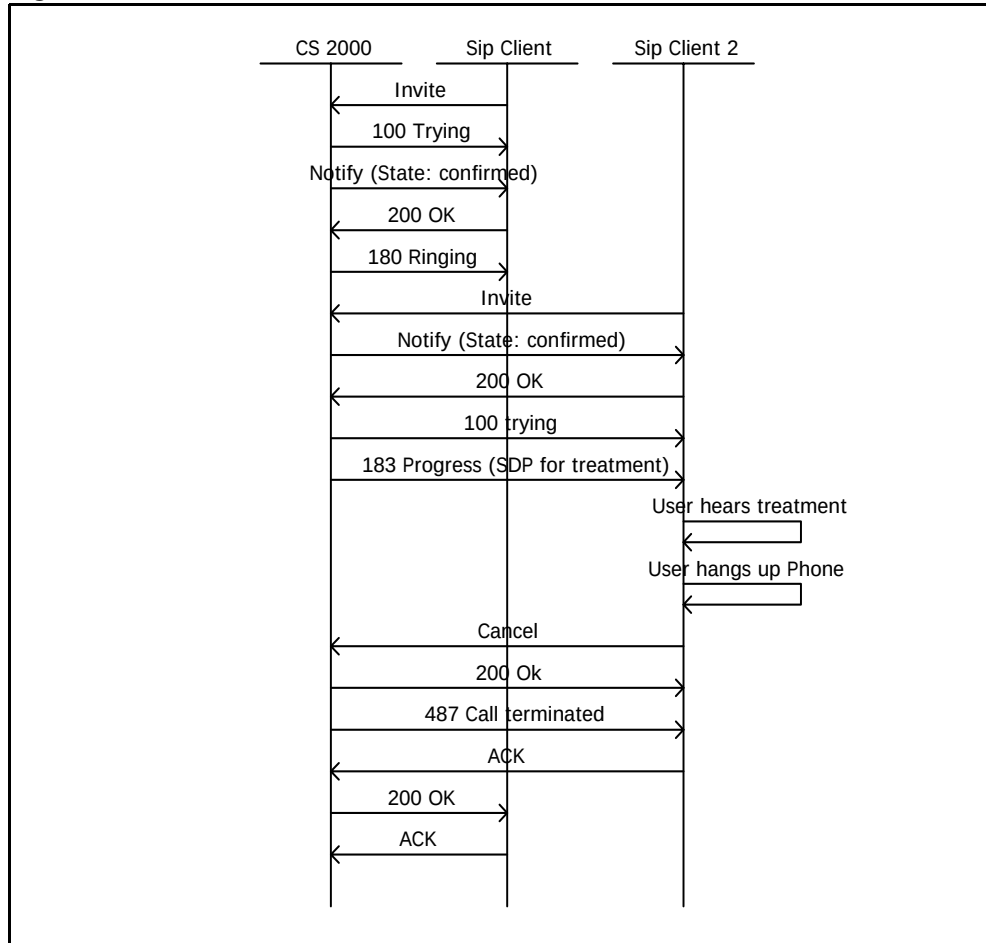


1.3.5.1 Race Conditions

There are really two race conditions that will commonly occur. The first occurs when placing an Inbound call and an outbound call pass on the wire. The Outbound call will be given treatment. The inbound call will then be delivered to the client. How the client behaves depends on the client. The assumption is that the client will send 486 busy to the Inbound call and the user will hang up the call getting treatment. After hanging up the call if the user takes the phone off hook this should be treated as a bridging request and the user will end up answering the call. The call flow is shown below up to the point of the bridging request:

Figure 7 Inbound/Outbound Race

The other major race condition is two clients attempting to perform outbound calls simultaneously. In this case the clients call who arrives second will be given treatment and denied the origination. This case looks like the above but the call flow is a little different.

Figure 8 Dual Outbound call race

1.4 Limitations and restrictions

- This feature supports a limited set of SIP devices. Only SIP client devices which adhere to the SIP Client Requirements laid out in this document will be supported.
- MADN Engineering Rules as they apply to SIP Lines with the DPL option are as follows:
 - MADN groups can have 32 members in either SCA arrangements
 - no more than 16 members of the same MADN group can appear on a single GWC
 - all members of a MADN group must belong to the same customer group

- No support for multiple SIP sessions with the exception of a second session invoking a Vertical Service Code (VSC) feature during an active / stable call
- MADN Bridging requires that MTM ports be available.
- BLV/BI is not supported to a busy call that involves a Multiple Appearance Directory Number (MADN) SIP DPL. The Operator is provided busy line treatment if either the BLV line or the connected party is a MADN SIP DPL.
- The following MADN options, suboptions and subfeatures are not supported on SIP clients:
 - MCA - Multiple Call Arrangement
 - CACH - Call Appearance Call Handling
 - EXB - Extension Bridging
 - MRFM - MADN Ring Forward Manual
 - MRF - MADN Ring Forward
 - CFMDN - Call Forward MDN Secondary Members - MCA
 - MLAMP - MADN Lamp
 - PRV - MADN Privacy
 - MHOLD - MADN HOLD

Note: MHOLD is not supported in 09FF; however Hold will be supported through client based hold.

Note: MRF is not supported in 09FF; however RF will be supported through client based RF.

Note: MDNNAME and MEMDISP will be supported only for non-DPL lines.

Note: MADN Bridging requires MTM be idl. If MTM ports are not available the following logs will be generated:

COMPACT2 FTR138 FEB17 17:01:45 4223 INFO TRMT

SSL1 00 0 01 00 DN 1418407730 KEY 1

TREATMENT SET = FNAL FEATURE = MDNBRG

CALLID = 163882

COMPACT2 FTR138 FEB17 17:01:45 4324 INFO TRMT

SSL1 00 0 03 07 DN 1418408723 KEY 1

TREATMENT SET = NOSC FEATURE = MDNBRG

CALLID = 98346

1.5 Interactions

- If a SIP client is provisioned with MADN group and the client comes into service while the MADN group is ringing, that member will be notified the MADN dialog is active, but it will not be instructed to apply ringing.
- If a MADN group is comprised solely of SIP clients, there is the possibility that all members of the group could reject a call termination attempt. If this occurs, the originator of the call will be sent to reorder treatment. With non-functional originators (i.e. 2500 sets) there are scenarios where the originator may hear audible ringing and then be sent to treatment when the SIP line terminator rejects the call.

1.6 Query Commands

The query commands allow you to perform various existing queries.

Command format:

- qdn <DN>
- qlen <LEN>
- qsip <DN,LEN>

Command usage:

To Query a DN

>>qdn 6213101

```
-----
DN: 6213101 (NON-UNIQUE)
TYPE: MULTIPLE APPEARANCE DIRECTORY NUMBER
SNPA: 613 SIG: DT LNATTIDX: N/A
XLAPLAN KEY: N/A RATEAREA KEY: N/A
LINE EQUIPMENT NUMBER: SS 00 1 00 21
PRIMARY LEN: SS 00 1 00 21
LINE CLASS CODE: IBN
IBN TYPE: MADN
MADN INFO - TYPE:SCA PRIMARY:Y RING:ALWAYS
```

```
MADN GROUP INFO - DENIAL_TRMT: TONE BRIDGING:Y
CONF_SIZE: 3 BRIDGE_TONE:Y INIT_STAT:NONPRIVATE
CUSTGRP:      BNR SUBGRP:0 NCOS: 0
CARDCODE: RDTLSG GND: N PADGRP: PKNIL BNV: NL MNO: N
PM NODE NUMBER : 214
PM TERMINAL NUMBER : 22
OPTIONS:
DGT DPL Y 10
OFFICE OPTIONS:
SRA
MADN MEMBER LENS INFO:
SS 00 1 00 21 SCA PRIMARY: Y RING: ALWAYS
SS 00 1 00 22 SCA PRIMARY: N RING: ALWAYS
FUNC 101 KEY: 1 SCA PRIMARY: N RING: ALWAYS NCOS: 0
FUNC 102 KEY: 1 SCA PRIMARY: N RING: ALWAYS NCOS: 0
```

To Query a LEN

qlen SS 00 1 00 21

```
LEN: SS 00 1 00 21
TYPE: MULTIPLE APPEARANCE DIRECTORY NUMBER
SNPA: 613
DIRECTORY NUMBER: 6213101 (NON-UNIQUE)
LINE CLASS CODE: IBN
IBN TYPE: MADN
MADN INFO - TYPE:SCA PRIMARY:Y RING:ALWAYS
MADN GROUP INFO - DENIAL_TRMT: TONE BRIDGING:Y
CONF_SIZE: 3 BRIDGE_TONE:Y INIT_STAT:NONPRIVATE
CUSTGRP:      BNR SUBGRP:0 NCOS: 0
SIGNALLING TYPE: DIGITONE
CARDCODE: RDTLSG GND: N PADGRP: PKNIL BNV: NL MNO: N
PM NODE NUMBER : 214
PM TERMINAL NUMBER : 22
OPTIONS:
DGT DPL Y 10
OFFICE OPTIONS:
SRA
```

To perform a sip query -- qsip <dn> or qsip <len>

>qsip 6213101

```
SIP USER DATA
=====
SIP URI: user21@rtp7ssb.com
ACCOUNT STATUS: ACTIVE
REGISTERED: Y
ALLOW POST BSY TERMINATIONS: N
```

NUMBER OF CONTACTS: 2
 CONTACTS: 47.142.66.155:5060 user21@47.142.91.49:5060
 SERVICE PACKAGE:
 basic_package
 SERVICES:
 ALCLNT N IM SIPLN ADVSCR 5 9 N CLNTCO N N N N ADHOC 4 ADDRKB 50 PRES
 10 N
 null N VIDEO N N IMCHAT NWLOG 50 50

SIP LINE DATA

=====

ENDPT ID: SS/000/1/0021
 VMG: rtp7ssb
 ZONE ID(s):
 CLIENT TYPE: ONT
 STATIC CLIENT: Y

SIP CALL DATA

=====

ACTIVE CALL APPEARANCES:
 NODENO TERMNO
 NUMBER OF ACTIVE SESSIONS IN CS2000 SESSION SERVER: 0

To post a dn or len at the map

mapci;mtc;pm;lms;ltm

Posting a dn or len at the map yields the same results.

post <dn> or post <len>

XAC	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
AMDI	RExByp	NODLOG	RExSch	2	SPM	2	RS	SYSB	117C..
ATM_6+									
M			*C*	*C*	*C*	*C*		*C*	
LTP									
0 Quit	POST	DELQ		BUSYQ		PREFIX			
2 Post_	LEN SS	00 1 00 21				BEAR IP_P			
3	LCC PTY	RNG				STA F S LTA	TE	RESULT	
4	IBN		DN 613 621 3101	IDL					
5 Bsy									
6 RTS									
7 Diag									
8									
9 AlmStat									
10 CktLoc	post d	6213101							
11 Hold									
12 Next									
13									
14									
15 FullDn									
16 Prefix									
17 LCO_									
18 Level_									

LMM:
<dn> post

dn call server cli call server line state endpoint state gateway profile time
6136213101 rtp7 idl unsupported_gw sipvoice 14.44:33

1.7 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

1.8 Glossary

Term	Description
New term	Definition

Product = MCS

A00012506--Border Control Point (BCP) Operational Measurement (OM) Enhancements

Functional Description

1: Applicable Solution(s)

MCS

1.1 Overview

1.1.1 Operational Measurements

Operational measurements (OMs) provide statistical information on the server operations and performances. OMs are represented in terms of groups, which contain registers (counters and gauges) that provide performance-related data. The Management Module (SysMgr) scans OM Group registers at configured intervals. The OM information associated with a selected component is then viewable by administrators in the OM Browser at any selected point in time (corresponding to the launching of the OM Browser). There are two types of OMs: active and holding. Active OMs are displayed as they are reported by the server to the management server/management console. Holding OMs have already been archived to files on the server hosting the active Management Module. The OM scan cycle is configurable using the OAM configuration options available in the System Management Console. OM scan cycles are configured per Network Element (NE). The configured value can be changed via the “Configuration Parameters” (see Figure 1: NE Configuration Parameters), under the “Parm Group: OM” shown in Figure 2: OM Parm Group Configuration Parameters.

Figure 1: NE Configuration Parameters

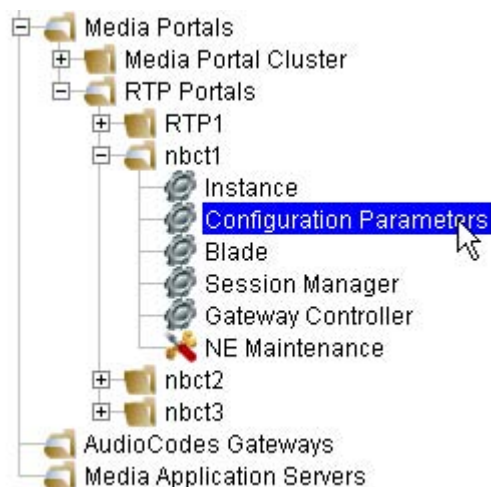
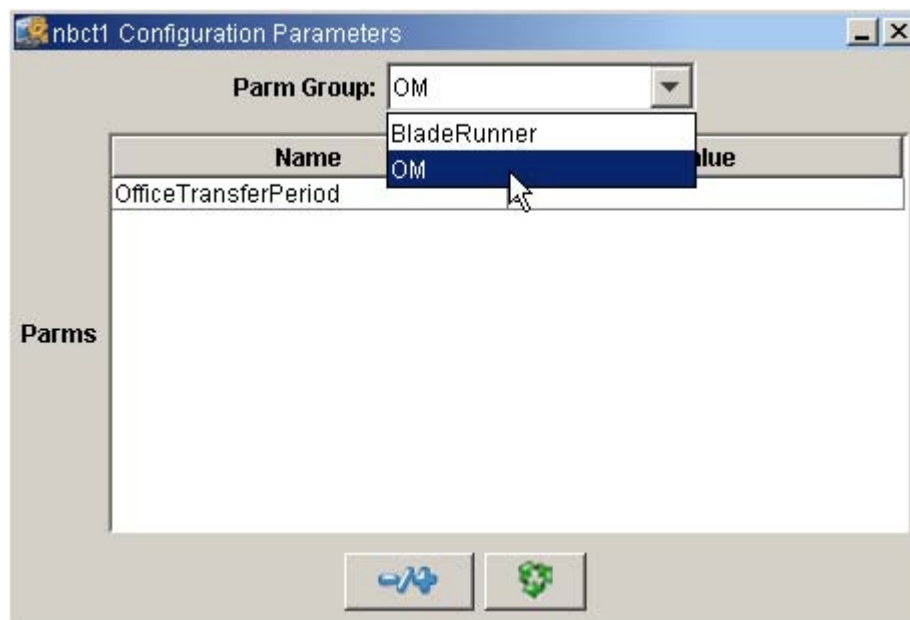
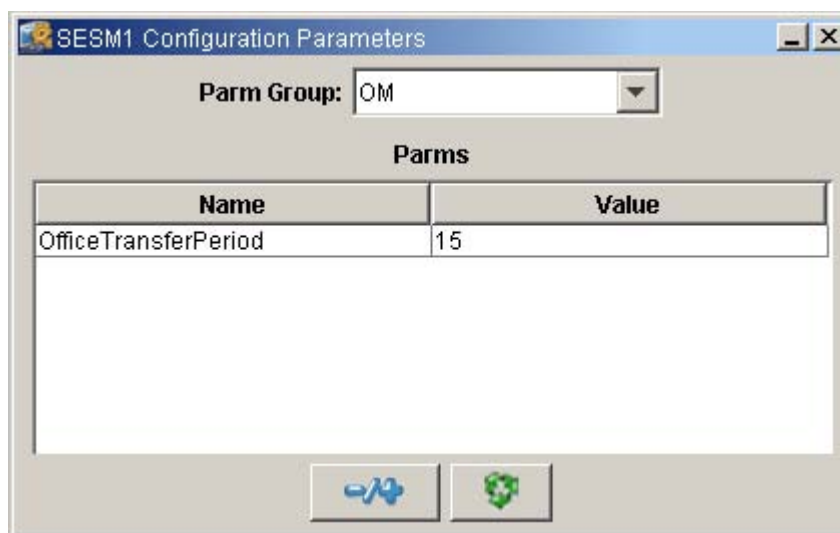


Figure 2: OM Parm Group Configuration Parameters

The parameter that controls how often OM's are collected is named "OfficeTransferPeriod" and the value is specified in minutes. Valid values for this parameter are 5, 15, 30 or 60 minutes.

Figure 3: OfficeTransferPeriodConfiguration Parameter

The OM Framework handles pushing OM's collected to IEMS.

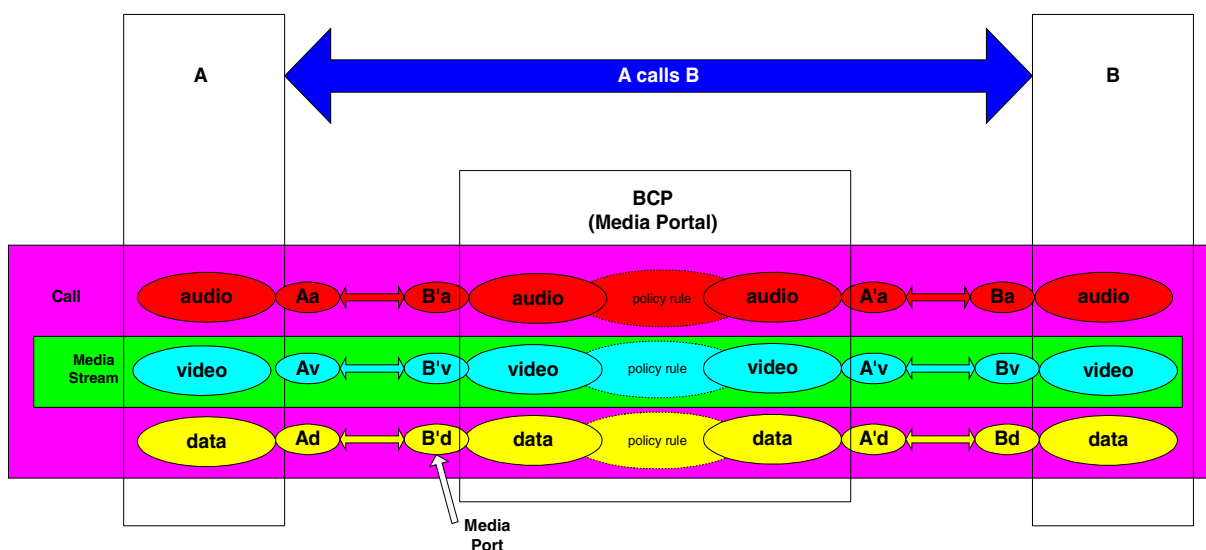
1.1.2 BCP

The BCP was previously referred to as the RTP Media Portal. Renaming existing references to RTP Media Portal is beyond the scope of this feature,

hence; the old terminology is used where needed to maintain consistency with what exists today.

BCP only understands ports and streams. Figure 4: BCP Media Streams shows an example of a basic “A calls B” scenario that involves three media streams. A media stream is successfully created once a policy rule connects two connections on the BCP. In the example shown below, the BCP knows that six ports have been allocated and that three policy rules have been created.

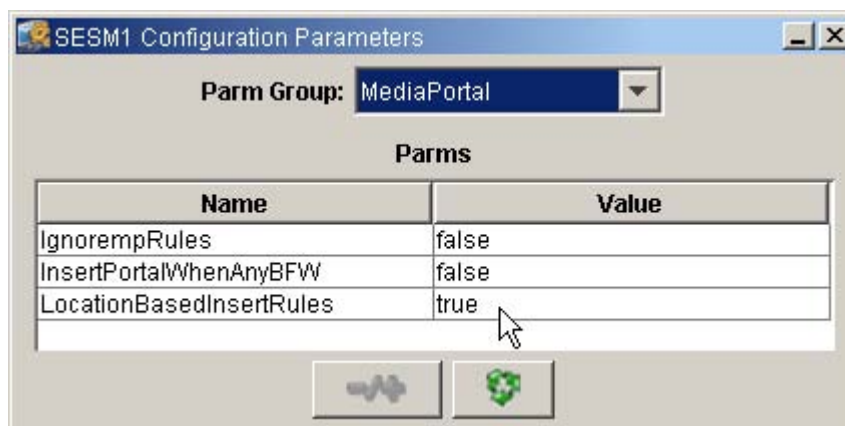
Figure 4: BCP Media Streams



1.1.2.1 BCP Insertion Configuration

The configuration parameters shown in Figure 5: SESM MediaPortal Configuration Parameters may need to be modified depending on network configuration for the Session Manager to insert a BCP for a given call.

Figure 5: SESM MediaPortal Configuration Parameters



IgnorempRules (default setting is false):

If set to true, the SESM would completely ignore BCP insertion rules, meaning the SESM would not insert any BCP to any call in the MCS system. This parameter should only be set to true when there is no BCPs configured in the MCS system. When this parameter is set to true, the settings for “InsertPortalWhenAnyBFW” and “LocationBasedInsertRules” are ignored.

InsertPortalWhenAnyBFW (default setting is false):

This parameter is only used when “LocationBasedInsertRules” is set to false. If “LocationBasedInsertRules” is not enabled, the SESM would use the non-“LocationBasedInsertRules” which is the default setting of the SESM BCP insertion rule. If non-“LocationBasedInsertRules” is used, by default, the SESM does not insert a BCP to a call unless one of the following criteria is met:

- If either or both of originating and terminating clients’ domain configurations on the PROV have “AlwaysUseMediaPortal” set to true with this call.
- If either or both of the origination and terminating clients are behind the firewall or NAT (BFW). Basically, with the legacy insertion rule, if there is any BFW client in the call, a BCP should be inserted. However, due to the consideration of the effective usage of BCP resources, it is assumed that if both clients are BFW and in the same domain, most likely they are behind the same firewall or NAT, they should be able to communicate with each other without having to consume any BCP resources. Therefore, in this case, a BCP is not inserted unless the “InsertPortalWhenAnyBFW” is set to true to override the assumption.
- If the call is traversed through two interfaces (public/private), a BCP is inserted.
- If the call is originated from or terminated to a device which is unable to handle media changes, a BCP is inserted.
- If privacy is required for this call, a BCP is inserted.

LocationBasedInsertRules (default setting is false):

This is the enhanced BCP insertion rule that is based on the location infrastructure of the virtual network topology. If this parameter is set to true, the SESM would ignore the legacy BCP insertion rules (e.g. firewall clients, InsertPortalWhenAnyBFW, AlwaysUseMediaPortal domain, etc). By default, the SESM inserts a BCP to every call unless there is a Routability Group provisioned via the Provisioning Module for the call with the originating and terminating clients’ location to suppress BCP insertion. Note that even though the originating and terminating clients are at the same location, a BCP is still inserted to the call if no Routability Group is configured with the location. When this parameter is set to true, the setting of “InsertPortalWhenAnyBFW” is ignored.

1.2 Description

This activity provides operational measurement enhancements for Border Control Point (BCP) usage. These enhancements are intended to provide some degree of parity between the GWC and the SIP Session Manager view of BCP performance measurements. Refer to Table 1: Session Manager vs GWC OMs for details on where the two diverge. This activity requests that additional Performance Measurements related to the BCP usage be generated on:

- Each controlling Session Manager
- Each Border Control Point

Table 1: Session Manager vs GWC OMs

OM	Session Manager	GWC
sesmSuccessCalls (GWC equivalent: “GWC successful calls” 5/10)	1 call = many BCPs Media streams for a single call may be distributed over multiple BCPs (e.g. audio + video + data).	1 call = 1 BCP Media streams for a single call are co-located on a single BCP.
sesmFailedCalls (GWC equivalent: “GWC failed calls” 5/10)	1 call = many BCPs Media stream for a single call may be distributed over multiple BCPs (e.g. audio + video + data) For example: a multimedia call (audio + video + data) would fail if any of the 3 policy rules on any of the BCPs suffered a failure.	1 call = 1 BCP Media streams for a single call are co-located on a single BCP.
mediaPortalCount (GWC equivalent: “Number of provisioned Media Proxies”)	The number of BCPs configured in the Management Console to support this Session Manager	The number of BCPs provisioned to support this GWC.
sesmSuccessStreams (GWC equivalent: “Media Proxy successful calls” 5/10)	(per-Stream) The number of stream setup requests (policy rules) that were successfully processed by this BCP.	(per-Call) The number of calls successfully setup by this BCP.
sesmFailedStreams (GWC equivalent: “Media Proxy failed calls” 5/10)	(per-Stream) The number of stream setup requests (policy rules) that were not successfully processed by this BCP.	(per-Call) The number of calls that failed to be setup by this BCP.

1.2.1 Session Manager OMs

1.2.1.1 Media Portal

There are three new OM Registers added to the OM Group “MediaPortal” defined in Table 2: OM Group Media Portal - New OM Registers. Figure 6: Example GUI snapshot of MediaPortal OM Group shows the new OM Registers in the OM Browser GUI.

Table 2: OM Group Media Portal - New OM Registers

Register Name	Type	Description
sesmSuccessCalls	Counter	The number of calls that were successfully setup using any available BCP on this Session Manager in the last collection period.
sesmFailedCalls	Counter	The number of failed attempts to setup a call on any available BCP on this Session Manager in the last collection period.
mediaPortalCount	Usage	The number of BCPs configured to support this Session Manager from the Management Console. This counter will be updated when BCPs are added or removed via the Management Console.

Figure 6: Example GUI snapshot of MediaPortal OM Group

The screenshot shows the 'OM Browser--SESM1_0' window. At the top, there's a search bar with 'OM Group: MediaPortal' and 'Type: Active'. Below this is a section titled 'OM Details:' with a timestamp '14:34:19 11-21-2005'. A table displays the following data:

OM Row	mediaPortalCount	sesmSuccessCalls	sesmFailedCalls	createConnectionCount	deleteConnectionCount	modifyConnectionCount	disable
MediaPortalOMs	6	0	0	0	0	0	0

At the bottom of the window, there is a 'Refresh' button.

1.2.1.2 Media Portal Instances

For OM Registers that are per-BCP, a new OM Group (“MediaPortalInstance”) is introduced. The OM Registers defined for this OM Group are described in Table 3: OM Group Media Portal Instance - New OM Registers. For each BCP configured to support this Session Manager, an OM Row is created. For CPX8216-T, the OM Row name is the NE-name. For BladeCenter-T, the OM Row name will be a label of the following form: <MediaPortalClusterName>.<ServiceID> (e.g. “MCP1.0”, “MCP1.7”, ...). An example using BladeCenter-T is shown in Figure 7: Example GUI snapshot of MediaPortalInstance OM Group. The OM Row for a BCP is not

added to the OM Group until the BCP registers with the Session Manager (sends a RSIP message). If a BCPs' configuration is removed via the Management Console, its operational measurements for the current OTP are lost. The OM Row is not removed when the BCP deregisters with the Session Manager.

Table 3: OM Group Media Portal Instance - New OM Registers

Register Name	Type	Description
sesmSuccessStreams	Counter	The number of stream setups that were successfully processed by this media portal.
sesmFailedStreams	Counter	The number of stream setups that were not successfully processed by this media portal.

Figure 7: Example GUI snapshot of MediaPortalInstance OM Group

OM Row	sesmSuccessStreams	sesmFailedStreams	rSipReceivedCount	createConnectionCount	modifyConnectionCount	deleteConnectionCount	CRCXErrorCount
RTP1	0	0	17	0	0	0	0
cluster1.0	0	0	17	0	0	0	0
cluster1.1	0	0	18	0	0	0	0
cluster2.0	0	0	17	0	0	0	0
cluster3.0	0	0	17	0	0	0	0
cluster3.1	0	0	18	0	0	0	0

1.2.1.3 Session Manager Call Processing

The following diagram shows the flow for pegging the requested call related OMs on the Session Manager and the requested per-BCP OMs for that Session Manager. The new OMs are:

- Session Manager failed calls (sesmFailedCalls)
- Session Manager successful calls (sesmSuccessCalls)
- BCP failed streams (sesmFailedStreams)
- BCP successful streams (sesmSuccessStreams)

Figure 8: Session Manager "Call" OM Generation Logic

1.2.1.4 Session Manager Failed Calls

The Session Manager Failed Calls OM (“sesmFailedCalls”) represents the number of failed attempts to setup a call on any available BCPs on this Session Server in the last collection period. Unlike the GWC, media streams for a single call can be distributed over multiple BCPs. As Figure 8: Session Manager "Call" OM Generation Logic8 shows, for each new call, if a BCP is required for the call, the Session Manager will check to see if there are any BCPs available (registered with this Session Manager). If not, then the “sesmFailedCalls” OM Register is pegged. If there is a BCP available, the Session Manager will then attempt to create a policy rule for each media request for the call (e.g. audio, video, data). If there is a failure on one BCP, the Session Manager will attempt to use the next available BCP. If the Session Manager exhausts its pool of available BCPs before creating all the policy rules needed for the call, then the “sesmFailedCalls” OM Register is pegged.

1.2.1.5 Session Manager Successful Calls

The Session Manager Successful Calls OM (“sesmSuccessCalls”) represents the number of calls that were successfully setup using any available BCPs on this Session Manager in the last collection period. For a single call, unlike the GWC, media streams can be distributed over multiple BCPs. Figure 8: Session Manager “Call” OM Generation Logic illustrates the logic used in pegging this OM Register. This OM Register is incremented only if the Session Manager successfully creates a policy rule for each media. Note that it is possible for there to be a failure to create a policy rule for a media stream; however, the Session Manager will attempt to create it on the next available BCP (if not already exhausted its pool of BCPs).

1.2.1.6 BCP Failed Streams

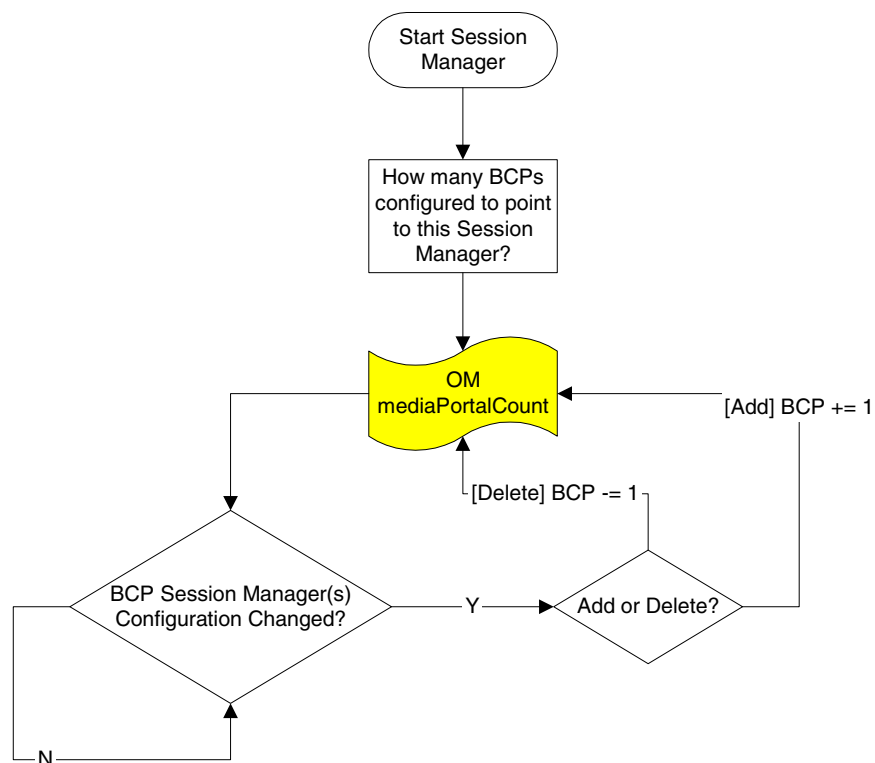
The BCP Failed Streams OM (“sesmFailedStreams”) represents the number of stream setup requests that were not successfully processed per BCP. Unlike the GWC, the BCP does not have a notion of a call, but of ports and streams as shown in Figure 4: BCP Media Streams. As the figure shows, there are six ports allocated to the call for three media streams. A failure to allocate a port on the BCP or a failure to join the two ports via a policy rule in order to establish a media stream increments this OM register by one. This OM register is pegged per media stream and not per call as illustrated in Figure 8: Session Manager “Call” OM Generation Logic.

1.2.1.7 BCP Successful Streams

The BCP Successful Streams OM (“sesmSuccessStreams”) represents the number of media stream setup requests that were successfully processed per BCP. A media stream is considered successfully setup when the BCP establishes a logical connection via a policy rule between the two endpoints at which point the BCP Successful Streams is incremented by one. This OM register is pegged per media stream and not per call as illustrated in Figure 8: Session Manager “Call” OM Generation Logic.

1.2.2 Session Manager Configured BCPs

The following diagram shows the flow for pegging the mediaPortalCount OM Register on the Session Manager indicating the number of configured BCPs for this instance of the Session Manager. This register is only updated when a BCP configuration is either added or removed via the Management Console. If no BCP configurations exist, this register value is set to zero. A Session Manager only counts the BCPs that are associated with it via the “Session Manager(s)” data in the BCP configuration from the Management Console.

Figure 9: Session Server Configured BCPs OM Generation Logic

1.2.3 BCP OMs

Due to the large number of registers already existing in the MPCP OM Group, a new OM Group, named “Ports” has been created. There are four new OM Registers added to the OM Group “Ports” defined in Table 4: OM Group Ports - New OM Registers. Figure 6 shows the new OM Registers in the OM Browser GUI. The pre-existing OM Registers “rtpMpPortUsage” and “connMapEntries” has been moved out of the MPCP OM Group to the new Ports OM Group.

Table 4: OM Group Ports - New OM Registers

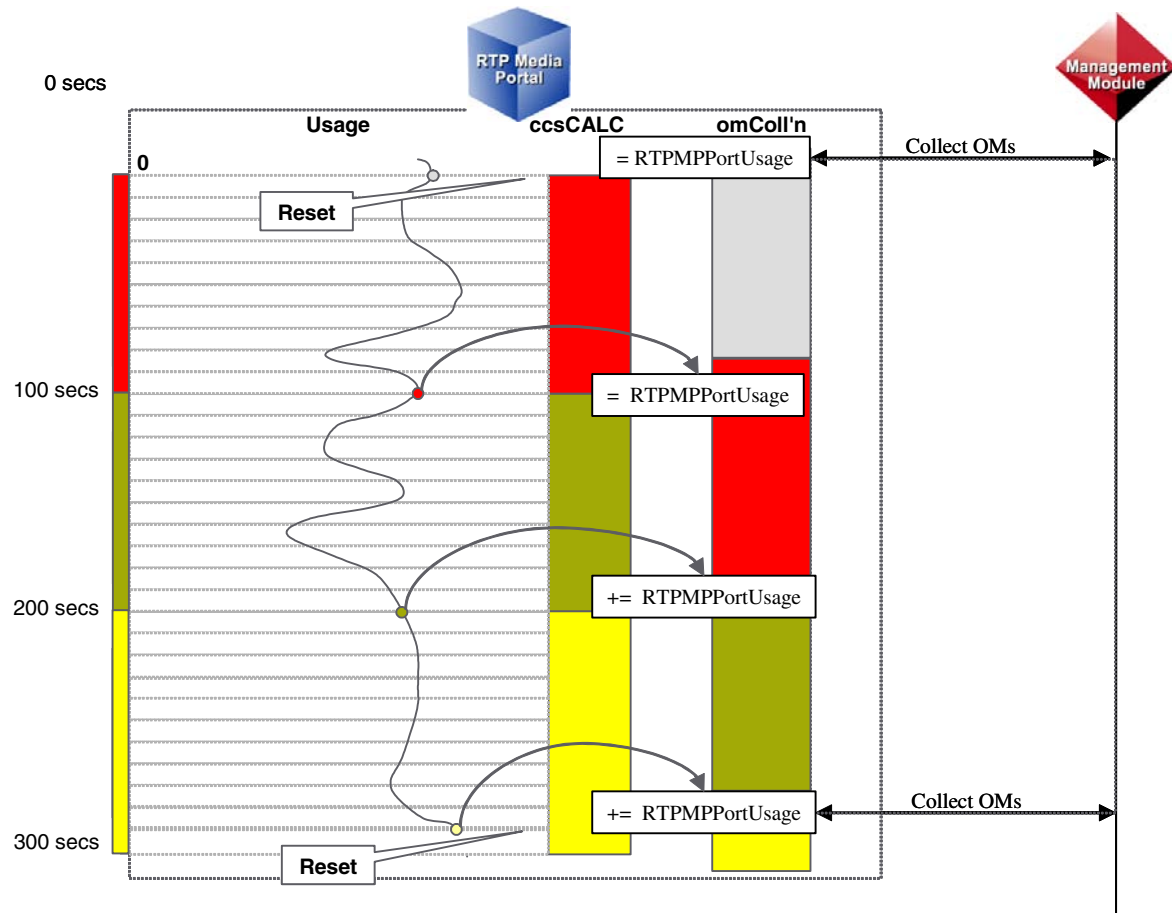
Register Name	Type	Description
sampledRtpMpPortUsage	Usage	Provides the summing of the in use ports every 100 seconds.
portUsageSampleCnt	Counter	The number of 100 second samples taken during this collection interval contributing to the averaged report.
connMapEntriesHWM	Usage	Highest number of simultaneous ports detected to be in use during this collection interval.
connMapEntriesLWM	Usage	Lowest number of simultaneous ports detected to be in use during this collection interval.

Figure 6:Example GUI snapshot of Ports OM Group

OM Row	rtpMpPortUsage	connMapEntriesLWM	connMapEntriesHWM	connMapEntries	portUsageSampleCnt	sampledRtpMpPortUsa...
RTP1	0	0	0	0	7	0

1.2.3.1 BCP Usage OM

The figure below illustrates the new sampledRtpMpPortUsage OM. This OM provides the summing of the in use ports every 100 seconds that gives a view of the CCS (hundred call seconds) of traffic. For example, in a five minute period, the BCP ports will be scanned three times (300 seconds/100 second scan). Each time there is a scan (every 100 seconds), and a port is in use, the count for that port is incremented. So for a five minute period, if a port is in use each time the scan occurs then a 3 is reported in the measurement. This measurement can then be plugged into traffic tables, like Erlang B, to compute the number of ports required for a given blocking probability. The number of 100 second reports sampled during the collection cycle will also be reported.

Figure 7 BCP: New "RTPMPPortUsage" OM

1.2.3.2 Port Usage Sample Count OM

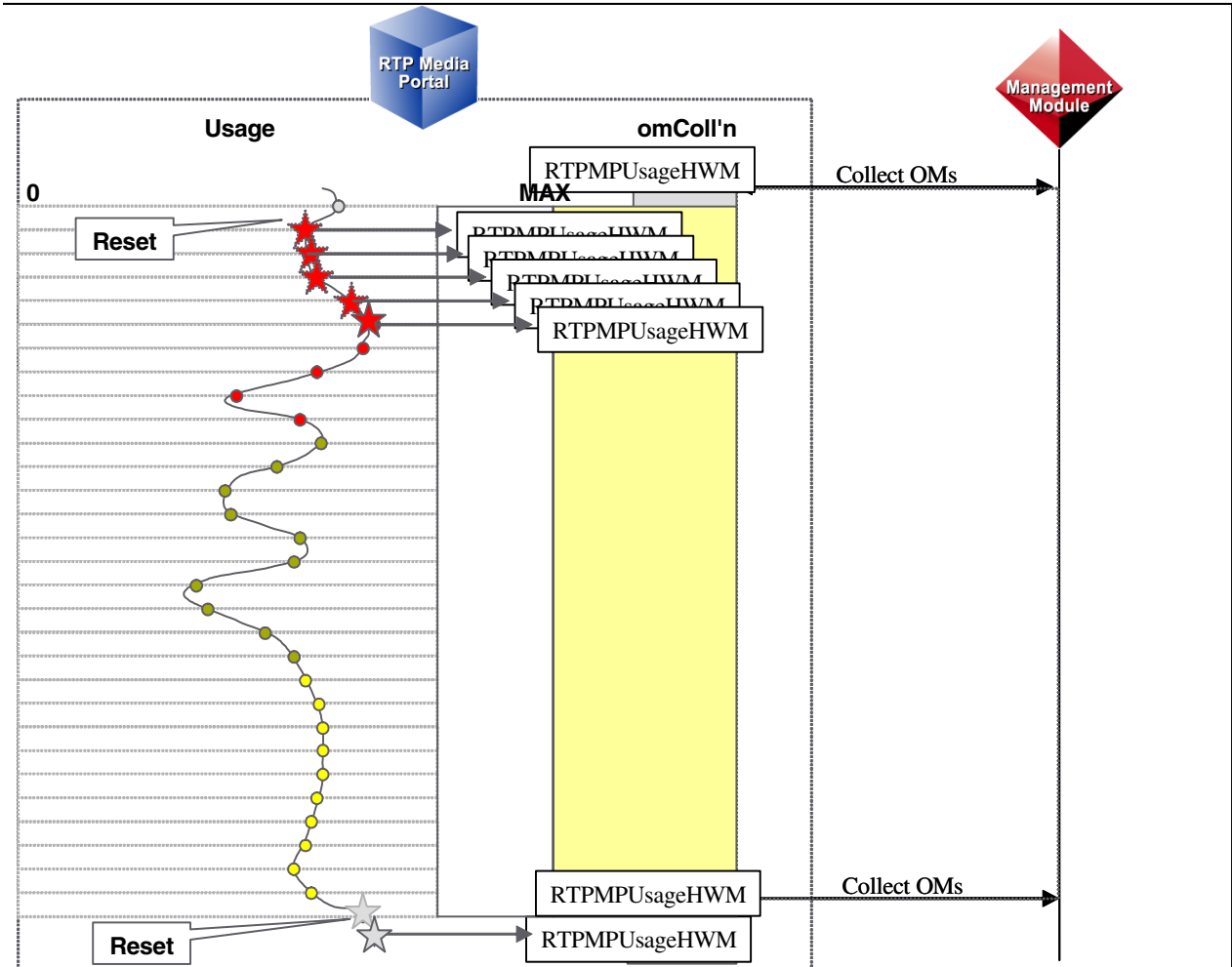
The Port Usage Sample Count OM ("portUsageSampleCnt") represents the number of 100 second port usage samples taken during a collection cycle. For example, for a five minute collection cycle, the value should be 3. This value can be used to determine if the "sampledRtpMpPortUsage" OM Register should be thrown out or not when used with traffic tables. There is the possibility of a Java Garbage Collection delaying a 100 second report.

1.2.3.3 BCP Usage High Water Mark OM

The figure below illustrates the new connMapEntriesHWM OM. This OM provides a high water mark of the ports in use on the BCP for a collection cycle. Each time a port is allocated, the number of ports in use is compared to the current value of the connMapEntriesHWM OM. If the current number of ports in use exceeds the value stored in the OM Register, then the OM

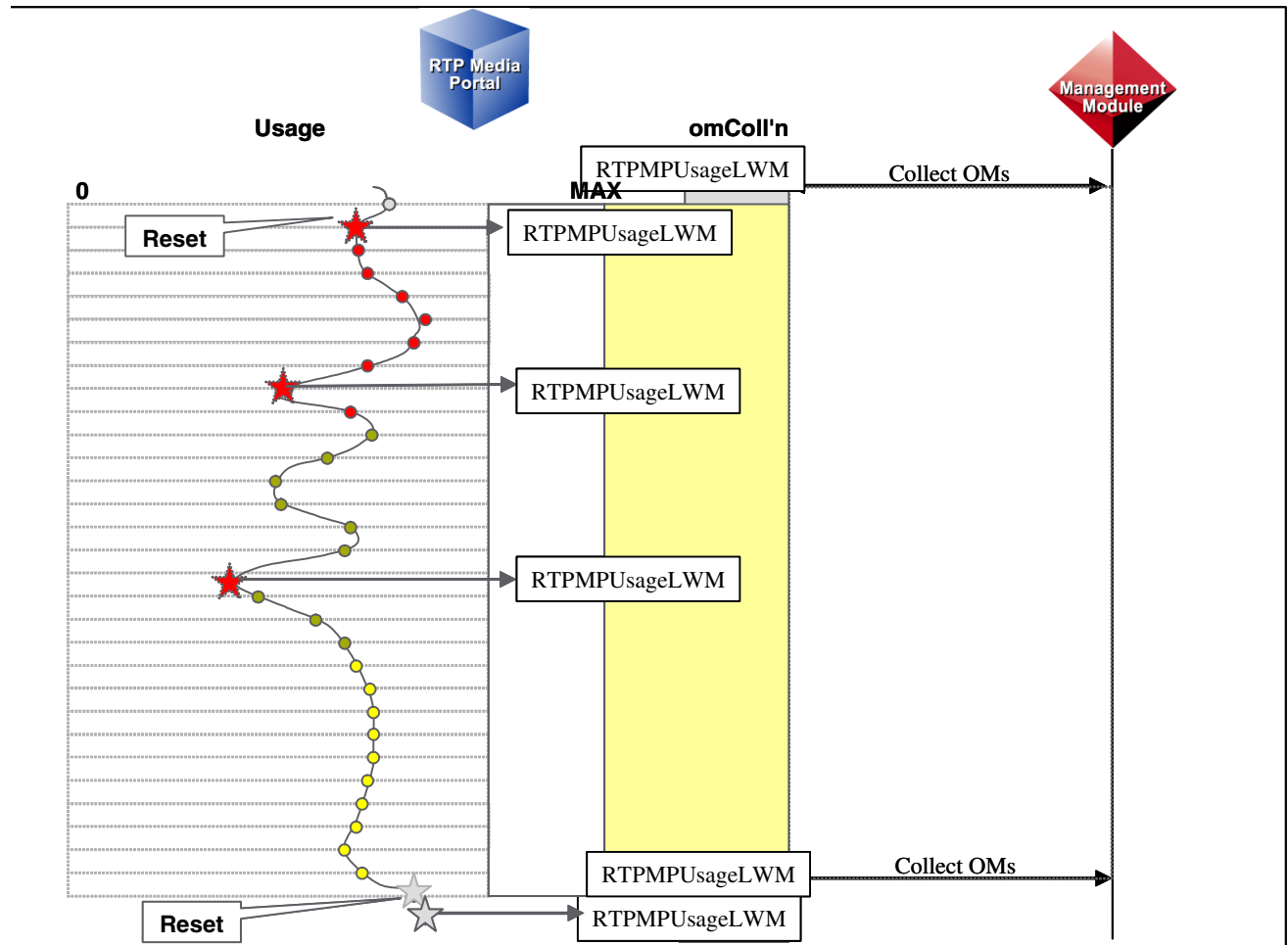
Register's value is set to the current usage value. At the beginning of each collection cycle, the HWM register is reset to the current usage level.

Figure 8: BCP: New "RTPMPUsageHWM" OM



1.2.3.4 BCP Usage Low Water Mark OM

The figure below illustrates the new connMapEntriesLWM OM. This OM provides a low water mark of the ports in use on the BCP for a collection cycle. At the beginning of each collection cycle, the LWM register is reset to the current usage level.

Figure 8: BCP: New "RTPMPUsageLWM" OM

1.3 Hardware Requirements or Dependencies

None

1.4 Software Requirements or Dependencies

None

1.5 Limitations and restrictions

If a BCPs configuration is removed via the Management Console, its operational measurements for the current OTP are lost.

The accuracy of reporting port usage every 100 seconds is at the mercy of the Java Garbage Collector.

1.6 Interactions

This feature will have negligible capacity and real time impact.

1.7 Glossary

Term	Description
Call	A communication context that involves two endpoints that are communicating using one or more forms of media.
Media Port	An entity representing one of the endpoints for a media stream..
Media Stream	A single media channel for conveyance of media (audio, video or data) between endpoints
OTP	Office Transfer Period.
Policy Rule	Refers to the internal connection between two proper connections on the BCP.

Product = MCS

A00012538, A00012537, A00012539--SIP Lines features

Functional Description

1: Applicable Solution(s)

MCS

1.1 Description

This activity, SIP Lines Support - Part 2, consists of 3 features:

- A00012538 - Additional Provisioning for SIP Lines
- A00012537 - SIP Lines - Data Sync Audit
- A00012539 - SIP Lines - Maintenance Enhancements

These features deal with meeting the Configuration and Provisioning requirements on CS2K SS for support of SIP Lines. It provides new OPI and OMI interfaces for configuration and provisioning. In addition new OPI methods are added for audit - which can be used by the clients to ensure that data on MCS is in sync with Data on other systems unknown to MCS.

The responsibility for audit and data correction is that of the client (SESM). The server provides mechanism to retrieve the data that exists on SS and use that for maintaining data consistency.

The requirements fall into the following work areas.

HUNT/MADN Group Provisioning
OPI methods for Data Audit
Version Service
Client Jars
Backward/ Forward compatibility
Number of simultaneous Endpoint postings

1.2 HUNT/ MADN Group Provisioning

The activity “A00009528 - Call Pickup” introduces a concept of grouping users on the Provisioning System. The group provisioning is generic and is associated with a group type. The group type defines what Call Processing Service the group is used for.

This feature requires addition on new group types such as MADN and Hunt Groups. Please refer to the “A00009528 - Call Pickup” FN for details.

The interfaces defined by the Call Pickup feature is leveraged for Group Provisioning. No additional methods are required for the same.

1.3 OPI methods for Data Audit

Several new methods are required to carry out the audit functionality for SIP Lines data on the client (SESM).

SIP Line Data Audit - SIP Line provisioning functionality was introduced as part of A00009043 SIP Lines Provisioning Support feature. Several new methods are required for auditing this data from the client.

The following methods are added to OPI web service.

1) public int getUserCountInSubDomain (String subDomainName) throws ProvisionException

Could be the root domain name. The output is the number of users in the actual domain specified.

2) public int getUserCountInDomain (String domainName) throws ProvisionException

Returns user count in the domain tree starting with the specified domain.

A new web service called “SIPLines” is added and the following methods will be exposed via this service.

1) public String[] getDomainsForVMG (String vmgName) throws ProvisionException

2) public String[] getVMGForDomain (String subDomainName) throws ProvisionException

This takes in the actual subdomain name.

3) public SipLineAuditData[] getSIPLineAuditDataByDomain (String domainName, int start, int stop) throws ProvisionException

Returns the users available in the actual domain specified.

The SIPLineAuditData object contains the following fields:

String endpointId

String vmg

String[] clientType

String userName (user@root domain only. Actual subdomain does not matter).

String dirNum

4) public SipLineAuditData[] getSIPLineAuditDataByDomainByVMG (String domainName, String vmgName, int start, int stop) throws ProvisionException

Returns the users available in the actual domain specified.

5) public String[] getUsersByRegistrationState (String domainName, boolean registered)

Returns the usernames in the actual domain specified.

This method returns the list of usernames in the domain specified that have any contacts registered if registered boolean is set to true.

It returns the list of users that are not registered at all if the registered boolean is set to false.

6) public String[] getUsersByRegistrationState (String domainName, boolean registrationState, String clientType)

Returns the usernames in the actual domain specified.

The client type is the name from the ClientType object that is returned by the getClientTypes() method.

Returns the same list as in the previous method, except that it is also filtered by the client Type. The client type check is done against the provisioned data

and has no bearing to what client actually registered. (No way of knowing that).

Group Data Audit - Refer to the Call Pickup FN for APIs.

1.4 Version Service

A new web service “VersionService” will run on the SM and Prov Mgr.

Interface: VersionService

Method: getLoadVersion() returns Version

Version {

int majorReleaseNum

int minorReleaseNum

int maintenanceReleaseNum

}

This service would be used by OPI and OMI clients to handle versions for maintenance releases. Refer to Backward/ Forward Compatibility section for more details.

1.5 Client Jars

The client jar (built based on the wsdl) for SIPLines web service will be available in the “OPIClient.jar”.

The client jar (built based on the wsdl) for OMI services will be available in “OMIClient.jar”.

These jars will be available as part of the MCS load. The location of these jars for SESM loadbuild is TBD.

1.6 Backward/ Forward Compatibility

There are new OPI and OMI interfaces as part of this feature. Existing interfaces work as is and do not get affected.

OPI and OMI web services support backward compatibility for 1 release. This section describes SESM’s specific requirement for forward compatibility. The details are based on the fact that these features are delivered in a maintenance release for MCS09.

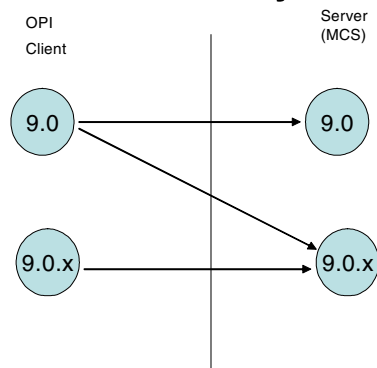
In the SIPLines solution, for provisioning and configuration using OPI and OMI services, MCS is a server and SESM works as a client. Since the client

(SESM) would be upgraded prior to MCS (server), there is a risk that a forward release client talks to the older MCS09 load for the new functionality.

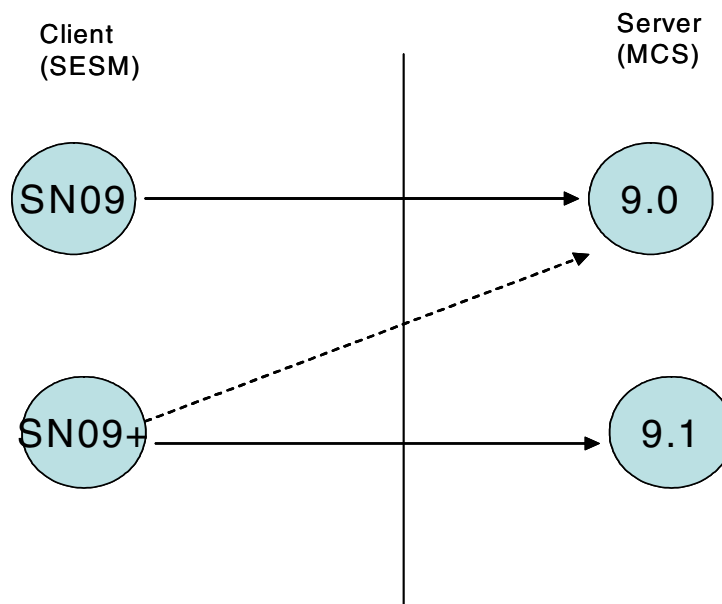
It is the client's job to ensure that appropriate methods are called on the respective servers.

MCS Supported Backward Compatibility for major and minor releases:

Backward Compatibility supported by MCS

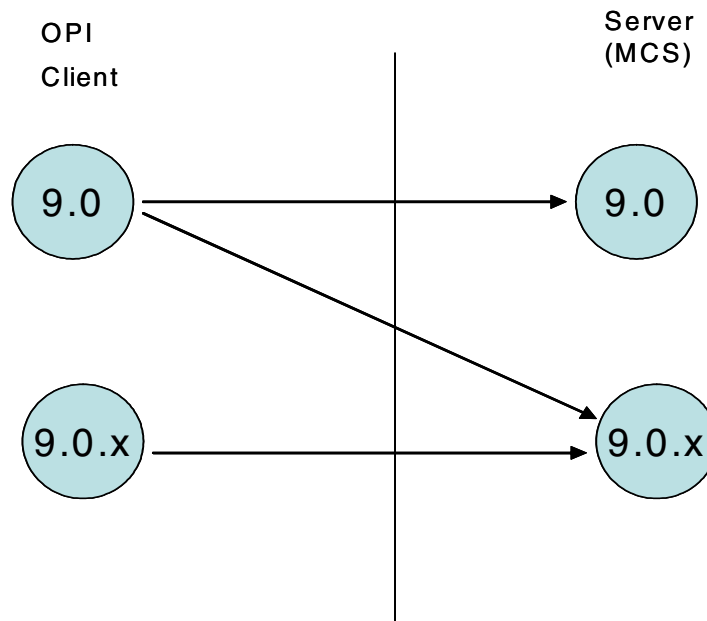


Forward Compatibility for major and minor releases:

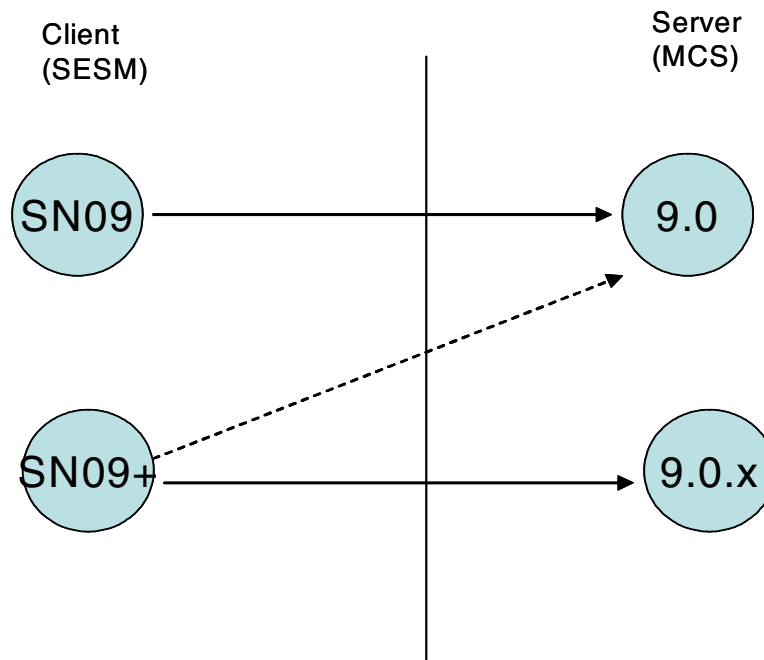


SESM would call the method `getCurrentOPIVersion` and based on the servers version, call the appropriate methods. The server would return the strings “9.0” and “9.1” respectively.

MCS Supported Backward Compatibility for maintenance releases:



Forward Compatibility for maintenance releases:



SESM would use VersionService to determine the MR number. Based on the MR number, SESM determines which methods to call. The server still expects the string “9.0” as the version number for any OPI method calls.

1.7 Number of simultaneous Endpoint posting

In the first release of SIP Lines on MCS (MCS 09) the number of endpoints which could be simultaneously posted from a single OMI login was limited to five. Since live monitoring of endpoint state must be done at the component which is aware of that state, endpoint state information is retrieved from the MCS Session Manager, which is responsible for Call Processing. This number was chosen as one which would not impact traffic rates on the Session Manager. However, it may be possible to increase the number without adversely affecting Call Processing. This feature will provide a mechanism to engineer the number of simultaneous endpoint posting per Session Manager via a configuration parameter against the System Manager.

1.8 Software Requirements or Dependencies

1.9 Limitations and restrictions

Interactions

A00009043 SIP Lines Provisioning Support

A00009528 Call Pickup

1.10 Glossary

Term	Description
Accounting Manager	CS2K MSM component which formats and stores billing records from the Session Manager. Turned off in MSM 9.0
AM	Accounting Manager
CPB	Call Processing Busy. Used to indicate that a SIP Line Subscriber is in the middle of a call.
Endpoint	Refers to a SIP Line Subscriber. In the context of SIP Lines, an endpoint does not actually refer to an IP port pair, but to a subscriber who may have registrations at multiple locations.
GCP	Gateway Control Protocol. Used for communication with GWCs
GWC	Gateway Controller. CS2K component to which Session Managers communicate for call processing

Term	Description
MCS	Multimedia Communication Server
MSM	Multimedia Session Manager
NCAS	Non Call Associated Signalling
NE	Network Element. A managed component of CS2K MSM. Includes Accounting Manager, Session Manager, and System Manager.
OAM	Operations, Accounting, and Management.
OID	Object Identifier. Unique ID used in the CS2K MSM database as a primary key.
OMI	Open Management Interface
Provisioning Manager	CS2K MSM component which manages CS2K MSM provisioning, including subscribers.
Session Manager	CS2K MSM component which manages SIP Sessions and call processing
SIP	Session Initiation Protocol
System Manager	CS2K MSM component which manages CS2K MSM configuration and maintenance.
VMG	Virtual Media Gateway. CS2K view of the CS2K MSM Session Manager.

Product = MCS

A00012622--Platform HW Alarm Reporting

Functional Description

1: Applicable Solution(s)

MCS

1.1 Description

This activity provides the capability for the MCS System Manager to monitor HP CC3310 servers, IBM blade servers, and the IBM BladeCenter chassis for hardware faults.

Alarms are generated for four kinds of hardware faults.

Power Supply. A minor alarm raised when any power supply operates outside of specifications or any voltage sensor reports a value outside of specifications.

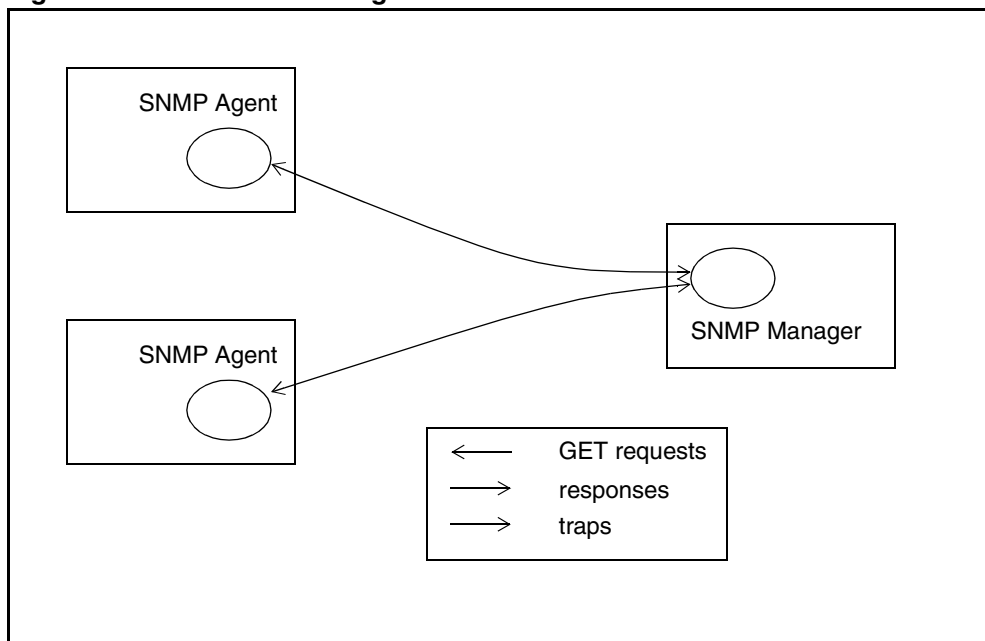
Cooling Device. A minor alarm is raised when any cooling device (fan or blower) operates outside of specifications.

Temperature. A minor alarm is raised when any temperature sensor exceeds its specified threshold.

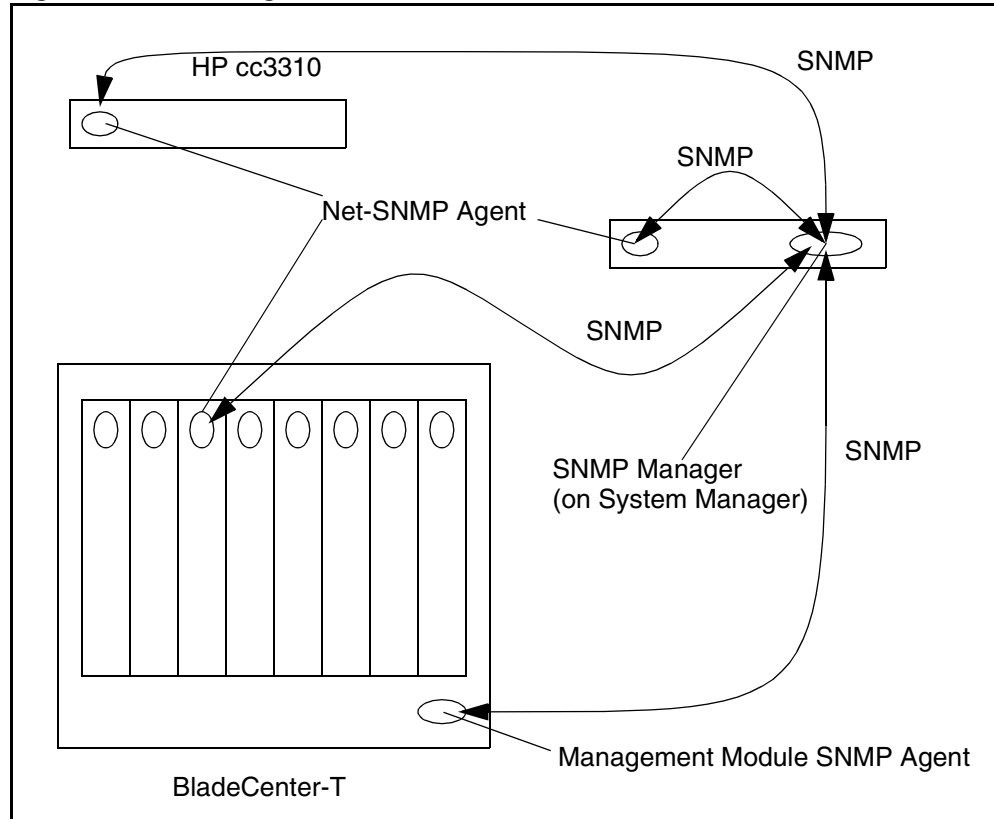
Processor. A minor alarm is raised when a CPU failure is detected (available on the CC3310 only).

The System Manager monitors configured servers using the SNMP protocol. A high level depiction of the use of SNMP is shown in Figure 1. The SNMP protocol is exchanged between an SNMP Agent and an SNMP Manager. An SNMP agent is responsible for reporting the values of variables defined by one or more Management Information Base specification documents. An SNMP manager is an entity capable of requesting MIB variable values from SNMP Agents. An SNMP agent may also be configured to spontaneously report events to an SNMP Manager; these event reports are called *traps*.

Figure 1 Network Monitoring via SNMP



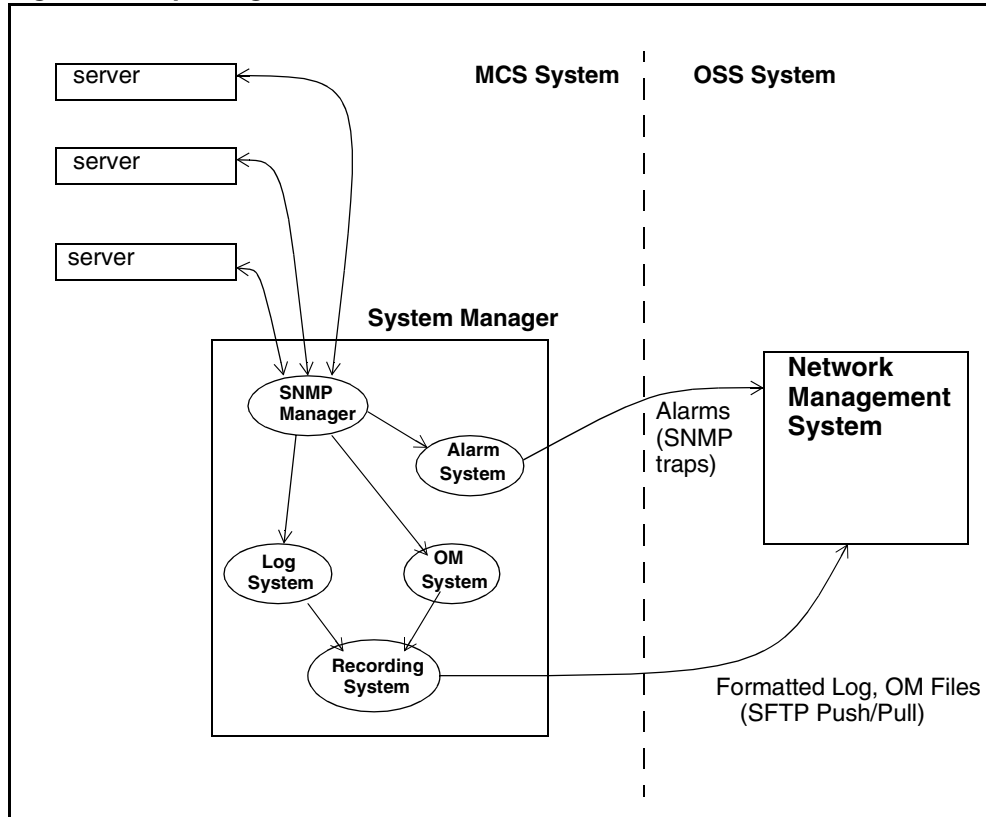
The SNMP protocol provides a mechanism enabling the SNMP Manager to cause an SNMP Agent to alter the values of some MIB variables. This mechanism, referred to as “SNMP Set”, justifies the term “management” in SNMP. This capability is disabled under MCS for security reasons. The MCS therefore *monitors* servers, but does not *manage* them.

Figure 2 Monitoring the CC3310 and BC-T

A more detailed view is shown in Figure 2. The open source Net-SNMP agent is installed on all MCS servers. Resource utilization measurements are available from these agents under the well known MIB-2 standard.

On the HP CC3310, hardware faults are reported through the Net-SNMP agent using the mapbase4 MIB provided by HP.

BladeCenter servers do not report their own hardware faults; this function is provided by an SNMP agent running in the BladeCenter Management Module using the mmblade MIB provided by IBM.

Figure 3 Reporting to the NMS

The general flow of network management information is shown in Figure 3. The System Manager polls SNMP agents running on monitored servers for the raw data from which to generate operational measurements. Some of these measurements are instrumented with configured alarm thresholds. The System Manager raises and clears alarms when these thresholds are crossed. Alarms are reported to registered parties as SNMP traps defined under the Nortel Reliable MIB. A log is generated whenever an alarm is raised or cleared.

Formatted logs and OMs are reported to the recording system on the System Manager which persists them in the local file system. Formatted record files are available via SFTP pull.

1.2 Hardware Requirements or Dependencies

The hardware fault reporting implemented under this activity is available only for the CC3310 and BC-T.

1.3 Software Requirements or Dependencies

The CC3310 implementation relies upon the dmi2snmp process supplied by HP and the SMUX capability of Net-SNMP.

1.4 Limitations and restrictions

Processor failure is reported only for the CC3310.

Monitoring must be started manually (from the System Management Console). Once started, the administrative state of the monitor is maintained over System Manager restarts so that monitoring will automatically resume.

1.5 Interactions

The Oracle SNMP agent must be configured not to use the well-known TCP port 199 for the SMUX protocol.

1.6 Glossary

Term	Description
BC-T	BladeCenter -Telco. A NEBS-compliant version of the IBM BladeCenter.
BIST	Built-In Self Test. A capability for equipment to test itself for defects by comparing self-administered known inputs to expected outputs.
DMI	Desktop Management Interface. A standard for remote computer maintenance.
DMTF	Distributed Management Task Force. The standards organization responsible for defining the Desktop Management Interface.
ITU	International Telecommunication Union
MIB	Management Information Base. A data structure and documentation describing the information accessible via SNMP
MM	Management Module. The BladeCenter management module.
PDU	Protocol Data Unit. A data packet formatted according to some particular protocol.
SMUX	SNMP Multiplexing. A standard for instructing an SNMP agent to delegate processing of a MIB subtree to another process.
SNMP	Simple Network Management Protocol. A standard networking protocol. UDP is unreliable, meaning that data may be lost, duplicated, or received out of order.

2: Fault Management for A00012622

Hardware alarms are reported under new alarm family HWER. Both the server and chassis monitors are capable of raising these alarms. Initially these four new reports are created.

HWER 701 - Cooling Device Malfunction

- For the BC-T platform: HWER 701 is derived from the monitors.blowers table. The alarm is raised when one or more blowers have any state value other than “good”. The alarm severity is Critical if both blowers are faulty, otherwise the severity is Major.
- For the Langley platform: HWER 701 is derived from the tCoolingDevice and tOperationalState tables. The alarm is raised when one or more cooling devices have an operational state not equal to vEnabled. The alarm severity is Critical if any of the faulty cooling devices are unspared, otherwise the severity is Major.

HWER 702 - Power Supply Malfunction

- For the BC-T platform: HWER 702 is derived from the powerModuleHealthTable table. The alarm is raised when one or more power modules have a state not equal to “good”. The alarm severity is Critical if any of the faulty power modules are unspared, otherwise the severity is Major.
- For the Langley platform: HWER 702 is derived from the tPowerSupply and tOperationalState tables. The alarm is raised when one or more power supplies have an operational state not equal to vEnabled. The alarm severity is Critical if any of the faulty power supplies are unspared, otherwise the severity is Major.

HWER 703 - Temperature Threshold Exceeded

- For the BC-T platform: HWER 703 is derived from the bladeTemperaturesTable and bladeTemperatureThresholdsTable tables. The alarm is raised when one or more bladeSensorNTemp probes report a value greater than the corresponding warning threshold. The sensor value table in the report text consists an inequality (“actual > expected” and the sensor name for each sensor out of spec. The alarm severity is Major.
- For the Langley platform: HWER 703 is derived from the tTemperatureProbe table. The alarm is raised when one or more temperature probes report that a55TemperatureStatus is any value other than vOk. The sensor value table in the report text consists of the a55TemperatureStatus and the a55TemperatureProbeDescription variables for each sensor out of spec. The alarm severity is Major

HWER 704 - Processor Malfunction

- For the BC-T platform: HWER 704 is not reported for BC-T.

- For the Langley platform: HWER 704 is derived from the tProcessor and tOperationalState tables. The alarm is raised when one or more processors have an operational state not equal to vEnabled. The alarm severity is Major.

2.1 Alarm templates

The template for HWER 701 appears in Table 1. The device state table consists of two columns containing the device name and the device state as reported through the relevant MIB. The severity is Major if the malfunction results in loss of redundancy, Critical if it results in total loss of cooling.

Table 1: HWER 701 Report Format

Property Name	Property Value
Report Number	HWER 701
Description Text	Cooling Device Malfunction <device-state-table>
Clear Condition	All cooling devices are functioning normally.
Corrective Action	Replace defective cooling devices.

The template for HWER 702 appears in Table 2. The device state table consists of two columns containing the device name and device state as reported through the relevant MIB. The severity is Major if the malfunction results in loss of redundancy, Critical if it results in loss of power.

Table 2: HWER 702 Report Format

Property Name	Property Value
Report Number	HWER 702
Description Text	Power Supply Malfunction <device-state-table>
Clear Condition	All power supplies are functioning normally.
Corrective Action	Replace defective power supplies.

The template for HWER 703 appears in Table 3. The sensor value table consists of two columns containing the problem text and description of each sensor for which the reported value exceeds the threshold. Sensors reporting normal values are not shown.

Table 3: HWER 703 Report Format

Property Name	Property Value
Report Number	HWER 703
Description Text	Temperature Threshold Exceeded <sensor-value-table>
Clear Condition	All temperature sensors report normal values.
Corrective Action	Restore effective cooling for this equipment.

The template for HWER 704 appears in Table 4. The device state table consists of two columns containing the device name and device state as reported through the relevant MIB. The severity is Critical.

Table 4: HWER 704 Report Format

Property Name	Property Value
Report Number	HWER 704
Description Text	Processor Malfunction <device-state-table>
Clear Condition	All processors are functioning normally.
Corrective Action	Replace defective processors.

Product = MCS

A00013063 -- PacketCable Multimedia for MCS and Carrier Grade

Functional Description

1: Applicable Solution(s)

IAC

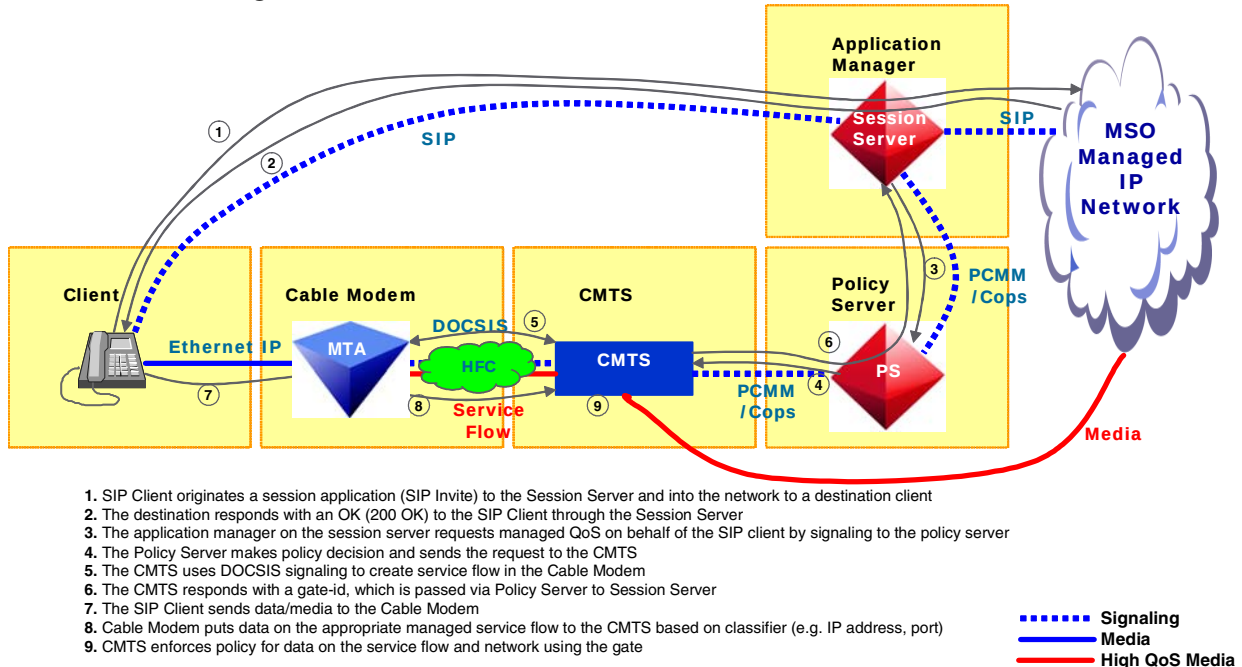
1.1 Description

1.1.1 Functional Overview

PacketCable Multimedia is an architecture developed by CableLabs to enable MultiService Operating Companies to deliver Quality of Service enabled multimedia services over DOCSIS networks. PacketCable Multimedia extends the Dynamic Quality of Service architecture developed as part of PacketCable 1.X to allow Application Managers in the MSO network to request and obtain Quality of Service treatment for multimedia traffic flows on behalf of an end user.

The PCMM signaling implementation is compliant with PacketCable specification PKT-SP-MM-I02-040930.

The following diagram illustrates a high level call flow for a PacketCable Multimedia (PCMM) SIP call.

Figure 1 PCMM SIP Call Flow

Activity A000011740 provided the PacketCable Multimedia (PCMM) service for the CS2K and can be referred to for the provisioning and activation of PCMM. This activity enables the use of PCMM in an MCS5200 environment. It also provides the following enhancements which apply to both the MCS and CS2K implementations except where otherwise noted:

Emergency Support - Raises the priority of the PCMM messages when a SIP call is made to an emergency number. Not supported for CS2K configuration.

Video Codec Flowspec Mapping - Allows the setting of the RSVP values for video codecs in order to communicate the bandwidth requirements for an instance of a given video session from the AM to the PS and CMTS. Audio codecs always use the values defined in PacketCable PKT-SP-CODEC specification.

Failover Support For PCMM - If the active Session Manager fails and the standby Session Manager takes over, then stable PCMM service flows (gates) are retained.

1.1.2 Emergency Support

The priority contained in the PCMM Gate-Set message is raised to the highest level when a SIP call is made to an emergency number. The Policy Server and the CMTS may use the priority value to implement priority based admission and to defend the resulting flow from being preempted. Provisioning of

emergency number is accomplished using the Provisioning Client's Emergency Number and Emergency Alias Lists.

1.1.3 Failover Support For PCMM

If the AM's active Session Manager fails, and the standby Session Manager takes over, then the newly active Session Manager can communicate with the Policy Server. Also, the newly active Session Manager has knowledge of all stable PCMM service flows (gates) so it can delete them when the session ends. A stable PCMM service flow is defined as a session that was answered and the AM has received acknowledgement from the Policy Server that the PCMM service flow request was successful.

1.1.4 Video Codec FlowSpec Mapping

The following sections describe how to configure the FlowSpec video codec values which will be delivered as part of this activity. Please refer to activity A000011740 to understand how to configure the Policy Server and assign the PCMM feature to subscribers. These steps must be taken first in order to make use of the FlowSpec data described in the following sections.

1.1.4.1 Configuring FlowSpec Data

FlowSpec RSVP values are used to determine how much bandwidth is provided for video calls. Audio codecs always use the values defined in PacketCable PKT-SP-CODEC specification.

The customer is allowed to adjust video quality through modifications of the FlowSpec RSVP values for a specific codec and frame rate. A customer may configure up to 32 codec name / frame rate combinations.

Configuration of these codec values is system wide and will be used in determining video bandwidth for PCMM calls. The subscribers service package must have the Video option selected before an attempt to use the video codec FlowSpec data described in this section is made.

If a video codec is supplied by a SIP client during call setup and it has not been configured as part of PCMM Codec configuration, then the call will receive Best Effort service (no PCMM Service Flow) and will not render the best video quality.

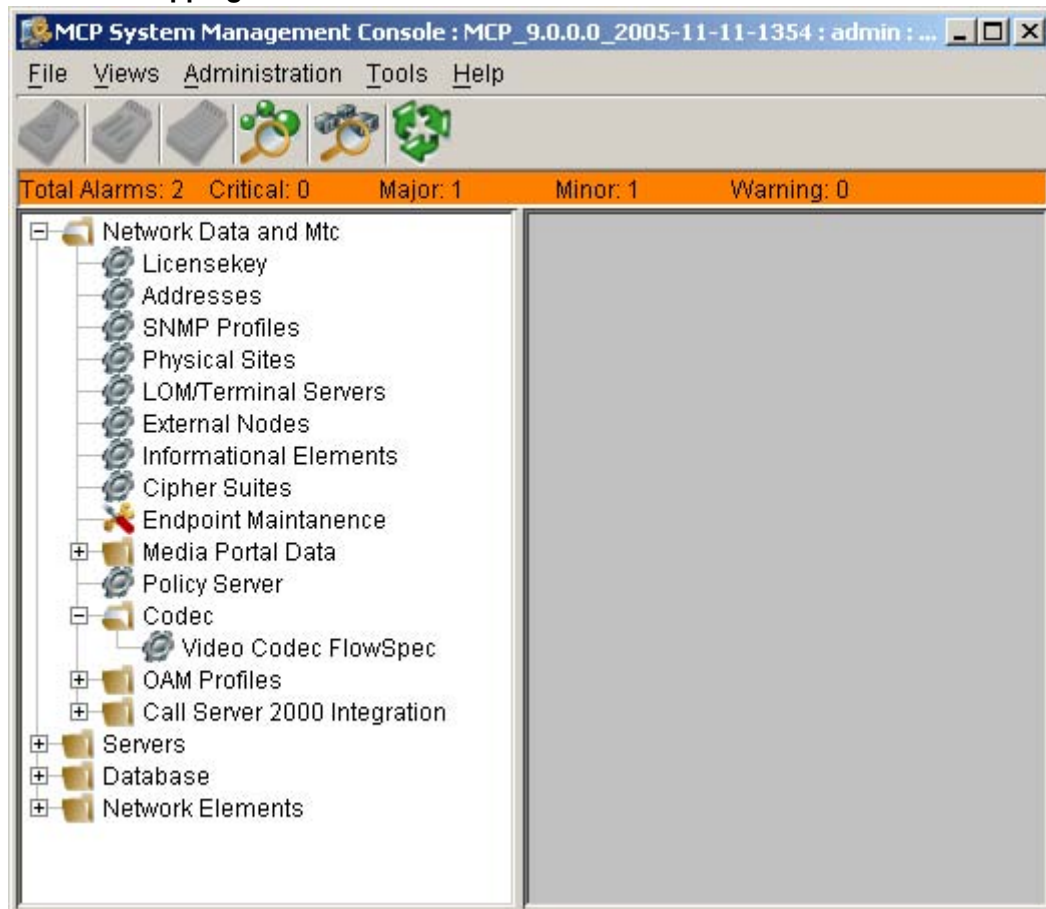
Two supported video codecs are pre-provisioned in the system and they contain default FlowSpec RSVP values as follows:

Frame Rate | Bucket Rate | Bucket Size | Peak | Min | Max | Rate | Slack

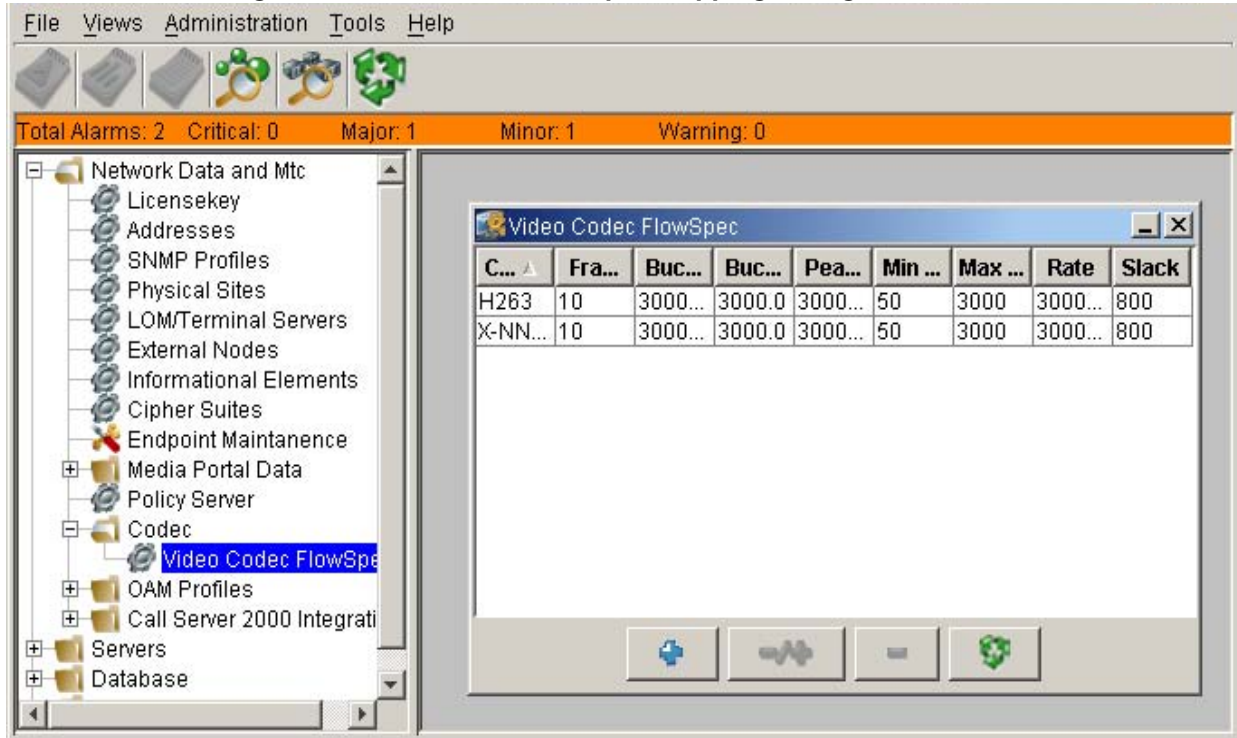
10	30000	3000	30000	50	3000	30000	800

To configure the video codec FlowSpec mappings from the MCP System Management Console expand the “Network Data and Mtc” folder and expand the “Codec” folder:

Figure 2 MCP System Management Console for Video Codec FlowSpec Mapping



- Select the “Video Codec FlowSpec Mapping” item and the following screen appears:

Figure 3 Video Codec FlowSpec Mapping Dialogue

- Select the '+' icon and a new window appears. Enter the following fields:

Figure 4 Add Video Codec

Add Video Codec FlowSpec

Video Codec FlowSpec

Codec :

Frame Rate :

Bucket Rate :

Bucket Size :

Peak Data Rate :

Min Policed Unit :

Max Packet Size :

Rate :

Slack :

- Codec:** Customer defined codec name up to 16 characters

- b. **Frame Rate:** Video frame rate. The default is 10
- c. **Bucket Rate:** Token bucket rate that the traffic conforms to in bytes per second. The default is 30000
- d. **Bucket Size:** Size of each token in bytes. The default is 3000
- e. **Peak:** Peak rate at which the source will send in bytes per second. The default is 30000
- f. **Min Unit:** Minimum policed unit, usually the smallest packet size that the source will generate, in bytes. The default is 50
- g. **Max Units:** Maximum packet size generated by the source in bytes. The default is 3000
- h. **Reserved Rate:** Reserved rate in bytes per second. The default is 30000
- i. **Slack:** Slack term in microseconds. The default is 800

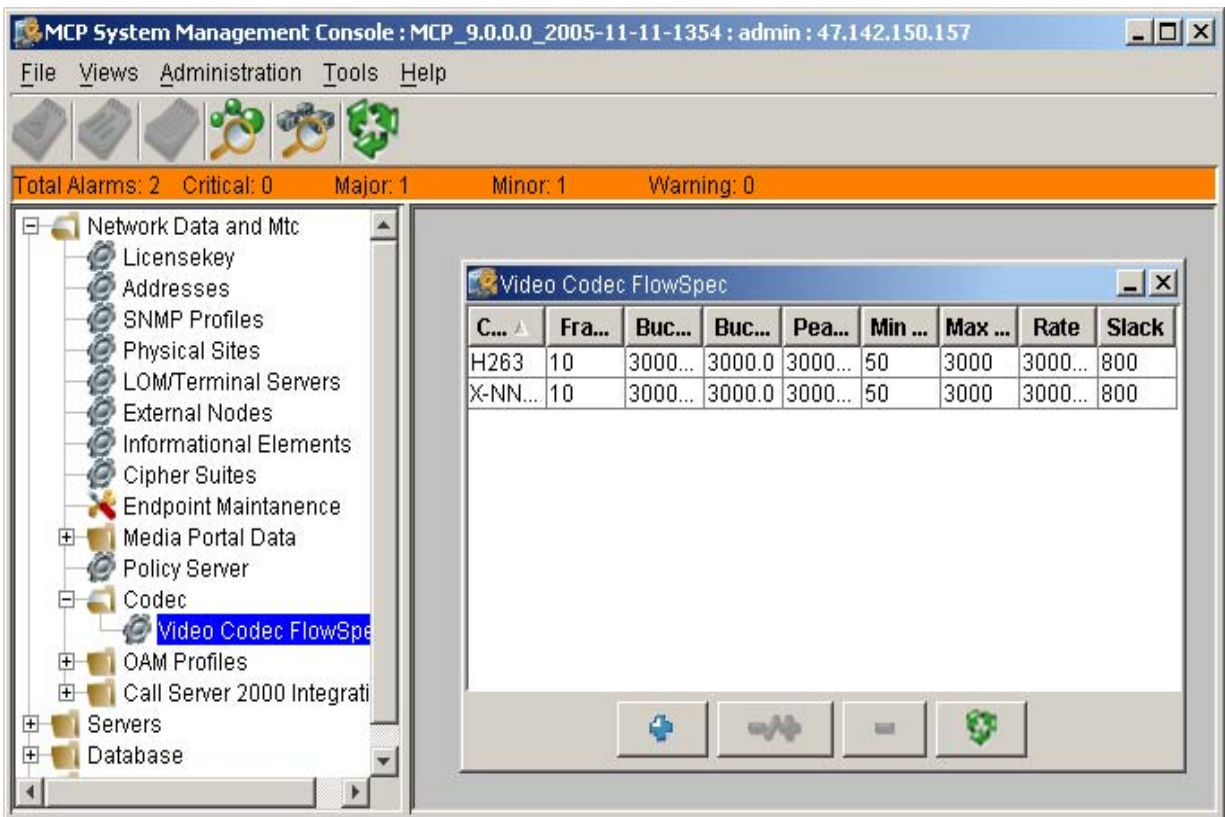
Once these fields are entered, click “Apply” and the video codec will be configured.

1.1.4.2 Deleting a PCMM Codec

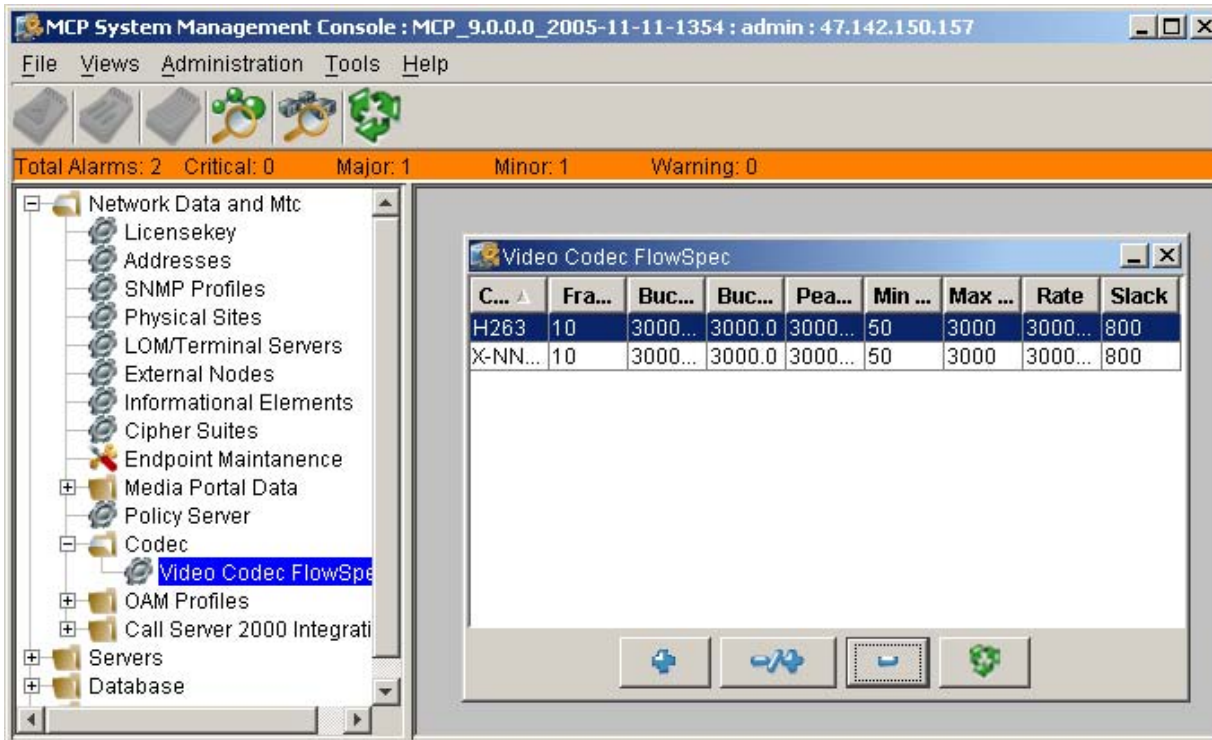
A video codec maybe deleted using the MCS System Management Console.

In order to delete a PCMM codec entry:

- Expand the “Network Data and Mtc” and “Codec” folders.

Figure 5 System Management for Video Codec FlowSpec Mapping

- Select the “Video Code FlowSpec Mapping” item and a new screen will appear as follows:

Figure 6 Video Codec FlowSpec Mapping Selected

- Highlight the PCMM codec to be deleted and click the “-” (minus) button
- A confirmation screen will appear- select ‘yes’ to delete, ‘no’ to cancel.

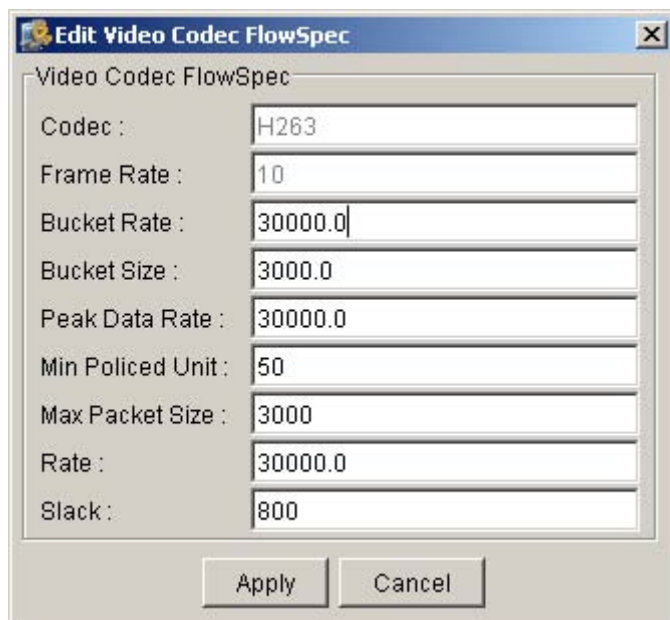
1.1.4.3 Modifying a PCMM Codec

A PCMM codec maybe modified using the MCS System Management Console.

Modifications of any field will take affect only on new calls which are established after the data is modified. Existing calls will retain their current video quality.-i.e video quality will not be renegotiated on active calls.

In order to modify a PCMM codec entry:

- Expand the “Network Data and Mtc” and “Codecs” items
- Select the “Video Code FlowSpec Mapping” item and the same screen as mentioned in the “Deleting a PCMM Codec” will appear.
- Highlight the PCMM codec to be modified and click the “+/-” button.
- The following screen will appear: Note that the codec name and framerate values cannot be modified. If a different codec/ framerate is desired you must add a new codec/framerate combination. All other fields can be modified.



Video Codec FlowSpec	
Codec :	H263
Frame Rate :	10
Bucket Rate :	30000.0
Bucket Size :	3000.0
Peak Data Rate :	30000.0
Min Policed Unit :	50
Max Packet Size :	3000
Rate :	30000.0
Slack :	800

Apply Cancel

- Modify any field which are allowed and depress apply. The new values will be modified stored.

1.2 Hardware Requirements or Dependencies

To deploy the PC-MM feature, the MSO needs to have PC-MM compliant cable network elements that are not supplied by Nortel. These third-party elements include cable modems, CMTSs, and a policy server.

1.3 Software Requirements or Dependencies

The policy server and CMTSs in the cable network must support PacketCable Multimedia specification PKT-SP-MM-I02-040930. The cable modems must support DOCSIS 1.1 or greater.

1.4 Limitations and restrictions

Failover for PCMM does not support the processing of unsolicited messages received from the Policy Server after the switch of activity. Therefore, the following scenario could occur:

1. A SIP session is answered and it has a PCMM service flow.
2. The active Session Manager fails and the standby Session Manager takes over.
3. Something happens on the network causing the CMTS to detect and report a loss of packets (through the Policy Server) to the Session Manager for the SIP session.

4. The call will lose its PCMM service flow and resort to Best Effort quality of service.

1.5 Interactions

The PCMM feature sets up managed quality of service for SIP calls originating from or terminating to the cable network. PCMM operates on a half-call basis. This means that PCMM signaling and managed QoS happen only for the half of the call that is in the cable network. For example, an on-net to off-net call will only do PCMM signaling for the originating line half of the call. The trunk half of the call is not touched by PCMM.

1.5.1 Basic Call

The PCMM feature attempts to set up managed quality of service when the SDP information is known for both of the media endpoints (originating and terminating). Therefore, application of the PC-MM protocol procedures will not cause call failures, but it is possible that under some network error conditions a call might receive “best effort” QoS rather than managed QoS.

1.6 Glossary

Term	Definition
AM	Application Manager - logical network element defined in the PacketCable Multimedia architecture responsible for making bandwidth requests on behalf of a cable agnostic client.
Best effort	The default service flow. The characteristics for this service flow are defined in the cable modem config file. If a packet does not match any classifier then it is assigned to the best effort service flow.
CableLabs	A standards body that writes interface specifications and defines functional behavior for cable network elements.
Classifier	The set of parameters by which a media packet is judged to determine which service flow the packet belongs on.
Client	A SIP client
CM	Cable Modem - a cable network device that provides access to the cable network from an ethernet IP network.
CM	Call Manager - an MCS architecture component responsible for managing call-halves.
CMTS	Cable Modem Termination System - gateway between the cable HF/C network and the ethernet IP network. The CMTS receives the PCMM messages and communicates with the cable modem via DOCSIS to set up managed service flows.
COPS	Common Open Policy Service - a protocol defined in RFC 2748 that sets up a master/slave relationship between network elements for policy decisions. The PCMM protocol is an extension of COPS.
CS2M	CS2000 Management Tools - the CS2K GWC provisioning GUI

Term	Definition
DOCSIS	Data Over Cable System Interface Specification - the protocol used between cable modems and their CMTS to set up service flows and classifiers.
DIFFSERV	Differentiated Services - an IP packet marking scheme that allows IP packets to be treated differently in the network
DSCP	DIFFSERV Code Point - the bit pattern used for DIFFSERV
GETS	Government Emergency Telephone Service - a telephony service that gives higher priority to some callers so that government services can function in the presence of extremely high call loads
HF/C	Hybrid-Fiber/Coax
KRS	Key Registration System
NAT	Network Address Translator - a device that translates between public network addresses and private network addresses.
PacketCable	A subdivision of CableLabs that focuses on standards for VoIP over cable and multimedia over cable.
PC	Personal Computer (in this case)
PCMM	PacketCable Multimedia - an architecture and protocol for managing cable network bandwidth on behalf of cable agnostic clients.
PDP	Policy Decision Point - the COPS network element responsible for formulating network policy. The AM is a PDP. The PS is a PEP w.r.t. the AM and a PDP w.r.t. the CMTS.
PEP	Policy Enforcement Point - the COPS network element responsible for enforcing policies created by the PDP. The CMTS is a PEP. The PS is a PEP w.r.t. the AM and a PDP w.r.t. the CMTS.
Policy	A policy in the context of PCMM defines the access to and level of managed QoS available to a PCMM subscriber.
PS	Policy Server - network element defined in the PacketCable Multimedia architecture responsible for receiving PCMM signaling from an AM and forwarding it to the correct CMTS.
QoS	Quality of Service - the set of network characteristics that determine how a media packet is treated
SA	IPSec or IKE Secure Association
Service Flow	A managed QoS pipeline through the cable HF/C network defined by the quality of service given to the packets that transit the service flow.
SIP	Session Initiation Protocol - a VoIP signaling protocol
Socket	The IP address and port number used to communicate over an IP network to a particular service.
SS-L	Session Server Lines - a name for the MCS application server when used with CS2000

Term	Definition
TOS	Type Of Service - a set of bits in the IP header that can be used to mark IP packets for different treatment in the network. Some of the TOS bits are used for DSCP.

Product = MG 9000

A00007814--REX testing for MG9000 from Element Manager ***Functional Description***

1: Applicable Solution(s)

UA-AAL1, UA-IP

1.1 Description

Routine Exercise (REX) of intelligent card pairs is being introduced in SN09 release to perform the diagnostics of the inactive card. During REX, the inactive card of a card pair will be diagnosed. Followed by the inactive card, REX is executed on the active card, after a SWACT is initiated on the active card which now becomes inactive.

The need for a REX test stems from the fact that the inactive card (standby card) may be prone to latent faults, as it does not get exercised on a regular basis. Exercising it in a way that an active side operates during normal operation will provide a means to detect dormant failures. Moreover, the impact of incorrect or failed operation is in itself a means of detecting problems. Thus REX tests improve fault coverage of hardware and software, repair can take place during off-peak hours and the system re-instated into service before peak hour begins.

User will be able to input the schedule for REX on a particular NE. Intelligent card pairs considered for REX on MG9000 are SCO/SCI/SCG (DCC), ITP and ITX cards. User will be able to see the progress of the REX on a particular NE from the REX GUI of Subnet View and on NE Desktop View. Success/failure of the operations in REX for a given NE are also logged.

1.1.1 REX Scheduling

REX NE option is provided in the configuration menu of Desktop view. On clicking the REX NE menu, REX GUI will be opened. User will be able to initiate REX on NE(s) using REX GUI. REX GUI contains options to Add, Remove, Suspend, Resume an NE for REX. User can perform the following from the REX GUI:

- 1** REX on an NE can be scheduled for a particular day, time from the GUI or can be executed immediately. Scheduling of REX is similar to that of Audit.
- 2** An option is provided to remove an NE for which REX is already scheduled. On removing the NE, if the REX is in progress, it would be suspended.
- 3** User can suspend the already scheduled REX.

- 4 User can resume the suspended REX.
- 5 User will be able to view the results/progress details of REX executed on the selected NE.

1.1.2 REX Results

During REX, inactive card of the intelligent card Diagnosed. The results of all these operations are logged and progress of REX is shown on the progress details field of the REX GUI. Progress details are also shown on the REX tab of NE Desktop View. Success/Failure of SWACT and diagnostics are displayed to the user as part of the progress details and also in the Logs.

1.2 Hardware Requirements or Dependencies

None

1.3 Software Requirements or Dependencies

None

1.4 Limitations and restrictions

- 1 REX will not be supported on ABI cards. ABI cards behave as master-slave and hence SWACT is not possible on ABI cards.
- 2 REX will not be supported on DS1 cards as they adhere to 1:N protection scheme.
- 3 Any swact on ITPs should be followed by a wait period of at least 1 minute prior to locking the newly inactive card. Until ready for service calculations are handled on the inactive, the possibility remains that an ITP newly swacted to, may give up activity, shortly after the swact (as it discovers its not truly capable of providing service)
- 4 A critical datasync fault on the inactive card must not block Rex from locking/diagnosing/unlocking the inactive. A corollary to this restriction is that the card pairs exhibiting CPU overload alarms (or cards subtending a card with CPU overload alarms, like an ITP below an overloaded Supercore) must not be REX tested. A log should be output if a card pair is skipped due to CPU overload.

1.5 Interactions

None

1.6 Glossary

Term	Description
REX	Routine EXercise

Term	Description
MG9000	Media Gateway 9000
EM	Element Manager
SCG	SuperCore GigE
GigE	Gigabit Ethernet
SWACT	SWitch ACTivity
DCC	Data Control Card
SCO	SuperCore OC3
SCI	SuperCore IMA
ITP	Internet Telephony Processor
ITX	Internet Telephony Extender
CPU	Central Processing Unit

2: Fault Management for A00007814

2.1 Fault management strategy

There are no faults generated by this feature.

2.2 Fault management tools and utilities

This feature generates the customer logs.

2.3 Logs

2.3.1 Log Title/Log ID: REX 600

2.3.1.1 Formats

REX Start/Completed log:

MSH10_I06BR REX600 JUN5 14:12:56 2164 INFO MG9K Card
REX LOG NOTIFICATION
NE Number: 2 NE Name: HS9K
Card.frame0.shelf3.slot15.ITX REX completed on:
Time: Thu Jun 05 14:12:56 EDT 2003

2.3.1.2 Explanation

Description: Log report REX600 indicates the start or completion of REX on a card/card-pair. The cards under consideration are ITP, ITX and DCC.

2.3.1.3 Field Descriptions

This log report has no selected fields.

2.3.1.4 Action

None

2.3.1.5 Associated Operational Measurements or Performance Measurements

None

2.3.1.6 Additional information

None

2.3.2 Log Title/Log ID: REX 601**2.3.2.1 Formats****REX Success/Failure log:**

MSH10_I06BR REX601 JUN5 14:12:56 2164 INFO MG9K Card
REX LOG NOTIFICATION
NE Number: 2 NE Name: HS9K
Card.frame0.shelf3.slot15.ITX REX successful on:
Time: Thu Jun 05 14:12:56 EDT 2003

2.3.2.2 Explanation

Description: Log report REX601 indicates the success or failure of REX on a card/card-pair. The cards under consideration are ITP, ITX and DCC.

2.3.2.3 Field Descriptions

This log report has no selected fields.

2.3.2.4 Action

None

2.3.2.5 Associated Operational Measurements or Performance Measurements

None

2.3.2.6 Additional information

REX601 is generated for the failure conditions also. When the diagnostics of the card fails, REX is failed for the card under consideration.

2.3.3 Log Title/Log ID: REX 602**2.3.3.1 Formats****REX Skipped log:**

MSH10_I06BR REX602 JUN5 14:12:56 2164 INFO MG9K Card
REX LOG NOTIFICATION

NE Number: 2 NE Name: HS9K
Card.frame0.shelf3.slot15.ITX REX skipped on:
Time: Thu Jun 05 14:12:56 EDT 2003

2.3.3.2 Explanation

Description: Log report REX602 indicates that the REX for the card/card-pair under consideration has been skipped. The card types considered are ITP, ITX and DCC.

2.3.3.3 Field Descriptions

This log report has no selected fields.

2.3.3.4 Action

None

2.3.3.5 Associated Operational Measurements or Performance Measurements

None

2.3.3.6 Additional information

Various reasons for which REX is skipped on a card/card-pair are:

1. Unable to SWACT the card.
2. In the case of a card-pair if the REX on inactive card fails, REX for the card-pair is skipped.
3. If the duration for REX specified by the user exceeds, REX for the card/card-pair is skipped.

2.4 Alarms

NA

3: Configuration Management for A00007814

3.1 Hardware and Software Requirements

None.

3.2 Initial Configuration

NA

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

NA

3.4 Upgrade Considerations

NA

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

3.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
REX_SCHEDULE	NEW	OLD

3.5.2 Table/MIB/Remote Database Schema information

3.5.2.1 Name: REX_SCHEDULE

Routine EXercise Schedule database table.

3.5.2.1.1 Functional description

Table REX_SCHEDULE lists the schedule assignments for every NE that has to undergo REX.

REX_SCHEDULE table is used to store the schedule information for the NEs that have to execute REX. This table is updated when the user inputs a schedule to execute REX on an NE, removes the REX for an NE, after the execution of REX on an NE.

3.5.2.1.2 Usage sequence and implications (CM Only)

None.

3.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
REX_SCHEDULE	0	Number of NEs present in a subnet	TBD

3.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for REX_SCHEDULE

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SUBNETID	NEW	N/A	1	

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
NEID	NEW	N/A	1 to 999	
NENAME	NEW	N/A	1 to 32 characters	
STARTTIME	NEW	N/A	00:00 to 23:59	
PERIOD	NEW	N/A	00:00 to 23:59	
DURATION	NEW	N/A	00:00 to 23:59	
WEEKDAYS	NEW	N/A	It can be either of: 1. Sunday 2. Monday 3. Tuesday 4. Wednesday 5. Thursday 6. Friday 7. Saturday	
MODE	NEW	N/A	1. Without SWACT 2. With SWACT	
CARD_TYPE	NEW	N/A	It can be a combination of the below given cards: 1. DCC 2. ITP 3. ITX	This field contains the selection of card types on which REX will be executed.

3.5.2.1.5 Datafill example

None.

3.5.2.1.6 Table release history update

A new table REX_SCHEDULE is introduced in SN09 to store the REX schedule information of all the NEs under a given subnet.

3.5.2.1.7 Supplementary information

None.

3.5.2.1.8 Translation verification and other tools

None.

3.6 Service Orders (SO) (CM & SESM)

NA

3.7 Software optionality control (SOC)

NA

3.8 Element Management

MG9000 Element manager will be used to execute REX on a given NE.

The EM user will be able to schedule REX and view the progress details of REX on a given NE. REX GUI can be launched from the configuration menu of Subnet view. User will be able to monitor the progress details of REX on the REX GUI and in NE Specific Desktop View.

REX views are similar to that of audit in MG9000 EM.

3.8.1 New/modified GUIs

Table 4 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
REX NE View	NEW
NE Specific Desktop View	CHANGED

3.8.2 GUI information**3.8.2.1 GUI name: REX NE View****3.8.2.1.1 Functional description**

REX NE View: This new GUI is introduced under the submenu option MG9KEM NE Specific Desktop view ->Configuration. This GUI allows the user to schedule REX and also view the progress details on the selected NE.

User is allowed to “Add” an NE to be REXed. During “Add” of NE for REX, user inputs the schedule for an NE, by checking the day of the week, hour and

minutes on the day of the week when the REX will be executed and duration of REX to be executed and mode of REX.

User can also remove the REX scheduled for an NE.

Progress details of the REX on the selected NE is made available to the user on this GUI.

Note: *REX GUI is subject to change in its appearance to match the enhanced Audit GUI. This change will happen after the IT completion of REX feature. It will be done as part of a CR.*

3.8.2.1.2 GUI usage and implications

To schedule an NE for REX

- 1 “Add” button is pressed to add the NE for REX.
- 2 On pressing “Add”, a new panel is opened which will list all the NEs in the given subnet. Select the NE. select mode of REX, select card types on which REX has to be executed, select the day of the week, hour and minutes on the day of the week selected, duration of REX on the selected NE.
- 3 “Apply” button has to be pressed. On pressing Apply, NE is scheduled for REX with user input data. Newly opened panel closes and the user is in REX NE View.
- 4 REX NE View lists all the NEs whose schedule is already input by the user. On selecting the NE, state of REX and the progress details are displayed on REX NE View.

To remove REX on already scheduled NE

- 1 Select the NE from the NE list of REX NE View.
- 2 On pressing “Remove” button, REX for the selected NE is aborted.

To View the Progress details of REX

- 1 Select the NE from the NE list of REX NE View.
- 2 Text area called “Progress details” of REX NE View shows the status of REX on the selected NE.

3.8.2.1.3 GUI size**Table 5 New or modified GUIs**

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
REX NE View	1	1	TBD

3.8.2.1.4 GUI fields

The following table lists fields for GUI REX NE View.

Table 6 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
"Add" Button	New	-	-	1. "Add" button is pressed to add the NE for REX. 2. On pressing "Add", a new panel is opened which will list all the NEs in the given subnet. Select the NE. Select the day of the week, hour and minutes on the day of the week selected, duration of REX on the selected NE. On pressing "Add" button, a check is made if an Audit schedule exists on the current NE 3. "Apply" button has to be pressed. On pressing Apply, NE is scheduled for REX. Newly opened panel closes and the user is in REX NE View. On pressing "Apply" button, validations on the fields are done and prompted to the user. If an Audit schedule on this NE is scheduled at the same instant as REX, a warning message is prompted to the user. If the user confirms REX is scheduled. 4. REX NE View lists all the NEs whose schedule is already input by the user. On selecting the NE, state of REX and the progress details are displayed on REX NE View.	NA

Table 6 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Remove Button	New	-	-	1. Select the NE from the NE list of REX NE View. 2. On pressing "Remove" button, REX for the selected NE is aborted.	NA
Suspend Button	New	-	-	1. Select the NE from the NE list of REX NE View. 2. On pressing "Suspend" button, REX for the selected NE is Disabled/suspended.	NA
Resume Button	New	-	-	1. Select the NE from the NE list of REX NE View. 2. On pressing "Resume" button, REX for the selected NE is Resumed/enabled.	NA
REX Mode	New	-	1. Without SWACT 2. With SWACT	1. If the user selects "without SWACT" option, in that case, REX is executed only on the inactive card of the card pair. 2. If the selected option is "with SWACT", REX is executed on both the cards of a pair. Inactive card undergoes REX execution, followed by a SWACT on active card and REX on newly inactive card.	NA

Table 6 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Card Types	New	1. DCC 2. ITP 3. ITX	-	1. On selecting DCC, REX will be executed on DCC cards of the NE under consideration which otherwise will be skipped. 2. On selecting ITP, REX will be executed on ITP cards of the NE under consideration which otherwise will be skipped. 3. On selecting ITX, REX will be executed on ITX cards of the NE under consideration which otherwise will be skipped.	NA
REX Schedule	New	Run Immediately	-	If run immediately option is chosen, Day of week, Hour and minute fields are disabled. On clicking on Apply, REX is immediately executed on the given NE.	NA
Day of Week	New	1. Sunday 2. Monday 3. Tuesday 4. Wednesday 5. Thursday 6. Friday 7. Saturday 8. Hour 9. Minutes	-	If Run immediately is deselected, Day of Week, Hour and Minute is enabled. User is able to select the day of the week on which the REX needs to be executed. Hour and Minute would enable user to input the time at which, REX will be executed on the day(s) of week selected.	NA
Current State	New	-	-	This field is a non editable field. It informs the user the state of the REX on the selected NE. State of the REX being "Ready to run", "Running REX", "Completed REX".	NA

Table 6 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Progress Details	New	-	-	This text area displays the success/failure of the operations performed during REX on the selected NE. Operations during REX being, LOCK, UNLOCK, SWACT and Diagnose.	NA
REX Duration	New	1. Hour 2. Minutes	-	The fields Hour and Minutes enable the user to input the duration for which the REX can execute at its maximum limit. If the duration of REX exceeds the input value, REX is failed for such an NE	NA

3.8.2.1.5 Usage example

The following Figure-1 shows the GUI for REX NE View. Figure-2 shows the Create Schedule View which is displayed when “Add” button of REX NE View is clicked.

Figure 1: REX NE View

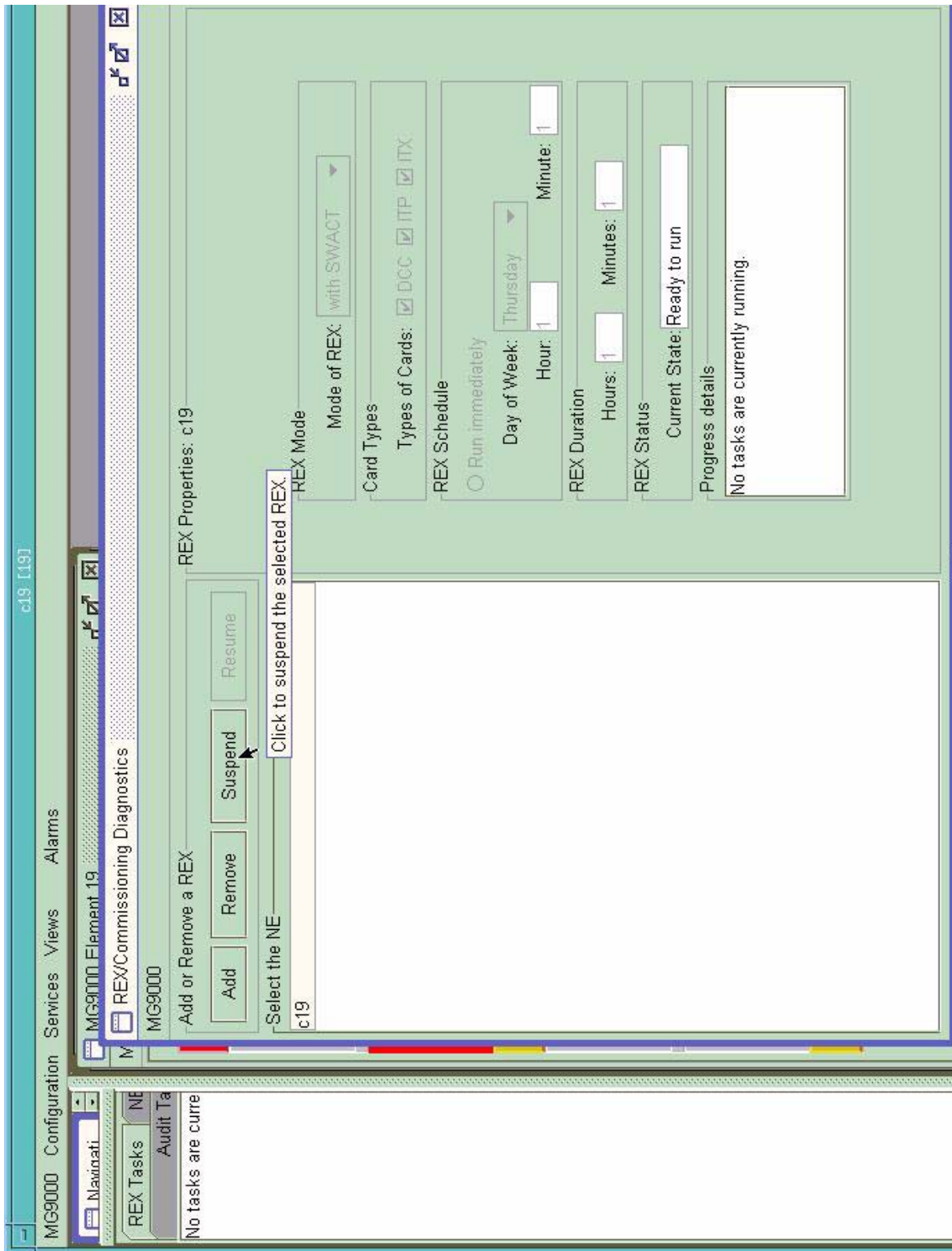


Figure 1.1 -Warning message if an Audit schedule exists at the same instant when REX is being scheduled.

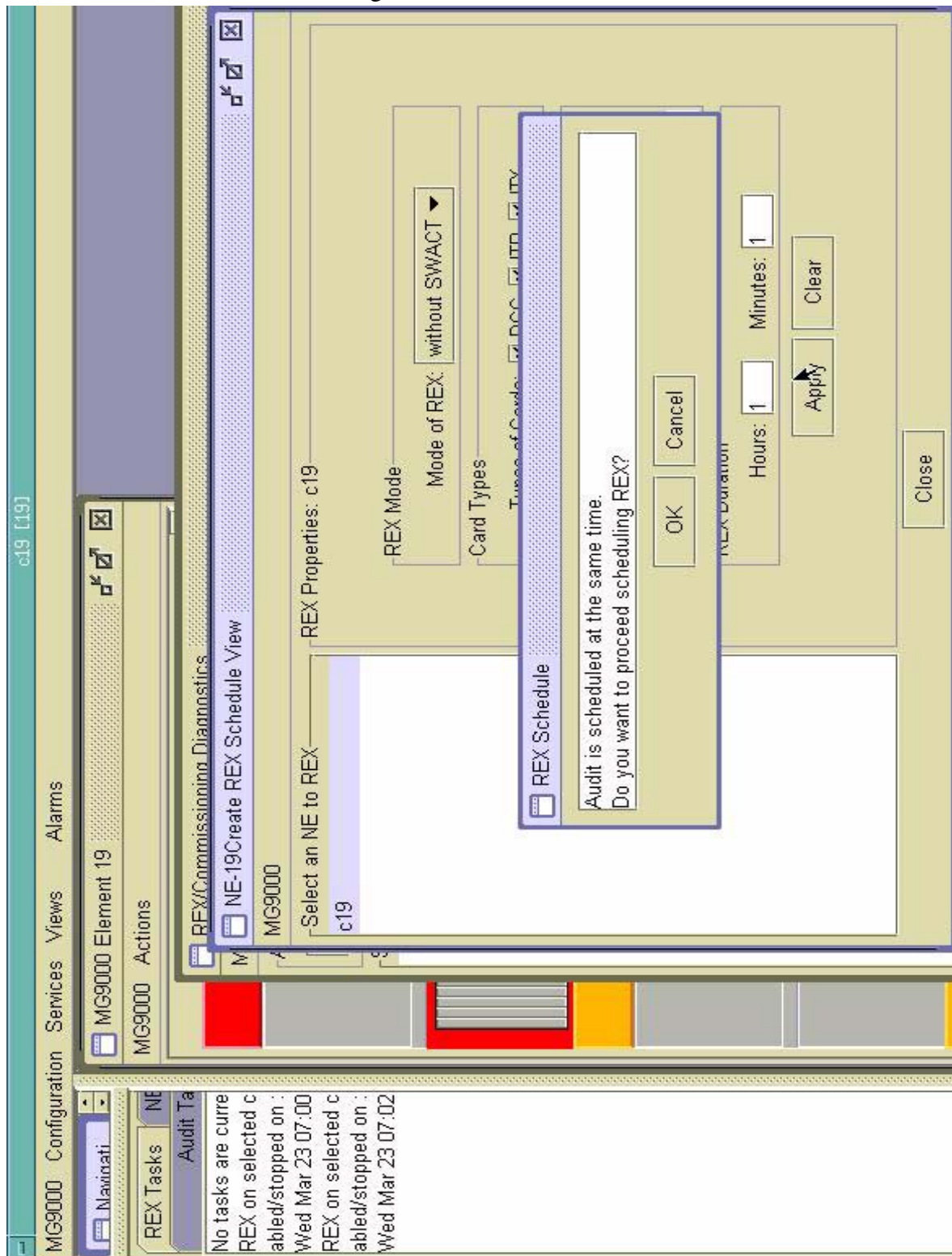
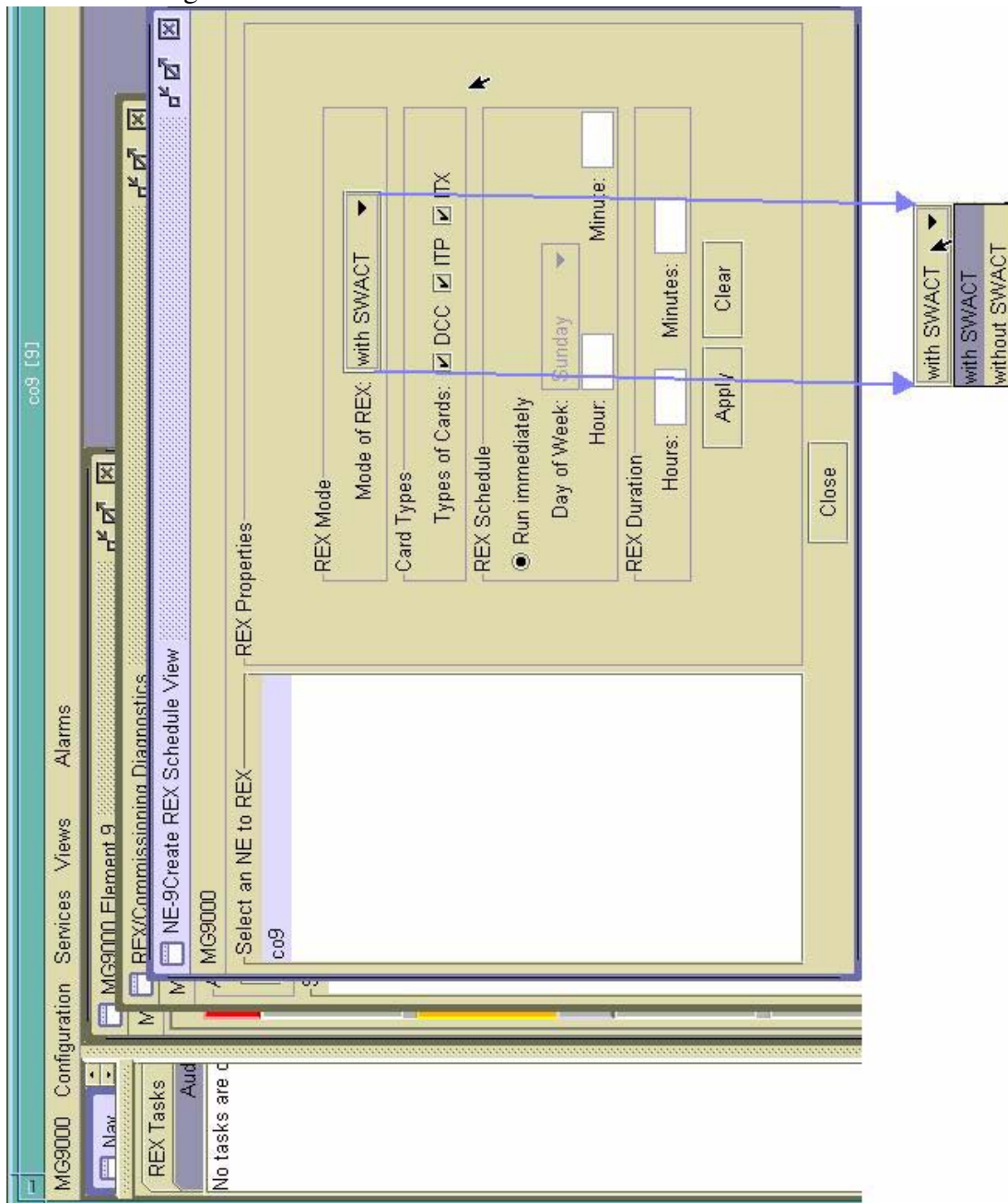


Figure-2 Create Schedule View



3.8.2.1.6 GUI release history update

A new GUI is introduced to schedule REX. REX NE View allows the user to schedule REX on an NE.

3.8.2.1.7 Context sensitive launching information

On clicking “REX NE” of Configuration menu from NE Specific Desktop view, REX NE View is launched. On clicking the “Add” button of REX NE View, Create Schedule View is launched.

3.8.2.1.8 Supplementary information

None.

3.8.2.2 GUI name: NE Specific Desktop View

NE Specific Desktop View provides REX progress details on its left panel.

3.8.2.2.1 Functional description

NE Specific Desktop View opens on clicking on MG9000 from subnet view. The configuration submenu of this view contains a new menu item “REX NE” as shown in Figure-3. This option enables user to launch REX GUI.

A tab is added on the left of NE Specific Desktop View to display the status of REX. Progress details of REX such as success/failure of operations like LOCK, UNLOCK, SWACT, Diagnose are displayed to the user.

3.8.2.2.2 GUI usage and implications

On clicking the NE from the Subnet view, NE Specific Desktop View is launched.

Following Figure-3 shows the GUI when the configuration menu item is clicked from NE Specific Desktop view. Menu item “REX NE” is introduced, which, when clicked, launches REX GUI.

3.8.2.2.3 GUI size

Table 7 New or modified GUIs

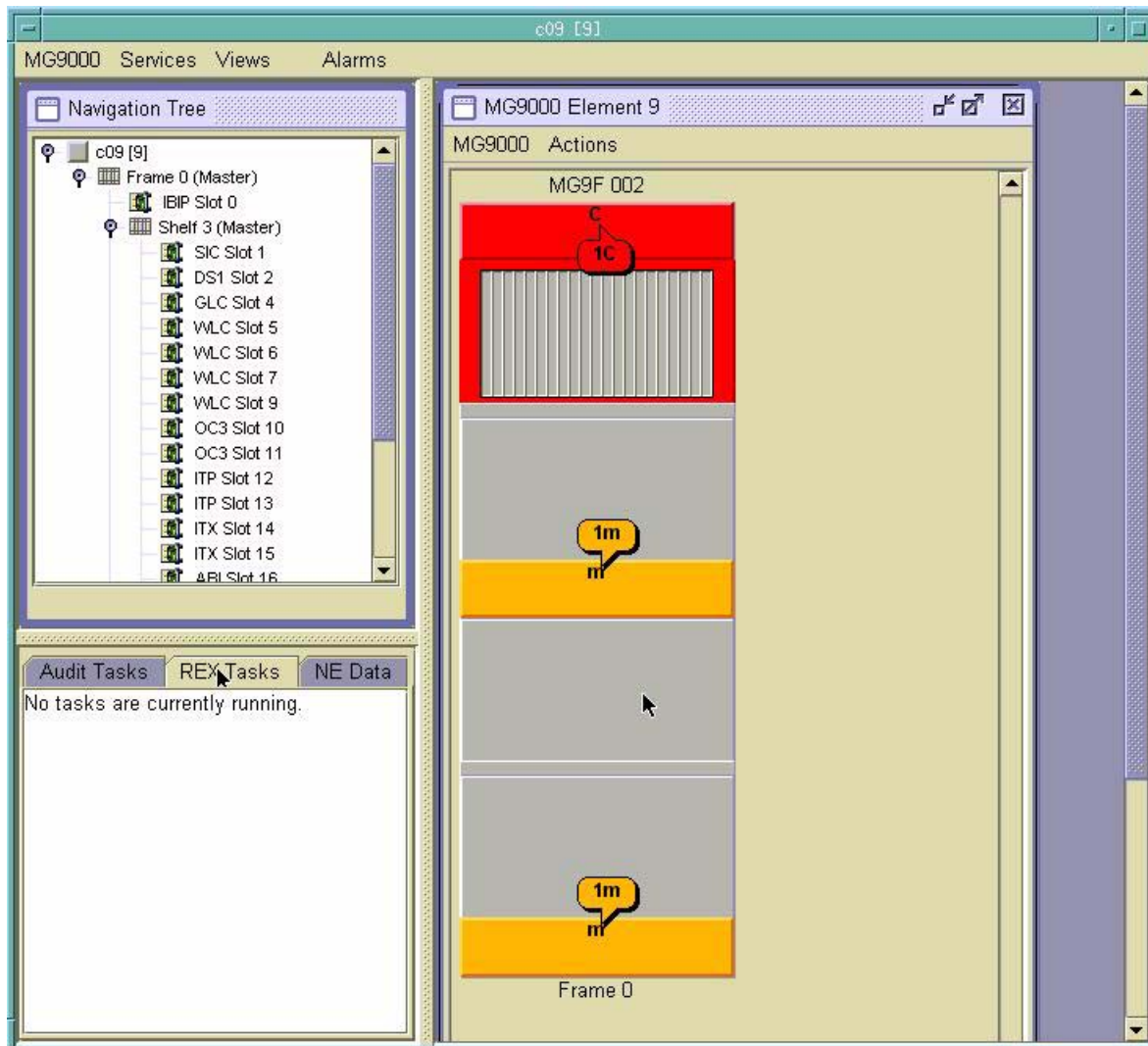
Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
NE Specific Desktop View	1	1	TBD

3.8.2.2.4 GUI fields

The following table lists fields for GUI NE Specific Desktop View that are related to REX.

Table 8 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
REX NE	New	-	-	On clicking REX NE option of Configuration menu, REX NE View is launched	NA

Figure -4 REX tasks tab on NE Specific Desktop View**3.8.2.2.6 GUI release history update**

A new submenu item “REX NE” is added to Configuration menu of NE Specific Desktop View

A new tab is introduced on the left panel of NE Specific Desktop View to display the status of REX on the current NE.

3.8.2.2.7 Context sensitive launching information

REX NE option and the REX tasks tab is present only if the EM release is SN09 or higher.

3.8.2.2.8 Supplementary information

None.

3.8.3 CLUI Interface

None

3.9 User interface changes

NA

3.10 OSSGate Interface Changes

None

3.11 Security

NA

3.12 Configuration Walkthrough

None.

Product = MG 9000

A00012198--GLC12 Coin Card Support from EM

Functional Description

1: Applicable Solution(s)

UA-AAL1, UA-IP

1.1 Description

This GLC12 card is replacing the existing SAA12 card. So this card has to support all the capabilities of the SAA card inclusive of the coin telephone support.

This feature is supported in SN09.1 release. When the user opens the GLC12 card view, the GLC12 card details will be displayed and with twelve port graphics for the GLCports (The GLC12 card has twelve ports). When the user double clicks on the port icon, the GLC circuit view will be displayed. The GLC12 circuit view will display circuit details.

The user will be able to replace the SAA12 with GLC12 without deprovisioning the card. When the card is replaced, the EM will update its details.

1.2 Hardware Requirements or Dependencies

GLC12 card with 12 ports is required.

1.3 Software Requirements or Dependencies

The MG9000 with GLC12 card and support load is required.

1.4 Limitations and restrictions

Since this new GLC12card is patched back in GW till SN08, but not on EM, this card would be displayed as SAA12 in SN08 and SN09 EM.

1.5 Interactions

NONE

1.6 Glossary

SAA12: Service Adaptive Access Line Card w/12 circuits, Supports POTS, GND, Pphone, Coin

GLC12: Global Line Card w/12 circuits Supports POTS, GND, Pphone, Coin.

MG9000: Media Gateway 9000

MG9KEM: MG9K Element Management System

2: Configuration Management for A00012198

2.1 Hardware and Software Requirements

The MG9000 and MG9000 software load which supports GLC12 card should be available.

2.2 Initial Configuration

The GLC12 card should be present on the MG9000.

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

NA

2.4 Upgrade Considerations

Since this card is supported in SN09.1 release, upgrade and downgrade scenarios have to be taken care.

No special care to be taken for EM upgrade/downgrade. The normal upgrade procedure will be followed for upgrading the EM to SN09.1. If SN09.1 EM is managing a node which has a GLC12 card, it would be displayed as GLC12 as against SAA12 in previous releases.

When a SN09.1 EM managing a SN09.1 MG9000 (with a GLC12 card) has to be downgraded to SN09, the MG9000 has to be downgraded (with proper patches for GLC12) prior to downgrading the EM. In SN09 EM the GLC12

card would be displayed as SAA12 card. The functionality is same when SN09.1 EM is downloaded SN08. In SN07EM, the GLC12 card will not be discovered.

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

NA

2.6 Service Orders (SO) (CM & SESM)

NA

2.7 Software optionality control (SOC)

NA

2.8 Element Management

There are no new views added for this feature. The card view will display the GLC12 card details and when the user double clicks on the port, the Line circuit view will open as shown in the following figures,

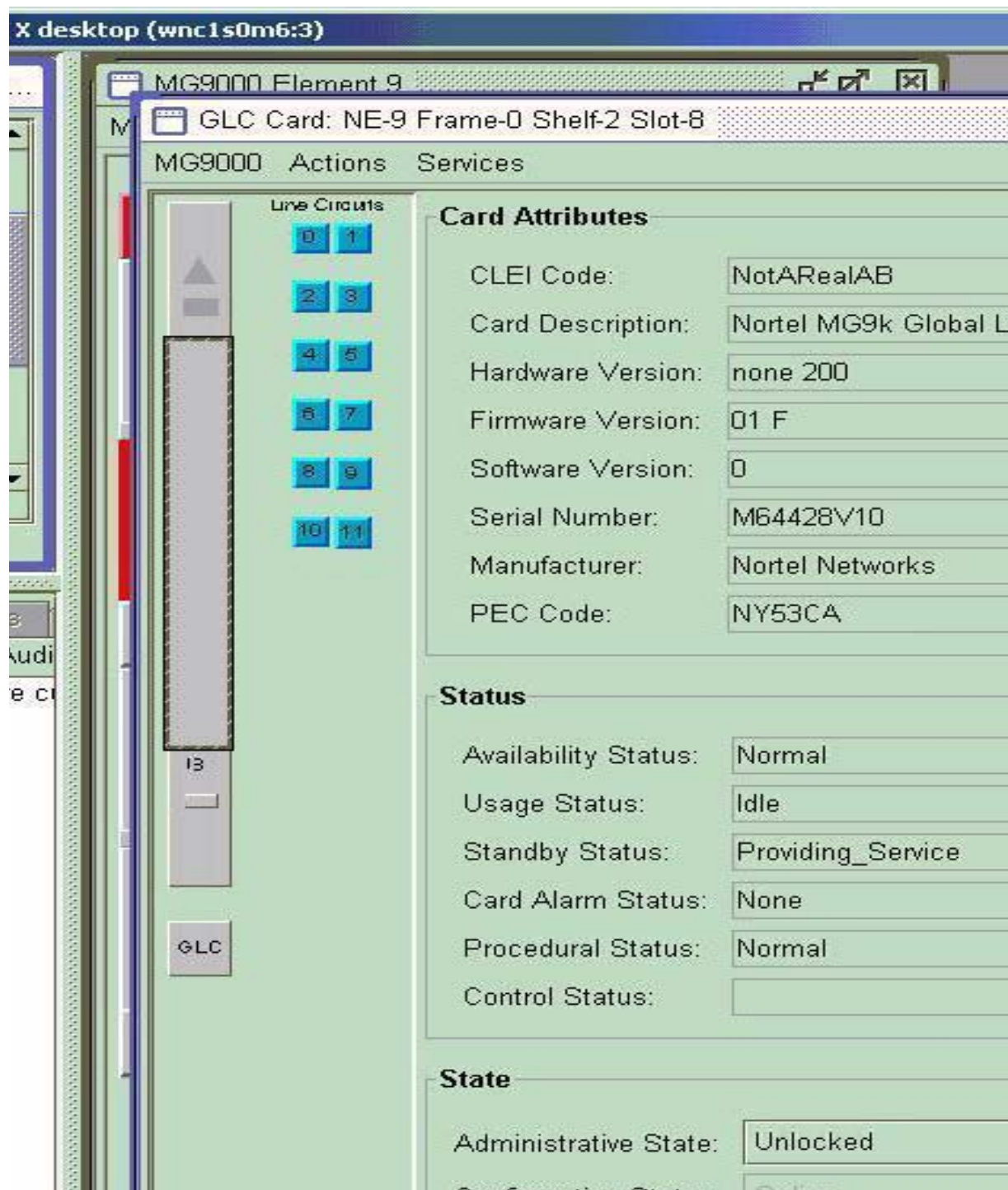


Figure 1: GLC12 Card View

The screenshot displays the 'GLC12 Circuit View' interface. At the top, there are three tabs: 'Element 18', 'Card: NE-18 Frame-0 Shelf-3 Slot-21', and 'Circuit: NE-18 Frame-0 Shelf-3 Slot-21 Ckt-1'. Below the tabs, there are buttons for 'Actions' and 'Services'. The main section is titled 'Provisioning' and contains several fields: 'Service Type' (a dropdown menu with 'potsLoopStart' selected and a list of options: 'potsLoopStart', 'pPhone', 'potsGroundStart', 'coin'), 'Coefficient', 'Min Flash Duration', 'Min Disc Time', 'Min Inter Digit Time', and 'Termination DN'. Below the 'Provisioning' section, there are four rows of status fields: 'Fault State: notInFault', 'Protection State: notInProtection', 'Babble State: notInBabble', and 'Cut Off Relay: normal'. The next section is titled 'Status' and contains three rows of status fields: 'Administrative Status: Locked', 'Operational Status: Disabled', and 'Faulty: No'. At the bottom, there is a 'Circuit Alarms' section with two checkboxes: 'Critical' and 'Minor', both of which are currently unchecked.

Provisioning	
Service Type:	potsLoopStart
Min Flash Duration:	
Min Inter Digit Time:	

Status	
Fault State:	notInFault
Protection State:	notInProtection
Babble State:	notInBabble
Cut Off Relay:	normal

Status	
Administrative Status:	Locked
Operational Status:	Disabled
Faulty:	No

Circuit Alarms	
Critical:	☐
Minor:	☐

Figure 2: GLC12 Circuit View

The GLC12 line circuit will support pPhone, potsGroundStart, potsLoopStart and coin service types. The SAA12 can be replaced with a GLC12 (and vice versa) without deprovisioning the card. When the card is replaced, if the circuit

view and circuit listing views will be closed if they are open. When the user opens the views again, the GLC information will be displayed in these views. When a SAA12 card is replaced with a GLC12 card, in the card view the actions submenu will be added. This actions submenu will have 'Coefficient Table Manager' entry. Clicking on which 'Line Coefficient Table' will be opened. The circuit listing view which can be opened from Services submenu will display coefficient with other details.

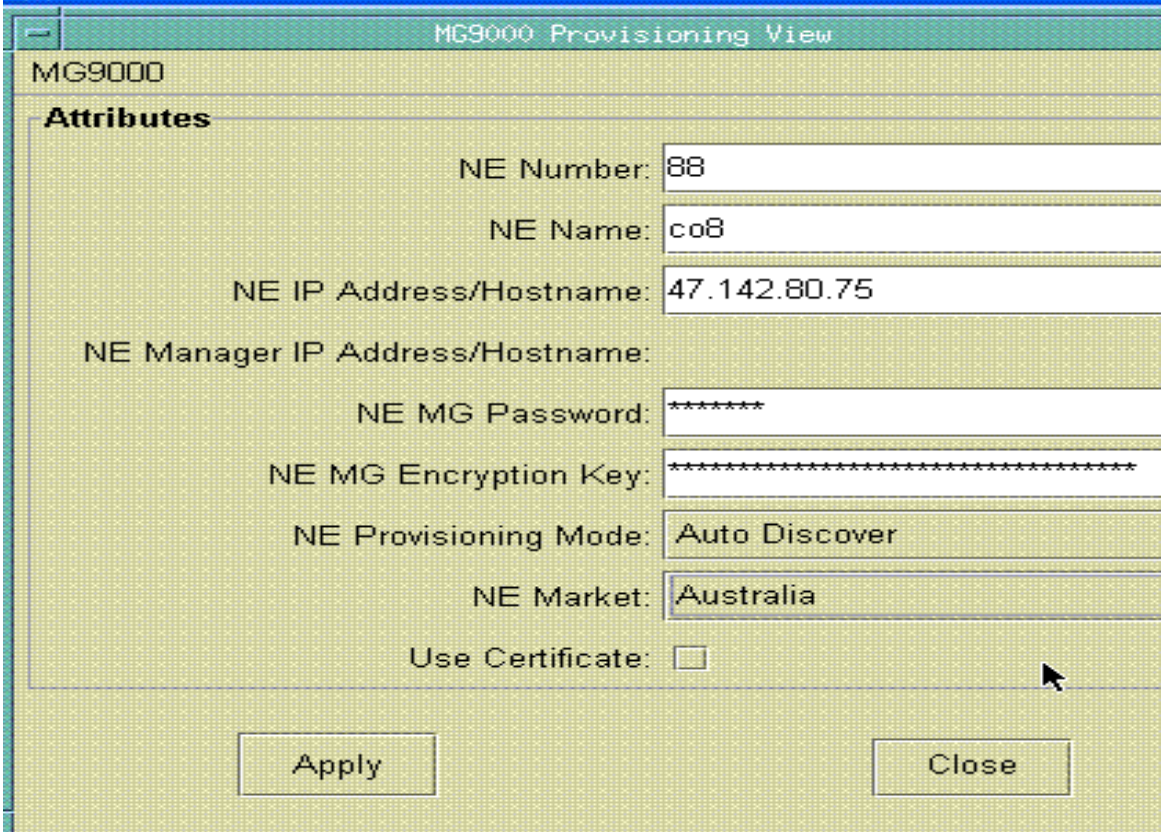
When a GLC12 card will be replaced with a SAA12 card, the actions submenu will be removed and the circuit listing view will not display coefficient details with other existing details.

The audit will correct if there is a mismatch in the PEC code types, the proper card types would be decided depending on the PEC code and the same would be updated in the EM

Line Coefficient Download:

With this design, the EM is limiting the market the user can select for VMGs which in turn will limit the line coefficients on the GW.

A combobox 'NE Market' has been added to Add New MG9000 view. The user has to select the market from the market list while adding the NE. By default the market in the officewide defaults will be selected. The user can modify the market and apply the market to NE. The same market has to be selected for the VMGs which will be created.



The image shows a 'MG9000 Provisioning View' dialog box. It has a title bar with a minus sign and the text 'MG9000 Provisioning View'. Below the title bar, the text 'MG9000' is displayed. The main area is titled 'Attributes' and contains several fields for configuration. The fields are: 'NE Number' with value '88', 'NE Name' with value 'co8', 'NE IP Address/Hostname' with value '47.142.80.75', 'NE Manager IP Address/Hostname' (empty), 'NE MG Password' with masked characters '*****', 'NE MG Encryption Key' with masked characters '*****', 'NE Provisioning Mode' with value 'Auto Discover', 'NE Market' with value 'Australia', and 'Use Certificate' with an unchecked checkbox. At the bottom of the dialog are two buttons: 'Apply' and 'Close'.

Attribute	Value
NE Number	88
NE Name	co8
NE IP Address/Hostname	47.142.80.75
NE Manager IP Address/Hostname	
NE MG Password	*****
NE MG Encryption Key	*****
NE Provisioning Mode	Auto Discover
NE Market	Australia
Use Certificate	☐

Figure 3: Add New MG9000 View

The market set for the NE can be viewed from 'Add/Modify NE Properties View'. This market's coefficients will be downloaded onto the GW during LineCoefficient audit.

Properties View

MG9000

NE Properties | NE Security | IESA PVR Provisioning

Properties

NE Number: 88

NE Name: co8

NE IP Address/Hostname: 47.142.80.75

NE Password: *****

NE Encryption Key: *****

MG9000 Manager IP Address: 47.142.211.68

SNMP Trap IP(from MG): Not Discovered

NE Provisioning Mode: Auto Discover

Vendor: Nortel Networks

MG9000 Software Version: Unknown, DCC not discovered.

SNMP Trap Port (expected): 8002

SNMP Trap Port (from MG): Not Discovered

NE Market: Australia ▼

OMCollection: ☐

Discovery Status Info

No discovery has been attempted for this NE.

Figure 4: Add/Modify NE Properties View

Once the VMGs are created, the market can be modified only if the new market selected belongs to the same country code as that of the set market. If the user tries to select a market which does not belong to the same country code, an error message will be displayed to the user. If there are no VMGs the market can be modified to any other market (different country code) and the line coefficient audit will run which will push those coefficients onto the GW.

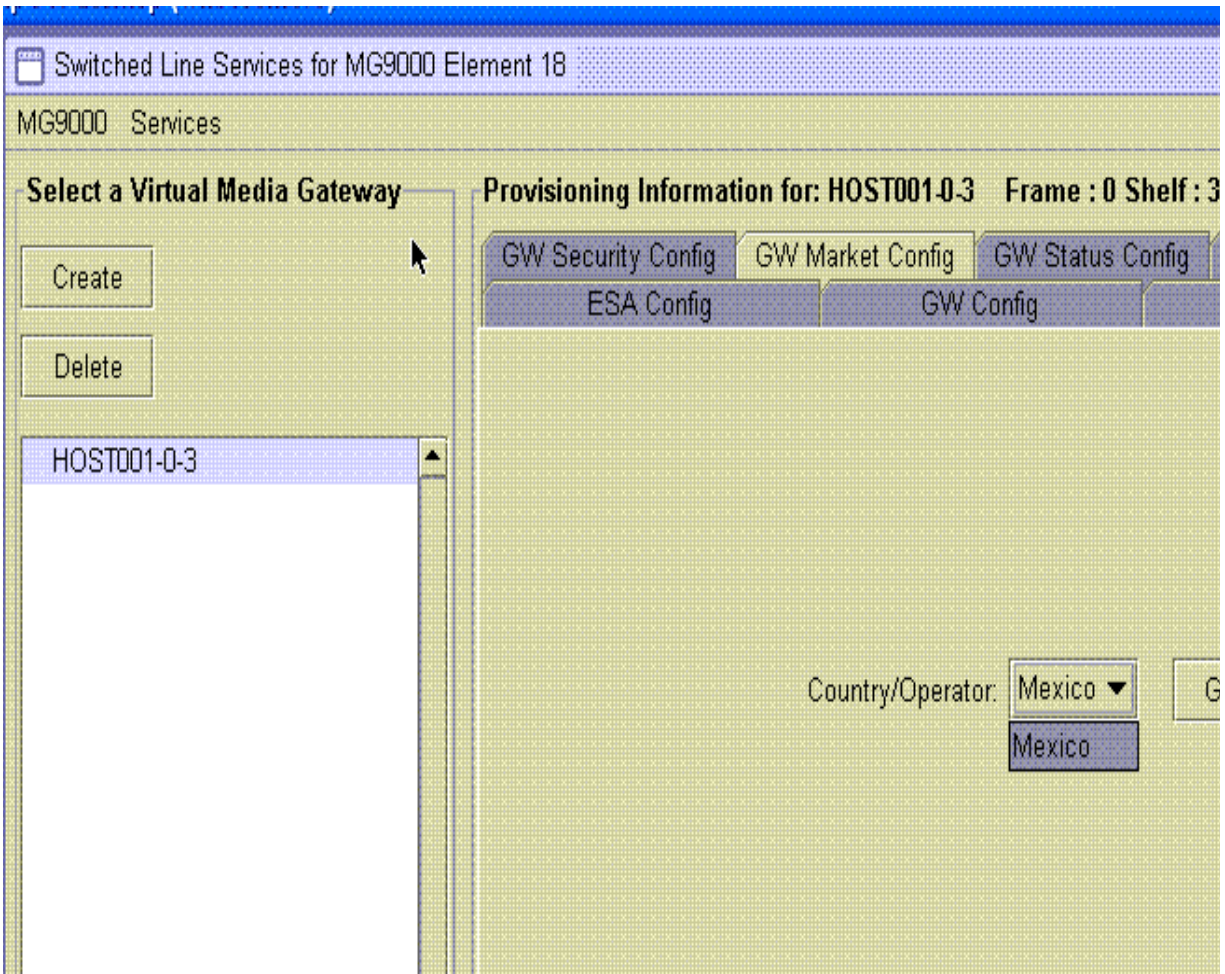


Figure 5: Get market for VMG.

Once the market is set for the NE, the VMGs created will have to use the same NE market. In SwitchLineServices View in the getMarket() tab in the VMG displays only the market set for that NE. But if a VMG already exists (before setting the NE's market, this can happen during upgrade scenarios) which has a different market, then both VMG market and the NE market will be displayed. The user will be able to change the market to NE market.

2.9 User interface changes

NA

2.10 OSSGate Interface Changes

None

2.11 Security

2.11.1 Network configuration

NA

2.11.2 Key management

NA

2.11.3 Protocol

NA

2.11.4 Authentication

NA

2.12 Configuration Walkthrough

None

Product = MG 9000

A00012199--MG9K EM CPR Robustness

Functional Description

1: Applicable Solution(s)

UA-AAL1, UA-IP

1.1 Description

This feature is supported for MG9Ks with version SN091 and greater. This feature will be supported for all the types of NEs present in subnet (e.g. discovered and undiscovered). The following will be supported for this feature.

- 3 The craftsperson will be able to initiate an LCI session directly from the MG9K EM subnet screen for all the nodes. It is mandatory that browser path is defined in OS environment. LCI will be invoked on Netscape

browser for Unix OS and default browser on a Windows PC. As EM GUI can be launched only from Solaris and Windows PC, this behavior is supported only in Solaris and Windows OS.

The craftsperson must be warned that modification made at LCI may result in node isolation and hence will be required to type (not click) “Agrees” before launching browser.

The craftsperson will be given an option of connecting to LCI through inband or out of band.

4. The craftsperson will be able to launch a “clear persist and discover” operation from the MG9K EM for all the nodes.

The craftsperson will be warned that the “clear persist and discover” operation will disrupt services, and will result in an outage condition, and will be required to type (not click) “Agrees” prior to action being taken.

1.2 Hardware Requirements or Dependencies

There is no specific hardware required for this feature.

1.3 Software Requirements or Dependencies

This feature needs changes on the MG9K also and depends on the same.

1.4 Limitations and restrictions

- 1 The MG9K EM client should have browser path defined on the OS environment. For Unix OS “PATH” environment must have Netscape path defined. For Window OS, the default browser must be set to either Netscape or Internet Explorer.
- 2 If the browser is already open, LCI session will be launched on the same browser window.
- 3 When craft person selects the option of launching LCI through inband IP of MG9K, he/she must be aware that if inband address of MG9K is allocated from a private co-lan address space, a client located on the same co-lan or a client which had been connected to the co-lan via a VPN firewall will be able to launch the LCI session. Hence the networking routing is very important while launching the LCI through inband IP. Valid network routing can be checked using ping & traceroute commands. Either command line or “Configuration -> Tools” subnet EM menu can be used for these utilities.
- 4 LCI out of band access is only available if face plate ethernet is connected on the supercore and a valid out of band IP has been previously configured at LCI.

- 5 If the LCI browser session returns 404 not found, use the ping command to verify that the out of band address on MG9K responses. The out of band address is the address in the URL shown on the browser screen when out of band LCI is launched.
- 6 If ping and traceroute do not succeed, the swact of SCO on MG9K may restore connectivity.

1.5 Interactions

N/A

1.6 Glossary

Term	Description
CPR	Capacity Performance and Robustness
DCC	Data Controller Card
EM	Element Manager
GW	Gateway. It refers to MG9K here.
LCI	Local Craft Interface
MG9K	Media Gateway 9000
OS	Operating System

2: Fault Management for A00012199

2.1 Fault management strategy

No additional fault management is provided by this feature.

2.2 Fault management tools and utilities

2.2.1 Faults, Alarms and Logs

Customer logs will be generated whenever EM user opts for “clear persist and discover” functionality. Existing Reinitialize Gateway log will be used.

2.3 Logs

NE606

2.3.1 Formats

Jun 3 02:18:19 wnc0s0pe
MG9kEMFactory_9:_V2_~I=MG9K~H=wnc0s0pe~A=MG9kEMFactory_9

~S=2663~~ NE606 NONE INFO MG9K Reinitialize Gateway Event
Description: Reinitialize Gateway Event Sent Time: Fri Jun 03 02:18:19
EDT 2005

2.3.2 Explanation

Each time user clicks on “Clear persist and discover” button in NE Discovery View, NE606 log will be generated.

2.3.3 Field descriptions

Table 1:

Field	Description	Example
Date/Time	Date and time stamp of the log	Jun 3 02:18:19
Host Name	Host machine name	wnc0s0pe
Application Name	The application producing the log	MG9kEMFactory_9
User Name	MG9K EM User name	rtpu
Log Number	The log number	NE606
Log Text	The action being taken	Reinitialize Gateway Event

2.3.4 Action

This is information log only. No action required.

2.3.5 Associated Operational Measurements or Performance Measurements

None

2.3.6 Additional information

None

2.4 Alarms

None

2.5 Related documentation

None

3: Configuration Management for A00012199

3.1 Hardware and Software Requirements

There is no specific hardware required for this feature.

3.2 Initial Configuration

The browser path should be defined in operating system environment where EM client is running.

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

NA

3.4 Upgrade Considerations

NA

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

3.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
NORTEL-UEMG-NODE-MIB	Changed	Unchanged

3.5.2 Table/MIB/Remote Database Schema information

3.5.2.1 Name: NORTEL-UEMG-NODE-MIB

3.5.2.2 Functional description

Two scalar MIB variables will be added in this MIB for LCI launch functionality. One MIB variable will store slot 10 out of band IP and another MIB variable will store slot 11 out of band IP. One additional MIB will be introduced for clear persist and discover functionality.

3.5.2.3 Usage sequence and implications (CM Only)

None

3.5.2.4 Size

NA

3.5.2.5 Fields/OIDs

The following table lists fields/OIDs added in NORTEL-UEMG-NODE-MIB.

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
slot 10 outofbandIP	New	NA	This MIB will hold Slot 10 ethernet DCC IP.	When craftperson wants to launch LCI out of band thorough slot 10, this IP will be required to form the URL. For e.g. if this IP is 47.142.80.80 the URL for launching browser will be "https://47.142.80.80".
slot 11 outofbandIP	New	NA	This MIB will hold Slot 11 ethernet DCC IP.	When craftperson wants to launch LCI out of band thorough slot 11, this IP will be required to form the URL. For e.g. if this IP is 47.142.80.81 the URL for launching browser will be "https://47.142.80.81".
norNodeClear PersistOp	New	NA	Off	This MIB once set from EM would trigger clear persist and discover functionality on MG9K.

3.5.2.6 Datafill example

None

3.5.2.7 Table release history update

NA.

3.5.2.8 Supplementary information

These MIBs will be supported for all the types of DCC cards.

3.5.2.9 Translation verification and other tools

None

3.6 Service Orders (SO) (CM & SESM)

NA

3.7 Software optionality control (SOC)

NA

3.8 Element Management

3.8.1 New/modified GUIs

Table 3 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
NE Discovery View	Changed

3.8.2 GUI information

3.8.2.1 GUI name: NE Discovery View

3.8.2.2 Functional description

The NE Discovery View will now show one more button for “Clear persist and discover” functionality.

Impact on existing functionality of NE Discovery View:

This new button will be shown for all the NEs. When user clicks this button for GW version less than SN091, an appropriate information message will be shown for not supporting this feature. This field cannot be grayed out for lower release NEs because this feature needs to be supported for undiscovered NEs also and EM will not have GW version information for undiscovered NEs.

3.8.2.3 GUI usage and implications

None

3.8.2.4 GUI size

Table 4 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
NE Discovery View	1	Number Of NEs in subnet	TBD

3.8.2.5 GUI fields

As discussed before NE Discovery view will have one more button next to “Discover” button.

3.8.2.6 Usage example

The following example shows the NE Discovery View on EM GUI.

NE Discovery View

MG9000

NE Properties

Properties

NE Number: 9

NE Name: c09

NE IP Address/Hostname: 47.142.105.9

NE Password: *****

NE Encryption Key: *****

MG9000 Manager IP Address: 47.142.211.35

SNMP Trap IP(from MG): Not Discovered

NE Provisioning Mode: Auto Discover

Vendor: Nortel Networks

MG9000 Software Version: Unknown, DCC not discovered.

SNMP Trap Port (expected): 8002

SNMP Trap Port (from MG): Not Discovered

OMCollection: ☐

Discovery Status Info

No discovery has been attempted for

Discover Clear persist and discover Abort Refresh Close

3.8.2.7 Context sensitive launching information

None

3.8.2.8 Supplementary information

None.

3.8.2.9 GUI name: Subnet Configuration Menu

3.8.2.10 Functional description

LCI session will be invoked through a new submenu in configuration menu of subnet view.

3.8.2.11 GUI usage and implications

None

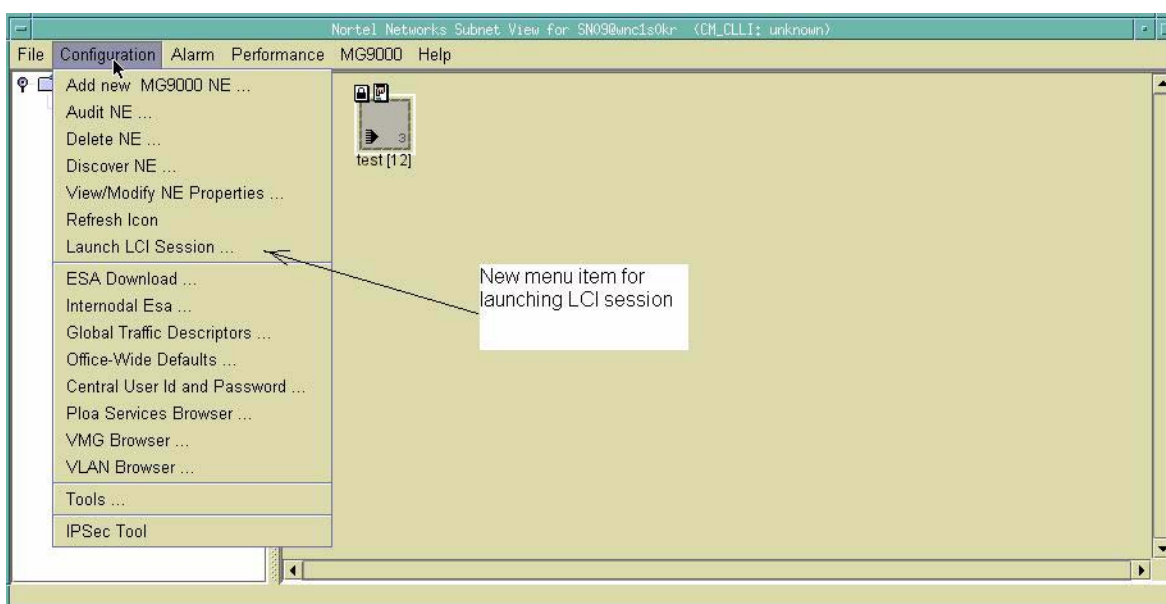
3.8.2.12 GUI size

Table 5 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Configuration menu	1	1	TBD

3.8.2.13 GUI fields

The new menu item will look like as shown below.



3.8.2.14 Usage example

The example above shows the new menu item details.

3.8.2.15 Context sensitive launching information

None

3.8.2.16 Supplementary information

None.

3.8.2.17 GUI name: Launch LCI View

3.8.2.18 Functional description

After clicking on “Launch LCI Session”, a new view will be invoked for launching LCI. This view will give user option of connecting to LCI either inband or out of band. The inband invocation will be successful only if proper

network routing is done. The details are given functional description document on the inband IP and network routing. Out of band invocation can be done either through slot 10 or slot 11.

3.8.2.19 GUI usage and implications

None

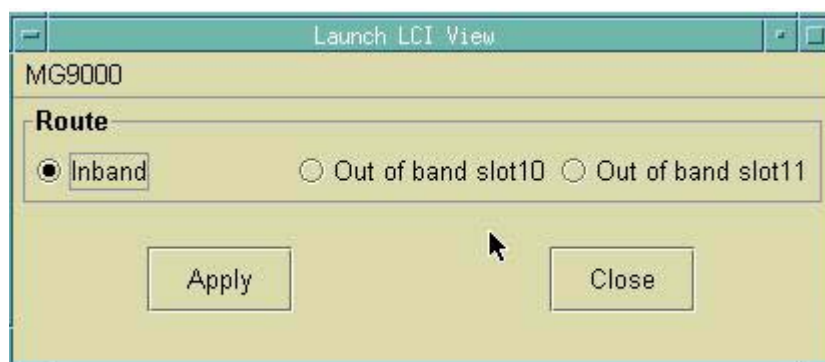
3.8.2.20 GUI size

Table 6 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Launch LCI View	1	1	TBD

3.8.2.21 GUI fields

The new view will look like as shown below.



3.8.2.22 Usage example

The example above shows the new menu item details.

3.8.2.23 Context sensitive launching information

None

3.8.2.24 Supplementary information

None.

3.8.3 CLUI Interface

NA

3.9 User interface changes

NA

3.10 OSSGate Interface Changes

None

3.11 Security

3.11.1 Network configuration

NA

3.11.2 Key management

NA

3.11.3 Protocol

NA

3.11.4 Authentication

The clear persist and discover functionality will be allowed for EM users with admin privileges for e.g. users with emsadm and higher permissions.

Launching LCI session is also supported only for admin users.

3.12 Configuration Walkthrough

None

Product = MG 9000

A00012215--Global Line Card Field Programmable Gate Array download

Functional Description

1: Applicable Solution(s)

UA-AAL1, UA-IP

1.1 Description

Currently, GLC cards do not have any loads which need to be downloaded from the MG9k Element Manager. The FPGA is currently flashed directly onto the board. In SN09.1, new GLC hardware is introduced which has the capability for the FPGA to be downloaded. The GLC cards must provide the capability for software download of the FPGA. This capability prevents any class "A" retrofits of the GLC-32 or GLC-12 due to a configuration load issue in the FPGA on the card. The NY53BA card replaces the existing POTS-32 and GLC-32 cards.

This feature also covers the need to be able to reload a single circuit controller on the GLC card from the EM. Currently, when the line card is force locked all 8 of the circuit controllers on the GLC-32 cards are reloaded. Each circuit controller controls 4 line circuits. The reload is taking upwards of 4 minutes for a single card which is too long to reload a card. Therefore, we need to be able to reload a single circuit controller on the GLC instead of all 8 being reloaded at the same time.

1.2 Hardware Requirements or Dependencies

Hardware produces the GLC loads for the FPGA configuration load. It is assumed different GLC loads are produced for each different GLC PEC code. The MG9kEM depends upon hardware to produce the different GLC loads for each GLC PEC code.

The GLC can be plugged into any version of the gateway but until the ITP card is running a load that is able to download the GLC FGPA's, the download will not work since the ITP is used to perform the software download to the GLC FPGA. The ITP provides a temporary location to store the FPGA load until it is moved to the GLC card.

Hardware must provide a mechanism to read the FPGA load name in order to display the loadname to the customer. The load name would allow the customer to figure out if the FPGA for the particular vintage of GLC needed to be software downloaded with a new load.

Hardware also produces the coefficients for each GLC PEC code. This new GLC card depends upon hardware to produce a copy of coefficients for this new GLC PEC code.

1.3 Software Requirements or Dependencies

The new GLC download file is loaded onto the SDM/CBM along with the other gateway loads. The MG9kEM software must be at SN09.1 or patched with this feature content in order to provide the software download capability to the GLC card.

Replacing GLC FPGA loads is a function of the gateway loadbuild process. The MG9kEM assumes there is a process in place for replacing GLC loads at the customer site in the event a new GLC load is required outside the normal software release cycle.

1.4 Limitations and restrictions

GLC NTNY53AA and NTNY53AB cards can not be software downloaded.

The GLC downloading capability is available once the GLC card PEC code is NTNY53BA or greater.

Software downloading FPGAs on GLC cards require the GLC card to be locked and thus affects call processing.

The GLC cards are not downloaded as part of a release to release upgrade. The GLC cards can be downloaded after the entire network element, MG9k, has been upgraded if required. Or can be downloaded prior to a release to release upgrade if absolutely required. The preferred method of downloading is to download once the entire network element has already been upgraded.

Running diagnostics on the circuit controller affects 4 circuits at the same time. If the circuit controller needs to be restarted, call processing is affected.

No alarms are output in the event two GLC cards with the same PEC code have different configuration loads.

Unlike the MTA Card View where the customer sees two downloadable loads which can be used to restart the card. The GLC card view only shows a single FPGA configuration load. There is no backup load for the GLC FPGA. There is no restart load capabilities on the GLC card.

1.5 Interactions

Software upgrades - From the frame view, all of the GLC cards for a particular vintage can be downloaded. The GLC software download does not apply to every release to release upgrade. Hopefully, only in rare instances would a new GLC FPGA load be release. Therefore, the upgrade CLUI does not include GLC as a downloadable component. GLC cards must be locked prior to attempting a software download.

Diagnostics- If the circuit controller needs reloading during a circuit controller diagnostic test, 4 circuits are affected. Call processing is dropped during a circuit controller reload. If the circuit controller does not need reloading during the diagnostic, as determined by the gateway, no reload occurs and calls remain operational.

There are no patching interactions since the GLC card can not be patched. The GLC card can not be imaged as well.

1.6 Glossary

Term	Description
CLUI	Command Line User Interface
EM	Element Manager
FPGA	Field Programmable Gate Array
GLC	Global Line Card

Term	Description
SDM	Succession Data Manager

2: Configuration Management for A00012215

2.1 Hardware and Software Requirements

The NTNY53BA GLC card can replace any NTNY53AB or NTNY53AA card. The NTNY53BA GLC card provides all the supported capabilities of the NTNY53AB GLC card. The ITP cards must be at a release that allow the GLC card to be downloadable.

2.2 Initial Configuration

Lock and offline an existing NTNY53AB GLC card. Replace with the NTNY53BA GLC card. Online and unlock the NTNY53BA card. Select the GLC card and examine the FPGA configuration load to determine if the card needs to be downloaded and enter the information to download a new FPGA configuration load if needed.

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

None

2.4 Upgrade Considerations

2.4.1 Dump and Restore (CM)

None

2.4.2 Element Management Upgrade

Once the GLC, WLCor SAA hardware is replaced with a GLC NTNY53BA or NTNY53CA PEC code, any changes to the FPGA configuration load can be made via software downloading a new FPGA configuration load onto the GLC card. Normally, the FPGA configuration load for a GLC card is not changed. Only under rare circumstances would the FPGA configuration load be changed. Therefore, normal release to release upgrades do not include downloading GLCs.

The process for upgrade would be to upgrade the entire office utilizing the mg9kuptool upgrade CLUI tool. Once the entire office is upgraded, the customer should examine the FPGA configuration load on the GLC cards and make sure there is not a new release of the GLC configuration load. If there is a new release of the configuration load, the upgrade GUI from the frame view can be utilized to download multiple GLCs per PEC code. If only one GLC needs the new FPGA configuration load, for example to soak the new configuration load prior to releasing to all GLC cards, the software download manager should be selected from the card view for the chosen GLC card.

No alarms are output in the event two GLC cards with the same PEC code have different FPGA configuration loads.

2.4.3 Downgrade impact

If the ITP card is downgraded to a release that does not support downloading of GLC cards, any NTNY53BA and any NTNY53CA GLC cards can be attempted to download the FPGA however, since the ITP card does not support the software download of the FPGA, an error from the ITP is output. The customer is not prevented from attempting to download the FPGA as long as the correct GLC hardware is still in place.

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

norLineVineticReload 1.3.6.1.4.1.562.38.6.8.18

The norLineMib is changed to add in a new nnUemgLineTestTypes. This new test type tests to see if the circuit controller associated with this circuit needs to be reloaded. If no reload is necessary the test is completed. If the circuit controller needs to be reloaded, the controller for the 4 associated circuits is reloaded.

2.6 Service Orders (SO) (CM & SESM)

None

2.7 Software optionality control (SOC)

None

2.8 Element Management

2.8.1 New/modified GUIs

GUI name	NEW, CHANGED, or DELETED
GLC card View	Changed
GLC diagnostic View	Changed
Upgrade View from Frame View	Changed

2.8.1.1 GUI name: GLCC

GLC Card View

2.8.1.1.1 Functional description

The GLC Card View is modified to allow a new action of software downloading to occur. The software download manager menu item allows the configuration load of the FPGA on the GLC card to be software downloaded from the SDM/CBM. This prevents a hardware retrofit of the GLC card in the unlikely event the FPGA configuration load needs to change once the card is in the field. Also the GLC Card View is modified to show the FPGA

configuration load on the GLC card. Showing the FPGA configuration load allows the customer to visibly see what configuration load is currently on the hardware and allows the customer to determine if a new load needs to be downloaded to the FPGA.

2.8.1.1.2 GUI usage and implications

The floating IP must be assigned prior to using the GLC software downloading action. Also, the GLC card must be locked before the software downloading can take place. The software download manager invokes the existing software download GUI used to software download MTA and XDSL cards. The customer would have to input the file name including the directory path, IP address of the SDM/CBM, the user name on the SDM/CBM used to upgrade/software download loads, and the server password to the SDM/CBM just as they do today for MTA and XDSL cards.

2.8.1.1.3 GUI size

2.8.1.1.4 GUI fields

Table 1 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
GLCC	0 if no GLCs assigned in the office	one per GLC card in the office(14 per shelf for master shelf and 18 per shelf for each subtending shelf)	no increase in memory

The following table lists fields for GUI GLCC.

Table 2 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Actions Menu	Changed	Software Download Manager	none	Added new Software Download Manager menu selection for GLC cards. This brings up the existing software download GUI view.	None for new menu option, existing NorNodeSWLoadEntry for software download GUI view.
FPGA Configuration Load	New	None	none	Displays the current FPGA load on the GLC card	norNodeSWLoadCurrentLoadName

2.8.1.1.5 Usage example

The following example shows the software download manager menu selection and the Configuration load name area for GUI GWCC.

GLC Card: NE-55 Frame-0 Shelf-2 Slot-8

MG9000 Actions Services

Software Download Manager...
Coefficient Table Manager...

GLC Code: NotARealAB

Card Description: Nortel MG9k Global Line Card 32

Hardware Version:

Firmware Version:

Software Version:

Serial Number:

Manufacturer: Nortel Networks

PEC Code: NY53AB

Status

Availability Status: Normal

Usage Status: Idle

Standby Status: Providing_Service

Card Alarm Status: None

Procedural Status: Normal

Control Status:

State

Administrative State: Unlocked

Configuration State: Online

Operational State: Enabled

Configuration Load

FPGA Configuration Load:

Card Alarms

Critical: 0 Minor: 0

Major: 0 Warning: 0

Apply Refresh Close

2.8.1.1.6 GUI release history update

Add Software Download Manager menu under the action menu for GLC card views. Add new area, configuration Load, to display the FPGA configuration load to the user.

2.8.1.1.7 Context sensitive launching information

In order to allow the user to select the software download, the user must have read write privileges. The software download manager and configuration Load are only visible to GLCs which have a PEC code of NTNY53BA or above. The software download manager and configuration load do not appear on NTNY53AA or NTNY53AB GLC cards.

2.8.1.1.8 Supplementary information

None

2.8.1.2 GUI name: GLCD

GLC Circuit Diagnostic View

2.8.1.2.1 Functional description

In order to perform the new diagnostic test, Circuit Controller Diagnostic, the GLC Line Circuit View for a particular circuit is opened from the GLC Card View. The Circuit Controller diagnostic is designed to determine if the circuit controller needs to be reloaded, and reload if necessary as determined by the gateway. The Actions menu from the GLC circuit View is selected. Maintenance menu is selected. Diagnostic menu is selected and inside the Diagnostic View, a new Diagnostic type is added for checking to see if a circuit controller requires reloading. The new diagnostic type is Circuit Controller Diagnostic.

2.8.1.2.2 GUI usage and implications

This new circuit controller diagnostic could be used if all four circuits of a circuit controller were in the operational disabled state and there were no other readily apparent reason for the 4 circuits to have an issue. The GLC card GUI indicates which 4 circuits are in a circuit controller group by alternating between dark blue and light blue. The first 4 GLC circuits are in one circuit controller group. Circuits 4 - 7 are in the next circuit controller group, and so on. So if a group of 4 circuits have no dialtone and there is no other apparent cause, run the circuit controller diagnostic or perform a lock-forced unlock if it appears to be an entire card.

2.8.1.2.3 GUI size

The GLC Circuit View and Diagnostic View are existing GUIs. Adding in a new selectable diagnostic type does not add any memory to the GUI.

2.8.1.2.4 GUI fields

The following table lists fields for GLCD

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Diagnostic Type	Changed	Controller Diagnostic	None	Selecting the new Controller diagnostics determines if the controller for this line circuit and the other 3 line circuits on this controller needs to be reloaded and reloads if appropriate	norLineVineticReload

2.8.1.2.5 Usage example

The following example shows menu selection for GLCD GUI to invoke the controller diagnostic:

2.8.1.2.6 GUI release history update

Add a new diagnostic type for circuit controller diagnostic for GLC Circuits. All GLCs, NTNY53AA/AB/BA/CA, are able to perform the circuit controller diagnostic. This diagnostic tests the circuit controller to determine if this single circuit controller needs to be reloaded.

2.8.1.2.7 Context sensitive launching information

In order to allow the new diagnostic, circuit controller diagnostic, to be selected the user must have maintenance privileges. The circuit controller diagnostic is available to any GLC PEC code including NTNY53AA and NTNY53AB.

2.8.1.2.8 Supplementary information

None

2.8.1.3 GUI name: UPGF

Upgrade View from the Frame View

2.8.1.3.1 Functional description

In order to provide the customer with the ability to software download all GLCs of a certain PEC code, the Upgrade Wizard invoked from the upgrade view for multiple cards is changed to add in the GLC-32 BA and GLC-12 CA check boxes to indicate software download of the FPGA is required for these GLC PEC codes.

2.8.1.3.2 GUI usage and implications

The customer selects the frame view. From the frame view, the customer selects the Actions pull down menu and selects Software Upgrade, the user then selects the Configure button from the upgrade view. The upgrade wizard opens and the user selects complete upgrade (GLC FPGAs can not be prep downloaded) and clicks on the Next button. The Card Type Selection portion of the upgrade wizard is shown and the user selects GLC-12 CA Cards and may optionally chose to select GLC-32 BA Cards. The software upgrade order would be GLC-32 BA cards, GLC-12 CA cards, XDSL cards, MTA cards, DS1 cards, ABI cards, ITP cards, ITX cards, and then Supercore cards. Downgrading order would be the opposite starting with Supercore cards and ending with GLC-32 BA cards.

2.8.1.3.3 GUI size

Table 4 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
UGPF	0	1 per NE	no increase

2.8.1.3.4 GUI fields

The following table lists new or modified fields for the Upgrade Wizard invoked from the UpgradeView >

Table 5 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
GLC-32 BA Cards	New	None	N/A	Check this box to software download all GLC-32 BA cards in the office	N/A
GLC-12 CA Cards	New	None	N/A	Check this box to software download all GLC-12 CA cards in the office	N/A

2.8.1.3.5 Usage example

The following example shows the addition of the GLC-32 BA and GLC-12 CA cards to the upgrade wizard.:

2.8.1.3.6 GUI release history update

Add GLC cards to the upgrade wizard only when opened from the frame view. Since there are separate FPGA loads for each GLC PEC code, the different PEC codes for the GLCs may be selected.

2.8.1.3.7 Context sensitive launching information

In order to view the upgrade wizard and see the GLC cards, the user must have administration privileges. Also, the GLC selection boxes only appear if the customer has those GLC PEC codes in the office. For example, if the customer only has NTNY53AB cards in the system, no GLC cards are shown in the upgrade wizard. If the customer has only NTNY53BA GLC cards in the office then only the GLC-32 BA Cards selection box would appear. Only GLCs with PEC codes above NTNY53BA are shown in the upgrade wizard.

2.8.1.3.8 Supplementary information

None

2.8.2 CLUI Interface

Not applicable

2.9 User interface changes

None

2.10 OSSGate Interface Changes

None

2.11 Security

No changes

2.12 Configuration Walkthrough

Replace GLC or WLC card with the NTNY53BA version of the GLC hardware. The ITP must be running with a software load capable of allowing the software download to the FPGA on the GLC card.

Once the NTNY53BA or NTNY53CA version of the GLC is resident in the system, the FPGA for those GLCs can be attempted to be software downloaded. First, select a GLC card and open the GLC card view. Examine the FGPA configuration load to determine if the FPGA has the correct load. If the FPGA does not have the correct load, verify the GLC Administrative State is locked. Lock the card if the administrative state is unlocked. Select the action menu, select the software download manager item. A new software download view is opened. Enter the File Path (the directory path and FPGA load name on the SDM/CBM), Server IP (IP address of the SDM/CBM where the loads reside), Server userName (user name on the SDM/CBM used to software download or upgrade loads), Server password (password on the SDM/CBM used to software download). Select Download button. Once the download has completed, unlock the GLC card.

Product = MG 9000

A00012386--Media Gateway 9000 Public Key Infrastructure

Functional Description

1: Applicable Solution(s)

UA-IP

1.1 Description

This feature tracks the development and implementation of various Public Key Infrastructure features on the MG9K for IP security (IPsec).

IP security is employed to protect traffic flow between endpoints on a network. This standard protocol accomplishes this task by first authenticating the endpoint involved (verify endpoint identity) and also by encrypting the transmitted data. Public Key Infrastructure (PKI) is a standard that allows entities to establish trust relationships between endpoints and thereby aids authentication. For this feature, the MG9K IPsec interfaces will use a digital certificate to authenticate the peers with which it establishes IPsec sessions.

MG9K will use PKI to authenticate its IPsec sessions to the Element Manager (EM) and to the Gateway Controller (GWC). These channels are also known as the OAMP and signaling channels respectively.

1.2 Hardware Requirements or Dependencies

This feature is restricted to IP capable ITP controller cards.

1.3 Software Requirements or Dependencies

The Element Manager and the Gateway controller loads must be PKI capable.

1.4 Limitations and restrictions

None.

1.5 Interactions

As with previous releases, the user will use the Local Craft Interface (LCI) to configure IPsec on the DCC cards. The LCI screens were modified to allow the user to select the authentication method, the options being Pre-shared key and Digital certificate. A similar change was made to the MG9K EM VMG security view.

1.5.1 IPSec Configuration Steps DCC

The MG9K commissioned as usual with the LCI in addition the steps below to enable IPsec with PKI

1. Navigate to the DCC's IPsec Provisioning page

- Configure IKE and IPsec SA lifetimes
 - Select 'Certificate' as Authentication Method
 - Submit the request
 - Navigate to the DCC's IPsec Control page
 - Enable IPsec
2. Configure IPsec with PKI at the EM server's SSM tool (See EM doc for Details)
 3. Add the MG9K node data at the EM provisioning view (See EM doc for Details)
 - Tab the Node Security view
 - Submit a request to download a digital certificate to the MG9K
 4. Continue with the normal discovery process

1.5.2 IPsec Configuration Steps VMG

1. Provision IPsec policies at the GWC with certificate, in FLEX mode
2. Create VMG at the Switched line Services View in the MG9K EM
 - At the GW Security Tab configure IKE and IPsec SA lifetime
 - Select Authentication method as Certificate
 - Submit the request
 - Turn Admin state 'ON'
3. Once IPsec is operational switch the GWC FLEX policy to secure mode

1.5.3 Trouble Shooting

Once the system is operational, if the EM loses connection to the MG9K the user can launch the remote LCI

from the EM GUI. The LCI can then display current alarm status of the MG9K. IPsec and other alarm information can also be displayed.

Refer to the MG9K EM doc for SSM trouble shooting procedures.

The screenshot shows a web browser window titled "MG 9000 - Microsoft Internet Explorer provided by Nortel Networks". The page has a dark blue header with the Nortel Networks logo on the left. In the center of the header are the labels "N.E." and "Net.Interface" with a small orange "m" icon below "N.E.". On the right of the header is the text "Voice over IP" and two buttons: "Connections" (green) and "Maintenance" (blue). Below the header, the main content area has a dark blue background. On the left, it says "Frame #0 Shelf #0 Selected" and "select a shelf view below:" with a button labeled "frame #0 shelf #0". To the right of this is a vertical label "FRAME" and a large horizontal slot containing a grid of 16 vertical bars. The 10th bar from the left is highlighted with an orange "m" icon and a small orange triangle below it. Below the grid, the text "DCC" is visible. The main section is titled "OAMP IPsec Provisioning" in white. It contains several input fields and buttons: "Peer IP Address" (47.142.101.137), "Authentication Method" (Certificate), "IKE Lifetime" (3600), "Unit" (SEC), "IPsec Lifetime" (3600), "Unit" (SEC), "Shared Key" (masked), "Confirm Shared Key" (masked), "Submit", "Query", "SSH Host Key Fingerprint" (empty), and "Query". The bottom of the browser window shows a status bar with "Done", a lock icon, and "Internet".

The LCI will also display alarms for digital certificates that are within 4 Days of expiration, that has expired or otherwise invalid. The procedures for clearing these alarms are described in the Element Manager document PKIMgr_opten.fm.

1.5.4 Transitions between IPsec authentication modes:

1.5.4.1 Background:

The MG9K IPsec feature supports 2 authentication modes Preshared Key and digital certificate.

Whatever the cause, there are situations where the need will arise to change the authentication mode from one to the other without loss of service.

This capability is aided by the following list.

- Node managers, MG9K EM and GWC, can simultaneously be configured to support either modes.
- Whereas the MG9K can only be configured in one mode or the other.

Transitions are done by first ensuring that both authentication modes have been configured on device manager. Once the manger is configured to support the new mode, the craft person then uses the LCI or VMG security screen to select the authentication mode on the MG9K.

Therefore general steps needed to transition an IPsec link would first include configuring the manager device with the new mode, then matching it on the MG9K.

1.5.5 OAMP Link: Transition from PSK to Digital Certificate:

Initial condition: Link operational, secured, and authenticate via a PSK

1. Add a digital certificate transform at the MG9K EM server with the SSM tool (See MG9K EM documentation for details)
2. At the EM node Property view (See MG9K EM documentation for details)
 - Select the security tab
 - Click the download digital certificate button (this requests and downloads a certificate to the MG9K)
3. Use MG9K LCI
 - Navigate to active DCC IPsec provisioning tab
 - Select Certificate as authentication mode
 - Check IPsec operation (at the IPsec control page) state to ensure success
 - Check alarms for IPsec alarms. Trouble shoot the alarm (at LCI alarm browser) to resolve the problem. Otherwise, revert DCC to PSK mode.

If the OAMP link goes down (Alarm at the EM) revert DCC to PSK mode, then troubleshoot the alarm

4. On a successful transition the user has the option to delete the PSK transform at the SSM (See MG9K EM documentation for details)

1.5.6 OAMP Link: Transition from Digital Certificate to PSK:

Initial condition: Link operational, secured, and authenticate via a Digital Certificate

1. Add a PSK transform at the MG9K EM server with the SSM tool (See MG9K EM documentation for details)
2. Enter a PSK
3. Use MG9K LCI
 - Navigate to active DCC IPsec provisioning tab
 - Select PSK as authentication mode
 - Enter the same PSK entered in step 1
 - Check IPsec operation (at the IPsec control page) state to ensure success
 - Check alarms for IPsec alarms. Troubleshoot the alarm (at LCI alarm browser) to resolve the problem. Otherwise, revert DCC to Certificate mode.

If the OAMP link goes down (Alarm at the EM) revert DCC to Certificate mode, then troubleshoot the alarm

4. On a successful transition the user has the option to delete the Certificate transform at the SSM (See MG9K EM documentation for details)

1.5.7 VMG Callp Link: Transition from PSK to Digital Certificate

Initial condition: Link operational, secured, and authenticate via a PSK

1. Request a digital certificate for the GWC using the CS2K SESM tool (See CS2K documentation for details)
2. Add a digital certificate transform at the GWC with the SESM tool (See CS2K documentation for details)
3. At the EM node Switched Lines view (See MG9K EM documentation for details)
 - Select the GW security tab
 - Click the download digital certificate button (this requests and downloads a certificate to the VMG)
 - Select the authentication mode as Certificate and submit the request
4. Check IPsec operation (at the IPsec control page) state to ensure success

5. Check for IPsec alarms. Troubleshoot the alarm (alarm browser) to resolve the problem. Otherwise, revert the VMG to PSK mod
6. On a successful transition the user has the option to delete the PSK transform at the GWC (See MG9K EM documentation for details)

1.5.8 VMG Callp Link: Transition from Digital Certificate to PSK:

Initial condition: Link operational, secured, and authenticate via a Digital Certificate

1. Add a PSK transform at the MG9K EM server with the CS2K SESM tool (See CS2K documentation for details)
2. Enter a PSK
3. Use MG9K EM Switched Lines view
 - Navigate to active GW Security tab
 - Select PSK as authentication mode
 - Enter the same PSK entered in step 1
 - Check IPsec operation (at the IPsec control page) state to ensure success
4. Check for IPsec alarms. Trouble shoot the alarm (alarm browser) to resolve the problem. Otherwise, revert VMG to Certificate mod
5. On a successful transition the user has the option to delete the Certificate transform at the GWC (See CS2K SESM documentation for details)

1.5.9 Downgrade to 9.0 or 8.0

If Ipsec is enabled with Digital certificates the node must first be converted to PSK mode and the pre-shared keys entered.

1.6 Glossary

Term	Description
PKI	Public Key Infrastructure

Product = SIP Lines

A00012326--SIP Lines: Authentication and Authorization account codes

Functional Description

1: Applicable Solution(s)

CHS

1.1 Description

The Account code functionality allows a subscriber to enter a billing number into a Station Message Detail Recording (SMDR) record for charge-back purposes.

An authorization code is a specified set of digits assigned to and used by station end users. These codes can range in length from 2 to 14 digits. When set, the length does not change for the customer group. Authorization codes provide cost control. These codes control access to specified networks. Authorization codes raise or lower the network class of service (NCOS) of a call.

This feature supports Account/ Auth Codes Flash Entry for SIP Lines.

1.2 Hardware Requirements or Dependencies

Not applicable

1.3 Software Requirements or Dependencies

Not applicable

1.4 Limitations and restrictions

The following limitations and restrictions:

- When a call is in progress, and we try to dial Acct/Auth code in a new session, if the client starts a conference call, then the tones provided will be heard in the conference.
- Multiple call appearances are not supported.
- In case the Originator is SIP ONT, the special dialtone received when the originator dials Account/Auth FAC/VSC, is provided by the PMA and not the ONT.
- Account codes can range from 2 to 14 digits in length. The length of the account code is the validation method in the North American and the Canadian market.
- The reset dialing does not work if the STARACPT suboption is set to Y and the account code is entered voluntarily.
- The STARACPT subfield is set to N for the Asia Pacific CALA markets.
- The account code validation is by content when subfield STARACPT is set to N.

- The log AMAB150 displays a blank space for the asterisk as the valid digit for the voluntary account code.
- The functionality for POTS digit collection applies to the voluntary account code activation only.

1.5 Interactions

A description of the interactions between Acct/Auth codes flash entry and other functionalities appear in the following paragraphs.

- If the invoker of ACCT/AUTH or the connected party is being verified by the Operator, verified by the Operator, the request is denied. ACCT/AUTH is not permitted if an Operator Busy Line Verification (BLV) connection exists.
- In case of analog clients like the ONT where one call is already established and a new session is initiated to enter the FAC followed by the prompt for account/auth code, if the user invokes a client based conference, then the first session would hear the DN prompt and RODR treatment before the second leg is collapsed.

1.6 Glossary

Term	Description
FAC	Feature Activation Code
VSC	Vertical Service Code

2: Fault Management for A00012326

2.1 Fault management strategy

The fault management information is provided using LOGs. The LOGUTIL CI provide the access to the LOGs generated. The LOGs are generated based on LOG framework. This feature uses the existing framework to add new LOGs.

2.2 Fault management tools and utilities

2.2.1 Faults, Alarms and Logs

The LOGUTIL CI command is used as tools in the CS2K Core software. All existing tools and utilities are applicable in case of CS2K software.

2.3 Logs (For CS2K only)

The following reasons have been added in the existing LOG IBN110 as part of this activity.

- AUTH_ACCT_ON_MULTIPLE_SESSIONS: Reason added to LOG IBN110. It is generated when Multiple sessions are present while invoking the Acct/Auth codes flash entry feature.
- BLV_IN_PROGRESS: Reason added to existing LOG IBN110. It is generated if the invoker of ACCT/AUTH or the connected party is being verified by the Operator.

2.4 Log Title/Log ID, Log Reason: IBN110, AUTH_ACCT_ON_MULTIPLE_SESSIONS

2.4.1 Formats

```
<Switch ID> IBN110 <DATE> <TIME> INFO AUTH_ABUSE  
<LEN> <DN> <KEY>  
TYPE=AUTH ACCT ON MULTIPLE SESSIONS  
<CUSTOMER_GROUP>  
<DIGITS_DIALLED>
```

Example:

```
RTPT08BM   IBN110 SEP29 11:25:56 0425 INFO AUTH_ABUSE  
SS 00 0 00 27  DN 6136215077  KEY 1  
TYPE = AUTH ACCT ON MULTIPLE SESSIONS  
CUSTOMER_GROUP =      IBNTST  
DIGITS_DIALLED = BB
```

2.4.1.1 NTSTD

Not Applicable

2.4.1.2 SCC2

Not Applicable

2.4.1.3 Syslog

Not Applicable

2.4.1.4 SNMP

Not Applicable

2.4.2 Explanation

Description: This log provides information regarding behavior of Acct/Auth codes flash entry on Multiple sessions (More than 2 sessions). When multiple sessions are present, this log is generated to indicate that Acct/Auth codes flash entry is not allowed.

2.4.3 Field descriptions

Field	Value	Description
TYPE	AUTH ACCT ON MULTIPLE SESSIONS	This reason in AUTH_ABUSE_KIND indicates why the LOG has been generated.

2.4.4 Associated Operational Measurements or Performance Measurements

None

2.4.5 Additional information

None

2.5 Log Title/Log ID, Log Reason: IBN110, BLV_IN_PROGRESS

2.5.1 Formats

```
<Switch ID> IBN110 <DATE> <TIME> INFO AUTH_ABUSE  
<LEN> <DN> <KEY>  
TYPE=BLV IN PROGRESS  
<CUSTOMER_GROUP>  
<DIGITS_DIALLED>
```

Example:

```
RTPT08BM   IBN110 SEP29 11:25:56 0425 INFO AUTH_ABUSE  
SS 00 0 00 27  DN 6136215077  KEY 1  
TYPE = BLV IN PROGRESS  
CUSTOMER_GROUP =      IBNTST  
DIGITS_DIALLED = BB
```

2.5.1.1 NTSTD

Not Applicable

2.5.1.2 SCC2

Not Applicable

2.5.1.3 Syslog

Not Applicable

2.5.1.4 SNMP

Not Applicable

2.5.2 Explanation

Description: This log provides information regarding interaction of Acct/Auth codes flash entry with BLV. This log is generated to indicate that Acct/Auth is not permitted if an Operator Busy Line verification (BLV) connection exists.

2.5.3 Field descriptions

Field	Value	Description
TYPE	BLV IN PROGRESS	This reason in AUTH_ABUSE_KIND indicates why the LOG has been generated.

2.5.4 Associated Operational Measurements or Performance Measurements

None

2.6 Alarms

Not Applicable

Product = SIP Lines

A00012402--911 Hold/Ringback support on SIP Lines

Functional Description

1: Applicable Solution(s)

CHS

1.1 Description

1.1.1 Overview

This activity will implement the support for the following two E911 features on SIP Lines in SN09:

- E911 Network Hold
- Ringback

The scope of this feature is provide implementation of the above mentioned features on SIP Lines for two types of SIP User Agents. First being a 911 Enabled SIP UA, such as an ONT (Optical Network Terminal) and the second being a generic SIP Client with no support for 911 specific behavior.

1.1.2 Brief description of 911 Hold and Ringback features

- **E911 Network Hold**

The Network Hold feature provides the ability to hold the Network of the 911 call in the event that the Network goes on-hook prior to disconnect from PSAP operator. If the Network Hold is present in the network the PSAP operator will

hear a tone to indicate that a caller has gone on-hook and the hold has been activated.

The session and the call resources will be held in the network until either:

- The PSAP operator releases the call.
- SIP Client reconnects to the original 911 session.
 - For 911 Enabled SIP Users, since the session is also put on hold in the client, the client will be reconnected to the 911 session as soon as the off-hook is detected.
 - In case of other generic SIP UAs, where all the media resources have been released, the user will be reconnected to the prior 911 session only when he attempts to make a new call.

In the CS2000 Network the Network Hold is controlled by the ORIGHOLD subfield provisionable on the E911 incoming trunks to the E911 Tandem. Both MF and ISUP IT with the E911 Option trunks provide the support for Network Hold.

Example of ORIGHOLD option datafilled on the ISUP IT incoming trunk to the E911 Tandem is as follows:

TABLE: TRKGRP >pos e911ics7 E911ICS7 IT 0 ELO NCRT IC NIL MIDL 613 AT1 NSCR 613 613 000 N N (E911 0747 113 E911_STD N Y 0 0 Y) \$

ORIGHOLD bool

- **Ringback**

Gives the E911 PSAP operator the ability to ring the 911 caller back who has gone on-hook and who is being held by the Network Hold Feature. It also provides the ability to, at any point, send the receive off hook (ROH) to the caller's phone set which is off hook.

Ringback is controlled by the RBACK feature option assignment in the E911 Tandem found in table IBNXL A.

1.1.3 E911 Call Setup.

1.1.3.1 E911 Call Setup with 911 Enabled as the SIP UA.

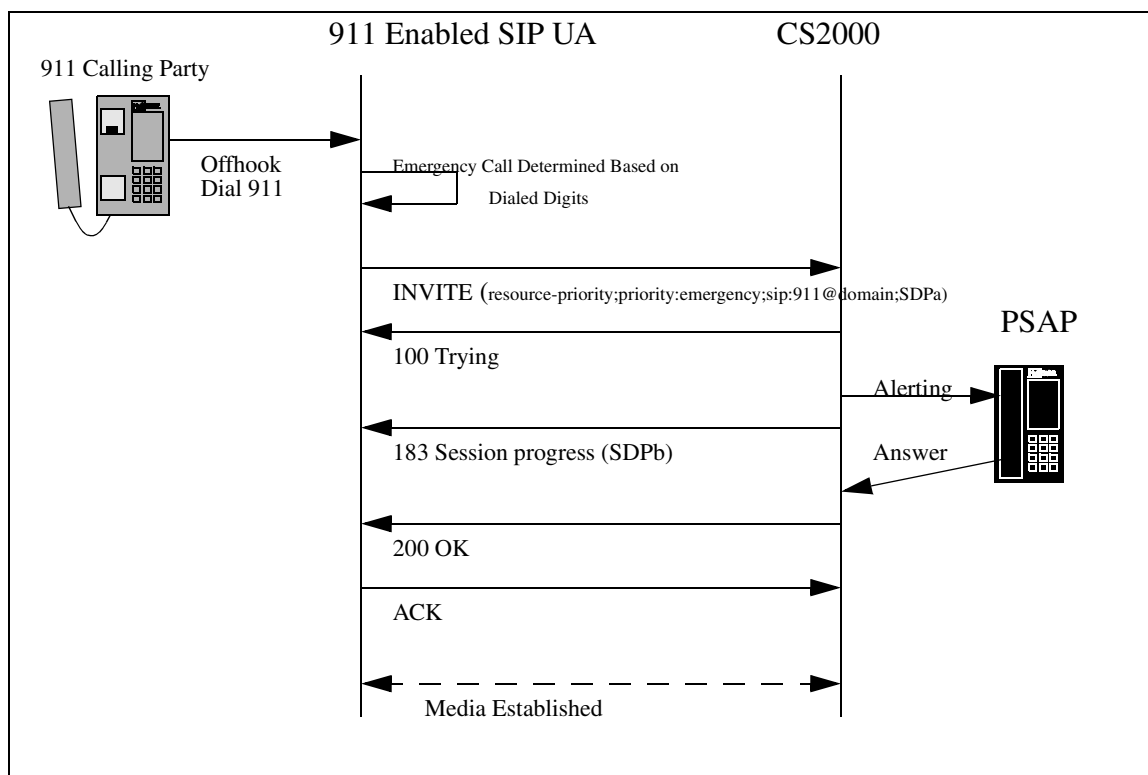
911 Enabled SIP UA Dial plan specifically identifies the digit string '911' as an Emergency call. For such calls a combination of "Resource-Priority" and "Priority:Emergency" headers will be included in all sip INVITE messages sent to and received from the CS2000.

The Priority Header provided by the SIP UA client in the initial INVITE and all subsequent INVITEs will allow the CS2000 to differentiate between the 911 Enabled and generic SIP clients. The differences in 911 call processing by having Priority Header included in INVITE messaging are as follows:

- During the initial call setup, INVITE messages received with Resource and Priority Headers will receive preferential handling by CS2000 Overload Controls and thus will be less likely to be rejected during overload times.
- INVITE with a 0 SDP and a Resource and Priority Headers received from a 911 Enabled SIP UA will be handled as a “Network Hold” Request for the 911 session and processed as such. The session and all its resources will be put on hold.
- An INVITE with 0 SDP and with NO Priority Header received during an established 911 session will be handled as a regular hold request (which are not supported on 911 calls) and thus will be denied. CS2000 will respond with a 403 Forbidden message to deny the request. Figure 5 illustrates the message flow.

Figure 1 illustrates the messaging exchange occurring during the setup of the E911 Call when 911 Enabled SIP US is present in the network.

Figure 1 911 Call Setup with 911 Enabled SIP UA

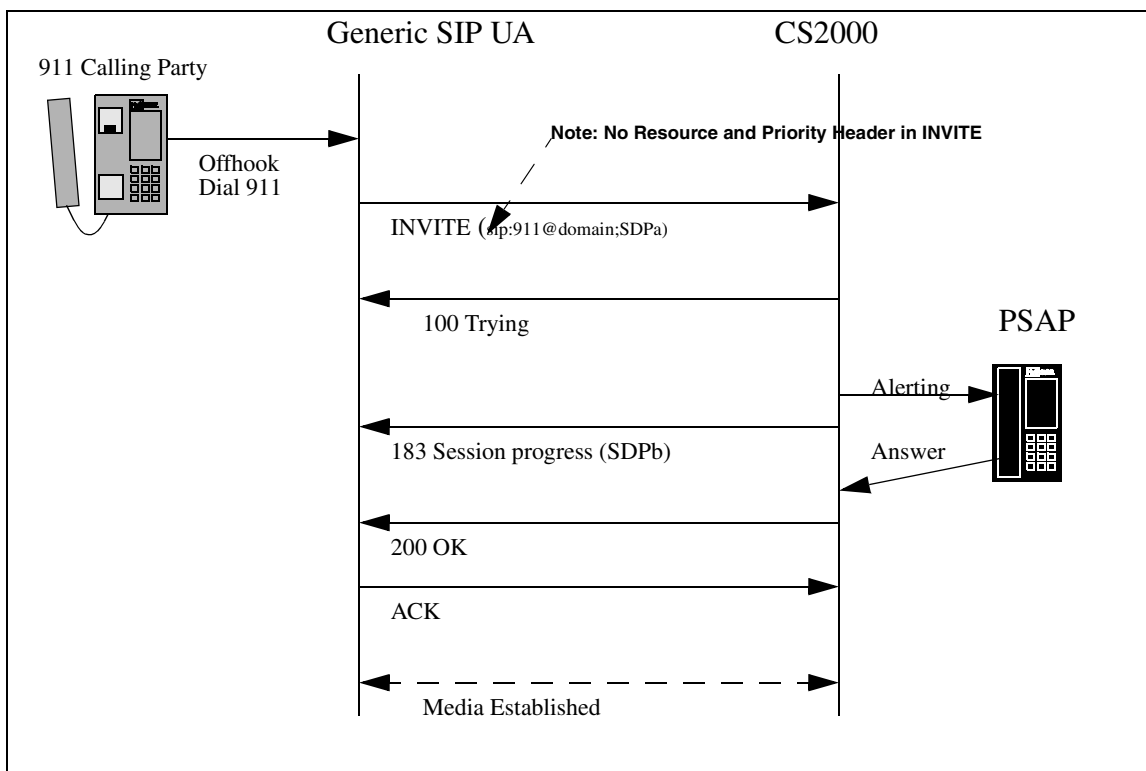


1.1.3.2 E911 Call Setup with a Generic SIP UA

Figure 2 illustrates the messaging exchange that occurs during the setup of the E911 call with a generic SIP UA. In contrast with the messaging received from the 911 Enabled SIP UA, there is no Resource-Priority and Priority:Emergency Headers in the sip INVITE received by the CS2000.

The main impact of not having these headers during the initial 911 call setup, is that the 911 call will NOT receive any preferential treatment from the CS2000 during the call setup stage.

Figure 2 911 Call Setup- Generic SIP UA



1.1.4 Caller Disconnect Message Handling

1.1.4.1 911 Caller Disconnect on 911 Enabled SIP UAs

Call flow in Figures 3 illustrates the disconnect/ message handling on the 911 Enabled SIP UA. The Handling of an invalid hold request is shown in Figure 4.

Upon detecting on hook from the 911 user, the SIP UA maintains all call resources and places the session on hold. An INVITE with 0 SDP and a combination of resource and priority headers is sent to CS2000 to request the session to be held. In the event that these headers are not included in the INVITE with 0 SDP, the hold request will be denied by the CS2000 and a sip 403 will be returned. See Figure 4.

Once the session has been successfully put on hold, it will remain on hold until either the PSAP operator disconnects, or the 911 caller tries to re-connect to the session.

While the session is on hold, any incoming calls to the SIP user will receive BUSY Tone.

Figure 3 Disconnect Handling on the 911 Enabled SIP UA

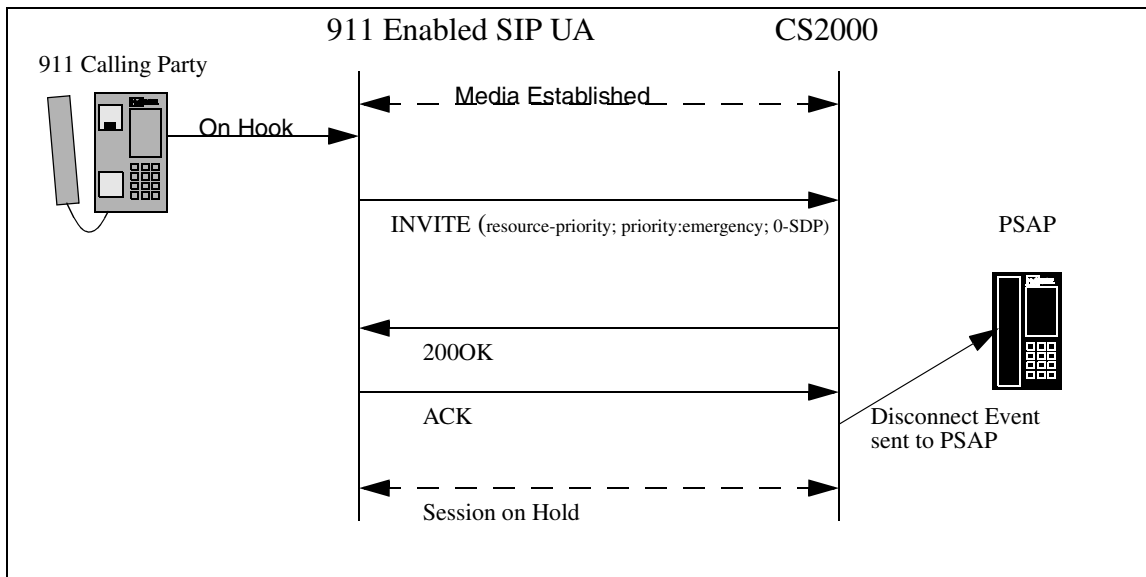
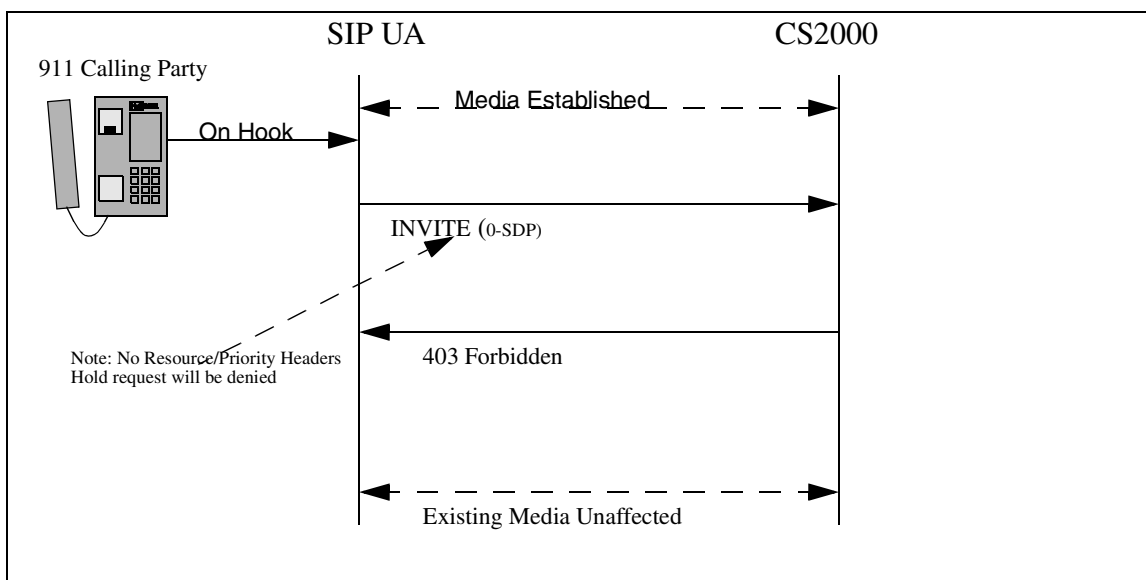


Figure 4 Invalid Hold Request



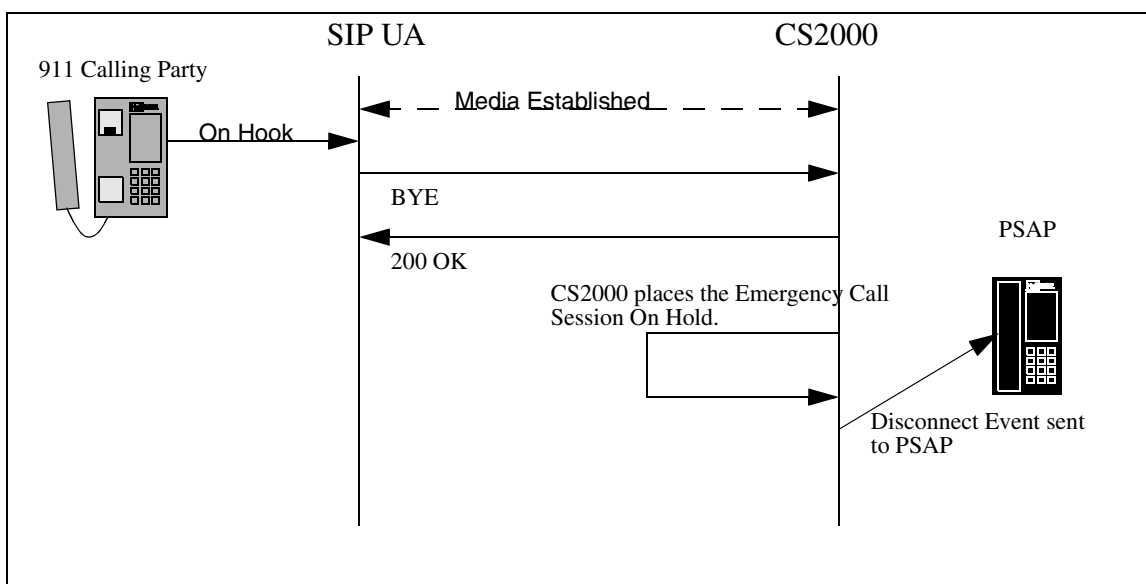
1.1.4.2 911 Caller Disconnect - Generic SIP UA Scenario

For generic SIP clients the user disconnect handling is illustrated in Figure 5. Typically SIP UAs don't have the logic to differentiate between 911 and regular calls and thus will take their media resources down as soon as the on-hook from the set is detected but prior to sending the BYE to the CS2000. This behavior makes it necessary for CS2000 to support the sip BYE message as a request for network hold. Upon receipt of the BYE message the CS2000 session resources would be placed on hold and the PSAP operator notified of user's disconnect.

The session resources on the CS2000 will be held until either the PSAP operator disconnects, or the 911 caller goes off-hook and tries to originate a call.

While the session is on hold, any incoming calls to the SIP user will be sent to BUSY treatment.

Figure 5 Disconnect Handling - Generic SIP UA



1.1.5 Reconnect Following Activation of Network Hold

The 911 caller can “reconnect” to the existing 911 session by either of the following methods:

- If the SIP UA is 911 Enabled, simply going off-hook will re-establish the 911 session.
- In the Generic SIP UA scenario, the user will need to go off-hook and attempt to originate a call. SC2000 will respond to the incoming INVITE by reconnecting the client to the previous session.

Figures 6 and 7 illustrate the possible message flows for the reconnect scenarios.

Figure 6 Reconnect Handling with 911 Enabled SIP UA in the Network

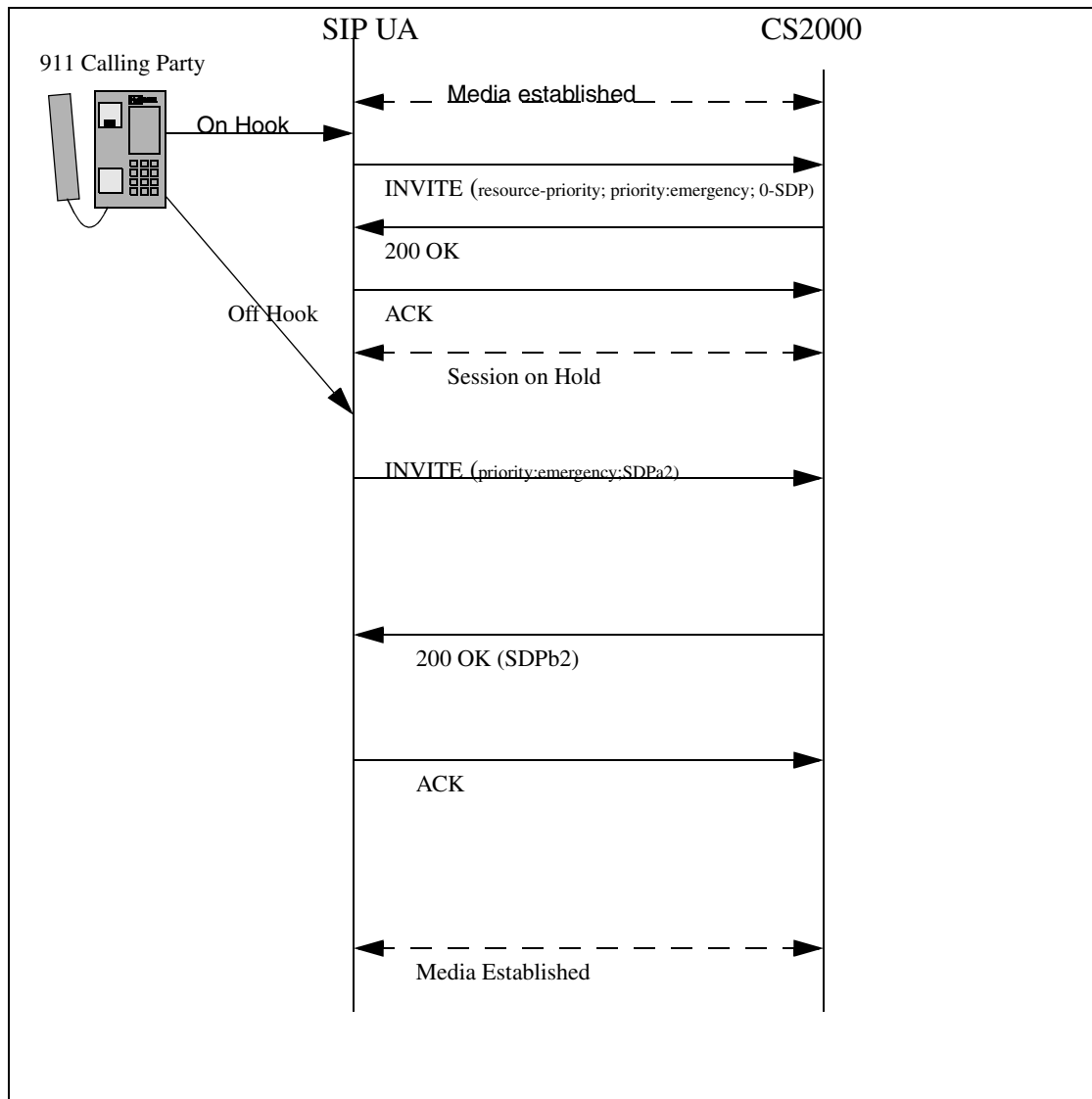
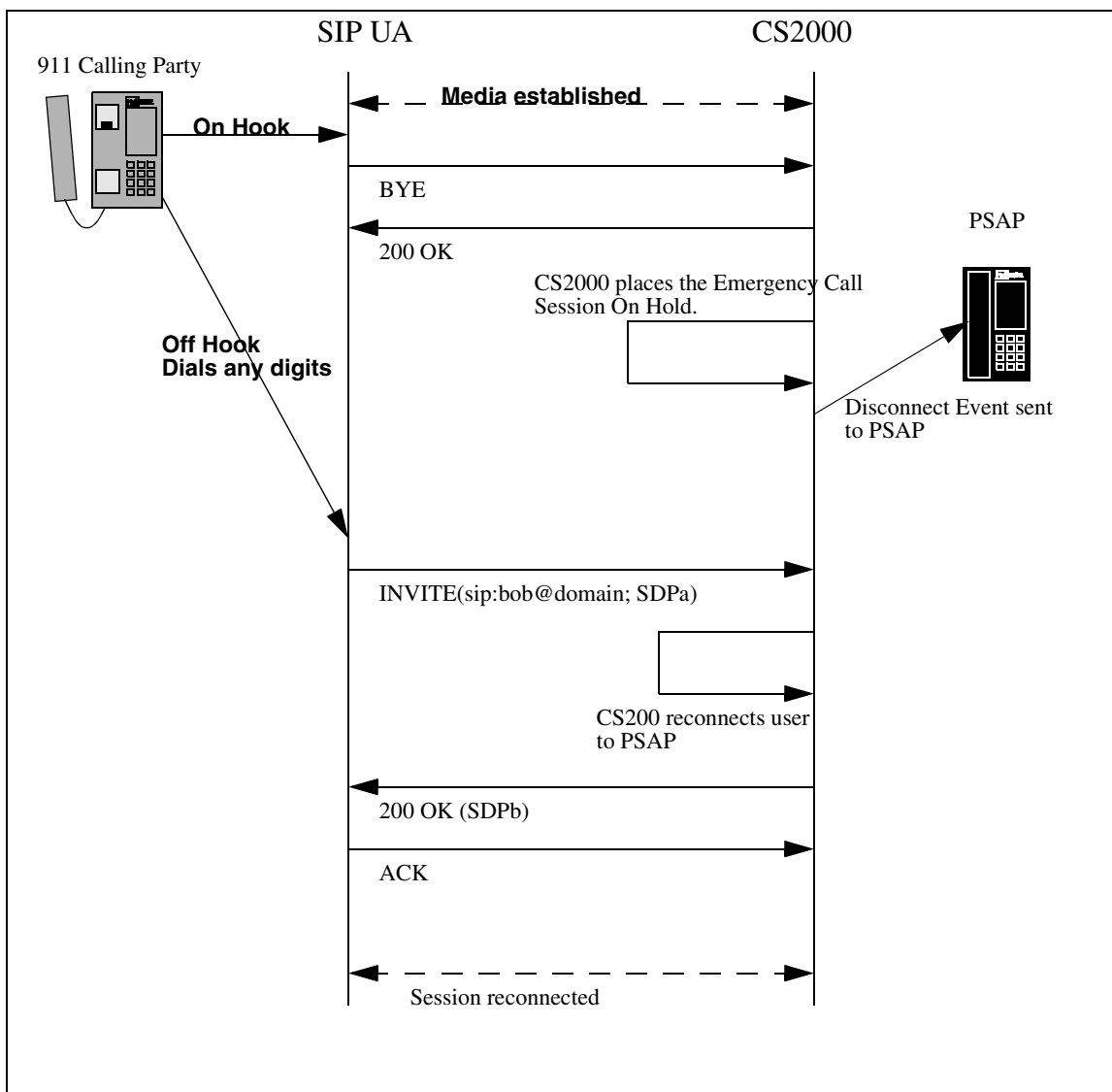
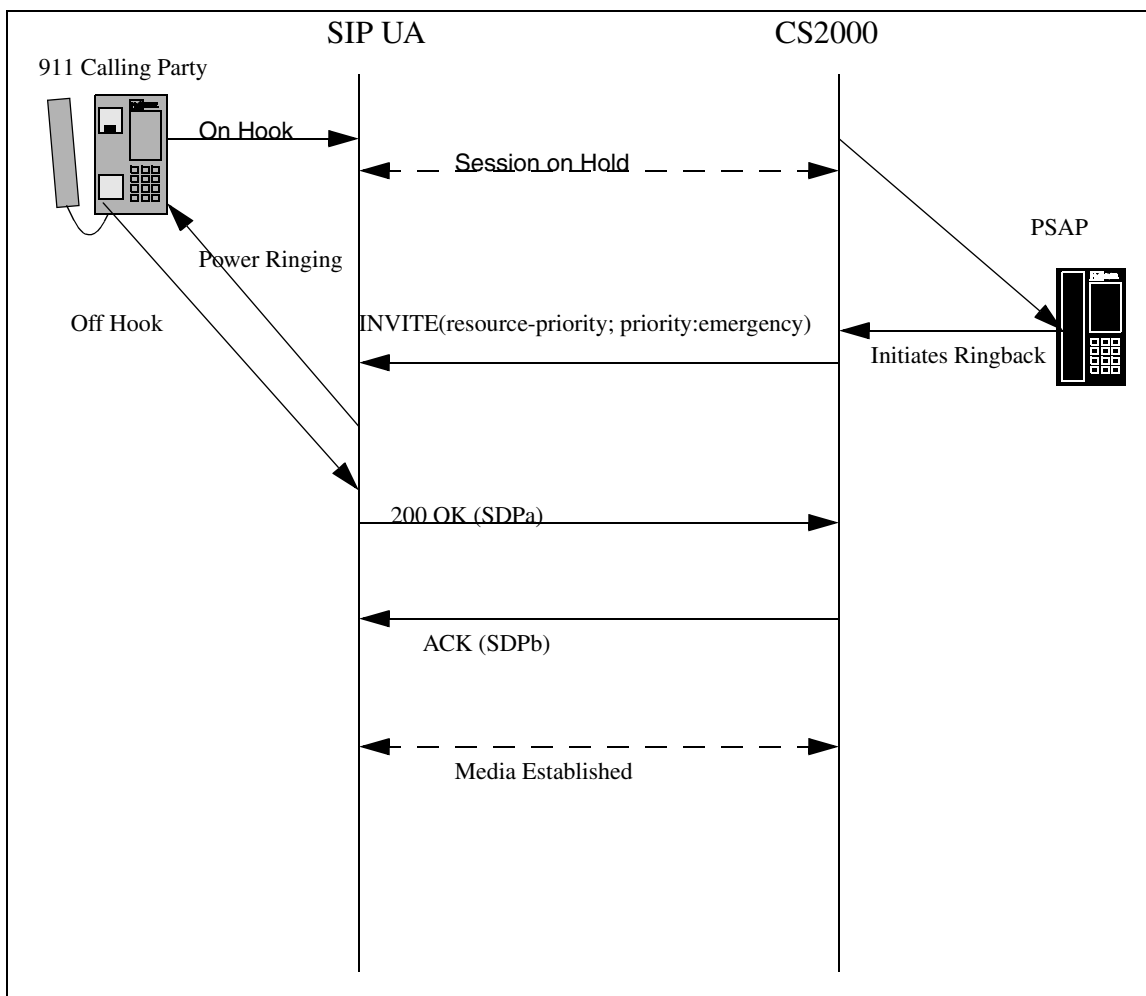


Figure 7 Reconnect Handling - Generic SIP UA

1.1.6 Ringback Activation following Network Hold

At any point while the call is being held the E911 PSAP operator can ring the 911 caller back. Once Ringback is activated, the CS2000 restores the held session and the SIP UA applies power ringing to the user's set.

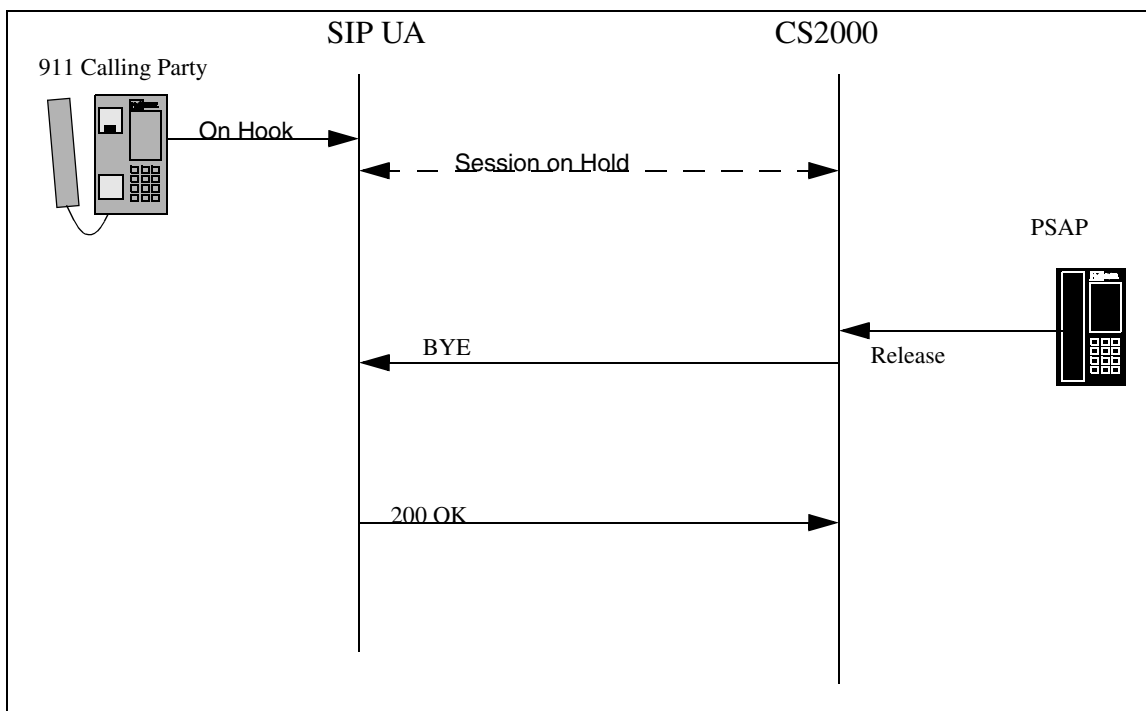
Once the session is placed on hold, there is no difference in the message flows between the 911 Enabled SIP UA and other SIP UAs.

Figure 8 Ringback Handling in the Network

1.1.7 PSAP Disconnects following Network Hold

At any point while the call is being held the E911 PSAP operator can disconnect the session by going on hook

Figure 9 illustrates a Release received from the PSAP following the onhook from the SIP UA.

Figure 9 PSAP Disconnect Handling in the Network

1.2 Hardware Requirements or Dependencies

No new hardware dependencies are introduced beyond the general requirements for SIP Lines

1.3 Software Requirements or Dependencies

In addition to the general software requirements for SIP Lines and E911, this feature also introduces the support for the 911 Enabled SIP UA. Such a SIP UA differs from other Agents in that it has the smarts to identify emergency calls and handle them accordingly.

911 Enabled SIP UA's Dial plan specifically identifies the digit string '911' as an Emergency call. For such calls the "Resource-Priority" and "Priority:Emergency" Headers will be included in all sip INVITE messages sent to the CS2000.

The 911 Enabled SIP UA Service Profile will have the following provisionable boolean parameter: Emergency Call On-Hook Hold. If On-Hook Hold is set to true, then the on-hook from the 911 caller will be treated like a call hold and all session resources will be held. Once the On-Hook is detected an INVITE with the "Resource-Priority" and "Priority:Emergency" Headers and 0 SDP will be sent to CS2000 to request the hold.

Since PSAP can at any point request to alert the caller, the 911 Enabled SIP UA will either provide a distinctive power ringing if the Network's set is off-hook or a "howler" tone if the set is on-hook.

1.4 Limitations and restrictions

- In case where a BYE message is received from SIP UA and the session is being held in the CS2000, simply going off hook by the user will not cause the session to be reconnected. The user will need to dial digits and an INVITE (sip:cdn@domain) will need to be received by CS2000 in order to reconnect the user to the PSAP operator.
- This activity does not provide support for Enhanced Call Party Hold (ECPH) feature, thus the ECPH timer in the E911 Tandem needs to be set to 0.
- This feature does not provide support for Hold and Ringback over VFG facilities.

1.5 Interactions

CS2000 will require the "911 Enabled" SIP UAs support all behaviors outlined above.

1.6 Applicable customer facing sections

none

1.7 Glossary

Term	Description
FTTP	Fiber-To-The-Premises
E911	Enhanced 911
UA	User Agent
PSAP	Public Safety Answering Point
ROH	Receive OffHook
911 Enabled	Optical Network Terminator
SIP	Session Initiated Protocol

Product = SIP Lines

A00012403--Data Protection for SIP Lines

Functional Description

1: Applicable Solution(s)

CHS

1.1 Description

This feature inherits all functionality from legacy lines.

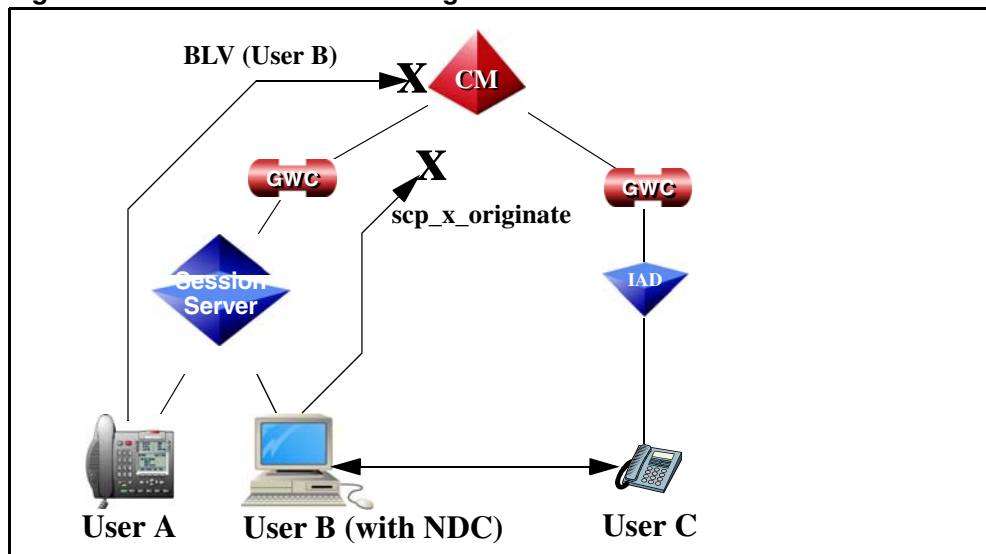
Data protection prevents interruption or mutilation of data calls caused by the application of warning tones and voice energy associated with attendant camp-on, busy verification, busy override and call waiting.

Data protection is provided by assigning the No Double Connect (NDC) option to a line. A line assigned NDC, cannot use the call transfer, or any of the conference features, nor participate when invoked from another subscriber. This option prevents the user of such a line from providing access to data or to computers from other, possibly unauthorized lines.

The NDC option is activated/deactivated via Data Modification Order (DMO).

No Double Connect (NDC) option has two roles: First is to prevent a user with NDC assigned from making multiple calls, Second is to ensure any feature that is incompatible with NDC does not operate on a user with NDC option.

Figure 1 Functional Behavior Diagram



User B (with NDC option) is in a call with User C. User A is prevented from activating a feature (e.g. Busy Line Verification) against User B. User B is prevented from making a new origination.

1.2 Hardware Requirements or Dependencies

None.

1.3 Software Requirements or Dependencies

None.

1.4 Limitations and restrictions

The NDC option is not compatible with the following line options:

This component is to validate the feature is compatible with the No Double Connect (NDC) option. Certain features cannot be assigned to a line with NDC option. These features are as follows:

3WC, 3WCPUB, CHD, CNF, CRT,CWD, CWI, CWO, CWT, CWTC, CWX, CXR, DCBX, DSCWID, FXR, HLD, LDSA, LDSO, LDSR, LDST, LNPTST, MPB, PCWT, PRK, VOWDN¹.

Incompatibility is assigned through table OPTOPT.

1.5 Interactions

Camp-on is not compatible with stations that have NDC assigned. If the customer group parameter is camp-on with tone, camp-on will not apply to stations assigned option NDC.

Call Transfer and Blind Call Transfer is not compatible with NDC.

Busy Verification is denied to stations assigned NDC.

Call Waiting, Call Waiting Origination, and Dial Call Waiting are incompatible with lines assigned NDC option.

Directed Call Pickup-Barge In is incompatible with lines assigned NDC option.

Executive Busy Override, also known as Executive Right of Way, Executive Busy Override, Executive Override, Override, Break-In, Barge-In, is incompatible with lines assigned NDC option.

Trunk Busy Verify is incompatible with NDC option, when the busy circuit is connected to a line with NDC option.

Click to Call, and PA Simring are not compatible with NDC. (These services must have 3WC option).

¹ See Glossary for Definition.

When the client device is programmed with 3xx/Redirect/Call Forward All, the NDC check will be made against the client as well as the target to which the redirect occurs.

1.6 Applicable customer facing sections

Fault Management

Logs x_____

Alarms _____

Configuration

Data Schema _____

User Interface _____

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

1.7 Glossary

Term	Description
New term	Definition
3WC	Three Way Calling. The 3WC option allows the subscriber, on the assigned line, to place a call on hold. When the call is on hold, the subscriber can set up a request call to another subscriber. The subscriber that initiates the three-way call can switch speech paths between the held party and the talking party. The subscriber can connect all parties into a three port conference. When the three way call is in progress, the subscriber can drop the conference. When the subscriber drops the conference, the subscriber connects to a single-party call again.
3WCPUB	Three Way Calling Public Announcement. The 3WCPUB option allows all parties on a call extension from a 50B customer premises system (CPS) to bridge together. The parties do not wait for the controlling party to flash all the parties together.

Term	Description
CHD	Call Hold. The Call Hold (CHD) option allows a subscriber with a 500/2500 set to hold a call. If a party does not go off-hook, the subscriber can hold a call for any period of time. When this action occurs, the station with CHD can perform other tasks. These tasks include speed call programming or call pickup, as a call holds. The subscriber can only put one call on hold at a time.
CNF	Station Controlled Conference. The station Controlled Conference (CNF) option allows a station to have a conference call to a maximum of 30 parties. With the CNF option, the station does not require the help of an attendant for a conference call to a maximum of 30 parties. The members of the conference can belong to the same customer group or belong to different customer groups. The members also can belong to a station on a trunk. The JOIN option works with CNF to add a held party to a conference without having to hang up and redial the held party. CNF is a prerequisite to adding JOIN to the business set.
CRT	Call Redirect. Call Redirect (CRT) provides residential subscribers with the ability to transfer calls to a predefined routing directory number (DN) or to a voice mail DN. The transfer occurs when the subscriber flashes and dials the CRT access code during an established two-party call. After successful feature activation, the subscriber receives a confirmation treatment. Only the terminator in a two-party call can activate CRT. After activating, the terminator becomes the CRT controller.
CWD	The Dial Call Waiting (CWD) option allows a business set user to impose call waiting on a busy station. The busy station can be a 500/2500 set or a business set with a call waiting (CWT) feature key.
CWI	The Call Waiting Intragroup (CWI) option allows a subscriber to apply the CWT option to intragroup calls, in addition to those allowed with CWT.
CWO	The Call Waiting Originating (CWO) option allows an originating line to impose a call waiting tone automatically on a busy line.
CWT	The Call Waiting (CWT) option allows the system to alert a busy station when an incoming call attempts to reach the directory number (DN).
CWTC	The Call Waiting Conference (CWTC) option allows the subscriber to conference a waiting party.
CWX	The Call Waiting Exempt (CWX) option does not allow Dial Call Waiting (CWD) and Call Waiting Originating (CWO) to interrupt a business set user.
CXR	The call transfer option (CXR) allows the assignment of a call transfer type other than the type that the customer group has.

Term	Description
DCBX	The Directed Call Pickup Barge-In Exempt (DCBX) option allows a station to block the attempts of other stations with DCBI assigned to barge in.
DSCWID	Deluxe Spontaneous Call Waiting Identification (DSCWID) allows the subscriber to receive calling-party information during call waiting. The subscriber also receives this information with basic SCWID. The DSCWID presents the subscriber with a set of option to treat the incoming calls. These options include the following: - Answer the new call and put the current call on hold. - Disconnect the call. Answer the new call. - Forward the new call. - Connect the new call to a busy announcement. - Conference the new call with the current call.
FXR	The Fast Transfer (FXR) option reduces the number of keystrokes required to transfer a call. The user does not need to conference all parties before the user transfers calls.
HLD	The Permanent Hold (HLD) option allows a single-line set to put an active call on hold and return the handset to the handset cradle. The party on hold hears a ringback tone, a recorded announcement, music, or silence.
LDSA	The long distance signal activate (LDSA) line option (activation code *49 or 1149) allows the end user to activate or deactivate Long Distance Alerting (LDA) on a line. The operating company personnel can assign the LDSA line option through SERVORD.
LDSO	The Long Distance Signal Option (LDSO) option provides Long Distance Alerting (LDA) subscribers with a different ring and a different tone.
LDSR	The Long Distance Signal Ringing (LDSR) option provides Long Distance Alerting Enhancement (LDAE) subscribers with a distinctive ring when the subscriber line is idle.
LDST	The Long Distance Signal Tone (LDST) option provides Long Distance Alerting Enhancement (LDAE) subscribers with a distinctive ring when the subscriber line is busy.

Term	Description
LNPTST	The system assigns the local number portability test (LNPTST) option to a single-party residential (1FR RES) line to allow a local number portability (LNP) test call. The system assigns this option through SERVORD. The SERVORD blocks subscription to this option by any other type of line. The only line option compatible with LNPTST is Digitone (DGT). The SERVORD does not allow assignment of LNPTST and line options that are not compatible on the same line.
MPB	The Multi-Party Bridging (MPB) option allows a multi-party group with a maximum of four subscribers with a different line equipment to associate in a multiparty group. The liens appear to the subscribers to be different parties of a multiparty line. Each member of a MPB group has a different directory number and a different line equipment number. The MPB option creates a bridge among subscriber lines that wires cannot bridge. Wires cannot bridge subscriber lines because these lines do not have analog appearance in the central office. An example of these lines are lines that connect to an integrated digital loop carrier.
PCWT	The Precedence Call Waiting Terminating
PRK	The Call Park (PRK) option allows a business user to park a call against the directory number (DN) of the user. Retrieval of the parked call can occur from any station. When the call is parked, the user can originate and receive calls on that DN.
VOWDN	The Virtual Office Worker (VOW) feature allows telecommuters who do not have dedicated physical phone sets to access their dedicated directory number (DN) and associated features and options. They do this by logging into their dedicated DN from any of a pre-designated group of phone sets. Once logged in, all features and options operate normally, and all calls to the dedicated DN terminate to the set on which the login occurred. All predesignated 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. The VOWDN option is not compatible with any other line options/features except SETMODEL, DGT, DISP, M0200, and NAME.

2: Fault Management for A00012403

2.1 Fault management strategy

This feature will inherit all the functionality currently available with legacy implementation.

2.2 Fault management tools and utilities

2.3 Logs

2.3.1 Explanation

Log Title: Aud501

Name: Data Dump for a Local Test Desk (LTD) extension block

Description: The Audit subsystem generates this report when there is a data dump for a local test desk (LTD) extension block. Extension blocks are used to provide additional data space for a call condense block (CCB), which stores only enough data to describe a basic call.

Event type: The log is encountered when performing a test against a line with NDC option.

Please refer to the North American DMS-100 Log Report Reference Manual Volume 2 for a description of this log.

2.3.2 Format

2.3.3 Field descriptions

2.3.4 Action

2.3.5 Associated Operational Measurements or Performance Measurements

2.3.6 Explanation

Log Title: TRMT 22

Name: NDC_IN_EFFECT

Description: Busy Verify fails because there is no double connection call.

Event type: The log is encountered when performing a test against a line with NDC option.

Please refer to the North American DMS-100 Log Report Reference Manual Volume 2 for a description of this log.

2.3.7 Format

2.3.8 Field descriptions

2.3.9 Action

2.3.10 Associated Operational Measurements or Performance Measurements



Chapter 4: International-only features

Publication History

June 2006

Version 01.065, re-release of the Standard version of this document for ISN09FF. No changes made in the International chapter.

May 2006

Version 01.05, re-release of the Standard version of this document for ISN09FF. No changes made in the International chapter.

April 2006

Version 01.04, release of the Standard version of this document for ISN09FF at Customer Ready. The following feature has been re-classified as Prep, so it is removed from this version of the document:

- A00012291, MG15K Call-waiting Tone Support & Additional International Tones

January 2006

Version 01.03, release of the Standard version of this document for ISN09FF. The following features have been added under World Trade since the previous version:

- A00009297, QOSR: Support of AAL2 and Timestamp
- A00012291, MG15K Call-waiting Tone Support & Additional International Tones
- A00013286, Core Flex Large Line GWC Prof (Ph1)

December 2005

Version 01.02, release of the Standard version of this document for ISN09FF. No changes made in the International chapter.

November 2005

Version 01.01, release of the Preliminary version of this document for ISN09FF.

Overview

This chapter supports Nortel's International Carrier VoIP Solutions ISN09FF release. It describes ISN09FF features that affect inputs to or outputs from the solutions. These changes, therefore, affect the use of the Operations Support System (OSS) for ISN09FF. The document includes copies of International-only feature descriptions used in software design.

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 ISN09FF. DO NOT use this document to make changes to existing software.

How the International section is organized

This section of the document is divided into the following areas:

- *International activities mapping tables.* These tables relate the activity identifier associated with each International-only feature to:
 - the product/application/network element, or market area affected
 - affected software object types (data schema, for example)
- *International features list.* This list shows ALL features applicable for the International market. Therefore, it includes both International-only features as well as features that apply to both the International and North American markets.
- *New or changed for ISN09FF.* This section provides a table for each software object type, as follows:
 - Office parameters
 - Logs and alarms
 - Operational and Performance Measurements (OMs and PMs)
 - Data Schema tables or MIBs
 - User Interface (commands)
 - Service Orders (Servord+)
 - AMA/billing
 - Software Optionality Control (SOC)

Each table gives a summary of the changes caused per feature. Within each table, features are arranged by product/application, network element, or market and then in numeric order by the ACTID of the feature which creates new information or causes the change.

- *Feature descriptions.* This section provides feature descriptions, based on design documents, limited to International-only features. **Features that apply to both the International and North American markets may be found in Chapter 3 which contains North American market feature descriptions.** The feature descriptions in Chapter 3 are organized by product/application/ network element. The feature descriptions in Chapter 4 (this chapter) are grouped first by CS 2000 features and then by World Trade features. Within each group, the features are arranged in numeric order by ACTID.

ISN09FF Activity mapping tables

Introduction

This document contains advance information about differences in operations, administration, maintenance, and provisioning (OAM&P) for International Release ISN09FF. The purpose of this document is to provide early information about new, modified or deleted items related to OSS-impacting areas.

The table below shows the mapping from the activity identifier (ACTID) associated with each new feature to the following:

- the associated product, application, network element, or market
- the international solution that the feature affects, of the following:
 - International PT-AAL2
 - International PT-IP
 - International IAC
 - International IAW
 - International UA-IP
 - International DMS
 - International CHS
- the software object type or area that the feature affects, of the following:
 - Logs/faults
 - Data schema tables/MIBs
 - Office parameters
 - Service orders (ServOrd)
 - User interface/human-machine interface
 - Operational and performance measurements (OMs/PMs)
 - Automatic Message Accounting (AMA)/billing
 - Software Optionality Control (SOC)

Activity Mapping Table: Solutions Affected

PRODUCT or APPLICATION	ACTID	ISN09FF Solutions						
		Int'l PT-AAL2	Int'l PT-IP	Int'l IAC	Int'l IAW	Int'l UA-IP	Int'l DMS	Int'l CHS
Call Server 2000	A00009297	X						
Call Server 2000	A00013275					X		
Call Server 2000	A00013286					X		
World Trade	A00009037					X		

Activity Mapping Table: Software object types or areas impacted

ISN09FF Solutions		SW object types / areas impacted							
ISN09FF Solutions	ACTID	Logs/Faults	Data Schema	Office Parms	ServOrd	Commands/User Interf/HMI	OMs/PMs	AMA/Billing	Optionality
Call Server 2000	A00009297	X							
Call Server 2000	A00013275					X			
Call Server 2000	A00013286					X			
World Trade	A00009037		X						

International Features List

Introduction

The following table shows ALL features applicable for the International market. Therefore, it includes both International-only features as well as features that apply to both the International and North American markets.

Features for International Solutions

ACTID	Feature Title	Solution	Location
A0009026	RMGC Security	Int'l IAC	Chap. 3
A00009037	Core Enhance ESA for International MG9000	Int'l UA-IP	Chap. 4
A00009297	QOSR: Support of AAL2 and Timestamp	Int'l PT-AAL2	Chap. 4
A00010742	GWC EM Enhancements to support SIREN	Int'l IAW, Int'l IAC, Int'l PT-IP, Int'l UA-IP	Chap. 3
A00012349	U3WC Support for SIP Lines	Int'l CHS	Chap. 3
A00012478	Compact Call Agent: Geo Support for GigE	Int'l IAW, Int'l IAC, Int'l PT-IP, Int'l UA-IP	Chap. 3
A00012526	TDM Call Recording Feature	Int'l UA-IP	Chap. 3
A00012527	Provisioning of CS2K trunks on GW and Carrier basis	Int'l PT-IP	Chap. 3
A00013275	C&W: CS2M support for variable sized LGRP	Int'l UA-IP	Chap. 4
A00013286	Core Flex Large Line GWC Prof (Ph1)	Int'l UA-IP	Chap. 4

New and Changed for ISN09FF

Introduction

This section of the document contains tables which give an overview of the feature-based changes occurring in this International release for the following areas:

- Office parameters
- Logs/faults
- Operational measurements (OMs) and performance measurements (PMs)
- Data Schema tables or MIBs
- User interface (commands)
- Service Order (Servord+)
- AMA/billing
- Software Optionality Control (SOC)

Within each table, the changes are arranged by associated product, and then in numeric order by the activity identifier (ACTID) of the feature which creates new information or causes the change.

Office Parameter changes overview

The following office parameters are new or changed for ISN09FF. More complete descriptions appear in the Feature Descriptions section of this document.

Summary of new or changed Office Parameters

Office Parm Name	New or Changed	Description
Product = CS 2000		
(NONE)		
Product = World Trade		
(NONE)		

Logs/faults changes overview

The following logs or faults are new or changed for ISN09FF. More complete descriptions appear in the Feature Descriptions section of this document.

Summary of new or changed Logs/Faults for ISN06

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
Product = CS 2000		
QCA logs	see list in the FN, Appendix A	A00009297 (Int'l PT-AAL2) provides a complete list of QCA customer logs in its Appendix A and multiple examples of exact log format in its Appendix B.
IEMS log	IEMS616	Per CR Q01267955, IEMS616 is an INFO log generated when an SNMP protocol authentication failure occurs.
Product = World Trade		
(NONE)		

Operational Measurements/Performance Measurement changes overview

The following OMs or PMs are new or changed for ISN09FF. More complete descriptions appear in the Feature Descriptions section of this document.

Summary of new or changed OMs/PMs

OM Group or PM name	New or Changed	Description
Product = CS 2000		
(NONE)		
Product = World Trade		
(NONE)		

Data Schema tables/MIBs changes overview

The following Data Schema tables or MIBs are new or changed for ISN09FF. More complete descriptions appear in the Feature Descriptions section of this document.

DS Table/MIB	Changed or New
Product = CS 2000	
LNINV (changed)	A00013286 (Int'l UA-IP) modifies table LNINV to add new GRPTYPE entry LL_3RDPTY_2K to support large line gateways with 2047 endpoints.
Product = World Trade	
ESADGCOD (new)	A00009037 (Int'l UA-IP) creates table Emergency Stand Alone Digit Analysis Code (ESADGCOD) which contains customer group information and the digit analysis data that applies to specified types of calls in ESA mode of MG9000. According to datafill in ESADGCOD, number of digits to collect in ESA mode is determined. NOTE: ESAPXLA table has priority over ESADGCOD table. So, if there are overlapping prefixes in tables ESAPXLA and ESADGCOD, the ESAPXLA tuple is used.

User Interface (commands) changes overview

The following User Interface GUIs or Commands are new or changed for ISN09FF. More complete descriptions appear in the Feature Descriptions section of this document,

Field	Command/User Interface Description
Product = Call Server 2000	
CS2M Associate Media Gateway GUI (changed)	A00013275 (Int'l UA-IP) modifies this GUI as follows: - Support for the Audiocodes TP6310 card as a large line gateway or a trunk gateway for use in the Mediant 8000 Gateway chassis. - Support for large line GWs of capacity <= 2047 endpoints. - Support for both International and North American market fit. - Support for both 750 and 905 GWC types.
Product = World Trade	
(NONE)	

Service Order changes overview

The following Service Order information is new or changed for ISN09FF. More complete descriptions appear in the Feature Descriptions section of this document.

Summary of new or changed Service Orders

Area	New or Changed	ServOrd Description
Product = Call Server 2000		
(NONE)		
Product = World Trade		
(NONE)		

AMA/billing changes overview

The following AMA/Billing information is new or changed for ISN09FF. More complete descriptions appear in the Feature Descriptions section of this document.

Summary of new or changed AMA/billing

AMA/billing item	New or Changed	Description
Product = Call Server 2000		
(NONE)		
Product = World Trade		
(NONE)		

Software Optionality Control (SOC) changes overview

The following SOC information is new or changed for ISN09FF. More complete descriptions appear in the Feature Descriptions section of this document.

Summary of new or changed SOC

SOC code	New or Changed	Description
Product = CS 2000		
(NONE)		
Product = World Trade		
(NONE)		

ISN09FF Feature Descriptions

Product = Call Server 2000

A00009297 -- QoS Reporting: QoS Collector Application

1: Applicable solution(s)

Int'l PT-AAL2

Note: The following Functional Description includes both the original QoS feature 89007819 and the updates related to A00009297, QoS SR: Support of AAL2.

1.1 Description

This document covers the QoS Collector Application functionality supported in SN09.1 time frame.

In Voice over IP/VoATM networks, Quality of Service (QoS) can be adversely affected by the components in the network. Unlike TDM networks where the voice quality is consistent for all calls, VoIP/VoATM networks can experience different voice quality on all calls.

The common parameters that make up voice quality are:

- Packets sent
- Packets received
- Packet loss
- Octets sent
- Octets received
- Inter-arrival latency
- Jitter

All gateways beginning SN06 VoIP solutions report these statistics via end-of-call reporting mechanisms specific to the protocol used for MGC - VMG communication.

Beginning SN09.1, QCA will collect QoS Reporting statistics from ATM AAL2 Gateways too. The statistics collected are;

- Packets-sent (aal2/ps - H248 representation)
- Packets-Received (aal2/pr - H248 representation)

- Total Packets lost (aal2/tpl - H248 representation)
- Jitter (aal2/jit - H248 representation)

It is the purpose of this activity to design a method for reporting these QoS parameters on a per call basis for the purposes of;

- Network engineering
- Trend analysis
- Trouble-shooting network problems
- SLA validation

This is accomplished by implementing a reporting mechanism that will allow QoS reports (as IPDR records) to be delivered to a customer provided OSS for processing. In order to achieve SLA validation, QoS reports are correlated to appropriate billing records so that the QoS of billed calls can be determined.

QoS Reporting is applicable for more than just VoIP networks. It can be used in hybrid networks as well. From SN06 time frame to SN09 time frame QoS Reporting was limited to pure IP networks which consist only of GWC driven GWs.

Support for SPM peripherals and hybrid networks will be accomplished in a later release.

Beginning SN09.1 time frame QoS Reporting is extended to ATM AAL2 fabric which consists of GWC driven GWs (which support reporting of End of Call QoS statistics)

The proposed architecture for QoS Reporting beginning SN06 consists of the following components;

1. QoS Correlation ID and billing
2. QoS Reporting Application (on GWC)
3. Provisioning
4. QoS Report collection
5. QoS Report processing

This activity implements component 4. QoS Report collection, the QoS Collector Application (QCA)

1.1.1 System behavior

All QoS (IPDR) records are stored on a QoS Collector Application (QCA) host. The QCA will receive binary QoS records from the GWCs, converts these to QCA IPDR records and stores them in a file. The QCA IPDR records can be obtained by the OSS for processing.

Table 1 QCA properties

Name	Description	Units	Range	default
recycleToD	the hour in the day the directories will be recycled	hour	0 to 23	0
fileExt	the output file extension	N/A	String	xml
nodeName	the node name to be used in the output files	N/A	String	QCA
closedFileCompression ¹	whether the file should be compressed when closed and moved to today	boolean	true or false	true
oldFileCompression ^{1,2}	whether the files should be compressed at the first directory recycle	boolean	true or false	true

Notes:

1. File compression may be required as there is limited disk space for QCA IPDR record storage.
2. If *closedFileCompression* is true the value of the *oldFileCompression* property is negated as the files will have already been compressed.
3. A range of port numbers is provided for flexibility. The main use is for upgrade purposes, where two QCA instance may be running on a single host. Multiple QCAs, and therefore port numbers, should not be used to segregate QCA traffic.
4. Starting SN09FF the default value of MaxFileSize used in qca.properties file is 5 MB. This change is to improve QCA performance especially on Large Offices where the traffic rate could be as high as 2M BHCA. CR fix for Q01225163 adds this change.

The qca.properties file is read when the QCA is started, therefore the QCA must be stopped and restarted for changes in the qca.properties to be picked up.

When the qca.proprties file is read the contents is validated. If any of the properties are not present or invalid, the default value is automatically used. A warning customer log is generated to indicate that the default value is being used.

An example customer log warning:

```
Oct 11 12:00:02 wmdhs0j8 main:0001 QCA201 WARNING init label:
RetainFileTime property in properties/qca.properties is out of
range. QCA is starting with default retain file time of 5 days
```

Figure 2 Example of the QCA properties file

```
# QCA Properties file
# The QCA will have to be restarted for changes in the properties
# file to be reflected in the application's operation

# The maximum size of a file, in MBytes, before it is closed
# Range is 1 to 100. Default is 1.
MaxFileSize=1

# The maximum time, in minutes, a file can be open before
# it is closed
# Range is 1 to 240. Default is 15.
MaxFileTime=15

# Hour of the day that the directory structure is recycled
# Range 0 (12:00 AM) to 23 (11:00 PM). Default is 0 (12:00 AM).
# Do NOT specify minutes.
recycleToD=0

# port number to start application on.
# Range is 20000 to 20004. Default is 20000.
portNumber=20000

# How long, in days, the files are kept before deleting
# VERY IMPORTANT: Depending on the call volume and the number of
# days for file retention it could be possible to exhaust all
# available disk space, therefore the value of this property
# should be considered in great depth. If QCA is started with
# the value of this property less than the number of today
# directories for a given port the older directories will be
# deleted.
# Range 1 to 30. Default is 5.
RetainFileTime=5

# File Extension used in the QCA output file name.
# Default is xml.
fileExt=xml

# Node name to be used in the QCA output file name.
# Default is QCA.
nodeName=QCA

# true or false value indicating whether the output file
# should be compressed when closed. Default is true.
closedFileCompression=true

# true or false value indicating whether the file should be
# compressed at the first directory recycle
# Note: If closedFileCompression is true the value of the
# oldFileCompression property is negated as the files will have
```

1.1.3 Starting QCA

The `qca_server` script is used to start the QCA. The user should log in as root to execute this script.

When the `qca_server` script is run the following warning is displayed:

Attempting to register QCA as Qca with PMFADM.

If a QCA instance has not already been started with `qca_server` the following message is displayed:

```
Registration as Qca was ok. QCA started.
```

If a QCA instance has already been started with `qca_server` the following message is displayed:

```
pmfadm: Request "Qca" already queued  
Could not register QCA as Qca with PMFADM, this suggests a QCA  
instance is already running.
```

When the QCA is started the following steps are performed:

- the QCA is registered with PMFADM (processes monitor facility administration).
- This is a Solaris utility that monitors register processes and restarts the process if no longer running.
- configuration details (`qca.properties` file) are read
- If any of the properties information is not present or is invalid the default value is used and a customer log is generated to indicate this. It is at this point the user can stop the QCA if using default values is not acceptable.
- the QCA attempts to open a server socket on the specified port.
- If the specified port is in use the QCA can not be started.
- a file management process is started
- If the QCA output directory is not available when the QCA is started the directories are created.
- If a file exists in the active output directory, this indicates that QCA did not stop gracefully, the QCA will attempt to complete the file and move it to the today directory.
- the QCA waits for connections from clients (GWCs and SPMs) on the port number specified in the `qca.properties`.

1.1.4 Stopping QCA

The `stop_qca` script is used to stop the QCA. The user should log in as root to execute this script.

When the `stop_qca` script is run the following warning is displayed:

```
Are you sure you want to stop the QCA? Have you checked the port  
number in qca.properties? [ no or yes ]
```

If the port number in `qca.properties` has been checked and is correctly specified for the QCA to be stopped, this should be validated against the QCA datafill in PTM, then **yes** should be entered, otherwise **no** should be entered and the port number checked.

If a QCA instance was started by `qca_server` the following message will be displayed:

```
Attempting to unregister QCA as Qca from PMFADM.  
Attempting to stop local QCA on port: 20001  
QCA stopped successfully.
```

If a QCA was not started by `qca_server` the following message will be displayed:

```
Attempting to unregister QCA as Qca from PMFADM.  
pmfadm: "Qca" No such <nametag> registered  
  
QCA not registered with PMFADM as Qca, so stop_qca aborted.
```

If the above message is seen the `query_qca` script should be used to determine if a QCA instance is running on the host.

When the QCA is stopped the following steps are performed, in order:

- the QCA is unregistered with PMFADM
- the QCA stops accepting connections from clients
- the connection to the client(s) is closed
- the IPDR / XML structure in the output file is closed
- the output file is closed and moved to the today directory

Note: to avoid alarms being generated by all the GWCs sending QoS records to the QCA when the QCA is stopped the QCA details must be removed from PTM first. Please refer to activity 89007781 - QoS Reporting: Provisioning for QoS Reporting provisioning details.

1.1.5 Client (GWC) connection to QCA

When the QoS reporting mechanism is started on a client (GWC) it will connect to the QCA as specified in PTM, e.g. IP Address and port.

When a connection is established the QCA waits to receive data from the client (GWC).

1.1.6 Client (GWC) Connection heart beat

The TCP/IP connection between the client and QCA will be automatically closed if it is not used for more than 2 hours. To ensure the connection is not closed in this circumstance, the client will send a 'heart beat' message after 2 hours of inactivity.

The QCA simply receives the client ‘heart beat’, and does not generate a QCA IPDR record.

1.1.7 QCA File Management

The active output file is in the active directory. When a file is closed it is moved to the today directory.

1.1.7.1 Initialization

When the QCA is started the following file management steps are performed:

- the output directories are created if they do not already exist.
- any files in the active output directory are validated, ensuring that the last IPDR is complete and that the file structure is closed. Once the file is complete it is moved to the today output directory.
- all ‘today’ directories older than the file retention period are deleted. This can occur if the qca.properties is change such that file retention period is reduced.
- a new file is created using the naming convention given below. If the file name already exists the new file will have the number 0 added before the file extension, if this exists, the number 1 will be used, then 2 and so on.

1.1.7.2 Output directory

The directory used for the current QCA output is:

`/data/qca/"port number"/output/active`

Note: In SN07, QCA registers with the ‘servman’¹ on the SSPFS machine. Depending on your selection of `RetainFileTime` property in qca.properties file and your calculation of Disk consumption depending on Call traffic at your CO, proper disk partition size of /data/qca should be requested during SSPFS installation. For calculation on how much disk space should be allocated, refer to section 2.2.7.5.

Where “port number” is the port number that is specified in qca.properties and that the QCA accepts connections on. This allows the output of two QCAs running on the same host to be distinguished.

1.1.7.3 File names

The QCA will use the following file naming convention:

`<Node Type>.<Node Name>.<ReportName>.Year.Mon.Date_HR.MN_<TZ>.<File Ext>`

For example:

1. servman is the application service manager on the SSPFS platform starting SN06.2. servman manages registration and deregistration of all client applications running on the SSPFS machine whether it is simplex or clustered.

QCA.Telco_Switch_35.QoS.2002.04.11_02.45_EDT.xml

Where each of the elements is described as:

<NodeType> - A Nortel defined string identifying the product origination. Always "QCA".

<Node Name> - This name should MATCH the name of the node that is used in faults, in configuration (FQDN), in accounting and in GUIs. This value is configurable as property nodeName in qca.properties.

<Report Name> - The name of the script/filter/report that is used to create this file. There may be 1 or more report names in operation for a given NE simultaneously. Each report type must be identified in the filename. Always "QoS"

<Year.Mon.Date_HR.MN_> - This field when present in the active directory refers to the time when the file was opened or created in the active directory. The same field when present in today directories refers to the time the file was closed i.e the time when the files are closed and recycled to the today directories.

<TZ> - This is the Time Zone of the NE the Performance data is being collected from. This can be an off set from UMT or GMT.

<File Ext> - The file extension specified in qca.properties or the default xml.

1.1.7.4 Output file rotation (closure)

QCA file management provides file rotation (closure) based on file size and time the file has been open, on a 'which ever comes first' basis. These values are MaxFileSize and MaxFileTime, respectively, in qca.properties.

1.1.7.5 Output file compression

Due to the size of each QCA IPDR record (maximum about 840 bytes) the required disk space to store several days of QCA output files could be very large.

The required disk space storage requirement calculation is as follows:

Assuming:

- BHCA = 550K
- Calls per day = 10 x BHCA = 5.5 M
- QoS records per day = 2 x Calls per day = 11 M
- Record size = 840-bytes
- Compression ratio = 88% (achieved in testing)

Per day disk space required = 11 M x 840 = 8.6 GBytes

When using compression = 8.6 GBytes * 0.12 = 1 GByte

It can be seen that file compression offers a major saving in disk space requirements. And without compression the disk space in the /data/qca partition would be quickly exhausted.

The file compression is controlled by two properties, `closedFileCompression` and `oldFileCompression`.

`closedFileCompression` controls whether the active file should be compressed when it is closed and moved to the today directory.

`oldFileCompression` controls whether the retained files should be compressed when the output directories are recycled. When `oldFileCompression` is enabled, the files in the today-n directories will be checked, and compressed if required, every time directory recycling occurs.

1.1.7.6 Output file retention

The file management of the QCA follows that implemented for the SN05 feature SNMP Performance Measurement Poller (59039902). The output directory structures will contain a *number* of directories, for the current active file, today's closed files and the last *number-1* days closed files.

The clean-up mechanism is described by two parameters:

- 'retain file duration' (`RetainFileTime`) - how long (in days) should the files be retained on the local disk.
- 'recycle time of day' (`recycleToD`) - the hour of the day that the today directories are recycled.

Both are parameters specified in the `qca.properties` file read when the QCA is started.

At a predefined time (`recycleToD` in `qca.properties`, default is 12:00 AM), the output directories will be recycled.

The today-n directories are not created when the QCA is started but when the output files are recycled.

When the today directory reaches the maximum file retention period the information is discarded.

E.g. Output file structure if *number* were 30:

/data/qca/"port number"/output/active

/data/qca/"port number"/output/today

```
/data/qca/"port number"/output/today-1
/data/qca/"port number"/output/today-2
.
/data/qca/"port number"/output/today-28
/data/qca/"port number"/output/today-29
```

Note: if the QCA is stopped and restarted with a new 'retain file duration', that is less than the previous 'retain file duration' the QCA operated with, any existing today directories older than the new 'retain file duration' will be deleted.

The value for the 'retain file duration' should be considered carefully as the operation of the QCA and other applications may be impacted if there is no free disk space because it is used to store QCA output files.

In arriving at a value for the 'retain file duration' the following should be considered:

- the BHCA and total number of calls per day.
- total disk space available for file retention
- whether file compression is used.

A similar calculation to that in section 2.2.7.5 'Output file compression' should be used to determine the required 'per day' disk space requirements and therefore the 'retain file duration', e.g.:

$$\text{'retain file duration'} = \frac{\text{available disk space in MBytes}}{\text{required MBytes/day}}$$

Suppose the /data/QCA partition size is 8GBytes. Using the assumptions in section 2.2.7.5 'Output file compression' and the above calculation the maximum 'retain file duration' value is:

$$\frac{8000 \text{ MBytes}}{1000 \text{ MBytes}} = 8 \text{ days}$$

However, you may request a higher partition size of /data/qca during SSPFS installation as per the calculation shown in section 2.2.7.5.

1.1.7.7 Retaining modified qca.properties over an Upgrade

Note: Applicable only if values of parameters in qca.properties have been modified (different than default), and the same are required to be maintained over QCA upgrade.

When QCA is installed, qca.properties at /opt/nortel/qca/properties contains default values of various parameters (For example portNumber = 20000, and retainFileTime = 5). If customers are using other than default values of parameters in qca.properties file, and are planning for upgrade of QCA, following procedure needs to be followed to retain these customized values after upgrade, without having to stop/re-start QCA:

1. Before proceeding with upgrade, change the qca.properties on the inactive side of the cluster as required. (for example, portNumber = 20001, retainFileTime = 5)
2. State of QCA on the inactive side of the cluster: NOT RUNNING
3. Perform the upgrade. (The procedure will involve swacting of the cluster).
4. After the upgrade is complete, the newly active unit of the cluster will have the qca.properties of the previous inactive unit. This way we can expect the modified qca.properties to be maintained over an upgrade, without having to stop/re-start QCA.
5. If the above procedure is not followed, default values of parameters will remain in qca.properties.

For example, consider the present qca.properties have the values for portNumber and retainFileTime to be 20001 and 1 respectively. (It is 20000 and 5 respectively by default). If this qca.properties is to be maintained over an upgrade, the qca.properties of the inactive unit of the cluster has to be updated with these values, before performing the upgrade.

Problem scenario (Before Upgrade):

Active unit	Inactive unit (qca.properties not modified)
-----	-----
(SN08)	(SN09)
portNumber: 20001	portNumber: 20000
RetainFileTime=1	RetainFileTime=5
State: QCA running	QCA Not running

Problem scenario (After Upgrade):

Active unit	Inactive unit
-----	-----

(SN09)	(SN08)
portNumber: 20000	portNumber: 20001
RetainFileTime=5	RetainFileTime=1
State: QCA Running	QCA Not running

As seen in above problem scenario, qca.properties will not be maintained over an upgrade if qca.properties not modified in the inactive unit of the cluster.

Solution (Before Upgrade):

Active unit	Inactive unit (qca.properties modified)
-----	-----
(SN08)	(SN09)
portNumber: 20001	portNumber: 20001
RetainFileTime=1	RetainFileTime=1
State: QCA running	QCA Not running

Solution (After Upgrade):

Active unit	Inactive unit
-----	-----
(SN09)	(SN08)
portNumber: 20001	portNumber: 20001
RetainFileTime=1	RetainFileTime=1
State: QCA Running	QCA Not running
(No records lost)	

As seen above, updating qca.properties of inactive unit of the cluster will result in maintaining modified qca.properties over an upgrade.

1.1.7.8 Reporting disk space issues

As the QCA operates, disk space in /data/qca is used for the active file and to retain closed files. If the disk space in /data/qca becomes exhausted this would effect the operation of the QCA. The QCA uses customer logs to report disk space issues before all the space is used to reduce the possibility of completely filling the partition.

Every time the QCA creates a new file it will attempt check the available disk space, in the unlikely event that available space is not determinable the QCA will write a debug log to a file.

The QCA determines the number of free bytes available in the /data/qca partition and compares this with 3 boundary values; 1 GByte, 500 MBytes and 100 MBytes.

1 GByte boundary

If the available disk space is greater than 1 GByte then no further action is taken. However, if the available disk space is less than 1Gb and more than 500Mb, a minor customer log/alarm is generated.

If some disk space is made available in the /data/qca partition, after a customer alarm was raised, to make the available disk space great than 1GByte, the QCA raises a clear customer log for the minor alarm when the next new file is created.

However, if no action is taken and the available space still lies with between 1 GByte and 500 MBytes when the next file is created, the QCA will generate another minor customer log/alarm.

500 MByte boundary

If the available disk space is less than 500 MBytes and more than 100 MBytes, a major customer log/alarm is generated

If the available disk space goes above 500 MBytes, but below 1 GByte, the QCA raises a clear customer log for the major customer log/alarm when the next new file is created.

If the available disk space goes above 1 GByte the QCA raises clear customer logs for both the major and minor customer logs/alarms when the next new file is created.

However, if no action is taken and the available space still lies with between 500 MBytes and 100 MBytes when the next file is created, the QCA will generate another major customer log/alarm.

100 MByte boundary

If the available disk space is less than 100 MBytes a critical customer log/alarm is generated

If the available disk space goes above 100 MBytes, but below 500 MBytes, the QCA raises a clear customer log for the critical customer log/alarm when the next new file is created.

If the available disk space goes above 500 MBytes, but below 1 GByte, the QCA raises clear customer logs for both the critical and major customer logs/alarms when the next new file is created.

If the available disk space goes above 1 GByte, the QCA raises clear customer logs for the critical, major and minor customer logs/alarms when the next new file is created.

However, if no action is taken and the disk space is completely exhausted the QCA will generate a critical customer log/alarm and the QCA will be stopped.

In the scenario where write access is prevented the application will raise a critical customer log/alarm and the QCA will be stopped.

1.1.8 Growing the Size of /data/qca

See Appendix C for the Procedure to grow the size of Partition /data/qca.

1.1.9 QoS record processing

At the end of every call the client reports the QoS statistics to the QCA in a binary QoS record. The QCA validates the record, ensuring the record sequence number, version and length are correct. The QCA then converts the record to an IPDR form. The QCA IPDR record is then written to a file.

Until SN07 the QoS record had only 1 version (size 132 Bytes). In SN08 the QoS Record message version is 2 (size 136 Bytes).

Beginning SN09 the QoS record has version 3 (size 180 = 136 Bytes + 10 Bytes Timestamp - 2 byte filler in Version 2 + 32 Bytes (GWName is changed to 64 Bytes as compared to 32 Bytes prior to SN09) + 4 byte filler for Version 3.)

Beginning SN09.1 the QCA supports version 4 and version 5 QoS binary Records that come from patched SN07 and SN08 GWCs respectively.

1.1.9.1 Binary QoS record format

The QoS record sent from the client (GWC) is a binary message. A description of the binary QoS record fields is shown in the following table.

Table 2 Binary QoS record fields (version 1 SN07)

Name	Description	Range
MT (MGC Type)	The type of client (MGC) the QoS record was generated by	0 - GWC 1 - SPM
Msg Type	Message type	0 - QoS record 1 - heart beat
Sequence number	Record sequence number	0 to 16777215
RT (Report Type)	Report Type	0 - local 1 - remote
ver (version)	The QoS record version	0 to 15
MGC number	The number of the client (MGC) the QoS record was generated by	0 to 255
Msg length	The length of the message (including header)	0 to 255 (should be 130)
Gateway port number	The port number on the Gateway used in the call	0 to 65535
Gateway IP Address	The IP Address of the Gateway used in the call	4-bytes
Gateway FQDN	Consists of two separate fields; the Gateway name (32 Bytes) and End Point (32 Bytes).	64-bytes
Switch CLLI	The CLLI of the CS2K the client is subtended to	16-bytes
Correlation ID	The correlation id that can be used to correlate the QoS record to an AMA record	10-bytes
Packets Sent	The total number of packets transmitted	0 to 4294967294
Packets Received	The total number of packets received	0 to 4294967294
Octets Sent	The total number of payload octets transmitted	0 to 4294967294
Octets Received	The total number of payload octets received	0 to 4294967294
Packets Lost	The total number of packets lost	0 to 4294967294
Jitter	Estimate of packet interarrival time (milliseconds)	0 to 65534
Latency	Estimate of network latency (milliseconds)	0 to 65534

Table 3 Binary QoS record fields (version 2 SN08)

Name	Description	Range
MT (MGC Type)	The type of client (MGC) the QoS record was generated by	0 - GWC 1 - SPM
Msg Type	Message type	0 - QoS record 1 - heart beat
Sequence number	Record sequence number	0 to 16777215
RT (Report Type)	Report Type	0 - local 1 - remote
ver (version)	The QoS record version	0 to 15
MGC number	The number of the client (MGC) the QoS record was generated by	0 to 255
Msg length	The length of the message (including header)	0 to 255 (should be 130)
Gateway port number	The port number on the Gateway used in the call	0 to 65535
Gateway IP Address	The IP Address of the Gateway used in the call	4-bytes
Gateway FQDN	Consists of two separate fields; (the Gateway name and end point)	64-bytes
Switch CLLI	The CLLI of the CS2K the client is subtended to	16-bytes
Correlation ID	The correlation id that can be used to correlate the QoS record to an AMA record	10-bytes
Packets Sent	The total number of packets transmitted	0 to 4294967294
Packets Received	The total number of packets received	0 to 4294967294
Octets Sent	The total number of payload octets transmitted	0 to 4294967294
Octets Received	The total number of payload octets received	0 to 4294967294
Packets Lost	The total number of packets lost	0 to 4294967294
Jitter	Estimate of packet interarrival time (milliseconds)	0 to 4294967294
Latency	Estimate of network latency (milliseconds)	0 to 4294967294

Table 4 Binary QoS record fields (version 3 SN09)

Name	Description	Range
MT (MGC Type)	The type of client (MGC) the QoS record was generated by	0 - GWC 1 - SPM
Msg Type	Message type	0 - QoS record 1 - heart beat
Sequence number	Record sequence number	0 to 16777215
RT (Report Type)	Report Type	0 - local 1 - remote
ver (version)	The QoS record version	0 to 15
MGC number	The number of the client (MGC) the QoS record was generated by	0 to 255
Msg length	The length of the message (including header)	0 to 255 (should be 130)
Gateway port number	The port number on the Gateway used in the call	0 to 65535
Gateway IP Address	The IP Address of the Gateway used in the call	4-bytes
Gateway FQDN - GW Name	Consists of two separate fields; (the Gateway name	64-bytes
Gateway FQDN Endpoint	End point	32-bytes
Switch CLLI	The CLLI of the CS2K the client is subtended to	16-bytes
Correlation ID	The correlation id that can be used to correlate the QoS record to an AMA record	10-bytes
Packets Sent	The total number of packets transmitted	0 to 4294967294
Packets Received	The total number of packets received	0 to 4294967294
Octets Sent	The total number of payload octets transmitted	0 to 4294967294
Octets Received	The total number of payload octets received	0 to 4294967294

Name	Description	Range
Packets Lost	The total number of packets lost	0 to 4294967294
Jitter	Estimate of packet interarrival time (milliseconds)	0 to 4294967294
Latency	Estimate of network latency (milliseconds)	0 to 4294967294
StartTimeStamp*	Call Start Timestamp	5 -bytes.
EndTimeStamp*	End Time Timestamp	5 -bytes.

*Start and End timestamp addressed in the following section.

1.2 Timestamp (Call Start Time and Call End Time)

1.2.1 DISCLAIMER:

- QoS records contain performance measurement data only and they are never intended to be used as a source for billing information.
- Call durations for billing/revenue generation purposes have to be based on the time data in the billing records, such as AMA and CDR records, and not QoS records.

1.2.2 Timestamp Support

Timestamp support (Call Start Time and Call End Time) for QoS IPDR records are supported beginning SN09. This activity is tracked under A0009297 and provides support to display correct call start time and call end time in the QoS IPDR XML records.

All QoS (IPDR) records are stored on a QoS Collector Application (QCA) host. The QCA receives binary QoS records from the MGCs, converts these to QCA IPDR records and stores them in a file. The QCA IPDR records can be obtained by the OSS for processing

Prior to SN09, the timestamp parameter (Call Start time and Call End time) was hardcoded to a default value 1970-01-01T00:00:00.000Z and thus the QoS record output in the XML file show this default value for all calls irrespective of the actual call start time and call end time for the particular call and does not depict the correct value.

GWC sends end of call statistics to active QCA servers. Timestamps (Call Start and Call End Timestamp) are IPDR parameters that would be displayed on a QoS Report along with other IPDR parameters such as timezone, call completion code, hostname, subscriberID, unique Call ID, IP Address, port

number, sequence number and End of Call QoS Statistics such as average packet latency, inbound byte count, outbound byte count, inbound packet count, outbound packet count, packet lost and packet delay.

1.2.2.1 Timestamp Format

Timestamp (Call Start Time and Call End Time) are in ISO 8601 format. The format is shown below:

YYYY:MM:DD:HH:MM:SS:MS Where,

YYYY - Year

MM - Month

DD -Day

HH - Hour

MM - Minute

SS - Second

MS - Millisecond

This timestamp is included in the QoS Binary message and this in turn is parsed by the QCA to extract the Call Start Time and Call End Time. QCA IPDR records show these extracted timestamp.

The timestamp used for the QoS Binary records and QoS IPDR XML records (Call Start Time and Call End Time) will be in Universal coordinated time (UTC) previously known as Greenwich Mean Time (GMT). Time represented as UTC will be universal and will not have to worry about Daylight saving time.

GMT is World Time and the basis of every world time zone which sets the time of day and is at the centre of the time zone map. Call Start Time and Call End Time use UTC time format and these timestamp will be represented in QCA XML reports.

Note: Since Timestamps are in UTC time format they do not support Day Light Saving time. Hence the Time value in the start and End time might be off by 1 hour compared to the time in billing records during the period between 1st April to 31st October every year.

1.2.2.2 Call Start Time and Call End Time

Call Start TimeStamp (STS) and End TimeStamp (ETS) will be depicted in the QCA Xml records. An example of the timestamp is given below:

<StartTime>2005-01-01T14:52:57.000Z</StartTime>

<EndTime>2005-01-01T14:59:01.000Z</EndTime>

1.2.3 QCA IPDR record format

The output of the QCA is a single stream (file) of IPDR Version 3.1-A.0.2 compliant records.

1.2.3.1 QCA IPDR elements

The IPDR elements used in the QoS output format are shown in the following table.

Table 5 QCA IPDR tags

QoS Field Tag	Type	Range
StartTime	dateTime	ISO 8601 format.
EndTime	dateTime	ISO 8601 format.
timeZoneOffset	integer	Time offset, in minutes, of local time zone referenced to GMT.
callCompletionCode	String	Final call completion code for billing use.
originalDestinationId	String	Called-party (designation) number
hostName	String	0 to 22 characters
subscriberId	String	0 to 65 characters (version 1 and 2) 0 to 97 characters (version 3)
uniqueCallId	String	20 hexadecimal digits
ipAddress	String	7 to 15 numerical characters
portNumber	String	0 to 2147483647
seqNum	integer	0 to 16777215
averagePacketLatency	integer	0 to 65536 (version 1) 0 to 2147483647 (version 2 and 3)
inboundByteCount	integer	0 to 2147483647
outboundByteCount	integer	0 to 2147483647
inboundPacketCount	integer	0 to 2147483647
outboundPacketCount	integer	0 to 2147483647
inboundLostPacketCount	integer	0 to 2147483647
packetDelayVariation	integer	0 to 65536 (version 1) 0 to 2147483647 (version 2 and 3)

An example QCA IPDR record (for IP/AAL2 fabric):

```
<IPDR>
<StartTime>2005-10-05T15:30:09Z</StartTime>*
<EndTime>2005-10-05T15:32:12Z</EndTime>
<timeZoneOffset>0</timeZoneOffset>
<callCompletionCode>CC</callCompletionCode>
<originalDestinationId></originalDestinationId>
<hostName>GWC3@COMITIP</hostName>
<subscriberId>aaln/1@ttp018.mgsite-2.b4sky.ott</subscriberId>
<uniqueCallId>43c01738000f13e30d05</uniqueCallId>
<ipAddress>10.0.15.1</ipAddress>
<portNumber>2427</portNumber>
<seqNum>18</seqNum>
<averagePacketLatency>0</averagePacketLatency>
<inboundByteCount>41538</inboundByteCount>
<outboundByteCount>0</outboundByteCount>
<inboundPacketCount>301</inboundPacketCount>
<outboundPacketCount>0</outboundPacketCount>
<inboundLostPacketCount>0</inboundLostPacketCount>
<packetDelayVariation>0</packetDelayVariation>
</IPDR>
```

* Note: Starting SN09, the value of the timestamp in the IPDR records will show the actual value and not the defaulted value of 1970-01-01T00:00:00.000Z. This is tracked under the activity A00009297 and is addressed in section <2.3>

An example QCA IPDR record (for AAL2 fabric):

```
<IPDR>
<StartTime>2005-10-05T15:30:09Z</StartTime>*
<EndTime>2005-10-05T15:32:12Z</EndTime>
<timeZoneOffset>0</timeZoneOffset>
<callCompletionCode>CC</callCompletionCode>
<originalDestinationId></originalDestinationId>
<hostName>GWC3@COMITIP</hostName>
<subscriberId>aaln/1@ttp018.mgsite-2.b4sky.ott</subscriberId>
<uniqueCallId>43c01738000f13e30d05</uniqueCallId>
<ipAddress>10.0.15.1</ipAddress>
<portNumber>2427</portNumber>
<seqNum>18</seqNum>
<averagePacketLatency>0</averagePacketLatency>
<inboundByteCount>41538</inboundByteCount>
<outboundByteCount>0</outboundByteCount>
<inboundPacketCount>301</inboundPacketCount>
<outboundPacketCount>0</outboundPacketCount>
<inboundLostPacketCount>0</inboundLostPacketCount>
<packetDelayVariation>0</packetDelayVariation>
</IPDR>
```

* Note: Starting SN09, the value of the timestamp in the IPDR records will show the actual value and not the defaulted value of 1970-01-01T00:00:00.000Z. This is tracked under the activity A00009297 and is addressed in the Timestamp section.

The maximum size of a QCA IPDR record is around 840 characters, this equates to 840-bytes (using UTF-8 encoding).

Not all of the QoS statistics are provided by all media gateways, e.g. the UAS does not support the Jitter and Latency statistics, therefore if the received binary QoS record does not contain a valid value for any of the QoS statistics the element will not be included in the output QCA IPDR record.

1.2.3.2 QCA IPDR element values

Refer to the following table.

Table 6 Mapping of input binary QoS Record fields to output QCA IPDR record elements

Output QCA IPDR elements	Input Binary QoS field	Comment
StartTime	Call Start Time	A00009297 feature: Starting SN09, QoS IPDR records will show correct timestamp (Call start Time) and not the Hardcoded value used: 1970-01-01T00:00:00.000Z earlier.
EndTime	Call End Time	A00009297 feature: Starting SN09, QoS IPDR records will show correct timestamp (Call End Time) and not the Hardcoded value used: 1970-01-01T00:00:00.000Z earlier.
timeZoneOffset	N/AN/A	Not applicable. Hardcoded value used: 0
callCompletionCode	N/A	Not applicable. Hardcoded value used: CC (call completed normally)
originalDestinationId	N/A	Not applicable. Empty String
subscriberId	Concatenation of Endpoint and Gateway Name (from Gateway FQDN)	<EndPoint>@<GW Name>
hostName	Concatenation of MT (MGC Type), MGC Number and Switch CLLI	<MGC Type><MGC Number>@<Switch CLLI>
uniqueCallId	Correlation Id	
ipAddr	Gateway IP Address	standard 4-part format
portNumber	Gateway Port Number	
seqNum	Sequence number	
averagePacketLatency	Latency	Element not present in IPDR if the received binary QoS record value is
inboundByteCount	Octets Received	
outboundByteCount	Octets Sent	

Table 6 Mapping of input binary QoS Record fields to output QCA IPDR record elements

Output QCA IPDR elements	Input Binary QoS field	Comment
inboundPacketCount	Packets Received	less than 0, indicating that the GW did not support the statistic.
outboundPacketCount	Packets Sent	
inboundLostPacketCount	Packet Loss	
packetDelayVariation	Jitter	

Starting SN09.1 - aal2/ps, aal2/pr, aal2/pl, aal2/jit AAL2 parameters (A00009297 feature) are also reflected in QoS Records using inboundPacketCount, outboundPacketCount, inboundLostPacketCount, packetDelayVariation respectively.

The following elements are 'required' IPDR elements so have been included in the QCA output for IPDR compliancy.

- StartTime
- EndTime
- timeZoneOffset
- CallCompletionCode
- originalDestinationId

1.2.3.3 QCA IPDR file format

The output of the QCA is a file with format conforming to the IPDR structure. The first line in the file is the header, providing details about the XML version and encoding. The next line is the 'open' IPDR tag which gives information about the version of QCA and indicates the start of records. The last line in the file is the 'close' IPDR tag which indicates the end of the file.

Refer to the following figure for an example QoS XML file format.

Figure 3 QCA IPDR file format

Line no.	Line	Description
1	<?xml version="1.0" encoding="UTF-8" ?>	File header

Figure 3 QCA IPDR file format

2	<pre><IPDRDoc xmlns="http://www.ipdr.org/namespaces/ipdr" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" IPDRRecorderInfo ="qca.nortelnetworks.com" xsi:schemaLoca- tion="http://www.ipdr.org/namespaces/ipdr VoIP3.1- A.0.2.xsd" version="3.1-A.0.2"></pre>	IPDRDoc is the file open tag
3	<pre><IPDR></pre> 	Start of record
n-1	<pre></IPDR></pre>	End of record
n	<pre></IPDRDoc></pre>	/IPDRDoc is the file close tag

The IPDRDoc tag gives information about the IPDR format used and the device that generated the IPDR file, e.g.

IPDRRecorderInfo = "qca.nortelnetworks.com"

1.3 Detecting Events and Errors

In the situation that the QCA detects an event (e.g. client closes the connection) or an error (e.g. out of sequence record), a customer log is generated and an error IPDR record is written to the output file.

The error IPDR record is generated so that the OSS does not require two interfaces to the QCA host, one to retrieve IPDR records and one to monitor events and errors. All the relevant information to the QCA output processing is provided in the single output stream.

The error IPDR record is compliant to the IPDR specification, i.e. contains all of the required IPDR elements, some of which will contain default or empty values.

Multiple errors

This is only applicable to unsupported QoS record version and unsupported QoS record length errors.

The QCA allows up to 9 consecutive unsupported QoS record version and up to 9 consecutive unsupported QoS record length errors. When the 10th consecutive error is detected a customer log is generated to indicate this and the connection is being closed.

If a client sends a QoS record with valid length or version before sending 10 unsupported QoS record version or 10 unsupported QoS record length records, a customer log is generated to indicate that the alarm condition has been cleared.

Table 7 QCA Error and Event actions

Error/Event	QCA Action
out of sequence record	customer log generated error IPDR record generated binary QoS record processed
unsupported QoS record version (less than 10 consecutive records)	customer log generated error IPDR record generated binary QoS record discarded
unsupported QoS record version (10th consecutive records)	customer log generated error IPDR record generated binary QoS record discarded connection closed
unsupported QoS record length (less than 10 consecutive records)	customer log generated error IPDR record generated binary QoS record discarded
unsupported QoS record length (10th consecutive records)	customer log generated error IPDR record generated binary QoS record discarded connection closed
unknown message type	customer log generated error IPDR record generated binary QoS record discarded connection closed
unable to read binary QoS record header	customer log generated error IPDR record generated binary QoS record discarded connection closed

Table 7 QCA Error and Event actions

Error/Event	QCA Action
unable to process binary QoS record body	customer log generated error IPDR record generated binary QoS record discarded
connection closed (not by QCA) ^a	customer log generated error IPDR record generated connection closed (from QCA end)
QCA stopped	customer log generated error IPDR record generated
QCA started	error IPDR record generated
New GWC Connection	customer log generated error IPDR record generated

a. Note: This includes the 'GWC Swact' scenario.

Note: please refer to Appendix A for more details of the customer logs generated by the QCA.

1.3.1 QCA Error IPDR record

Depending on the type of error, different information can be used in the error IPDR record.

For example, if a message with an 'unknown message type' is received the whole message is unreliable so only the connection information can be used. Whereas, if an 'out of sequence' record is received the message format is valid so information from the connection and record header can be used.

Default values are used in the QCA error IPDR record for the following required IPDR elements:

- callCompletionCode - CC
- originalDestinationId - empty string
- subscriberId - empty string
- uniqueCallId - empty string

Depending on the type of error or event the following QCA error IPDR record elements may contain information:

- hostName - MGC Id, if the MGC Id is not available it is an empty string and the Node name (the value of the nodeName property in the qca.properties file). Below are some examples.

- GWC3@CS2K_LAB (if MGC Id is available)
- CS2K_LAB (if MGC Id is an empty string)
- seqNum - the sequence number of the QoS record with the error, the sequence number is not available it is 0

The following QCA error IPDR record elements are always used to convey information:

- ipAddress
- portNumber
- proprietaryErrorCode

The values for each element in the error IPDR record, other than the default elements, are given in the following table.

Table 8 Error IPDR record elements

Error/Event	Element	Value
Unexpected Record Sequence Number	hostname	MGC Id, Node name
	seqNum	record sequence number
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	0 (plus previous valid record sequence number, e.g. previous sequence number = 1638, proprietaryErrorCode = 01638)
Record Lost: Unsupported Version	hostname	MGC Id, Node name
	seqNum	record sequence number
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	1
Record Lost: Unsupported Record Length	hostname	MGC Id, Node name
	seqNum	record sequence number
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	2

Table 8 Error IPDR record elements

Error/Event	Element	Value
Connection closed: Unrecognized Message Type	hostname	Node name
	seqNum	0
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	3
Connection closed: Error while processing QoS record header	hostname	Node name
	seqNum	0
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	4
Record Lost: Error while processing binary QoS data	hostname	MGC Id, Node name
	seqNum	0
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	5
Connection closed	hostname	Node name
	seqNum	0
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	6
QCA Stopped	hostname	Node name
	seqNum	0
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	7
QCA Started	hostname	Node name
	seqNum	0
	ipAddress	IP Address of connection

Table 8 Error IPDR record elements

Error/Event	Element	Value
	portNumber	Port number of connection
	proprietaryErrorCode	8
New GWC Connection ^a	hostname	MGC Id, Node name
	seqNum	record sequence number
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	9

a. These records will be produced for every new connection from the GWCs.

1.3.1.1 Error IPDR record format

Examples for each of the QCA IPDR error records:

Unexpected Record Sequence Number

```
<IPDR>
  <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
  <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
  <timeZoneOffset>0</timeZoneOffset>
  <callCompletionCode>CC</callCompletionCode>
  <originalDestinationId></originalDestinationId>
  <hostName>GWC99@CS2K_LAB</hostName>
  <subscriberId></subscriberId>
  <uniqueCallId></uniqueCallId>
  <ipAddress>47.96.0.243</ipAddress>
  <portNumber>37559</portNumber>
  <seqNum>4</seqNum>
  <proprietaryErrorCode>02</proprietaryErrorCode>
</IPDR>
```

Record Lost: Unsupported Version

```
<IPDR>
  <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
  <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
  <timeZoneOffset>0</timeZoneOffset>
  <callCompletionCode>CC</callCompletionCode>
  <originalDestinationId></originalDestinationId>
  <hostName>GWC99@CS2K_LAB</hostName>
  <subscriberId></subscriberId>
  <uniqueCallId></uniqueCallId>
  <ipAddress>47.96.0.243</ipAddress>
  <portNumber>37665</portNumber>
  <seqNum>2</seqNum>
  <proprietaryErrorCode>1</proprietaryErrorCode>
</IPDR>
```

Record Lost: Unsupported Record Length

```
<IPDR>
  <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
  <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
  <timeZoneOffset>0</timeZoneOffset>
  <callCompletionCode>CC</callCompletionCode>
  <originalDestinationId></originalDestinationId>
  <hostName>GWC99@CS2K_LAB</hostName>
  <subscriberId></subscriberId>
  <uniqueCallId></uniqueCallId>
  <ipAddress>47.96.0.243</ipAddress>
  <portNumber>37676</portNumber>
  <seqNum>2</seqNum>
  <proprietaryErrorCode>2</proprietaryErrorCode>
</IPDR>
```

Connection closed: Unrecognized Message Type

```
<IPDR>
  <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
  <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
  <timeZoneOffset>0</timeZoneOffset>
  <callCompletionCode>CC</callCompletionCode>
  <originalDestinationId></originalDestinationId>
  <hostName>CS2K_LAB</hostName>
  <subscriberId></subscriberId>
  <uniqueCallId></uniqueCallId>
  <ipAddress>47.96.0.243</ipAddress>
  <portNumber>37642</portNumber>
  <seqNum>0</seqNum>
  <proprietaryErrorCode>3</proprietaryErrorCode>
</IPDR>
```

Connection closed: Error while processing QoS record header

```
<IPDR>
  <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
  <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
  <timeZoneOffset>0</timeZoneOffset>
  <callCompletionCode>CC</callCompletionCode>
  <originalDestinationId></originalDestinationId>
  <hostName>CS2K_LAB</hostName>
  <subscriberId></subscriberId>
  <uniqueCallId></uniqueCallId>
  <ipAddress>47.96.0.243</ipAddress>
  <portNumber>37642</portNumber>
  <seqNum>0</seqNum>
  <proprietaryErrorCode>4</proprietaryErrorCode>
</IPDR>
```

Record Lost: Error while processing binary QoS data

```
<IPDR>
  <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
  <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
  <timeZoneOffset>0</timeZoneOffset>
  <callCompletionCode>CC</callCompletionCode>
  <originalDestinationId></originalDestinationId>
  <hostName>GWC99@CS2K_LAB</hostName>
  <subscriberId></subscriberId>
  <uniqueCallId></uniqueCallId>
```

```
<ipAddress>47.96.0.243</ipAddress>
<portNumber>37676</portNumber>
<seqNum>2</seqNum>
<proprietaryErrorCode>5</proprietaryErrorCode>
</IPDR>
```

Connection closed

```
<IPDR>
  <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
  <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
  <timeZoneOffset>0</timeZoneOffset>
  <callCompletionCode>CC</callCompletionCode>
  <originalDestinationId></originalDestinationId>
  <hostName>CS2K_LAB</hostName>
  <subscriberId></subscriberId>
  <uniqueCallId></uniqueCallId>
  <ipAddress>47.96.0.243</ipAddress>
  <portNumber>37676</portNumber>
  <seqNum>0</seqNum>
  <proprietaryErrorCode>6</proprietaryErrorCode>
</IPDR>
```

QCA Stopped

```
<IPDR>
  <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
  <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
  <timeZoneOffset>0</timeZoneOffset>
  <callCompletionCode>CC</callCompletionCode>
  <originalDestinationId></originalDestinationId>
  <hostName>CS2K_LAB</hostName>
  <subscriberId></subscriberId>
  <uniqueCallId></uniqueCallId>
  <ipAddress>0.0.0.0</ipAddress>
  <portNumber>20000</portNumber>
  <seqNum>0</seqNum>
  <proprietaryErrorCode>7</proprietaryErrorCode>
</IPDR>
```

QCA Started

```
<IPDR>
  <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
  <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
  <timeZoneOffset>0</timeZoneOffset>
  <callCompletionCode>CC</callCompletionCode>
  <originalDestinationId></originalDestinationId>
  <hostName>CS2K_LAB</hostName>
  <subscriberId></subscriberId>
  <uniqueCallId></uniqueCallId>
  <ipAddress>0.0.0.0</ipAddress>
  <portNumber>20000</portNumber>
  <seqNum>0</seqNum>
  <proprietaryErrorCode>8</proprietaryErrorCode>
</IPDR>
```

New GWC Connection

```
<IPDR>
  <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
  <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
  <timeZoneOffset>0</timeZoneOffset>
  <callCompletionCode>CC</callCompletionCode>
  <originalDestinationId></originalDestinationId>
  <hostName>GWC77@CS2K_LAB</hostName>
  <subscriberId></subscriberId>
  <uniqueCallId></uniqueCallId>
  <ipAddress>47.96.0.243</ipAddress>
  <portNumber>37559</portNumber>
  <seqNum>567</seqNum>
  <proprietaryErrorCode>9</proprietaryErrorCode>
</IPDR>
* Note: Starting SN09, the value of the timestamp in the IPDR
records will show the actual value and not the defaulted value of
1970-01-01T00:00:00.000Z. This is tracked under the activity
A00009297 and is addressed in section <4.0.0.1>
```

1.3.2 Streaming to OSS

Real-Time streaming of the QCA IPDR record stream to the OSS is provided via the streamQoS utility. It should be used as follows:

1. Connect to the machine on which QCA is running, e.g. via telnet
2. Change directory to the QCA home directory, e.g. /opt/nortel/qca/
3. Start the logging to file of the window.
4. Type streamQoS to start the stream
5. The streaming utility is stopped by closing the connection

1.3.3 Display tool

A tool to display QCA IPDR records in an output QCA file is provided. There are three outputs from the tool:

- display all the QCA IPDR Records in the file
- display all the QCA IPDR Records for a particular Subscriber Id in the file
- display all the QCA IPDR Records for a particular MGC in the file

The command must have at least one argument, the file name. The command is able to handle the compressed and also uncompressed QCA output files.

To display only the records for a particular Subscriber Id, the Subscriber Id must be provided to the utility.

To display only the records for a particular MGC, the following information is necessary:

- MGC type (GWC or SPM), *mgcType* or *mt* field in QCA IPDR record
- MGC number (0 to 255), *mgcNumber* or *num* in QCA IPDR record

Displaying all QCA IPDR records in a file:

```
displayQoS <file name>
```

Displaying all QCA IPDR record from a particular client in a file:

```
displayQoS <file name> <Subscriber Id>
```

Displaying all QCA IPDR record from a particular client in a file:

```
displayQoS <file name> <MGC type> <MGC number>
```

If the file can not be found an error is displayed.

The first argument is always the file name. If only two arguments are provided the second argument is taken as the Subscriber Id. If more than two arguments are provided they are taken as the MGC type and MGC number.

Example displayQoS output:

```
Displaying QoS Records for GWC 80 from file:  
GWC.Telco_Switch_35.QoS.2002.04.11_02.45_EDT.xml
```

```
Record:  
Start Time*      = 1970-01-01T00:00:00.000Z  
End Time*        = 1970-01-01T00:00:00.000Z  
TimeZone Offset  = 0  
Call Comp Code   = CC  
Orig Dest Id     =  
Host name        = GWC171@3911296719576333  
Subscriber id     = 70961557517088778@4995546324  
Correlation Id   = 14714216668188184186  
IP Address       = 96.143.185.15  
Port Number      = 35187  
Sequence Number  = 9  
Latency          = 19685  
Octets Received  = 1894381033  
Octets Sent      = 1785294279  
Packets Received = 648495757  
Packets Sent     = 286520160  
Packets Lost     = 922391632  
Jitter           = 14826  
  
Record:  
Start Time*      = 1970-01-01T00:00:00.000Z  
End Time*        = 1970-01-01T00:00:00.000Z  
TimeZone Offset  = 0  
Call Comp Code   = CC  
Orig Dest Id     =  
Host name        = GWC99@CS2K_LAB  
Subscriber id     =  
Correlation Id   =  
IP Address       = 47.96.0.243  
Port Number      = 37559  
Sequence Number  = 4  
Previous seq num = 2  
Error Code       = 0 (Unexpected Record Sequence Number)
```

End of XML QoS File.

Example displayQoS output (for call over AAL2 fabric):

Displaying QoS Records for GWC 80 from file
GWC.Telco_Switch_35.QoS.2002.04.11_02.45_EDT.xml

Record:

Start Time* = 1970-01-01T00:00:00.000Z
End Time* = 1970-01-01T00:00:00.000Z
TimeZone Offset = 0
Call Comp Code = CC
Orig Dest Id =
Host name = GWC171@3911296719576333
Subscriber id = 70961557517088778@4995546324
Correlation Id = 14714216668188184186
IP Address . . . = 96.143.185.15
Port Number = 35187
Sequence Number = 9
Latency = 19685
Octets Received = 1894381033
Octets Sent = 1785294279

Packets Received = 648495757
Packets Sent = 286520160
Packets Lost = 922391632
Jitter = 14826

Record:

Start Time* = 1970-01-01T00:00:00.000Z
End Time* = 1970-01-01T00:00:00.000Z
TimeZone Offset = 0
Call Comp Code = CC
Orig Dest Id =
Host name = GWC99@CS2K_LAB
Subscriber id =
Correlation Id =
IP Address = 47.96.0.243
Port Number = 37559
Sequence Number = 4
Previous seq num = 2
Error Code = 0 (Unexpected Record Sequence Number)

End of XML QoS File.

* Note: Starting SN09, the value of the timestamp in the IPDR records will show the actual value and not the defaulted value of 1970-01-01T00:00:00.000Z. This is tracked under the activity A00009297 and is addressed in section <2.3>

Note: when displaying error IPDR records, the displayQoS utility adds a textual description to the error code value.

Note: when displaying Unexpected Record Sequence Number error IPDR records, the displayQoS utility extracts the previous sequence number value from the proprietaryErrorCode and displays it as a separate field, Previous seq num.

1.3.4 Installation

The QCA application (NTQCA.pkg) is available in the CS2M² software package. Below are the steps to install the QCA

- Insert the CD with the CS2M load and log onto the SESM server as root. Then change the directory to the bin directory on the CD.

```
cd /cdrom/cdrom0/bin
```

- To start the install process, enter the following command.

```
./appl_mgr.ksh
```

Note: Select option 1 to install all the application along with QCA.

Below are the steps when QCA needs to be installed on a SSPFS machine which does not run the CS2M load.

- FTP the NTQCA.pkg onto the SSPFS machine. Log in as root.
- Install the new QCA software using: `pkgadd -d NTQCA.pkg`

Below are the steps to follow to uninstall the QCA package.

- Connect to the host where the QCA is running.
- Log in as root.
- Stop the QCA server: `stop_qca`.
- Uninstall the original QCA package: `pkgrm NTQCA`.

1.3.5 Upgrades

As of SN06.2, the QCA is a patchable component. The patchability mechanism conflicts with the in-service upgrade mechanism. So the support for in-service upgrade of QCA on a single SSPFS machine is removed. Please see section 2.2.15 for more details.

The QCA software upgrades are performed using the install scripts provided with QCA as part of the new software release. Software upgrades of QCA must be coordinated with the OSS to avoid loss of data. The OSS would be redirected to an alternative QCA instance while the primary QCA is being updated. Once the primary instance is updated, the OSS can be redirected back to the primary instance and the other instances can be updated.

1.3.6 QCA customer logs

In addition to QCA Error IPDR Records the QCA raises alarms and events via the customer logging stream.

2. CS2M (CS 2000 Management Components) refers to a NCL software package used on the CS 2000 management tools server. This package includes SESM, NPM, SAM21EM, QCA.

The QCA uses the logging API introduced by activity 89008996 “Log Reporting and Storage Mechanism for Managed Elements”.

Figure 4 Sample customer log message generated by QCA

```
Oct 11 12:00:02 wmdhs0j8 main:0001 QCA201 WARNING init wmdhs0j8
RetainFileTime property in properties/qca.properties is out of
range. QCA is starting with default retain file time of 5 days
```

The QCA customer logs contain the following fields

- Report name
- Report Number
- Priority
- Event Type
- Device ID
- Message

All the QCA customer logs contain the following information:

- Report name = “QCA”
- Device ID = QCA host name

See Appendix A - QCA Customer Logs for a summary of QCA customer logs and the contents of the other fields in the logs.

The QCA also generates debug logs to report software errors.

1.3.7 Patchability

In SN06.2, the activity A00003229 provides the functionality of making the QCA a patchable OAM device. The Network Patch Manager is responsible for administering individual fixes to QCA. Patches for the QCA will be in the same format and have the same naming convention of OAM patches such as NPM, SAM21EM, etc

When a QCA patch (containing modified Java-based classes) is delivered to a customer site, the patch is applied and then the QCA application is required to be stopped and then restarted by the NPM for the patch to be ‘enabled’. The restart enables a new Java Virtual Machine to be started that picks up the patched/modified Java classes. This procedure also applies to removal of QCA patches. For a QCA patch to be truly removed, the patch is removed and then a restart must be performed via the NPM on the application.

The QCA application must be inservice to perform any maintenance operations such as application, removal, or restart. In addition, the QCA application must be inservice for an audit to succeed. Because QCA is monitored or polled by an external system (OSS) for performance data or SLA agreements, it is important that any changes to QCA be coordinated to avoid loss of data or duplication of data. The OSS should be moved from monitoring the primary instance of QCA to an alternative QCA instance while the primary QCA is being updated via the restart request initiated by NPM. Once the primary instance is updated, the OSS should be redirected back to the primary instance and the other instances can be updated.

Since QCA is an OAM software application, it will be registered in the NPM database upon system start-up and initialization, and it will appear as a device with the device name QCA_<node_name>, where node_name is the name of the SSPFS machine where the QCA is running. Reports and queries at the NPM Graphical User Interface (GUI) and NPM Command Line User Interface (CLUI) will show the QCA as a device.

In SN06.2, the support for in-service QCA upgrade (on a single SSPFS machine) is removed to enable QCA patchability. Hence, the scripts to start and stop the second instance of QCA (qca_server2 and stop_qca2) will be obsoleted in this release.

The following sections briefly give information about applying/removing patches to/from QCA.

1.3.7.1 Applying patch to QCA

The following steps are a recommended procedure in applying QCA patches to a QCA application.

- QCA patch files are delivered to a customer site to the SSPFS machine containing the NPM server via RPS/PFRS or by manual action.
- QCA patches are introduced to the NPM database via the NPM CLUI with the 'getpatch' command.
- QCA patches are applied to the QCA application via the NPM apply command at the NPM GUI or NPM CLUI.

After all the QCA patches are applied, a restart command from the NPM GUI or NPM CLUI is invoked on the QCA application to enable or activate the patches.

Note: A restart consists of stopping the QCA application and then starting the application. It is important that any maintenance activities associated with the QCA should be completed or stopped before the restart from the NPM GUI or CLUI is invoked. Also, the OSS should be directed from the primary instance of QCA to an alternative instance prior to the restart. The NPM restart will result in current active file being moved into the *today*

directory and a new active file will be opened. The whole of this operation will take around **60 seconds**, during this period any QoS records sent from GWC to QCA will be lost.

Also, a NPM restart will result in following logs.

1. NPM 620: Initiated restart on device,<qca_devicename>.
2. GWC 312: QCA connection failure, indicating that GWC is having communication problems with QCA.
3. NPM 620: A restart initiated by the NPM on device <qca_devicename> has completed.
4. QCA 322: New GWC Connection, indicating that QCA has come up after the restart, and is accepting connections.
5. GWC 399: Clear event for GWC312, indicating that previous 'Raise' event is cleared.

Note: It is important to note the NPM database could show patches to be applied to an OAM device, but the patch is not actually enabled or performing its task to address the original problem. It is only after a restart is performed from the NPM GUI or CLUI on the OAM device that the patch is enabled.

- After the restart is performed on the QCA an NPM audit needs to be executed to update OAM patch enabled statuses in the NPM database. The audit can be performed manually from the NPM GUI or CLUI or it will be done automatically on the device approximately 20-25 minutes after the restart has been completed.

1.3.7.2 Removing Patch from QCA

The following steps are a recommended procedure in removing QCA patches from QCA.

- QCA patches are removed via the NPM remove command at the NPM GUI or NPM CLUI.
- After all QCA patches are removed, a restart command from the NPM GUI or NPM CLUI is invoked on the QCA to disable the patches.

Note: A restart consists of stopping the QCA application and then starting the QCA application. It is important that any maintenance activities associated with QCA should be completed or stopped before the restart from the NPM GUI or CLUI is invoked. Also, the OSS should be directed from the primary instance of QCA to an alternative instance prior to the restart. The NPM restart will result in current active file being moved into the *today* directory and a new active file will be opened. The whole of this operation will take around **60 seconds**, during this period any QoS records sent from GWC to QCA will be lost.

Also, a NPM restart will result in following logs.

1. NPM 620: Initiated restart on device,<qca_devicename>
2. GWC 312: QCA connection failure, indicating that GWC is having communication problems with QCA.
3. NPM 620: A restart initiated by the NPM on device <qca_devicename> has completed.
4. QCA 322: New GWC Connection, indicating that QCA has come up after the restart, and is accepting connections.
5. GWC 399: Clear event for GWC312, indicating that previous 'Raise' event is cleared.

Note: It is important to note the NPM database could show patches to be removed from an OAM device, but the patch is still enabled or performing its task to address the original problem. It is only after a restart is performed from the NPM GUI or CLUI on the OAM device that the patch is disabled.

- After the restart is performed on the QCA, an NPM audit needs to be executed to update QCA patch enabled statuses in the NPM database. The audit can be performed manually from the NPM GUI or CLUI or it will be done automatically on the device approximately 20-25 minutes after the restart has been completed.

1.3.7.3 AutoApply

QCA patches can be automatically applied if the end user has the automated process scheduled to run. Refer to the NPM online help for more information on this automated process.

1.3.7.4 Restart and AutoRestart Restrictions

Due to the implications to the OSS, restrictions are placed on the NPM restart command for QCA devices. The following restrictions are enforced by the NPM:

- QCA devices are not included in the set of OAM devices that can be auto-restarted, nor can a QCA restart be included in any plans scheduled at a designated time. Only a manual restart of a QCA device is supported.
- Only one QCA at a time can be restarted. The multitasking ability of NPM is not utilized for QCA.

A warning will be displayed to the user by the NPM CLUI or GUI explaining the implications of restarting QCA. The user will be forced to choose whether to continue with the restart command or to cancel.

1.3.8 QCA Software Management

The QCA application is designed to allow multiple copies to run in the network to provide increased levels of reliability. Additional copies of the QCA

application should be installed on different servers and assigned in the GWC EM. Two instances of QCA can not be installed on the two halves of the same high availability cluster; they must be on separate servers. Because QCA is monitored or polled by an external system (OSS) for performance data or SLA agreements, it is important that any changes to QCA be coordinated with the OSS to avoid loss of data or duplication of data. These changes include starting or stopping the application, applying corrective content, or applying upgrades. The OSS must be able to move from monitoring one instance of QCA to another during patching or upgrades or any activity that interrupts the QCA application. The OSS can either be manually redirected to another instance of QCA or programmed to automatically redirect on command.

1.4 Hardware Requirements or Dependencies

The QCA application has the following requirements:

- SUN Netra T1400

440Mhz UltraSPARCC IIi with QFE card, 4MB Cache, 512MB RAM, 2x18.2GB Disk Running SUN Solaris 8 Oracle DB 8.1.6 Enterprise and Java Virtual Machine.

Note: The QCA can run on the same SUN Netra T1400 that SESM and other network management tools are running on.

1.5 Software Requirements or Dependencies

- SSPFS 3d party software suite Version 06.

1.6 Limitations and restrictions

1.6.1 Upgrades

To ensure that the QCA support the version of QoS record used in the network, the QCA must be upgraded before the QoS reporting clients are upgraded.

Note: For a major release upgrade, where the SSPFS software is upgraded before the QCA, a QCA running on a separate host is required to ensure no loss of QoS records.

Note: For a QCA maintenance release upgrade or when applying patches, a QCA running on a separate host is required to ensure no loss of QoS records.

Note: Corrective content is applied and managed by the Network Patch Manager (NPM) in SN06.2. Because of the need to coordinate QCA changes like patching with the external OSS, QCA patches are manually applied and activated. This allows the OSS to be redirected to an alternative QCA instance while the primary QCA is being updated. Once

the primary instance is updated, the OSS can be redirected back to the primary instance and the other instances can be updated.

1.7 Interactions

- Syslog daemon server

1.8 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) _____

1.9 Glossary

Term	Description
ATM	Asynchronous Transfer Mode
CLLI	Common Language Location Identifier
CLUI	Command Line User Interface
CMTS	Cable Modem Terminal System
DPT	Dynamic Packet Trunk
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
GW	Gateway
GWC	Gateway Controller
IP	Internet Protocol

Term	Description
IOM	Input/Output Module
OC	Optical Carrier
OSS	Operations Support System
MGC	Media Gateway Controller
MS	Message Switch
NCS	Network Control System
NE	Network Element
NPM	Network Patch Manager
OL	Octets Lost
OR	Octets Received
OS	Octets Lost
PFRS	Patch File Receipt System
PL	Packets Lost
PR	Packets Received
PL	Packets Sent
PSE	Patching Server Element
PVG	Passport Voice Gateway
QCA	QoS Collector Application
QoS	Quality of Service
RPS	Regional Patch Selector
SDM	SuperNode Data Manager
SESM	Succession Element and Subelement Manager
SLA	Service Level Agreement
SPM	Spectrum Peripheral Module
STM	Synchronous Transfer Mode
USP	Universal Signalling Processor
UTF	Universal Text Format
VMG	Virtual Media Gateway
VoIP	Voice over IP

Term	Description
XML	eXtensible Markup Language

1.10 References.

1. Activity 89007790 - QoS Reporting: Correlation ID and billing
2. Activity 89007749 - QoS Reporting: GWC QoS Reporting Application and Connection Management
3. Activity 89007781 - QoS Reporting: Provisioning
4. Activity 59039902 - SNMP Performance Measurement Poller
5. Activity 89008996 - Log Reporting and Storage Mechanism for Managed Elements
6. Activity 00009297 - QoS SR Support of AAL2 and Timestamp.
7. Activity 00009189 - CS2M support for 64 Character Gateway name.

Appendix A - QCA Customer logs

Table 1 Service summary (initialization) warning logs

Event / Error	Report Number	Priority	Event Type	Description	QCA Action	Customer Action
Qca.properties not available at QCA start-up.	201	Warning	INIT	Properties file (properties/qca.properties) not available. QCA is starting with default settings.	Default used	None
portNumber property not in properties/qca.properties at QCA start-up.	201	Warning	INIT	portNumber property not in properties/qca.properties. QCA is starting with default port number of 20000	Default used	None
portNumber property in properties/qca.properties not in range at QCA start-up.	201	Warning	INIT	portNumber property in properties/qca.properties not in range. QCA is starting with default port number of 20000	Default used	None
portNumber property in properties/qca.properties not a number at QCA start-up.	201	Warning	INIT	portNumber property in properties/qca.properties could not be used. QCA is starting with default port number of 20000	Default used	None
MaxFileSize property not in properties/qca.properties.	201	Warning	INIT	MaxFileSize property not in properties/qca.properties. QCA is starting with default maximum file size of 1 MByte	Default used	None

Table 1 Service summary (initialization) warning logs

Event / Error	Report Number	Priority	Event Type	Description	QCA Action	Customer Action
MaxFileSize property in properties/qca.properties not in range.	201	Warning	INIT	MaxFileSize property in properties/qca.properties not in range. QCA is starting with default maximum file size of 1 MByte	Default used	None
MaxFileSize property in properties/qca.properties not a number.	201	Warning	INIT	MaxFileSize property in properties/qca.properties could not be used. QCA is starting with default maximum file size of 1 MByte	Default used	None
MaxFileTime property not in properties/qca.properties.	201	Warning	INIT	MaxFileTime property not in properties/qca.properties. QCA is starting with default maximum file time of 15 minutes	Default used	None
MaxFileTime property in properties/qca.properties not in range.	201	Warning	INIT	MaxFileTime property in properties/qca.properties not in range. QCA is starting with default maximum file time of 15 minutes	Default used	None
MaxFileTime property in properties/qca.properties not a number.	201	Warning	INIT	MaxFileTime property in properties/qca.properties could not be used. QCA is starting with default maximum file time of 15 minutes	Default used	None
RetainFileTime property not in properties/qca.properties.	201	Warning	INIT	RetainFileTime property not in properties/qca.properties. QCA is starting with default retain file time of 5 days	Default used	None
RetainFileTime property in properties/qca.properties not in range.	201	Warning	INIT	RetainFileTime property in properties/qca.properties not in range. QCA is starting with default retain file time of 5 days	Default used	None
RetainFileTime property in properties/qca.properties not a number.	201	Warning	INIT	RetainFileTime property in properties/qca.properties could not be used. QCA is starting with default retain file time of 5 days	Default used	None
recycleToD property not in properties/qca.properties.	201	Warning	INIT	recycleToD property not in properties/qca.properties. QCA is starting with default recycle hour of day of 0	Default used	None
recycleToD property in properties/qca.properties not in range.	201	Warning	INIT	recycleToD property in properties/qca.properties not in range. QCA is starting with default recycle hour of day of 0	Default used	None

Table 1 Service summary (initialization) warning logs

Event / Error	Report Number	Priority	Event Type	Description	QCA Action	Customer Action
recycleToD property in properties/qca.properties not a number.	201	Warning	INIT	recycleToD property in properties/qca.properties could not be used. QCA is starting with default recycle hour of day of 0	Default used	None
fileExt property not in properties/qca.properties.	201	Warning	INIT	fileExt property not in properties/qca.properties. QCA is starting with default file extension of xml	Default used	None
oldFileCompression property not in properties/qca.properties.	201	Warning	INIT	oldFileCompression property not in properties/qca.properties. QCA is starting with default value of true	Default used	None
oldFileCompression property in properties/qca.properties not true or false.	201	Warning	INIT	oldFileCompression property in properties/qca.properties could not be used. QCA is starting with default value of true	Default used	None
closedFileCompression property not in properties/qca.properties.	201	Warning	INIT	closedFileCompression property not in properties/qca.properties. QCA is starting with default value of true	Default used	None
closedFileCompression property in properties/qca.properties not true or false.	201	Warning	INIT	closedFileCompression property in properties/qca.properties could not be used. QCA is starting with default value of true	Default used	None
nodeName property not in properties/qca.properties.	201	Warning	INIT	nodeName property not in properties/qca.properties. QCA is starting with default value of QCA	Default used	None
old file retention directory (today-x) is being removed.	202	None	INIT	File Recovery: removing closed file retention directory: <i>directory</i> as it is older than x days.	Directory removed	None
File found in active directory when QCA started.	202	None	INIT	File Recovery: file <i>file name</i> found in active directory. This could indicate that the QCA failed. Please check debug logs.	File completed (if necessary) and moved to today directory.	Check debug logs.

To comply with X.733, the structure of the logs will also contain following attributes. The logs are differentiated from each other by Specific Problem and Description attributes.

- Location : QCA Host Name
- Category : Appropriate category from X.733 list of available categories.
- Cause : Appropriate category from X.733 list of available cause-values.
- Time : Time at which log was generated.
- ComponentID : File /Directory path, GWC name (components causing generation of log)
- SpecificProblem : Text giving details of the specific-problem
- Description : Text describing the problem and/or giving more information.

Table 2 Trouble logs

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
File handler or server socket could not be started.	300	None	FAIL	QCA not started: Could not open server socket: <i>+reason</i> or QCA not started: Could not create File Handler: <i>+reason</i>	QCA not started	Rectify problem and re-start QCA.
Out of sequence QoS record received.	302	None	FLT	Out of Sequence QoS Record received. ' <i>MGC Type MGC number</i> ': sequence number = ' <i>record sequence number</i> ' previous sequence number = ' <i>last record sequence number</i> '	XML Error record generated.	None
Problem processing binary QoS record.	302	None	FLT	Problem processing binary QoS record: Sequence number = ' <i>record sequence number</i> ' Relevant MGC is mentioned in <i>Component ID</i> attribute of the log.	XML Error record generated. XML QoS Record not written to file.	None

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
QoS Record received with Unsupported Length. (Notification Id: 9)	301	Minor	FLT	Location: <hostName> Notification ID: 9 State: Raise Category:Processing Error Cause: Corrupt Data. Time:<time> Component Id: 'MGCType MGCNum' Specific Problem: The QCA has received records with <numberOfLengthErrors> length errors from the source. Description: If 10 (or more) records with unsupported length are received consecutively, Major fault log is generated and the connection is closed.	XML Error record generated. XML QoS Record not written to file.	Investigate why client is sent QoS Record with Unsupported Length
10 sequential QoS Records received with Unsupported Length.	301	Major	FLT	Location: <hostName> Notification ID: 9 State: Raise Category:Processing Error Cause: Version mismatch. Time:<time> Component Id: 'MGCType MGCNum' Specific Problem: 10 unsupported length records received. The connection to the client will be closed	Connection to client closed	Investigate why client is repeatedly sending Unsupported Length QoS records
QoS Record received with Unsupported Version. (Notification Id: 57)	301	Minor	FLT	Location: <hostName> Notification ID:57 State: Raise Category:Processing Error Cause: Version mismatch. Time:<time> Component Id: 'MGCType MGCNum' Specific Problem: The QCA has received records with <NumberOfVersionErrors> version errors from the source. Description: If 10 (or more) records with unsupported version are received consecutively, Major fault log is generated and the connection is closed.	XML Error record generated. XML QoS Record not written to file.	Investigate why client is sent QoS Record with Unsupported Version
10 sequential QoS Records received with Unsupported Version.	301	Major	FLT	Location: <hostName> Notification ID: 57 State: Raise Category:Processing Error Cause: Version mismatch. Time:<time>Component Id: 'MGCType MGCNum' Specific Problem: 10 unsupported version records received. The connection to the client will be closed.	Connection to client closed	Investigate why client is repeatedly sending Unsupported Length QoS records

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
The binary QoS Record header could not be processed.	305	None	FLT	Connection closed: Error while processing QoS record header: Client at, IP Address ' <i>client IP Address</i> '. Local Port ' <i>local port number</i> ' closed connection.	Connection to client closed	Investigate why client is sent QoS Record with faulty header
Disk space shortage, local disk requires more free space. Disk Space is below 100Mb.	310	Critical	TBL	Location: <hostName> Notification ID: 49 State: Raise Category:Processing Error Cause:StorageCapacityproblem. Time:<time>Component Id: /data/qca Specific Problem: checkDiskSpace() has shown that there is less than 104857600 bytes available on the local disk. More Space is required immediately.	None	More space must be created.
Disk Space is starting to run seriously low. This means that the available space is below 500Mb.	310	Major	TBL	Location: <hostName> Notification ID: 49 State: Raise Category:Processing Error Cause: StorageCapacityProblem. Time:<time>Component Id: /data/qca. Specific Problem:Less than 524288000 bytes available on the local disk.Critical alarm will be raised if disk space continues to drop.	None	More space must be created.
Disk space is below the minimum threshold. Initially set at 1Gb.	310	Minor	TBL	Location: <hostName> Notification ID: 49 State: Raise Category:Processing Error Cause: StorageCapacityProblem. Time:<time>Component Id: /data/qca. Specific Problem: Less than 1073741824 bytes available on the local disk. Major alarm will be raised if the disk space continues to drop.	None	More space must be created.
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.	315	Warning	FLT	Unable to get an unused file name for <fileName> Please check the output directory.	file null.xml used	Output directories need to be checked.

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
The QCA has failed to write the footer information to the active file whilst attempting to close. The active file might have been compressed without the footer information.	315	Warning	FLT	Cannot write the FOOTER to the active file. This file is corrupted FileName = <fileName>.	None	Check the file and confirm that all XML tags have been closed.
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.	315	None	FLT	Active file <fileName> has been removed. Data may have been lost. Creating new file, and attempting to write record again. Failure to do so will result in shutdown of the QCA	Attempts to create a new output file	File IO problems, if problem is resolved the Major alarm will be withdrawn.
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.	315	None	FAIL	Could not get new file to write records. File <fileName> is corrupted or removed. QCA shutting down.	QCA is stopped.	check: disk space and write permissions. If all is well try starting QCA again.
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.	315	None	FAIL	Could not write to the activefile. Active file exists but cannot write records to it. Reason unknown. QCA shutting down	QCA is stopped.	check: disk space and write permissions. If all is well try starting QCA again.

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
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.	315	None	FAIL	Cannot create directories under <i>output</i> directory. Cannot write records. QCA shutting down	QCA is stopped.	Check: directory structure, active and old files.
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.	315	None	FLT	Could not rename active file <fileName> to file <newFileName>. Please check write permissions for the output directory	Closed file remains in active directory.	Check the directories exist and all the write permissions.
Could not create new active file. Data is being lost.QCA must shut down.	315	None	FAIL	Could not get new file for writing. Critical Error: <reason>. QCA shutting down.	QCA is stopped.	Check the active directory for old files and permissions.
Attempt to compress an old active file has failed.	315	None	FLT	Could not compress file: <fileName>. File compression failed.	None	Check the active directory for old files and permissions.
Failed to rename directories on the Recycle_day proc. This is where all files are moved along a level and the last gets deleted.	315	None	FLT	Could not rename director from <dirName> to <newDirName>. Check disk space and permissions.	None	Check disk space and permissions.
New GWC connection received.	322	None	INFO	New GWC COnnection: ' <i>MGC Type MGC number</i> ': sequence number = ' <i>record sequence number</i> '	XML Error record generated	

Table 3 Information and alarm clear logs

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
Connection closed.	305	None	INFO	Connection closed. Client at, IP Address ' <i>client IP Address</i> '. Local Port ' <i>local port number</i> ' closed connection.	Connection to client closed	None
Client has stopped sending records with unsupported length (clear for QCA 301 Notification Id: 9)	399	None	INFO	Location: <Hostname> Notification Id: 9 State: Alarm Cleared Time: <time>	None	None
Client has stopped sending records with unsupported version (clear for QCA 301 Notification Id: 57)	399	None	INFO	Location: <Hostname> Notification Id: 57 State: Alarm Cleared Time: <time>	None	None
Critical disk space issue cleared (clear for 310 Critical Alarm)	399	None	INFO	Location: <Hostname> Notification Id: 49 State: Alarm Cleared Time: <time>	None	None
Major disk space issue cleared (clear for 310 Major Alarm)	399	None	INFO	Location: <Hostname> Notification Id: 49 State: Alarm Cleared Time: <time>	None	None
Minor disk space issue cleared (clear for 310 Minor Alarm)	399	None	INFO	Location: <Hostname> Notification Id: 49 State: Alarm Cleared Time: <time>	None	None

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
QCA cannot be stopped	203	None	INIT	Location: <Hostname> Category: PROCESSINGERROR Cause: CONFIGERROR Time: ComponentID: SpecificProblem: QCA not running on specified port: Description: Cannot stop QCA Action: Use query_qca command to determine the port QCA is running on. Make sure it matches with portNumber in qca.properties file."	Connection to client closed	None

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
QCA cannot be stopped	203	None	INIT	Location: <Hostname> Category: PROCESSINGERROR Cause: CONFIGERROR Time: ComponenetID: SpecificProblem: Missing qca.properties file. Description: Could not read properties. QCA cannot be stopped.Action:Restore qca.properties file.	None	None
QCA cannot be stopped	203	None	INIT	Location: <Hostname> Category: PROCESSINGERROR Cause: CONFIGERROR Time: ComponenetID: SpecificProblem: Attribute portNumber missing from qca.properties while trying to stop QCA. Description: Cannot determine QCA port number to stop QCA. Action: Add portNumber information to qca.properties file.	None	None
QCA cannot be stopped	203	None	INIT	Location: <Hostname> Category: PROCESSINGERROR Cause: CONFIGERROR Time: ComponenetID: SpecificProblem: Incorrect portNumber specified in qca.properties. Description: Cannot determine QCA port number to stop QCA Action: Use query_qca command to determine the port QCA is running on. Make sure it matches with portNumber in qca.properties file.	None	None
QCA cannot be stopped	203	None	INIT	Location: <Hostname> Category: PROCESSINGERROR Cause: CONFIGERROR Time: ComponenetID: SpecificProblem: Out of range portNumber specified in qca.properties. Description: Cannot determine QCA port number to stop QCA. Action: Use query_qca command to determine the port QCA is running on. Make sure it matches with portNumber in qca.properties file.	None	None
Connection closed.	305	None	ERROR	Location: <Hostname> Category: COMMUNICATIONS Cause: COMMSUBFAIL Time: SpecificProblem: MSGTYPEERROR Description: Client at, IP Address: closed connection.	None	None
Connection closed.	305	None	INFO	Location: <Hostname> Category: COMMUNICATIONS Cause: COMMSUBFAIL Time: SpecificProblem: CONNECTIONCLOSED Description: Client at, IP Address: closed connection.	None	None

Event / Error	Report Number	Priority	Event Type	Message	QCA Action	Customer Action
Connection closed.	305	None	ERROR	Location: <Hostname> Category: COMMUNICATIONS Cause: COMMSUBFAIL Time: SpecificProblem: HEADERERROR. Description: Client at, IP Address: closed connection	None	None
Connection closed.	305	None	INFO	Location: <Hostname> Category: COMMUNICATIONS Cause: COMMSUBFAIL Time: SpecificProblem: CONNECTIONCLOSED. Description: Client at, IP Address: closed connection	None	None
Connection closed.	305	None	INFO	Location: <Hostname> Category: COMMUNICATIONS Cause: COMMSUBFAIL Time: SpecificProblem: nCONNECTIONCLOSED Description: Client at, IP Address: closed connection	None	None

Appendix B- QCA Customer log Sample Exact Format

Log Report 201:

Table 1 201 Message

Report Number	Message
201	May 27 16:41:45 rtpysesm1 QCA: _V2_~l=rtpysesm1~H=rtpysesm1~A=QCA~S=0000~~ QCA201 WARNING INIT rtpysesm1 ^M Location: rtpysesm1^M Category: processingError^M Cause: configurationOrCustomizationError^M Time: May 27 16:41:45 2005^M ComponentID: /opt/nortel/qca/properties/qca.properties^M SpecificProblem: Missing qca.properties file.^M Description: Could not read properties. QCA is starting with default settings.^M

Log Report 202:

Table 2 202 Message

Report Number	Message
202	Aug 19 22:22:02 wnc0s0qu QCA: _V2_~l=wnc0s0qu~H=wnc0s0qu~A=QCA~S=0000~~ QCA202 NONE INIT wnc0s0qu ^M Location: wnc0s0qu^M Category: processingError^M Cause: fileError^M Time: Aug 19 22:22:02 2004^M ComponentID: /data/qca/20000/output/active/^M SpecificProblem: Old file(s) present in active directory.^M Description: Moving old file: QCA.QCA.QoS.2004.08.19_22.19_EDT.xml, found in active directory. This could indicate that QCA failed.^M

Log Report 203**Table 3 203 Message**

Report Number	Message
203	May 30 22:55:50 india1sesm QCA_STOP: _V2_~I=india1sesm~H=india1sesm~A=QCA_STOP~S=0000~~ QCA203 NONE INIT india1sesm^M Location: india1sesm^M Category: processingError^M Cause: configurationOrCustomizationError^M Time: May 30 22:55:50 2005^M ComponentID: /opt/nortel/qca/properties/qca.properties^M SpecificProblem: Missing qca.properties file.^M Description: Could not read properties. QCA cannot be stopped.^M Action: Restore qca.properties file.^M

Log Report 300**Table 4 300 Message**

Report Number	Message
300	May 31 04:22:08 india1sesm QCA: _V2_~I=india1sesm~H=india1sesm~A=QCA~S=0002~~ QCA300 NONE FAIL india1sesm ^M Location: india1sesm^M Category: processingError^M Cause: communicationsSubsystemFailure^M Time: May 31 04:22:08 2005^M ComponentID: GWC- 99^M SpecificProblem: Socket creation error.^M Description: QCA not started:^M

Log Report 302**Table 5 302 Message**

Report Number	Message
302	May 31 04:22:08 india1sesm QCA: _V2_~I=india1sesm~H=india1sesm~A=QCA~S=0002~~ QCA302 NONE FLT india1sesm ^M Location: india1sesm^M Category: processingError^M Cause: informationOutOfSequence^M Time: May 31 04:22:08 2005^M ComponentID: GWC-99^M SpecificProblem: Unexpected Record Sequence Number^M Description: Out of sequence QoS record received. Sequence Number = 1670001 Previous sequence number = 0^M

Log Report 305**Table 6 305 Message**

Report Number	Message
305	Aug 19 22:18:34 wnc0s0qu QCA: _V2_~l=wnc0s0qu~H=wnc0s0qu~A=QCA~S=0121~~ QCA305 NONE INFO wnc0s0qu ^M Location: wnc0s0qu^M Category: communications^M Cause: communicationsSubsystemFailure^M Time: Aug 19 22:18:34 2004^M SpecificProblem: Connection closed^M Description: Client at, IP Address: kiran-1.ca.nortel.com. Port: 2512 closed connection.^M

Log Report 310**Table 7 310 Message**

Report Number	Message
310	May 30 22:52:45 india1sesm QCA: _V2_~l=india1sesm~H=india1sesm~A=QCA~S=0000~~ QCA310 CRIT TBL india1sesm ^M Location: india1sesm^M NotificationID: 49^M State: Raise^M Category: Processing Error^M Cause: storageCapacityProblem^M Time: May 30 22:52:44 2005ComponentID: /data/qca/^M SpecificProblem: checkDiskSpace() has shown that there is less than ^M 104857600 bytes available on the local disk.^M Description: More Disk space is required immedietly.^M

Log Report 315**Table 8 315 Message**

Report Number	Message
315	Aug 19 22:15:43 wnc0s0qu QCA: _V2_~l=wnc0s0qu~H=wnc0s0qu~A=QCA~S=0001~~ QCA315 NONE FLT wnc0s0qu ^M Location: wnc0s0qu^M Category: processingError^M Cause: fileError^M Time: Aug 19 22:15:43 2004^M ComponentID:/data/qca/20000/output/active//data/qca/20000/output/active/QCA.QCA.QoS.2004.08. 19_22.12_EDT.xml^M SpecificProblem: Active file: /data/qca/20000/output/active/QCA.QCA.QoS.2004.08.19_22.12_EDT.xmlhas been removed/deleted.^M Description: Data may have been lost. Creating new file, and attempting to write records again. Failure to do so will result in QCA shutdown.^M

Log Report 322**Table 9 322 Message**

Report Number	Message
322	Aug 19 22:15:43 wnc0s0qu QCA: _V2_~l=wnc0s0qu~H=wnc0s0qu~A=QCA~S=0004~~ QCA322 NONE INFO wnc0s0qu ^M Location: wnc0s0qu^M Category: communications^M Time: Aug 19 22:15:43 2004^M ComponentID: GWC-17^M SpecificProblem: New GWC connection^MDescription: New connection from GWC-17. Sequence Number = 1^M

Log Report 399**Table 10 399 Message**

Report Number	Message
399	Aug 18 06:49:08 wnc0s0qu QCA: _V2_~l=wnc0s0qu~H=wnc0s0qu~A=QCA~S=0087~~ QCA399 NONE INFO wnc0s0qu ^M Location: wnc0s0qu^M NotificationID: 49^M State: Cleared^M Time: Aug 18 06:49:08 2004^M

*** NOTE: (There are no changes in Alarms as a result of feature A00008338)

1> There are 3 different Types of Alarms uniquely identified by the Notification ID

a> Notification ID: 9

Event: Client is sending Records with unsupported Length.

Raise Severity (Major or Minor)

Raise Customer Log Report Number: QCA 301

Clear Severity: (None)

Clear Customer Log Report Number: QCA 399.

b> Notification ID: 57

Event: Client is sending Records with unsupported Version.

Raise Severity (Major or Minor)

Raise Customer Log Report Number: QCA 301

Clear Severity: (None)

Clear Customer Log Report Number: QCA 399.

c> Notification ID: 49

Event: Critical/Major/Minor Disk Space issue.

Raise Severity (Critical, Major or Minor)

Raise Customer Log Report Number: QCA 310.

Clear Severity: (None)

Clear Customer Log Report Number: QCA 399.

Example of Raise/Clear Alarms:

Table 11 301 Message- Raise

Report Number	Message
301	May 31 07:37:20 india1sesm QCA: _V2_~I=india1sesm~H=india1sesm~A=QCA~S=0001~~ QCA301 MINOR FLT india1sesm ^M Location: india1sesm^M NotificationID: 9^M State: Raise^M Category:Processing Error^M Cause: corruptData^M Time: May 31 07:37:20 2005^M ^M ComponentID: GWC99^M SpecificProblem: The QCA has received records with 1 length errors from the source.^M Description: If 10 (or more) records with unsupported length^M are received consecutively, Major fault log is generated^M and the connection is closed.^M

Table 12 399 Message- Clear

Report Number	Message
399	May 31 07:39:47 india1sesm QCA: _V2_~I=india1sesm~H=india1sesm~A=QCA~S=0001~~ QCA399 NONE INFO india1sesm ^M Location: india1sesm^M NotificationID: 9^M State: Cleared^M Time: May 31 07:39:47 2005^M

Appendix C- Increasing the size of a file system on a Sun server

Application

Use one of the following procedures to increase the size of a file system on a Succession Server Platform Foundation Software (SSPFS)-based server:

- Simplex configuration (one server)

- High-availability configuration (two servers)

It is recommended you perform this procedure during off-peak hours.

The Succession Server Platform Foundation Software (SSPFS) creates file systems to best fit the needs of applications. However, it may be necessary to increase the size of a file system.

Not all file systems can be increased. The table below lists the file systems that cannot be increased, and lists examples of those that can be increased.

SSPFS file systems

Cannot be increased	Can be increased (examples)
/ (root)	/data
/var	/opt/nortel
/opt	/data/oradata
/tmp	/audio_files
/PROV_data	
/user_audio_files	
/data/qca	
/data/mg9kem/logs	

During the time file systems are being increased, writes to the file system are blocked, and the system activity increases. The more size that is added to the file system, the greater the impact on performance.

Prerequisites

Before you perform this procedure, verify that the file system is full or nearly full and that its content is valid application data. Remove any unneeded files or files generated in error that could be taking up disk space.

Action

Perform the following steps to complete this procedure.

Simplex configuration (one server)

At your workstation

1> Telnet to the Sun server by typing

> telnet <server>

and pressing the Enter key.

where

server

is the IP address or host name of the Sun server that has the file system you want to increase

2> When prompted, enter your user ID and password.

3> Change to the root user by typing

\$ su - root

and pressing the Enter key.

4> When prompted, enter the root password.

5> Access the command line interface by typing

cli

and pressing the Enter key.

Example response

Command Line Interface 1 - View

2 - Configuration

3 - Other

X - exitselect -

6> Determine which file system to increase by checking the current disk capacity utilization as follows:

a> Enter the number that corresponds to the "View" option in the menu.

Example response

View 1 - sspfs_soft (Display Software Installation Level Of SSPFS) 2 - chk_sspfs (Check SSPFS Processes) 3 - sw_conf (The software configuration of the znc0s0jx) 4 - cpu_util (Overall CPU utilization) 5 - cpu_util_proc (CPU utilization by process) 6 - port_util (I/O port utilization) 7 - disk_util (Filesystem utilization) X - exitselect -

b> Enter the number that corresponds to the “disk_util” option in the menu.

Example response

7> Determine the appropriate size for the file systems based on your specific needs.

8> Exit each menu level of the command line interface to eventually exit the command line interface, by typing

select - x

and pressing the Enter key.

9>

ATTENTION

Once you increase the size of a file system, you cannot decrease it.

Increase the size of the file system by typing

```
# filesystems grow -m <mount_point> -s <size>{m,g}
```

Where

mount_point

is the name associated with the file system

- /data
- /opt/nortel
- /data/oradata
- /PROV_data
- /audio_files
- /user_audio_files
- /data/qca
- /data/mg9kem/logs

size
is the size in megabytes (m) or gigabytes (g) you obtained in
step 7

Example# filesys grow -m /data/qca -s 512m

Note: The example above increases the “/data” file system by 512 megabytes (MB).

10> You have completed this procedure.

High-availability configuration (two servers)

ATTENTION

During this procedure, the cluster will be running without a standby node. The duration is estimated at approximately one hour.

At your workstation

1> Telnet to the inactive node of the server cluster by typing

> telnet <server>

and pressing the Enter key.

where

server

is the physical IP address of the inactive node in the server cluster

2> When prompted, enter your user ID and password.

3> Change to the root user by typing

\$ su - root

and pressing the Enter key.

4> When prompted, enter the root password.

5> Ensure the cluster is in a good state as follows:

a> Run the udstat command by typing

udstat

and pressing the Enter key.

If the system response contains “nodaemon”, “offline”, “down”, “not mounted”, contact your next level of support. Otherwise, proceed to the next step.

b> Run the ubmstat command by typing

```
# ubmstat
```

and pressing the Enter key.

If the system response is other than “ClusterIndicatorSTBY”. contact your next level of support. Otherwise, proceed to the next step.

c> Run the CheckConfiguration command by typing

```
# CheckConfiguration
```

and pressing the Enter key.

If the system response is other than “Checking local cluster configuration against <other node>”, contact your next level of support. Otherwise, proceed to the next step.

At the Inactive node

6>

ATTENTION

Once you increase the size of a file system, you cannot decrease it.

Increase the size of the desired file system by typing

```
# GrowClusteredFileSystem.ksh <mount_point> <size>{m,g}
```

Where

mount_point

is the name associated with the file system, for example

- /data
- /opt/nortel
- /data/oradata
- /PROV_data
- /audio_files
- /user_audio_files

•/data/qca

•/data/mg9kem/logs

size

is the size in megabytes (m) or gigabytes (g)

Example# GrowClusteredFileSystem.ksh /data/qca 10m

Note: The example above increases the "/data/qca" file system by 10 megabytes (MB).

7> Reboot the Inactive node by typing

init 6

and pressing the Enter key.

8> Wait for the Inactive node to reboot, then log in again using its physical IP address.

9> Telnet to the active node of the Sun server cluster by typing

> telnet <server>

and pressing the Enter key.

where

server

is the physical IP address of the active node in the Sun server cluster

10> When prompted, enter your user ID and password.

11> Change to the root user by typing

\$ su - root

and pressing the Enter key.

12> When prompted, enter the root password.

At the Active node

13> Stop the cluster by typing

StopCluster

and press the Enter key.

This action causes a cluster failover and makes the active node inactive, and the inactive node active.

At the newly Active node

14> Clone the other node using procedure Cloning the image of one node in a cluster to the other node on page 9 in this document.

15> You have completed this procedure.

Document Reference:

For increasing the size of a file system on an SSPFS-based server refer NN10402-600.

Appendix D: List of GWs that Report End of Call QoS Statistics.

12.1 GWs Supported

Table 1 : SN06

GW	SN06 Validation Level	SN06 Comments	Future Plans (Beyond SN06)
UAS (H.248)	Full	Does not currently report all stats. The stats that are reported depend on the mode: SendOnly: PS, OS SendRecv: PS, OS, PR, OR, PL RecvOnly: PR,OR,PL	
Motorola CG4500 (NCS)	Full	5.x stream. all stats reported. Latency calculation is not PacketCable compliant.	
PVG (Aspen/VS P2)	Full	All stats reported.	
PVG (Aspen/VS P3)	None	All stats reported.	
PVG (H.248)	None	All stats reported.	
Mediatrix (MGCP)	Partial		
Arris PacketPort (MGCP)	Full		

Table 1 : SN06

GW	SN06 Validation Level	SN06 Comments	Future Plans (Beyond SN06)
Arris TTM/TTP (NCS)	Partial		
Askey	Partial	Validated basic functionality during End to End IT. Will do further testing during PV.	
CICM	None	CICM does not currently report end of call stats to the GWC.	Requirement submitted to CICM team, negotiating inclusion into SN07.

Table 2

GW	SN06.2 Validation Level	SN06.2 Comments	Future Plans (Beyond SN06.2)
UAS		Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	
MS2010 (Megaco/H.248)		Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	
PVG (H.248)		All stats reported.	
H.248M2K		All Stats reported.	
Ambit MG1K		All Stats reported.	
Ambit 32		All Stats supported.	
PVG PP15K (VSP3 and VSP3oCard)		All Stats supported.	
PVG PP15K and PP7k (VSP2)		All parameters reported other than Jitter and inter-arrival latency which not measured.	

GW	SN06.2 Validation Level	SN06.2 Comments	Future Plans (Beyond SN06.2)
UAS		Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	
MS2010 (Megaco/H.248)		Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	
PVG (H.248)		All stats reported.	
H.248M2K		All Stats reported.	
Ambit MG1K		All Stats reported.	
Ambit 32		All Stats supported.	
PVG PP15K (VSP3 and VSP3oCard)		All Stats supported.	
PVG PP15K and PP7k (VSP2)		All parameters reported other than Jitter and inter-arrival latency which not measured.	

GW	SN07.0 Validation Level	SN07.0 Comments	Future Plans (Beyond SN07.0)
UAS		Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	
MS2010 (Megaco/H.248)		Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	
PVG (H.248)		All stats reported.	
H.248M2K		All Stats reported.	
Ambit MG1K		All Stats reported.	
Ambit 32		All Stats supported	
PVG PP15K (VSP3 and VSP3oCard)		All Stats supported	

GW	SN07.0 Validation Level	SN07.0 Comments	Future Plans (Beyond SN07.0)
PVG PP15K and PP7k (VSP2)		All parameters reported other than Jitter and inter-arrival latency which not measured.	

GW	SN08.0 Validation Level	SN08.0 Comments	Future Plans (Beyond SN08.0)
Motorola MTA2	Y	All Stats Reported	
TTM/TTP Profile	Y	All Stats Reported	
ASKEY (4/12/30 Port Profile)	Y	All Stats Reported.	
Mediatrix 1104/1124 Profile	Y	All Stats Reported.	
UAS	Y	Does not currently report all stats. Does not report Jitter and Inter- arrival Latency.	
MS2010 (Megaco/H.24 8)	Y	Does not currently report all stats. Does not report Jitter and Inter- arrival Latency.	
PVG (H.248)	Y	All stats reported.	
H.248M2K		All Stats reported.	
Ambit MG1K		All Stats reported.	
Ambit 32	Y	All Stats supported	
PVG PP15K (VSP3 and VSP3oCard)		All Stats supported	
PVG PP15K and PP7k (VSP2)	Y	All parameters reported other than Jitter and inter-arrival latency which not measured.	

Appendix E - QCA Versions available and the Binary content for each version

The following are the QoS Binary versions generated by loads in various releases. Version 1, 2, and 3 are for SN07, SN08 and SN09 Releases. Version 4, 5 are for patched SN07 and patched SN08 loads.

For Version 1:

132 byte - QoS binary message. Bytes are counted from 0 to N-1.

Header – 8 bytes (byte 0 to 7)
Codec – 2 bytes (byte 8 and 9)
Port Number – 2 bytes (byte 10 and 11)
IP Address – 4 bytes (byte 12 to 15)
GW Name – 32 bytes (byte 16 to 47) (first 32 bytes of FQDN)
End Point – 32 bytes (byte 48 to 79)
CLLI – 16 bytes (byte 80 to 95)
CorrID – 10 bytes (byte 96 to 105)
Two Byte Filler – 2 bytes (byte 106 and 107)
PacketSent – 4 bytes (byte 108 to 111)
PacketReceived – 4 bytes (byte 112 to 115)
OctetSent – 4 bytes (byte 116 to 119)
OctetReceived – 4 bytes (byte 120 to 123)
packetLost – 4 bytes (byte 124 to 127)
Jitter – 2 bytes (byte 128 and 129)
Latency – 2 bytes (byte 130 and 131)

For Version 4: (Jitter and latency mapping)

132 byte - QoS binary message. Bytes are counted from 0 to N-1.

Header – 8 bytes (byte 0 to 7)
Codec – 2 bytes (byte 8 and 9) (Byte 8 and 9 holds information about the MSBytes of Jitter)
Port Number – 2 bytes (byte 10 and 11)

IP Address – 4 bytes (byte 12 to 15)
GW Name – 32 bytes (byte 16 to 47) (first 32 bytes of FQDN)
End Point – 32 bytes (byte 48 to 79)
CLLI – 16 bytes (byte 80 to 95)
CorrID – 10 bytes (byte 96 to 105)
Two Byte Filler – 2 bytes (byte 106 and 107) (Byte106 and 107 holds the MSBytes of Latency component)
PacketSent – 4 bytes (byte 108 to 111)
PacketReceived – 4 bytes (byte 112 to 115)
OctetSent – 4 bytes (byte 116 to 119)
OctetReceived – 4 bytes (byte 120 to 123)
packetLost – 4 bytes (byte 124 to 127)
Jitter – 2 bytes (byte 128 and 129)
Latency – 2 bytes (byte 130 and 131)

Jitter and latency in Version 4 is of 4 bytes each, MSBytes of Jitter and Latency are obtained from Codec field and Filler byte fields of Version 1 respectively.

For Version 2:

136 byte - QoS binary message. Bytes are counted from 0 to N-1.

Header – 8 bytes (byte 0 to 7)
Codec – 2 bytes (byte 8 and 9)
Port Number – 2 bytes (byte 10 and 11)
IP Address – 4 bytes (byte 12 to 15)
GW Name – 32 bytes (byte 16 to 47) (first 32 bytes of FQDN)
End Point – 32 bytes (byte 48 to 79)
CLLI – 16 bytes (byte 80 to 95)
CorrID – 10 bytes (byte 96 to 105)
Two Byte Filler – 2 bytes (byte 106 and 107)
PacketSent – 4 bytes (byte 108 to 111)
PacketReceived – 4 bytes (byte 112 to 115)
OctetSent – 4 bytes (byte 116 to 119)

OctetReceived – 4 bytes (byte 120 to 123)
packetLost – 4 bytes (byte 124 to 127)
Jitter – 4 bytes (byte 128 and 131)
Latency – 4 bytes (byte 132 and 135)

For Version 5: (Timestamp Patched load)

144 byte - QoS binary message. Bytes are counted from 0 to N-1.

Header – 8 bytes (byte 0 to 7)
Codec – 2 bytes (byte 8 and 9)
Port Number – 2 bytes (byte 10 and 11)
IP Address – 4 bytes (byte 12 to 15)
GW Name – 32 bytes (byte 16 to 47) (first 32 bytes of FQDN)
End Point – 32 bytes (byte 48 to 79)
CLLI – 16 bytes (byte 80 to 95)
CorrID – 10 bytes (byte 96 to 105)
Two Byte Filler – 2 bytes (removed)
STime – 5 bytes (byte 106 to 110)
ETime – 5 bytes (byte 111 to 115)
PacketSent – 4 bytes (byte 116 to 119)
PacketReceived – 4 bytes (byte 120 to 123)
OctetSent – 4 bytes (byte 124 to 127)
OctetReceived – 4 bytes (byte 128 to 131)
packetLost – 4 bytes (byte 132 to 135)
Jitter – 4 bytes (byte 136 and 139)
Latency – 4 bytes (byte 140 and 143)

For Version 3:

180 byte - QoS binary message. Bytes are counted from 0 to N-1.

Header – 8 bytes (byte 0 to 7)

Codec – 2 bytes (byte 8 and 9)
Port Number – 2 bytes (byte 10 and 11)
IP Address – 4 bytes (byte 12 to 15)
GW Name – 64 bytes (byte 16 to 79) (first 64 bytes of FQDN)
End Point – 32 bytes (byte 80 to 111)
CLLI – 16 bytes (byte 112 to 127)
CorrID – 10 bytes (byte 128 to 137)
STime – 5 bytes (byte 138 to 142)
ETime – 5 bytes (byte 143 to 147)
PacketSent – 4 bytes (byte 148 to 151)
PacketReceived – 4 bytes (byte 152 to 155)
OctetSent – 4 bytes (byte 156 to 159)
OctetReceived – 4 bytes (byte 160 to 163)
packetLost – 4 bytes (byte 164 to 167)
Jitter – 4 bytes (byte 168 and 171)
Latency – 4 bytes (byte 172 and 175)
32 Bit Filler – 4 bytes (byte 176 and 179)

Header Field details:

```
// ----- Report Header variables -----
private int mgcType = -1;    // bits 0 to 3 of byte 0
private int messageType = -1; // bits 4 to 7 of byte 0
private int sequenceNumber = -1; // bytes 1 to 3
private int reportType = -1; // bits 0 to 3 of byte 4
private int version = -1;    // bits 4 to 7 of byte 4
private int mgcNumber = -1;  // byte 5
private int msgLength = -1;  // byte 6
private int ipVersion = -1;  // byte 7 (IP version 2-bits plus 6-bit filler)
// ----- End of Report Header variables -----
```

Product = Call Server 2000

A00013275 -- SESM Flex Large Line GWC Profile Support - Phase 1

1: Applicable solution(s)

Int'l UA-IP

1.1 Description

This feature provides generic support for large line gateways supporting up to a maximum of 2047 endpoints within a single virtual media gateway. This is initially aimed at supporting the Audiocodes TP6310 card as used within the Mediant 8000 chassis on behalf of C&W.

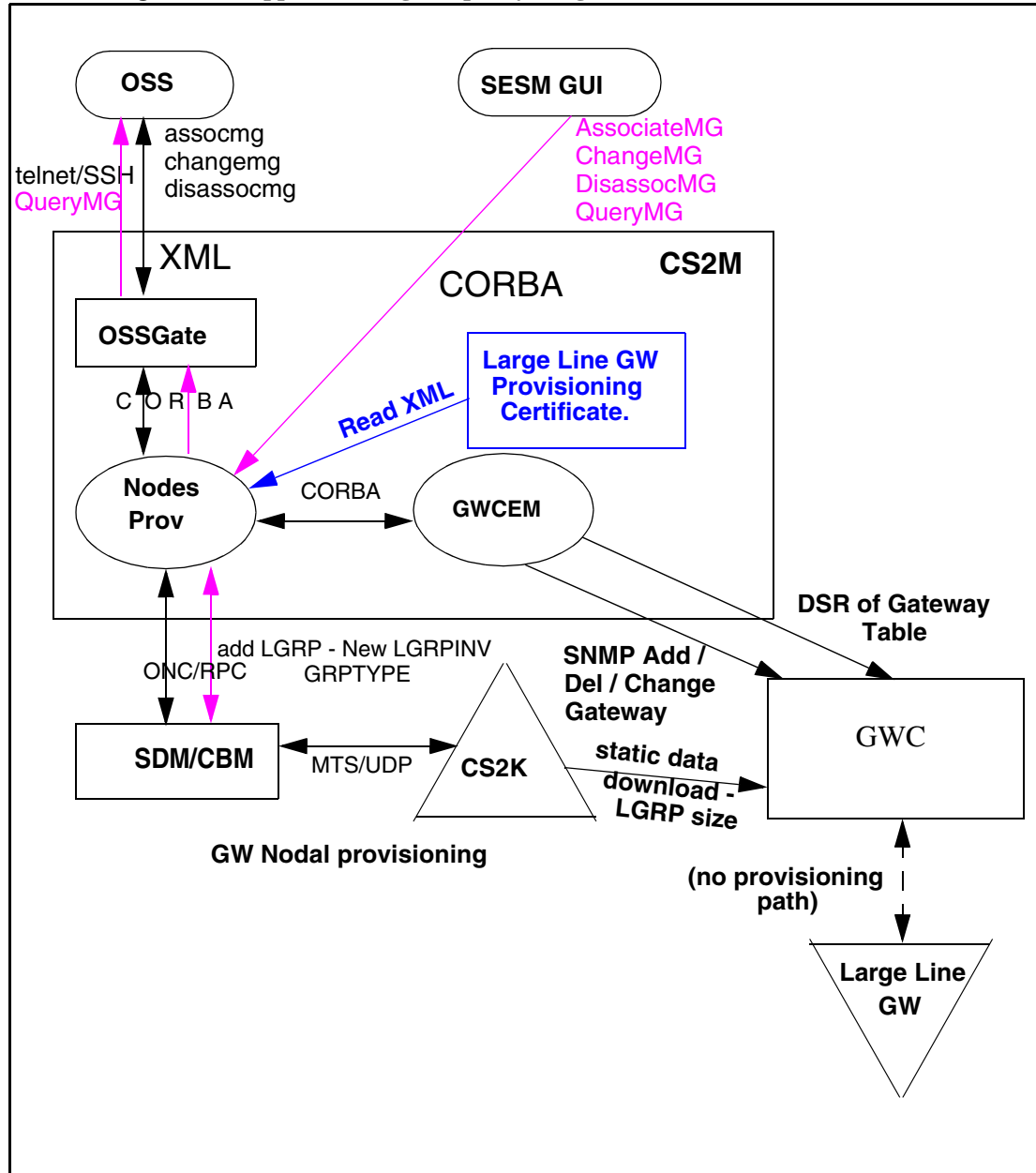
Additionally support is provided for the Audiocodes TP6310 card when configured as a trunk carrier gateway in order to support DPNSS.

The support for the Audiocodes TP6310 configured as a trunk gateway is restricted to this feature only, the corresponding associated GWC and CM features only cover the TP6310 when provisioned as a high capacity large line GW.

Prior to this feature large line gateways were limited to a maximum of 1024 endpoints, and in situations where additional endpoints were required this has been modelled by treating the gateway as multiple gateways from the perspective of the CM - examples being the CICM and SIP voice gateways.

This feature adds the following functionality to the CS2M:

- Support for the Audiocodes TP6310 card provisioned as a large line GW for use in the Mediant 8000 Gateway chassis.
- Support for the Audiocodes TP6310 card provisioned as a trunk GW for use in the Mediant 8000 Gateway chassis.
- Support for large line GWs of capacity <= 2047 endpoints.
- Support for both International and North American market fit.
- Support for both 750 and 905 GWC types.

Figure 1 Support For High Capacity Large Line GWs

1.1.1 Pre-Requisites

The following pre-requisites must be met before attempting to provision an Audiocodes M8K GW:

- The CS must be running an SN09.1 or later load.
- The CS2M should be running the SESM SN09.1 or later load.
- The GWC which will host the Audiocodes M8K GW must be provisioned with a profile supporting Large Line GWs and must be running the SN09.1 or later load.

1.1.2 Provisioning Of Audiocodes TP6310 Large Line GW - GUI Interface

Provisioning of the Audiocodes TP6310 Large Line GW is similar to existing 3rd party line GWs. The provisioning of 3rd party line type GWs is as per SN08 features A00007071 and A00007072. On selecting the “AUDIOCODES_6310_LINE” profile the Associate Media Gateway dialog will be populated as follows:

Figure 2 CS2M Associate Media Gateway GUI Population For TP6310 Line GW

The screenshot shows the 'Associate Media Gateway' dialog box with the following fields and values:

- Gateway name: audiocodes1.com
- Gateway IP address: 47.165.173.45
- Gateway controller name: GWC-105
- Gateway profile name: AUDIOCODES_6310_LINE
- Reserved terminations: (empty)
- Gateway site name: LG2K
- LGRP Location:
 - Frame number: 0
 - Unit number: 0
 - Frame type: (empty)
- Signal Protocol:
 - Protocol type: MEGACO (4)
 - Protocol port: 2944
 - Protocol version: 1.0

Annotations on the right side of the dialog:

- An arrow points to the 'Gateway profile name' dropdown with the text: **Select profile = AUDIOCODES_6310_LINE**
- An arrow points to the 'Reserved terminations' field with the text: **Reserved terminations 1 .. 2016. Default = 2016**

Buttons at the bottom: OK, Cancel

The Audiocodes TP6310 is a 3rd party GW. This means that the provisioning crafts person must define the LGRPINV tuple to be provisioned at the CM. The LGRPINV tuple consists of Site + Frame + Unit. In this example we are specifying and LGRPINV tuple of “LG2K 0 0”.

Table 1 Associate Media Gateway Field Population

Field	Contents
Gateway name	Provisioned GW Name. Max 32 characters. Follows DNS naming convention.
Gateway IP address	IP address for Audiocodes GW
Gateway controller name	GWC-nnn Name of a valid GWC provisioned with a large lines supporting profile.
Gateway profile name	AUDIOCODES_6310_LINE for TP6310 card as large line GW
Reserved terminations	In range 1 .. 2016. Defines number of terminations to reserve for use with this GW. If the field is left empty the default behaviour is to reserve 2016 terminations.
Gateway site name	From CM table SITE. Chosen site must be capable of supporting manually provisioned LGRPs of size 2048 (maximum 2047 endpoints)
Frame number	Logical frame number in range 0 .. 511 Combines with Site and unit number to form LGRP. The combination of all 3 must be unique.
Unit number	Logical unit number in range 0 .. 9 Combines with Site and Frame number to form LGRP. The combination of all 3 must be unique
Protocol type	MEGACO - H.248
Protocol port	defaults to 2944 but may be edited if desired
Protocol version	Fixed to version 1.0

Following successful provisioning of the Audiocodes TP6310 Line GW, the following will have occurred:

- GW will have been created at GWC.
- LGRP entry will have been created at CM.
- GW will exist within CS2M database.
- GW will be displayed at CS2M GUI (upon gateway list refresh).

Initially there will be no endpoints and associated LENSs provisioned at the GWC or CM, however the capacity to provision the required number of terminations will have been reserved.

Figure 3, on page 1619 shows an example of 2 provisioned Audiocodes GW as displayed by the CS2M Gateway List GUI.

Figure 3 Example Audiocodes TP6310 Line GWs Following Provisioning at CS2M

CS2000 Management Tools - 47.165.171.11 (CM CLI: CS2K1_MAID)

File Fault Configuration Maintenance Windows Help

Device Types
 APS
 Gateway Controller
 UAS

Contents of Gateway Controller
 Directory Find

Gateway Controllers:
 GWC-102
 GWC-105

GWC-105 Unit 0: 47.165.172.46
 Unit 1: 47.165.172.47

Maintenance Provisioning

Controller Gateways Lines Carriers Media Proxies QoS Collectors IPSec

Retrieval criteria: [] Retrieve

Limit results: 25 Replace List Append to List Retrieve All

Gateway List

Name	Do...	IP Address	Profile	Max Terms	Res Terms	Protocol	Prot Vers	Prot Poi
CICM-333		3.3.3.3	CICM	3069	1023	megaco	1.0	2944
afc1.com		1.1.1.1	AFC	1023	1023	megaco	1.0	2944
audiocodes1.com		47.165.173...	AUDIOCODES_6310_LINE	2016	2016	megaco	1.0	2944
audiocodes2.com		47.165.173...	AUDIOCODES_6310_LINE	2016	1800	megaco	1.0	2944

Max terms, Res terms set for large capacity GW full capacity

AUDIOCODES_6310_LINE profile reduced capacity

Number of results: 4 Associate... Disassociate Change... Details...

Last update: 08-Dec-2005 11:31 Retrieving lines for GWC-105...Done

Applet running...

The Audiocodes TP6310 large line GWs when provisioned have LGRPs of size 2048. This will have a direct impact on the number of gateways addressable by a GWC. The rules governing the number of provisionable GWs with relation to LGRP size are as follows:

- 1024 size LGRPs - Max 27 large line GWs.
- 2048 size LGRPs - Max 13 large line GWs.
- GWs comprising multiple LGRPs are considered to be multiple GWs from the perspective of this discussion.
- Number of supported GWs independent of reserved terminations.
- Total number provisionable large line GWs between 13 and 27 dependant on mix of 1024 and 2048 size LGRPs.

As the Audiocodes TP6310 large line GW requires the provisioning of a 2048 size LGRP, this will reduce the capability of a given GWC to support new GWs by 2.

1.1.3 Deprovisioning Of Audiocodes TP6310 Large Line GW

Deprovisioning of the Audiocodes TP 6310 Large Line GW uses the standard “Disassociate Media Gateway” GUI interface or the disassocmg XML interface from OSSGate.

As this type of gateway is treated as 3rd party for endpoint creation and deletion the user must ensure that all endpoints for the target GW are removed from the system prior to attempting the deletion operation.

1.1.4 Modifying An Audiocodes TP6310 Large Line GW

The only change interface supported in this release is the “change gateway capacity” interface to modify the number of reserved terminations.

Specifying Root / Adjacent ITRANS zones is currently unsupported for the Audiocodes TP6310 Large Line GW.

1.1.5 Provisioning Of Audiocodes TP6310 Large Line GW - OSSGate XML Interface

Provisioning of the Audiocodes TP6310 Large Line GW using the OSSGate XML interface is unchanged by this feature. Please refer to the OSSGate documentation for details of this interface.

1.1.6 Querying Of Provisioned GWs via the OSSGate XML Interface

The response from the queryMG interface is unchanged by this feature. Please refer to the OSSGate documentation for details of this interface.

1.1.7 Provisioning Endpoints For The Audiocodes TP6310 Large Line GW

Before an Audiocodes TP6310 Large Line GW endpoint may be used it must first be pre-provisioned. The pre-provisioning is a manual activity using the OSSGate or bulk provisioning tool functionality introduced by feature A00007072 to support 3rd party GW endpoint provisioning.

The reader of this document should be fully conversant with the information specified in the FN of feature A00007072 and the OSSGate user guide as we will only cover that information of direct relevance to the Audiocodes TP6310 Large Line GW here.

Examples for the addition and deletion of an endpoint associated with an Audiocodes TP6310 Large Line GW are shown in Figure 4 and Figure 5.

Figure 4 Example addLineEndpoint Request For Audiocodes TP6310 Large Line GW

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <addLineEndpoint usn="1" version="1.0">
        <Parameters>
          <mgUIName>audiocodes1.com</mgUIName>
          <endpointName>tp/2016</endpointName>
          <circuitNumber>2015</circuitNumber>
          <cardCode>GWL POT</cardCode>
          <padGroup>PKNIL</padGroup>
          <ground>N</ground>
        </Parameters>
      </addLineEndpoint>
    </Methods>
  </Command>
</CommandList>
```

Multiple addLineEndpoint operations may be submitted as part of a single XML document

Figure 5 Example delLineEndpoint Request For Audiocodes TP6310 Large Line GW

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <delLineEndpoint usn="1" version="1.0">
        <Parameters>
          <mgUIName>audiocodes1.com</mgUIName>
          <endpointName>tp/2016</endpointName>
        </Parameters>
      </delLineEndpoint>
    </Methods>
  </Command>
</CommandList>
```

Multiple delLineEndpoint operations may be submitted as part of a single XML document

1.1.7.1 Audiocodes M8K Shelf Brief Overview

The Audiocodes M8K GW shelf is comprised of one or more STM-1 / OC-3 TP6310 or lower capacity TP1610 cards.

The TP1610 can be used to support Trunk carriers and makes use of the existing AUDIOCODES profile (2 x AUDIOCODES profile trunk GWs per TP1610 card). This will not be discussed further as it is existing functionality.

The TP6310 can be configured for use as either a Trunk or a high capacity Large Line GW. The configuration of the TP6310 as a Trunk GW is considered later in this document - see section 1.1.14 on page 1628. The remainder of this section refers only to the use of the TP6310 as a Large Line GW.

When operating in line mode each TP6310 card can terminate 2016 POTS type lines via additional external demuxing.

Each TP6310 card in the Audiocodes M8K shelf operates as a separate independent gateway with its own unique IP address / protocol port, and will therefore be treated as a separate gateway by the CS2M and subtended GWC modules. Therefore the Audiocodes TP6310 Large Line GW as described by this document refers to a single TP6310 card configured within an M8K shelf to terminate lines.

The CS2M may have multiple Audiocodes TP6310 GWs provisioned which are in fact all line cards within a single Audiocodes M8K shelf. This is analogous to multiple independent CICM GWs occupying a SAM21 shelf.

The Audiocodes TP6310 Large Line Gateway must be configured via the Audiocodes element manager to expect the endpoint naming convention and range as present in this document so as to match what the CS2M is expecting to provision.

1.1.7.2 Endpoint Naming Convention

Endpoints as provisioned on the Audiocodes TP6310 Large Line GW will be of the following format:

tp/nnnn where:

- nnnn = endpoint number on card with nnnn in the range 1 - 2016.
- nnnn is not padded (no leading zeros for padding to 4 digits).

As an example the endpoints for a TP6310 Large Line GW will be as follows:

tp/1, tp/2, tp/3.... tp/2014, tp/2015, tp/2016.

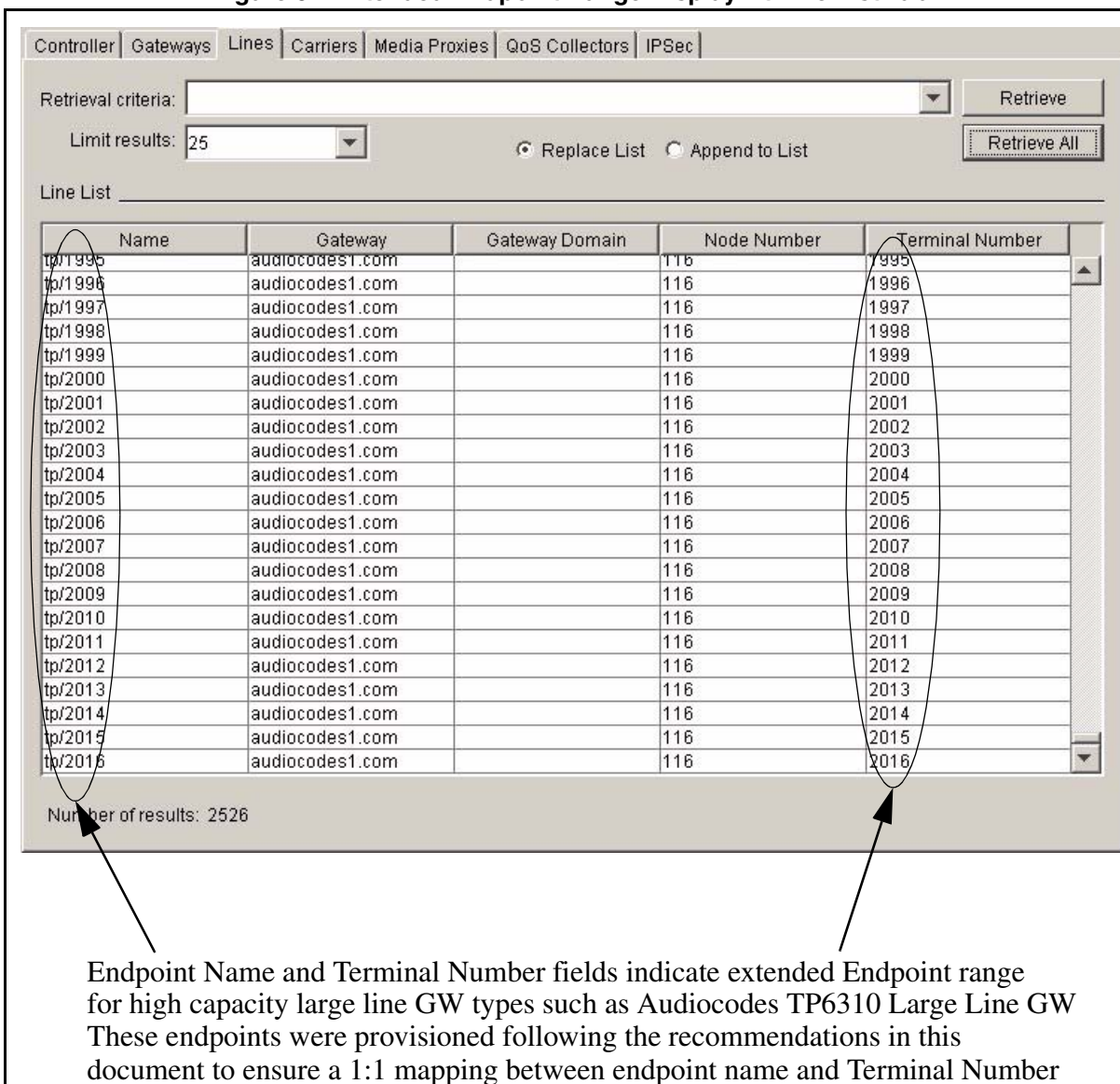
1.1.7.3 Circuit Number Allocation

The 3rd party GW provisioning interface allows flexible allocation of the LEN circuit number (and hence endpoint terminal number) independently of the endpoint name. The circuit number allocated for an endpoint must be unique and in the range 0 - 2046. This identifies directly the LEN to be created.

It is recommended that the circuit number be equal to the endpoint “nnnn” component -1. This will allow for easy correlation of endpoint to LEN and assist with maintenance. For example tp/1 associated with LEN <LGRP> 00 00.

1.1.8 Lines Panel Indication Extended Endpoint Range

Figure 6 Extended Endpoint Range Display At Line List Tab



Due to the larger LGRP size supported for the Audiocodes M8K, additional endpoints are directly addressable. This results in the endpoint range being increased for this GW as opposed to a normal pre SN09.1 GWs such as AFC.

Figure 6 shows the display of additional endpoints for the Audiocodes TP6310 Large Line GW provisioned using a 2048 size LGRP. Supported endpoints will be in the range tp/1 to tp/2016.

Note: Total number of possible endpoints is 2047 for the 2048 member LGRP as one TID will be reserved for signaling purposes.

1.1.8.1 Mapping Endpoint to LEN:

The mapping of endpoint to LEN is performed based on the terminal number which in turn is considered GW type independent. For the Audiocodes TP6310 Large Line GW there is no guaranteed logical mapping between the endpoint name and its associated terminal number. This is due to the terminal number being generated from the supplied circuit number at provisioning time.

It is recommended that the circuit number be set equal to the endpoint number - 1 at provisioning time to produce a 1:1 mapping but this is not enforced.

For LENs with LGRPType = LL_3RDPTY_2K the endpoint format is as follows:

LENs will be of the format <Node Name> <TT> <tt> where:

- Node Name - LGRPINV entry as auto generated on GW addition. Formed from <Site> <Frame> <Unit> where <Site> is used specified on GW addition, frame and unit are auto allocated.
- TT is in range 00 .. 20
- tt is in the range 00 .. 99 where TT < 20 and 00 .. 46 where TT = 20

For example with LGRP = "LG2K 01 5" the possible range of LENs for the LGRP as a whole will be:

LG2K 01 5 00 00 - LG2K 01 5 20 46 dependant on circuit number allocation.

It is recommended that the circuit number be tied to the endpoint name which would mean the range of recommended LENs for an Audiocodes TP6310 Large Line GW is:

LG2K 01 5 00 00 - LG2K 01 5 20 15.

The corresponding Terminal numbers will be as follows:

terminal number = (TT x 100) + tt + 1

And the reverse mapping will be:

TT = terminal number - 1 - tt

tt = (terminal number - 1) MODULUS 100

Assuming the recommendation on allocating circuit numbers at endpoint provisioning is followed, the endpoint name would be directly generated from the terminal number as:

tp/<terminal number>.

1.1.9 Line Provisioning Using the SERVORD+ Interface

Line provisioning using the servord interface is unchanged by this feature. Lines may be provisioned using either LENSs or endpoints as specified in the OSSGate documentation.

The OSS must however take into account the extended endpoint / LEN range introduced for the Audiocodes TP6310 Large Line GW.

1.1.10 Audits - CS2K and Line Audit

The CS2K Data integrity audit and Line Data integrity Audit are unchanged by this feature.

Please be aware that the Line Data Integrity Audit will report a greater range of lines where an Audiocodes TP6310 Large Line line GW is provisioned due to the greater capacity supported by this GW type.

1.1.11 Line Maintenance Manager

There will be no functional changes to the Line Maintenance Manager introduced by this feature. Currently Large Line H.248 gateways are unsupported by the Line Maintenance Manager. This restriction will apply equally to the Audiocodes TP6310 Large Line gateway.

1.1.12 Bulk Provisioning Tool

The bulk provisioning tool used for provisioning line data fill will not be impacted by this feature. Line provisioning for the Audiocodes TP6310 Large Line GW is supported as is, however the range of valid LENSs / endpoints is increased in accordance with the additional endpoint / LEN range.

1.1.13 Third Party Gateway Profile Certificate Changes

Third party gateway certificate profiles produced to support new large line type gateways generated in accordance with the guidelines for feature A00007071 and A00007072 are now required to indicate the size of CM LGRP to be generated to support the new GW. In addition the LGRP generated may be 1 of 2 sizes:

1024 - identical to all releases prior to SN09.1

2048 - double sized for higher capacity large line GWs.

A new tag value pair <LgrpSize>value</LgrpSize> is introduced to the certificate XSD to carry size information. This should be set to 1024 or 2048. The higher capacity size of 2048 should only be used where absolutely necessary as this will reduce the provisionable number of GWs that can be associated with a given GWC.

The value of the <LgrpType> tag value pair must be set to indicate the type of LGRP to be generated at the CM. For 3rd party large line GWs this will be

either LL_3RDPTY or LL_3RDPTY_2K dependant on whether a size of 1024 or 2048 is required.

The certificate files for all new 3rd party large line GWs should therefore contain either of the following entries:

Figure 7 LGRP of Size 2048: Between 1 and 2047 Endpoints Supported

```
<EndpointType>thirdPartyLens</EndpointType>
<LgrpType>LL_3RDPTY_2K</LgrpType>
<LgrpSize>2048</LgrpSize>
```

Figure 8 LGRP of Size 1024: Between 1 and 1023 Endpoints Supported

```
<EndpointType>thirdPartyLens</EndpointType>
<LgrpType>LL_3RDPTY</LgrpType>
<LgrpSize>1024</LgrpSize>
```

Note 1: LgrpSize tag should directly follow LgrpType

Note 2: If the LgrpSize tag is not present in a certificate the default size of 1024 is assumed to ensure backwards compatibility with existing certificates.

Note 3: Specifying LgrpSize for a non large line GW will result in a corrupt profile alarm being raised and the certificate will not be loaded.

1.1.14 Provisioning Of Audiocodes TP6310 Trunk GW - GUI Interface

The Audiocodes TP6310 card when provisioned as a Trunk GW can be considered as a higher capacity version of the existing Audiocodes Trunk GW as supported in both this and prior releases.

All functionality provided by the existing Audiocodes GW profile is adopted, with the range of possible carriers being increased due to the larger capacity offered by the OC-3 / STM-1 interface supported by this card.

A new gateway profile “AUDIOCODES_6310_TRUNK” is introduced by this feature to support the provisioning of the TP6310 as a Trunk GW. On selecting the “AUDIOCODES_6310_TRUNK” profile the Associate Media Gateway dialog will be populated as follows:

Figure 9 CS2M Assoc. Media Gateway GUI Population For TP6310 Trunk GW

The screenshot shows the 'Associate Media Gateway' dialog box with the following fields and annotations:

- Gateway name:** AC6310T2
- Gateway IP address:** 0.0.0.0
- Gateway controller name:** GWC-102
- Gateway profile name:** AUDIOCODES_6310_TRUNK (An arrow points to this field with the annotation: **Select profile = AUDIOCODES_6310_TRUNK**)
- Reserved terminations:** 620 (An arrow points to this field with the annotation: **Reserved terminations 1 .. 2016. Default = 2016**)
- Internet Transparency:**
 - ☐ MG outside CS2K VPN, not behind NAT
 - IP-VPN / LBL Selection:**
 - ☐ IP-VPN(NATs)
 - ☐ LBLs
 - ☐ IP-VPN(NAT)-LBLs
 - Adj Network Zone:** maidenhead (An arrow points to this field with the annotation: **ITRANS functionality inherited from AUDIOCODES GW**)
- Signal Protocol:**
 - Protocol type:** MEGACO (4)
 - Protocol port:** 2944
 - Protocol version:** 1.0

Buttons: OK, Cancel

Table 2 Associate Media Gateway Field Population

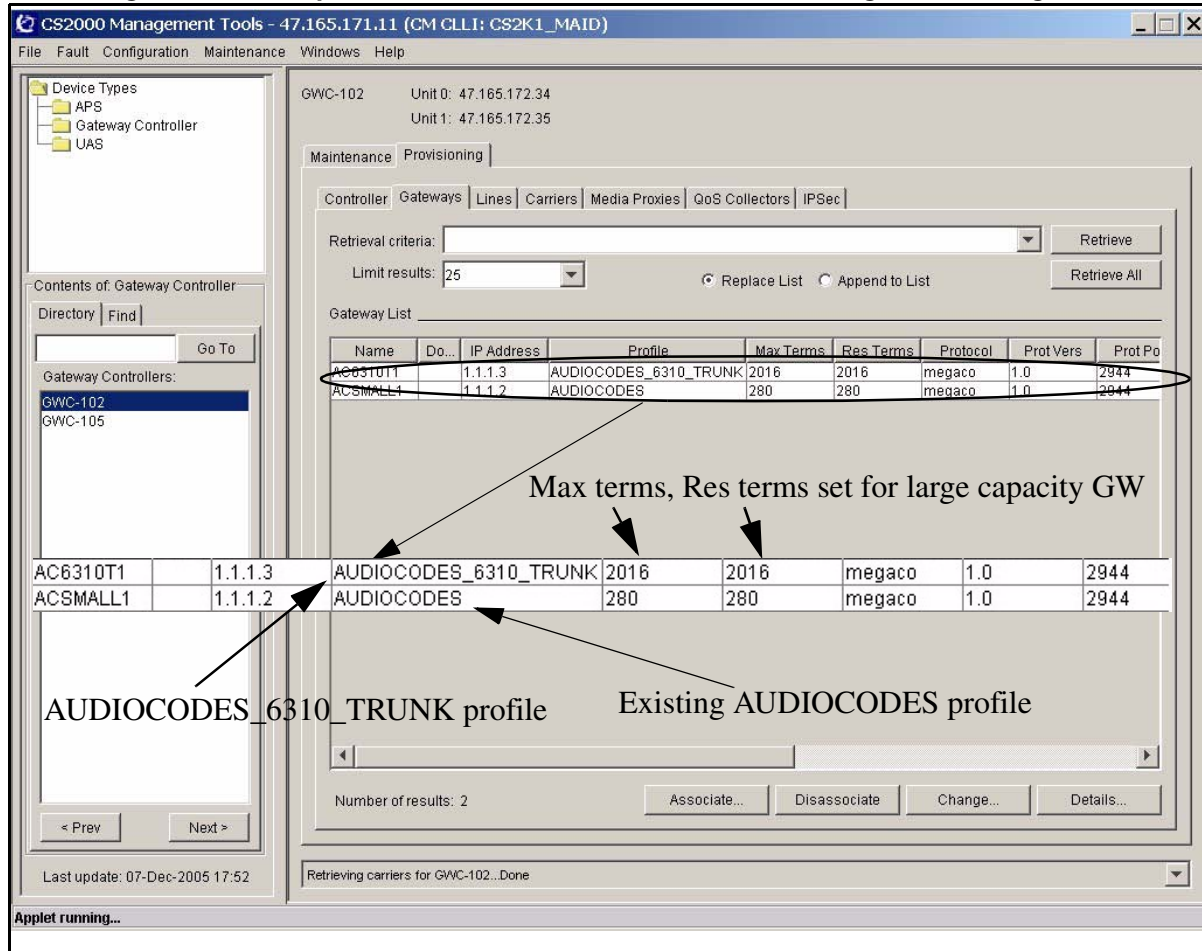
Field	Contents
Gateway name	Provisioned GW Name. Max 32 characters. Upper case alphanumerical characters only.
Gateway IP address	IP address for Audiocodes GW - or 0.0.0.0 if behind a NAT / LBL
Gateway controller name	GWC-nnn Name of a valid GWC provisioned with a large lines supporting profile.
Gateway profile name	AUDIOCODES_6310_LINE for TP6310 card as large line GW
Reserved terminations	In range 1 .. 2016. Defines number of terminations to reserve for use with this GW. If the field is left empty the default behaviour is to reserve 2016 terminations. As DS1 carriers require 24 terminations and E1 carriers 31 terminations the actual number of reserved terminations should form a multiple of 24 or 31 to avoid wastage. Note: A fully equipped TP6310 Trunk GW with E1 carriers will require 1953 terminations.
Adj Network Zone	ITRANS network zone GW is adjacent to if behind a NAT / LBL.
Protocol type	MEGACO - H.248
Protocol port	defaults to 2944 but may be edited if desired
Protocol version	Fixed to version 1.0

Following successful provisioning of the Audiocodes TP6310 Line GW, the following will have occurred:

- GW will have been created at GWC.
- GW will exist within CS2M database.
- GW will be displayed at CS2M GUI (upon gateway list refresh).

Initially there will be no carriers provisioned at the GWC or CM, however the capacity to provision the required number of carrier terminations will have been reserved.

Figure 10, on page 1630 shows an example of 2 provisioned Audiocodes GW as displayed by the CS2M Gateway List GUI.

Figure 10 Example Audiocodes TP6310 Trunk GW Following Provisioning at CS2M**1.1.15 Deprovisioning Of Audiocodes TP6310 Trunk GW**

Functionality is identical to existing Audiocodes GW.

1.1.16 Modifying An Audiocodes TP6310 Large Line GW

Functionality is identical to existing Audiocodes GW.

1.1.17 Provisioning Of Audiocodes TP6310 Large Line GW - OSSGate XML Interface

Functionality is identical to existing Audiocodes GW.

1.1.18 Querying Of Provisioned GWs via the OSSGate XML Interface

Functionality is identical to existing Audiocodes GW.

1.1.19 Provisioning Carriers For The Audiocodes TP6310 Trunk GW

The Audiocodes TP6310 Trunk GW supports the provisioning of either E1 or DS1 carriers based on market fit. The trunk range is a super set of that supported by the existing Audiocodes profile.

Carriers may be added / deleted using the existing addCarrier interfaces from either the CS2M GUI or the OSSGate interface.

1.1.19.1 E1 Carrier Provisioning

E1 Carrier support is as follows:

- Carrier range: E1/01 ... E1/63
- Optional DPNSS IID range: 1 .. 63
- Each E1 carrier supports 31 terminations and the appropriate number of terminations must be reserved in advance. A fully equipped TP6310 with E1 carriers will require $63 \times 31 = 1953$ terminations.

1.1.19.2 DS1 Carrier Provisioning

DS1 Carrier support is as follows:

- Carrier range: DS1/01 .. DS1/84
- Optional PRI IID range: 0 .. 31
- PRI IID value must be unique for a given GW.
- Each DS1 carrier supports 24 terminations and the appropriate number of terminations must be reserved in advance. A fully equipped TP6310 with DS1 carriers will require $84 \times 24 = 2016$ terminations.
- PRI IID range upper bound may be set in the range 32 .. 63 as functionality is shared with DPNSS IID although the extended range is not supported.

1.1.20 Carrier Panel - E1 Carriers For Audiocodes TP6310 Trunk GW

The following figure shows the carrier list panel displaying E1 type carriers for an Audiocodes TP6310 Trunk GW.

Figure 11 Carrier List Display For E1 Type Carriers

Carrier List

Name	Gateway	GW Domain	Node Num	Start Term	Num Ports	V5.2 IID	V5.2 Link ID	V5 UA Link ID	PRI/DPI
E1/44	AC6310T1		85	1334	31				44
E1/45	AC6310T1		85	1365	31				45
E1/46	AC6310T1		85	1396	31				46
E1/47	AC6310T1		85	1427	31				47
E1/48	AC6310T1		85	1458	31				48
E1/49	AC6310T1		85	1489	31				49
E1/50	AC6310T1		85	1520	31				50
E1/51	AC6310T1		85	1551	31				51
E1/52	AC6310T1		85	1582	31				52
E1/53	AC6310T1		85	1613	31				53
E1/54	AC6310T1		85	1644	31				54
E1/55	AC6310T1		85	1675	31				55
E1/56	AC6310T1		85	1706	31				56
E1/57	AC6310T1		85	1737	31				57
E1/58	AC6310T1		85	1768	31				58
E1/59	AC6310T1		85	1799	31				59
E1/60	AC6310T1		85	1830	31				60
E1/61	AC6310T1		85	1861	31				61
E1/62	AC6310T1		85	1893	31				62
E1/63	AC6310T1		85	1924	31				63

Number of results: 64

Carrier names are an extension of that support for the existing Audiocodes GW

1.1.21 Data Logging

There are no changes to data logging associated with this feature.

1.2 Hardware Requirements or Dependencies

This feature requires the presence of an Audiocodes M8K shelf equipped with one or more TP6310 cards for line GW use. Where trunk GW use the M8K should be equipped with either TP1610 or TP6310 cards as appropriate.

1.3 Software Requirements or Dependencies

1.3.1 SN09FF Formal Delivery

Software should be at the following release level or later:

GWC: Gx091FC

CM: PSNW090FC + 2K LGRP Support Patch

CS2M: SESM_091_FC

Note: FC software versions will not be known until the end of the SN09.1 release.

1.4 Limitations and restrictions

Provisioning of large line GWs with 2048 size LGRPs reduces number of provisionable GWs at the GWC.

CM must be patched with the 2K LGRP patch when running the PSNW090FC load (SN09FC). For SN10 onwards this patch will not be required.

1.5 Interactions

N/A

1.6 Glossary

Term	Definition
CM	Call Server 2000 Switch
CS2M	Call Server 2000 Management Platform
DNS	Directory Naming Service
ETSI	European Telecom Standards Institute
GUI	Graphical User Interface
GW	Gateway
GWC	Gateway Controller
HASU	Hardware Assigned Software Unassigned
LEN	Line Entity
LGRP	Line Group
OSS	Higher Level Management Platform
POTS	Plain Ordinary Telephone Service
TID	Termination ID
XML	External Markup Language

2: Configuration for A00013275

2.1 Hardware and Software Requirements

CS2M: SESM091FC

GWC: GI091FC or GN091FC dependant on market.

CM: PSNW09BS + SN09.1 2K LGRP patch.

Note 1: The CM patch is required to provide 2K LGRP Line GW support for the Audiocodes Mediant 8000 TP6310 card configured as a large line GW. This patch is not required where the TP6310 is to be configured as a Trunk GW.

2.2 Initial Configuration

CS2M and GWC components must be running the SN09.1FC software loads.

CM must be running the PSNW09BS with the 2K LGRP patch if provisioning of the Audiocodes Mediant 8000 TP6310 cards as large line GWs is required.

No patch is required if the TP6310 cards are to be used as Trunk GWs.

There are no additional initial configuration steps.

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

None.

2.4 Upgrade Considerations

For CS2M upgrade from versions 8.0, 9.0 to SN09.1.

2.4.1 Dump and Restore (CM)

Refer to feature A00013286.

2.4.2 Element Management Upgrade

For CS2M upgrade from versions 8.0, 9.0 to SN09.1.

No additional upgrade steps are required to the CS2M over and above the normal upgrade procedure.

2.4.3 Downgrade impact

None.

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

Unchanged.

2.6 Service Orders (SO) (CM & SESM)

2.6.1 Line equipment format changes

2.6.1.1 LEN

Provisioning of 2K LGRPs results in an extension to the existing LEN range supported for LL_3RDPTY LGRPs.

Len will be of the format:

<LGRP> TT tt

TT = 00 .. 20

tt = 00 .. 99 where TT < 20

tt = 00 .. 46 where TT = 20

The LGRP is a valid entry from CM table LGRPINV formed from the SITE + frame number + shelf number where

SITE = a valid entry from the CM table SITE.

frame number = logical frame number in range 00 .. 99

shelf number = logical shelf number in range 0 .. 9

For the Audiocodes TP6310 card provisioned as a large line GW a subset of the available LEN range will be required to support the full endpoint range (2016 endpoints / LENs in total). LEN assignment is user defined using functionality provided by features A00007071 / A00007072 however it is recommended that LENs are mapped directly to endpoints and run in the range: <lgrp> 00 00 ... <lgrp> 20 15.

2.6.1.2 Media gateway endpoint format

The Audiocodes Mediant 8000 TP6310 card provisioned as a large line GW supports endpoints for the format:

tp/nnnn where nnnn is in the range 1 ... 2016 is not padded.

i.e: tp/1 ... tp/2016

2.7 Software optionality control (SOC)

Unchanged.

2.8 Element Management

The CS2M configuration manager: GWCEM has been modified to support the provisioning of large line GWs with a capacity of up to 2047 endpoints within a single LGRP.

The CS2M configuration manager: GWCEM has been modified to support the provisioning of the Audiocodes Mediant 8000 TP6310 card configured as either a large line or a trunk GW.

2.8.1 New/modified GUIs

Unchanged.

2.8.2 Change To Certificate Model For Large Line GWs

This feature has modified the certificate schema used to process gateway certificates from that originally introduced by feature A00007071 and A00007072. Going forwards all creators of gateway certificate profiles designed for large line GWs must include LGRP Size support when generating a certificate.

Directly following the <LgrpType> tag value pair a new field <LgrpSize> is introduced. This must be set to one of the following 2 settings:

- <LgrpSize>1024</LgrpSize>
- <LgrpSize>2048</LgrpSize>

In the current release LgrpSize is directly coupled to LgrpType and the 2 must be aligned based on the following table.

Table 2: LgrpType To LgrpSize Alignment

LgrpType	LgrpSize
S	1024
M	1024
C	1024
LL_3RDPTY	1024
CALIX_C7	1024
SSDPL	1024
LL_3RDPTY_2K	2048

Any incorrect alignment of LgrpType against LgrpSize will result in either a reduction of capacity or wastage of resources.

Note 1: To maintain backwards compatibility with existing 3rd party gateway profile certificates, should the LgrpSize tag be missing from a large line GW certificate, it is assumed that the required size is 1024.

Note 2: It is forbidden to include the LgrpSize tag into gateway profiles that are not intended to support large line GWs.

2.9 User interface changes

Unchanged.

2.10 OSSGate Interface Changes

2.10.1 XML Command Changes

Extension to LEN range indirectly impacts the addLineEndpoint and delLineEndpoint interfaces. The circuitNumber tag within these interfaces will support a greater range of associated LENs.

For the TP6310 configured as a large line GW the endpoint range will be tp/1 ... tp/2016.

The TP6310 configured as a Trunk GW indirectly impacts the addCarrier and deleteCarrier interfaces as follows:

CarrierName field may be in range E1/01 ... E1/63 or DS1/01 ... DS1/84

DPNSS IID field may be in the range 1 ... 63 for E1 carriers.

2.10.1.1 Command XML

Figure 1 addLineEndpoint - Endpoint In Upper Half Of 2K LGRP

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <addLineEndpoint usn="1" version="1.0">
        <Parameters>
          <mgUIName>audiocodes1.com</mgUIName>
          <endpointName>tp/2016</endpointName>
          <circuitNumber>2015</circuitNumber>
          <cardCode>GWL POT</cardCode>
          <padGroup>PKNIL</padGroup>
          <ground>N</ground>
        </Parameters>
      </addLineEndpoint>
    </Methods>
  </Command>
</CommandList>
```

circuitNumber range is in range 0 - 2047 for a 2K LGRP

endpointName range increased due to large LGRP address space

Table 1 XML Command Tag Descriptions

tag name	description of valid values
endpointName	endpointName in range tp/1 ... tp/2016 for TP6310 large line GW
circuitNumber	circuitNumber in range 0 ... 2047 for 2K LGRP. Recommend 0 ... 2015 for TP6310 large line GW.

All other command tags are unchanged.

Figure 2 addLineEndpoint - Endpoint In Upper Half Of 2K LGRP

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <delLineEndpoint usn="1" version="1.0">
        <Parameters>
          <mgUIName>audiocodes1.com</mgUIName>
          <endpointName>tp/2016</endpointName>
        </Parameters>
      </delLineEndpoint>
    </Methods>
  </Command>
</CommandList>
```

endpointName range increased due to large LGRP address space

Table 2 XML Command Tag Descriptions

tag name	description of valid values
endpointName	endpointName in range tp/1 ... tp/2016 for TP6310 large line GW

All other command tags are unchanged.

Figure 3 addCarrier - Carrier Last E1 Carrier

```

<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>EndptGrpProvIf</Interface>
    <Methods>
      <addCarrier usn="1" version="1.0">
        <Parameters>
          <mgName>AC6310T1</mgName>
          <carrierName>E1/63</carrierName>
          <svcData>
            <DPNSS>
              <IID>63</IID>
            </DPNSS>
          </svcData>
          <firstTN>1924</firstTN>
        </Parameters>
      </addCarrier>
    </Methods>
  </Command>
</CommandList>

```

carrierName may be in range E1/01 ... E1/63 for E1 type carriers

DPNSS IID may be in range 1 ... 63 for E1 type carriers.

Table 3 XML Command Tag Descriptions

tag name	description of valid values
carrierName	E1 carrier in range E1/01 to E1/63
IID	DPNSS IID in range 1 .. 63

All other command tags are unchanged.

Figure 4 addCarrier - Carrier Last DS1 Carrier

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>EndptGrpProvIf</Interface>
    <Methods>
      <addCarrier usn="1" version="1.0">
        <Parameters>
          <mgName>AC6310T1</mgName>
          <carrierName>DS1/84</carrierName>
          <svcData>
            <PRI>
              <IID>31</IID>
            </PRI>
          </svcData>
          <firstTN>1992</firstTN>
        </Parameters>
      </addCarrier>
    </Methods>
  </Command>
</CommandList>
```

carrierName may be in range D1/01 ... D1/84 for DS1 type carriers

PRI IID may be in range 1 ... 31 for DS1 type carriers. The upper boundary is not enforced.

Table 4 XML Command Tag Descriptions

tag name	description of valid values
carrierName	DS1 carrier in range DS1/01 to DS1/84

All other command tags are unchanged.

Figure 5 deleteCarrier - Carrier Last E1 Carrier

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>EndptGrpProvIf</Interface>
    <Methods>
      <deleteCarrier usn="1" version="1.0">
        <Parameters>
          <mgName>AC63101</mgName>
          <carrierName>E1/63</carrierName>
        </Parameters>
      </deleteCarrier>
    </Methods>
  </Command>
</CommandList>
```

carrierName may be in range E1/01 ... E1/63 for E1 type carriers

Table 5 XML Command Tag Descriptions

tag name	description of valid values
carrierName	E1 carrier in range E1/01 to E1/63

All other command tags are unchanged.

Figure 6 deleteCarrier - Carrier Last DS1 Carrier

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>EndptGrpProvIf</Interface>
    <Methods>
      <deleteCarrier usn="1" version="1.0">
        <Parameters>
          <mgName>AC63101</mgName>
          <carrierName>DS1/84</carrierName>
        </Parameters>
      </deleteCarrier>
    </Methods>
  </Command>
</CommandList>
```

carrierName may be in range DS1/01 ... DS1/84 for DS1 type carriers

Table 6 XML Command Tag Descriptions

tag name	description of valid values
carrierName	DS1 carrier in range DS1/01 to DS1/84

All other command tags are unchanged.

2.10.1.2 Response XML

Response XML is unchanged.

2.11 Security

Unchanged.

2.12 Configuration Walkthrough

2.12.1 Provisioning an AUDIOCODES TP6310 Card As Large Line GW

CS2M and GWC are running SN09.1 FC loads. GWC is provisioned with a profile supporting large line GWs and has sufficient spare termination capacity to support an AUDIOCODES TP6310 card provisioned as a large line GW.

CM is running SN09 FC Load (PSNW09BS) with patch applied for large LGRP support (patch not required for SN10 onwards).

From the CS2M GUI interface (alternatively use OSSGate assocmg interface) launch the “Associate Media Gateway” dialog.

In the “Gateway profile name” selector locate “AUDIOCODES_6310_LINE”.

Set the “Gateway Site Name” selector to be a suitable SITE entry to support this gateway.

Set the Frame number and Unit number entries to values that will generate a unique LGRP entry in conjunction with the Site Name.

Populate the remainder of the fields as per normal for a H.248 supporting gateway and press the “OK” button to confirm.

Using either the bulk provisioning tool or OSSGate addLineEndpoint interface, add the desired number of endpoints in the range tp/1 ... tp/2016, associated circuit numbers will be in the range 0 ... 2015.

Using servord+ provision POTS type line services using the assigned endpoints.

2.12.2 Deprovisioning an AUDIOCODES TP6310 Card As Large Line GW

Using Servord+, remove all line services associated with GW endpoints.

Using the bulk provisioning tool or OSSGate delLineEndpoint interface, remove all endpoints associated with the GW.

Using either the CS2M GUI or OSSGate disassocmg interface delete the GW.

2.12.3 Provisioning an AUDIOCODES TP6310 Card As A Trunk GW

CS2M and GWC are running SN09.1 FC loads. GWC is provisioned with a profile supporting trunk GWs and has sufficient spare termination capacity to support an AUDIOCODES TP6310 card provisioned as a trunk GW.

CM is running SN09 FC Load (PSNW09BS). The large LGRP patch is considered optional in this scenario.

From the CS2M GUI interface (alternatively use OSSGate assocmg interface) launch the “Associate Media Gateway” dialog.

In the “Gateway profile name” selector locate “AUDIOCODES_6310_TRUNK”.

Data fill the dialog in exactly the same way as for an AUDIOCODES MG3200 / MG3500 GW. ITRANS may be specified if required - however the maximum termination setting is increased to 2016. Be aware that if E1 carriers are provisioned a maximum of 1953 terminations will be required for a fully equipped GW so the reserved terminations value may be lowered to save GWC capacity.

Using either the CS2M GUI Add Carrier dialog or corresponding OSSGate interface add the desired number of carriers to the GW. For E1 carriers the range is E1/01 to E1/63. For DS1 carriers the range is DS1/01 to DS1/84.

Where DPNSS support is required the IID may be set in the range 1 .. 63. Where PRI support is required the IID may be set in the range 0 .. 31. Be aware that the PRI upper bound is not enforced by the provisioning system and may be incorrectly set in the range 0.. 63. Be aware that the DPNSS IID may be incorrectly set to 0 by the provisioning system.

2.12.4 Deprovisioning an AUDIOCODES TP6310 Card As A Trunk GW

Using either OSSGate or the CS2M “delete carrier” dialog remove all carriers associated with the GW.

Using either the CS2M GUI or OSSGate disassocmg interface delete the GW.

Product = Call Server 2000

A00013286 -- Core Flex Large Line GWC Profile - Phase 1

1: Applicable solution(s)

Int'l UA-IP

1.1 Description

This feature is intended to address the following requirement:

- Add generic support for 2048 size LGRPs.

The current support for large line GWs has the following restrictions:

LGRPs are always a fixed 1024 elements regardless of the number of endpoints that a GW supports and the actual number of reserved terminations. Currently the available GWC TID size for subtending nodes other than trunks is 27000. So a maximum of 26 LGRPs can be configured per GWC if the existing LGRPs (1024) are used.

Due to time scale and resources issues it is intended that this feature will only address the following issue - specifically adding support for a 2047 size LGRP to be used initially in conjunction with the Audiocodes M8K GW. With the introduction of the new LGRP type, 13 to 27 LGRPs can be provisioned per GWC.

As part of this activity, the following changes will be made:

- Creation of a new LGRP type, LL_3RDPTY_2K which will support 2047 endpoints.
- Enhanced LNINV table to support 2047 LENs for the newly created LGRP type.

The new lgrp is an enhancement of the existing lgrp, LL_3RDPTY. The major difference between the newly created LGRP type, LL_3RDPTY_2K and the existing 3rd party profile, LL_3RDPTY is that, the new type supports 2047 lines per LGRP whereas the existing type supports only 1024 lines per LGRP. Total number of possible endpoints is 2047 for the 2048 member LGRP as one TID will be reserved for signaling purposes.

1.1.1 LGRP Type Data - Table LGRPINV

Table LGRPINV is an existing table that is used to associate a LGRP type to a gateway. This activity shall allow support of a new LGRP type, LL_3RDPTY_2K. The new type will support large line gateways with 2047

endpoints. Total number of possible endpoints is 2047 for LL_3RDPTY_2K as one TID will be reserved for signaling purposes.

The following figure shows sample datafill for table LGRPINV.

Figure 1 Prompting sequence and Range values for LGRPINV table.

TABLE: LGRPINV

```
>add
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
GRPNO:
>LG2K 25 0
SRVRNAME:
>gwc 24
GRPTYPE:
TYPE OF GRPTYPE IS LGRP_TYPE
TYPE IS LGRP_TYPE {S,M,C,LL_3RDPTY,CALIX_C7,SSDPL, LL_3RDPTY_2K}
GRPTYPE:
>LL_3RDPTY_2K
LGRPOPTS:
>$
WARNING: Adding tuples MUST be done via SESM node provisioning
         to avoid data mismatch between the CS2K and SESM components!
CAUTION: Confirming the operation could result in an impact to service.
TUPLE TO BE ADDED:
LG2K 25 0 GWC 24 LL_3RDPTY_2K $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE ADDED
```

1.1.2 LEN Entry - Table LNINV

In LNINV table 2047 LEN entries can be made corresponding to the new LGRP type, LL_3RDPTY_2K. The slots/drawer and circuit ranges supported for the new LGRP type are given below.

Slot - 0 - 20

Circuits - 00 - 99 for slots 0 - 19

00 - 46 for slot 20

The following figure shows sample tuple for table LNINV. The two tuples shown are the boundary conditions for the LGRP type, LL_3RDPTY_2K.

Figure 2 Sample LNINV Tuples

LEN	CARDCODE	PADGRP	STATUS	GND	BNV	MNO	CARDINFO
LG2K 25 0 00 00	RDTLSG	NPDGP	HASU	N	NL	N	NIL
LG2K 25 0 20 46	RDTLSG	NPDGP	HASU	N	NL	N	NIL

1.2 Hardware Requirements or Dependencies

N/A

1.3 Software Requirements or Dependencies

This feature requires the Core load to be a succession load greater than or equal to SN09FF. The required GWC load is GC09 and the CS2M load should be CS2M9.1 or greater.

1.4 Limitations and restrictions

N/A

1.5 Interactions

N/A

1.6 Glossary

Term	Description
GW	Gateway
GWC	Gateway Controller
LGRP	Logical Group

Product = World Trade

A00009037 -- Core Enhanced ESA for International MG9000

1: Applicable solution(s)

Int'l UA-IP

1.1 Description

This activity allows the download of information necessary to support International Emergency Stand Alone (ESA) call processing across all native (non ABI) and ABI lines served by a single MG9000 for intra and internodal ESA.

The download takes place from the CS2000 core to an MG9000 element manager. The data is generated by the core at 6:00 AM (configurable) and stored in a file called ESA_SYSTEM_SD\$XML on a device specified by existing OFCENG parameter ESA_GWDATA_DEVICE. It is then downloaded by the MG9000 EM through the SDM.

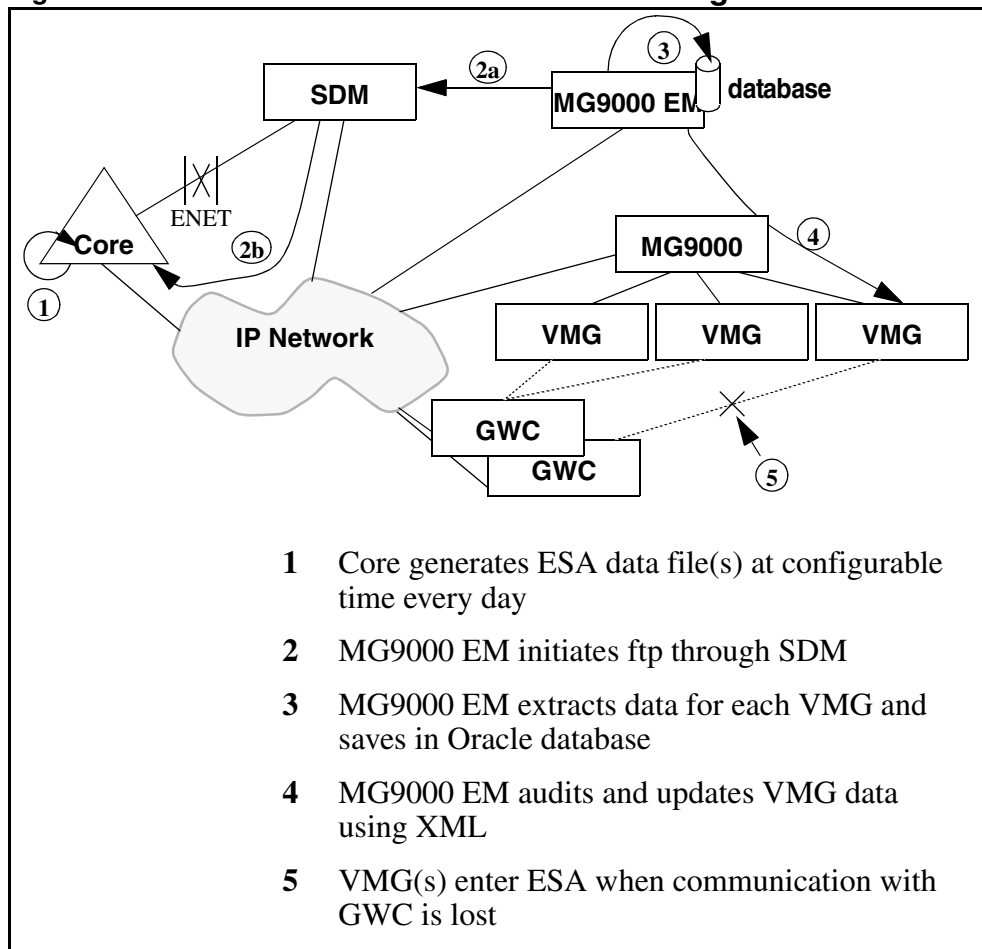
This activity is CS2000 data collection activity of Intl ESA support on MG9k. So, this FN covers only data collection part on CS2k. This activity can be broken into three parts:

- Intl ESA Data Collection Trigger
- Intl ESA Data Format
- Intl ESA Table

1.1.1 Background Information

ESA functionality is already provided for North American dialing plan which supports 10 digit national and 7 digit subscriber numbers. However, in international markets, subscriber numbers are based on ITU-T E.164 recommendations.

Data transmission and entering ESA mode of MG9k will be same as Basic/NA ESA modes. Please see **A00002020** and **A00002380** activities FNs for more information about ESA data transmission and entering ESA mode.

Figure 1 MG9000 ESA Functional Behavior Diagram

1.1.2 Desired Behavior

In international markets, dialling plan may vary each market regardless of actual DN definition on CS2000 core. For example, DN may be defined as 10 digits (3 digits SNPA + 3 digits OFC code + 4 digits STN number) but dialling plan only use 9 digits.

To support international dialling plan, new Intl ESA table is introduced with this activity. This new table contains customer group information and the digit analysis data that applies to specified types of calls. If new table does not contain digit analysis data, default tuple is used in this new table.

New table entries are explained in following sections.

1.1.3 Project Details

This activity (A00009037- CORE - ENHANCED ESA FOR INTERNATIONAL MG9000) is one of three activities to enhance ESA for the MG9000 in the SN09 time frame. The activity addresses the core code and will be sourced into the SN09 stream.

The other features are

- “A00009021 - Enhanced ESA for International MG9000”
- “A00009282 - MG9KEM - INTERNATIONAL ESA AND MLPP SUPPORT”

MG9000 ESA is supported by series of activities. Therefore, please also see Core portion of following activities:

- A00002020 - ESA Translation download
- A00002380 - MG9k ABI ESA

1.2 Intl ESA Data Collection Trigger

ESA data will be built by the core every 24 hours at 6:00 AM if existing office parameter in OFCENG table (ESA_GWDATAUPD_BOOL) is set or as the result of exiting manual CI command (ESACOLL under ESATOOLS directory). Changes to CS2000 line data will not be reflected in the MG9000 until the data has been

- built by the core
- downloaded by the MG9000 Element Manager (EM)
- downloaded to the MG9000

Data collection trigger time is also controlled by existing office parameter ESA_GWDATAUPD_HOUR in OFCENG table.

1.3 Intl ESA Data Format

This activity uses XML file format to store international data. XML file name would be ESA_SYSTEM_SD\$XML and stored device name would be datafilled by using existing office parameter ESA_GWDATA_DEVICE. Default value for this office parameter is SFDEV. But, the maximum size of SFDEV is 5 million bytes so a disk device must be available for large offices.

Please refer to ESADATA document of activity A00002020 “ESA Translation download” to see collected ESA tables and ESA information from code and their XML formats.

But, please note that EXTN index in table IBNXLA is not collected if ESADGCOD table is not empty.

1.4 Intl ESA Table

This activity introduces new ESA table (ESADGCOD) for international markets to support international dialling plan on VMGs.

This new table contains customer group information and the digit analysis data that applies to specified types of calls. Following is an example tuple datafill for new table ESADGCOD.

Figure 2 Tuple examples for new table ESADGCOD

TABLE ESADGCOD						
KEY			NUMDGTS	ADDIGS	STRIP	
IBN_ESA_DEFAULT*	00	50	7	216	0	
IBN_ESA_DEFAULT*	51	70	4	216783	1	
IBN_ESA_DEFAULT*	71	99	10	\$	0	
CUST783	0000	0920	8	\$	1	
CUST783	10	19	8	442	2	
CUST783	4	4	4	212442	0	
CUST783	5	5	7	\$	0	
PTTPUB	00	08	8	\$	1	
PTTPUB	1	9	4	102216	0	

* IBN_ESA_DEFAULT is used for customer groups which are not datafilled ESADGCOD table or it is used if related customer group does not have FROM-TOD digits range for dialled digits.

Table 1 Field explanations of new table ESADGCOD

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
KEY	NEW	DGNAME	alphanumeric (up to 16 chars)	Character entries can be entered up to 16 Chars. But, only "IBN_ESA_DEFAULT" and customer group names (datafilled in CUSTENG table) can be accepted.
		FROMD	up to eight digits (0 to 9, B, or C)	From digits.
		TOD	up to eight digits (0 to 9, B, or C)	To Digits
NUMDGTS	NEW	N/A.	Number {0 to 15}	NUMDGTS: Number of digits to collect (including prefix digits).
ADDIGS	NEW	N/A.	up to fifteen digits (0 to 9, B or C)	ADDIGS: The digits stream which will be added to collected digits.
STRIP	NEW	N/A.	Number {0 to 15}	STRIP: Number of digits to be removed from collected digits.

Use of IBN_ESA_DEFAULT tuple may have following advantages:

- If switch has same dialling plan for all customer groups only IBN_ESA_DEFAULT tuple may be provisioned.
- If only a few customer groups have different dialling plan, only different dialling plans may have datafill in ESADGCOD table. The rest of the customer groups may still use IBN_ESA_DEFAULT datafill.

Figure 3 Tuple examples for table ESAPXLA

TABLE ESAPXLA			
PXLAKEY RESULT			

ESAXLA	LGRP	VMG 2 0	911 L LGRP 02 0 00 08 N 0
ESAXLA	LGRP	VMG 3 0	911 L LGRP 03 0 00 10 N 0
ESAXLA	LGRP	VMG 2 0	0911 L LGRP 02 0 00 15 N 0

Following table shows the dialling examples according to datafills in figure 2 (Table ESADGCOD) and figure 4 (Table ESAPXLA).

Table 2 Dialling examples and results using ESADGCOD table

Dialled Number	Used Tuple in ESADGCOD/ESAP XLA	Result	Originating Line CUSTGRP
0550 - XXX	IBN_ESA_DEFAULT 00 - 50	216 - 0550 - XXX (Default tuple match)	CUST783
12 - XXXXXX	CUST783 10 - 19	442 - XXXXXX	CUST783
2 - XXXXXX	IBN_ESA_DEFAULT 00 - 50	216 - 2 - XXXXXX (Since CUST783 does not have FROMD - TOD for prefix 2. DEFAULT tuple is used.)	CUST783
3 - XXXXX	IBN_ESA_DEFAULT 00 - 50	Treatment (reorder). (since collected number of digits is not equal to NUMDGTS in DEFAULT tuple.)	CUST783
4 - XXX	CUST783 4 - 4	212442 - 4 - XXX	CUST783
5 - XXXXXX	CUST783 5 - 5	5 - XXXXXX	CUST783
911	ESAXLA 911	DN of LGRP 00 0 00 08 if originating DN is in VMG 2 DN of LGRP 01 0 00 10 if originating DN is in VMG 3	CUST783
0911	ESAXLA 0911	DN of LGRP 04 0 00 15 if originating DN is in VMG 2.	CUST783

1.4.1 Limitations and restrictions

- IBN_ESA_DEFAULT name should not be used in table CUSTENG. If it is used as customer group name, no default entry would be downloaded to MG9000.
- ESAPXLA table has priority over ESADGCOD table. So, if there is overlaps prefixes in tables ESAPXLA and ESADGCOD, ESAPXLA tuple is used.
- Maximum allowable tuple count in table ESADGCOD is 3000 (independent from customer group datafills)

1.5 Hardware Requirements or Dependencies

Since each VMG will include ESADGCOD data separately, XML file size may be greater than 5 million word (10 million bytes). Therefore a disk device must be available for large offices.

1.6 Software Requirements or Dependencies

All Software requirements and dependencies of activities A00002020 and A00002380 are also valid for this activity.

1.7 Limitations and restrictions

All Limitations and restrictions of activities A00002020 and A00002380 are also valid for this activity.

- EXTN table which stores EXTN information in table IBNXLA is not collected if ESADGCOD table is not EMPTY.
- ESADGCOD is supported for the lines which has Customer group information.

1.8 Interactions

The MG9000 EM downloads the ESA data file from the core daily. The time for this download should be set so the data has been freshly built. The default values in the core and MG9000 EM are set to ensure the data is downloaded soon after being built.

1.9 Applicable customer facing sections

Fault Management

Logs

Alarms

Configuration

Data Schema

__X__

User Interface

Element Management	_____
Security	_____
Service Order	_____
Office Parameters	_____
Accounting (includes AMA billing)	_____
Performance (includes operational measurements)	_____

1.10 Glossary

Term	Description
ABI	Access Bridging Interface
CS2000	Call Server 2000
EIOP	Ethernet Input/Output Packlet
EM	Element Manager
ESA	Emergency Stand Alone
MG9000	Media Gateway 9000
SDM	SuperNode Data Manager
VMG	Virtual Media Gateway

2: Configuration Management for A00009037

2.1 Hardware and Software Requirements

N/A

2.2 Initial Configuration

N/A

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

2.4 Upgrade Considerations

N/A

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

2.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
ESADGCOD	NEW	NEW

2.5.2 Table/MIB/Remote Database Schema information

2.5.2.1 Name: ESADGCOD

Emergency Stand Alone Digit Analysis Code Table

2.5.2.1.1 Functional description

This table contains customer group information and the digit analysis data that applies to specified types of calls in ESA mode of MG9000. According to datafill in ESADGCOD, number of digits to collect in ESA mode is determined.

2.5.2.1.2 Usage sequence and implications (CM Only)

This table can be datafilled after CUSTENG is datafilled.

2.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ESADGCOD	0	3000	Memory is automatically allocated. Minimum memory consumption if it has no datafill.

2.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for ESADGCOD table.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
KEY	NEW	DGNAME	alphanumeric (up to 16 chars)	Character entries can be entered up to 16 Chars. But, only "IBN_ESA_DEFAULT" and customer group names (datafilled in CUSTENG table) can be accepted.
		FROMD	up to eight digits(0 to 9, B, or C)	From digits.
		TOD	up to eight digits(0 to 9, B, or C)	To Digits
NUMDGTS	NEW	N/A.	Number {0 to 15}	NUMDGTS: Number of digits to collect (including prefix digits).
ADDIGS	NEW	N/A.	up to fifteen digits (0 to 9, B or C)	ADDIGS: The digits stream which will be added to collected digits.
STRIP	NEW	N/A.	Number {0 to 15}	STRIP: Number of digits to be removed from collected digits.

2.5.2.1.5 Datafill example

The following example shows sample datafill for table ESADGCOD.

CUST783 0 0 8 216 1

2.5.2.1.6 Table release history update

N/A.

2.5.2.1.7 Supplementary information

ESADGCOD table has the verify procedure. Therefore, error messages are displayed if wrong datafill is entered. Followings are the error conditions and its error texts:

- If the table is full (which means table has 3000 tuple), new tuple cannot be datafilled, following error is displayed:

"ESADGCOD TABLE IS FULL"

- If the table is full and telco worker tries to change a subset of existing key with different values. For example, table has following entry:

CUST783 0 9 10 \$ 2

If the worker tries to change CUST783 3 3 entry with 11 \$ 3 values, then table would have

CUST783 0 2 10 \$ 2

CUST783 3 3 11 \$ 3

CUST783 4 9 10 \$ 2

The tuple is divided into 3 tuples. In this case following error would be displayed:

“CHANGE operation is not allowed for this subrange.”

“Please change entire tuple range: <dgname> <fromdig> <todig>”

- If the table is full and telco worker tries to delete a subset of existing key. For example, table has following entry:

CUST783 0 9 10 \$ 2

The worker tries to delete CUST783 5 5 datafill. Then Table would have following entries after deletion.

CUST783 0 4 10 \$ 2

CUST783 6 9 10 \$ 2

The tuple divided into two tuples. In this case, if the table is full, then following error would be displayed.

“DELETE operation is not allowed for this subrange.”

“Please delete entire tuple range: <dgname> <fromdig> <todig>”

- Table ESADGCOD accepts customer group names datafilled in table CUSTENG or accepts “IBN_ESA_DEFAULT” string. For the other conditions, following error would be displayed:

“The DGNAME “given name” is not datafilled in the CUSTENG table.”

- TOD field should be greater than or equal to FROMD field. In case of wrong datafill, following error would be displayed:

“The TODIGs must be greater than the FROMDIGs”

- FROMD and TOD fields should contain at least one digit. In case of wrong datafill, following error would be displayed:

“At least one digit must be specified in both

the FROMD and the TOD fields.”

- If the FROMD and TOD fields contain invalid digits (D, E, F, N), error would be displayed.

“Invalid digit(s) in field FROMD” if FROMD includes invalid digits.

“Invalid digit(s) in field TOD” if TOD includes invalid digits.

- Since NUMDGTS field indicates the total number of digits which will be dialled by end user, number of digits in FROMD and TOD fields should not be greater than NUMDGTS field. In case of wrong datafill, error message would be displayed:

“Number of digits in FROMD field cannot be greater than NUMDGTS.” for FROMD field.

“Number of digits in TOD field cannot be greater than NUMDGTS.” for TOD field.

- Telco worker tries to delete a subset of existing key. For example, table has following entry:

CUST783 0 9 4 \$ 0

The worker tries to delete CUST783 50055 50055 datafill. Then Table may have following entries if deletion is permitted.

CUST783 0 50054 4 \$ 0

CUST783 500056 9 4 \$ 0

Since above tuples cannot be accepted, table gives following error and no tuple is deleted.

“DELETE operation is not allowed for this subrange.”

“Please delete entire tuple range: <dgname> <fromdig> <todig>”

- STRIP field value cannot be greater than NUMDGTS value. In this case table gives following error message.

“STRIP value cannot be greater than NUMDGTS value.”

- If the ADDIGS field contains invalid digits (D, E, F, N), error would be displayed.

“Invalid digit(s) in field ADDIGS”

- (Number of digits in ADDIGS field + NUMDGTS - STRIP) value cannot be greater than 15. Otherwise, following error would be displayed:

“(ADDIGS + NUMDGTS - STRIP) value cannot be greater than 15.”

2.5.2.1.8 Translation verification and other tools

N/A.

2.6 Service Orders (SO) (CM & SESM)

N/A.

2.7 Software optionality control (SOC)

N/A.

2.8 Element Management

N/A.

2.9 User interface changes

N/A.

2.10 OSSGate Interface Changes

N/A.

2.11 Security

N/A.

2.12 Configuration Walkthrough

N/A.



Chapter 5: Logs/faults and OMs/PMs

This chapter provides information on Logs/faults, and on operational measurements (OMs)/performance measurements (PMs). Some information appears in NE-specific Appendices to this document. Those appendices are referenced in the text of this chapter where appropriate.

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 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.

The network 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 MG15000, previously 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 - The network 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 - The network 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:

```
<SOL><LogOfficeId>_<NodeName>_<POA><Threshold><LogName><ReportNumber>_<DateIndicator>_<TimeIndicator>_<SequenceNumber>_<EventType>_<EventLabel>_<EquipmentIdentifier><EOLine><LOG BODY><EOLine><EOLog>
```

where:

- The < and > denote the beginning and end of a field.
- Bold text denotes optional fields that may or may not be there.
- _ denotes a space delimiter between fields.
- <SOL> = Start of Log delimiter - default is 0A0D in hexadecimal for NT STD and SCC2. (Line Feed followed by Carriage Return).
- <EOLine> = End of Line delimiter - default is 0A0D in hexadecimal for NT STD and SCC2. (Line Feed followed by Carriage Return).
- <LOG BODY><EOLine> = This sequence represents 0 to n lines of text in the log body each ending with EOLine - usually each line begins following an indentation of 8 spaces.
- <EOLog> = End of Log delimiter - default (in hexadecimal) is 200A0D0A0D00 for NT STD and 0A190A0D for SCC2

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_CLLI_NAME. (So OFFICE_CLLI_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 implementa-

tion. 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

The following table lists the AMS logs available. The MS2010 server is for IP networks and uses the AudioCode TP-1610 card. For detailed information on logs, refer to NN10275-909, *Fault Management Log Reference*.

AMS Logs/Faults available

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

The following table lists the APS logs available. For detailed information on logs, refer to NN10275-909, *Fault Management Log Reference*.

APS Logs/Faults available

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

The following table lists the Compact Call Agent (formerly Call Agent (CA)) Logs/Faults available. These logs were also previously referred to as 3PC. For detailed information on logs, refer to NN10275-909, *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 chapter in this document titled "IEMS Functionality."

For details on the SDM protocol/format, refer to FCAPS documentation NN10023-111.

CCA Logs/Faults available

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

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
CCA685	An INFO log which indicates that the CCA disabled OSPF in the local ERS8600 (formerly Passport 8600).
CCA686	An INFO log which indicates that the CCA enabled OSPF in the local ERS8600 (formerly Passport 8600).

CS2000--available logs/faults

The following table lists the CS 2000 Logs/Faults available.

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 chapter in this document titled "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, *Fault Management Log Reference*.

CS2000 Logs/Faults available

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 Data-base 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.
ATM log	ATM606 Generated when the 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.
Authorization logs	SESM MI2 applications have user authorization by group. Authorization failures generate logs through the SSPFS log reporting service.
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.
BKM logs	BKM600 Generated if a system backup is successful.
	BKM601 Generated if a system backup fails.
	class_securit y.ver01 Generated when a user attempts to invoke the Backup Manager and does not have the correct permissions.

CS2000 Logs/Faults available

Log/Fault	Description
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.
	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."
CALX logs	CALX300 Indicates unknown cause for a Calix-related issue.
	CALX301 Indicates a service-affecting issue related to Calix.
	CALX302 Indicates a non-service-affecting issue related to Calix.

CS2000 Logs/Faults available

Log/Fault	Description
	CALX501 Indicates a Calix remove event.
	CALX502 Indicates a Calix restore event.
	CALX800 Indicates a Calix Threshold Crossing alert is cleared.
	CALX801 Indicates a Calix Threshold Crossing alert is standing.
	CALX802 Indicates a Calix Threshold Crossing alert is transient.
	CALX803 Indicates a Calix Threshold Crossing alert is not applicable.
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.
	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.

CS2000 Logs/Faults available

Log/Fault		Description
CICM logs	Component initializes on master	An INFO log for a normal start-up event.
	Component initializes on slave	An INFO log for a normal start-up event.
	Slave component requests a bulk sync	An INFO log for a normal start-up event.
	Bulk sync of data completes	An INFO log for a normal start-up event.
	Component on master receives notification to SWACT	An INFO log generated as components perform an operator-initiated switch of activity.
	Component on slave receives request from its counterpart to assume the role of the master	An INFO log generated as components perform an operator-initiated switch of activity.
	Component on slave completes transition to active	An INFO log generated as components perform an operator-initiated switch of activity.
	Component on master receives acknowledgment from mate that it is now active	An INFO log generated as components perform an operator-initiated switch of activity.
CICM logs	CICM351	An alarm log to warn that, although started, the CICM/CICM-EM was unable to retrieve its basic configuration data, so it may be using old configuration data that is not up to date.
	CICM363	Raised when an INFO alarm occurs that indicates Subtract ConnectionAck cannot determine the destination for a message.
CEM logs	CSEM300	The log that encapsulates CS2K logs which have severity and are part of set and clear pairs.
	CSEM600	The log that encapsulates CS2K log which do not have severity.
CHKPT logs	CHKPT401	INFO log to inform the administrator that the Checkpointing OMs have been reset to 0 on the Active instance.

CS2000 Logs/Faults available

Log/Fault	Description
Client Session Monitor Security logs	The following security INFO logs are generated when the Client Session Monitor processes the notification of the authentication and client lifetime events: • User authenticated. • Successful session start. • Session stopped due to user exit. • Active session manually marked as done. • Client start or stop event is requested, but session ID is not valid.
CMT alarms	Communication with the GWC's associated gateways is down, raised if communication to the GWC's associated gateways is lost. This alarm is cleared when communication is detected with at least one associated gateway. It is also cleared when the GWC is manually or automatically SWACT and is raised again on the newly active unit if communication is still lost with all the associated gateways. Associated with log GWC319. Autonomous SWACT initiated, raised when an autonomous SWACT is initiated due to a loss of communication to all the associated media gateways. This alarm indicates that the system has taken action in an attempt to restore communication. This alarm remains active until manually cleared or gets automatically cleared when the GWC is SWACT back to the original active unit. Associated with log GWC318.
CPU Occupancy Alarms	CPU occupancy alarm Minor occurs at 80%, Major at 85%, and Critical at 90%.
CRTM logs	CRTM700 An INFO log which indicates that the user has requested a new private key. CRTM701 An INFO log which indicates that the user selected to generate a self-signed certificate.
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.

CS2000 Logs/Faults available

Log/Fault		Description
Data Server process logs		Desc Msg: Could not read switch name
		Desc Msg: Could not create tuple
		Desc Msg: Could not read VRINV table
		Desc Msg: Could not initialize OM Access
		Desc Msg: Could not initialize OM Access
		Desc Msg: Could not get keyinfo object, excluding group, <group>
		Desc Msg: Could not get key, excluding group, <group>
		Desc Msg: Could not get info, excluding group, <group>
		Desc Msg: Could not register initialization timer
		Desc Msg: Rejecting register request for excluded group: <group>
		Desc Msg: Could not open listening connection
		Desc Msg: Could not open listening connection: <service name>
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.
DPL logs	DPL100	DPL100 indicates that reconstruction of the VID resource pool has started.
	DPL101	DPL101 indicates that reconstruction of the VID resource pool has completed.
DQoS alarm	This raises a DQoS link alarm when link failure occurs.	
EMJS logs	EMJS340	Raise/Clear Alarms for the state of SNMP Communication with the device during its OM Collection.
	EMJS341	Log for Complete failure of SNMP Collection Job
	EMJS350	FTP/SFTP/STREAM communication Failure Event per device. This raise/clear log is modified in SN09FF to make the structure and content of the Location & Component ID fields consistent. The raise indicates that the system is not able to establish the SFTP connection with the device <IP address>. The clear indicates that the system has successfully established the SFTP connection with the device <IP address >.
	EMJS351	Raise or Clear log created in two possible instances: - the user configured in the indicated Job Instance does not have the privileges required to rename an OM file on the specified device. - the IEMS is not able to login to the System Manager with the configured Username and the password details.

CS2000 Logs/Faults available

Log/Fault	Description
EMJS360	Raise or Clear log for the error occurred in generating a Report File.
EMJS371	Raise or Clear log for the error/successful execution of Transfer jobs. Or, Raise log for Transmit failures during FTP or SFTP.
EMJS540	Collection Job State Changed Logs. Executed. Stopped. Disabled.
EMJS560	Report Job State Changed Logs. Executed. Stopped. Disabled.
EMJS570	Report Job State Changed Logs. Executed. Stopped. Disabled.
EMJS607	Log for MDM Performance & Fault Swact.
EMJS640	Log for: Invalid Template Version. Invalid OIDs for the device. Invalid CVS File Format.
EMJS641	Log Successful processing of SNMP Collection Job.
EMJS642	Partial/Complete Failure of SNMP Collection Job.
EMJS651	Log for Successful Processing of CSV Collection Job.
EMJS652	Log for Partial/Complete failure in processing of CSV Collection Job.
EMJS661	Log for complete success for Report Job.
EMJS662	Log for partial/complete failure for Report Job.
EMJS671	Log for Successful transfer job Attempts.
EMJS672	Log for partial/complete failure of transfer job attempts.
EMJS840	Threshold raise alarm.
EMJS841	Threshold clear Alarm.
EMSS logs	EMSS300 Produced when ever the client side PAM + RADIUS SPI is unable to communicate with the server-side RADIUS Interface.
	EMSS301 Produced when ever a serious problem is detected by the RADIUS Server in the process of handling a given authentication request. Problems that fall into this category are unexpected exceptions thrown by RADIUS Server plug-ins (as a result perhaps of improper RADIUS server setup/configuration or a critical RADIUS server dependency being unavailable). Recovery Action: Check the status of Sun IS and restart if necessary.
	EMSS302 Produced when the radius server policy plugin detects no single-sign-on token is available indicating there is a problem with the Sun Identity Server or that it is in fact not running.
	EMSS303 Indicates a communication failure with the PAM+Radius group daemon. This log indicates that the pam_radius_auth cannot establish or maintain a communications session with the group daemon on the client machine.
	EMSS304 Produced when the pam_mkhomedir module invokes the script mkhomedir but the script does not return within the timeout time (default 30 seconds).

CS2000 Logs/Faults available

Log/Fault	Description
EMSS305	Produced when ever the client side PAM+ RADIUS SPI is unable to communicate with the server-side RADIUS Interface.
EMSS306	Produced when ever the client side PAM+ RADIUS SPI is unable to communicate with the server-side RADIUS Interface.
EMSS307	Produced when ever the client side PAM+ RADIUS SPI is unable to communicate with the server-side RADIUS Interface.
EMSS308	Produced when ever the client side Pam + RADIUS SPI is unable to communicate with the server-side RADIUS Interface.
EMSS309	Produced when ever the client side PAM+ RADIUS SPI is unable to communicate with the server-side RADIUS Interface.
EMSS310	Produced when ever the client side PAM+ RADIUS SPI is unable to communicate with the server-side RADIUS Interface.
EMSS311	Produced when ever the client side PAM+ RADIUS SPI is unable to read information for required to communicate with the configured RADIUS server(s) from the /etc/raddb/server file
EMSS312	Produced when ever the pam_mkhomedir module tries to get the user information from NSSwitch by using getpwnam and fails.
EMSS313	Produced when ever the radius server health monitor detects the radius process is not functional.
EMSS314	Produced when ever the identity server health monitor detects the identity server process is not functional.
EMSS315	Produced when ever the PAM login servlet health monitor detects the PAM login servlet is not functional.
EMSS316	Produced when ever the pam_mkhomedir module checks the ownership of the script and the script is not owned by the user root.
EMSS317	Produced when ever the pam_mkhomedir module tries to get the script and the script is not there.
EMSS318	Produced when ever the pam_mkhomedir module tries to check the euid of the current process and finds the euid is not root.
EMSS319	Produced when ever the module tries to get the configuration file and the file is not there.
EMSS320	Produced when ever the module tries to read the contents of the configuration file but fails.
EMSS321	Produced when ever the module tries to get the auth url but the url got is null.
EMSS322	Produced when ever the module is timed out during the authentication. The default timeout is 30 seconds.
EMSS323	Produced when ever the module tries to get the configuration file and the file is not there.

CS2000 Logs/Faults available

Log/Fault	Description
EMSS324	Produced when ever the module tries to read the contents of the configuration file but fails.
EMSS325	Produced when ever the module tries to get the auth url but the url got is null.
EMSS326	Produced when ever the module is timed out during the validation. The default timeout is 30 seconds.
EMSS327	Produced when ever the script has an error to access the directory or files.
EMSS330	Produced when ever the module failed to initialize single sign on facility. SSO tokens will not be generated.
EMSS331	Produced when ever the module could not authenticate user due to unhandled internal error.
EMSS332	Produced when ever there is no single-sign-on token available after authentication.
EMSS333	Produced when ever the module could not generate single-use tokens due to unhandled internal error.
EMSS334	Produced when ever the module could not read user's unix profile due to unhandled internal error.
EMSS351	Produced when ever an exception is caught while making request to the servlet.
EMSS352	Produced when ever the module failed to authenticate.
EMSS353	Produced when ever there is an error processing response from the servlet.
EMSS354	Produced when ever the module failed to attempt to access the shadow database by user with uid <uid>.
EMSS360	Produced when ever the module failed to initialize SAML.
EMSS361	Produced when ever the module failed to process the configuration file.
EMSS362	Produced when ever the module failed to configure log4cpp.
EMSS363	Produced when ever the module failed to read the "password_file" property from the configuration file.
EMSS364	Produced when ever the module failed to find the configuration file.
EMSS600	An INFO log produced when ever the PAM Radius daemon modifies the /etc/passwd or /etc/group files.
EMSS601	An INFO log produced when ever there are successful or failed authentication requests of the authentication module.
EMSS602	An INFO log produced when there are successful or failed PAM SPI events from PAM + Plug-Ins.
EMSS603	An INFO log that indicates a SunOne Identity Server Single Sign On (SSO) token activity for a token create event. Sensitive token information is not included in these logs.

CS2000 Logs/Faults available

Log/Fault	Description
	EMSS604 An INFO log that indicates a SunOne Identity Server Single Sign On (SSO) token activity for a token destroy event. Sensitive token information is not included in these logs. EMSS605 An INFO log that indicates a SunOne Identity Server Single Sign On (SSO) token activity for a token timeout event. Sensitive token information is not included in these logs.
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.
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.
Hardware fault alarms	Power Supply. A minor alarm raised when any power supply operates outside of specifications or any voltage sensor reports a value outside of specifications. Cooling Device. A minor alarm is raised when any cooling device (fan or blower) operates outside of specifications. Temperature. A minor alarm is raised when any temperature sensor exceeds its specified threshold. Processor. A minor alarm is raised when a CPU failure is detected (available on the BC-T only).
IEMS logs	IEMS350 Indicates that an IEMS device is changed to an unmanaged state by the user. IEMS398 Raise Log for a Loss of Communication with the EMS/NE IEMS399 Clear Log for regain of Communication with the EMS/NE IEMS601 SNMP trap from unknown device Log IEMS602 Unknown SNMP trap from managed device Log IEMS603 Missed Notifications Log. Also generated whenever IEMS detects a trap loss, i.e. when the sequenceNumber in the trap is greater than the previous sequenceNumber plus one. IEMS604 Generated only if the incoming clear log does not have a logname and lognumber in it AND does not have a matching raise alarm in the IEMS database. IEMS605 Log for Manually Cleared Alarms by the user in IEMS GUI

CS2000 Logs/Faults available

Log/Fault	Description
IEMS606	Log generated by DBCleanUpPolicy. Threshold crossed log. Log for Data clean up
IEMS607	Automatic Clear alarms by IEMS during resynchronization of alarms.
IEMS608	Generated when an alarm in IEMS has been cleared automatically due to an aging policy coming due. In SN08, by default the ERS8600 (formerly Passport 8600) has a 7 day aging policy implemented.
IEMS609	Generated by IEMS when it clears the entire active alarm list for a managed component. Generally this might happen for SNMP managed devices when they send a cold start trap. OSSs can use this log as an indicator that IEMS no longer considers the alarms against that component valid and has removed them. The OSS may wish to consider clearing the trouble tickets against that managed component.
IEMS610	Generated by IEMS when the /data disk partition of the SSPFS platform in which it resides exceeds 80% utilization and the disk space cleanup job detects it. When detected, IEMS will attempt to bring /data under 80% utilization by removing OM report directories under /data/oms. Sub-directories will be removed as required and will start with the oldest first (that named 7), then 6 and end with 2. The 1 directory will not be removed.
IEMS614	Generated whenever IEMS receives an OSI State Change SNMP Notification (nortelNMIneOSIStateChangeNortification).
IEMS615	Generated whenever IEMS receives a Stateless Clear (Orphaned Clear), that is, whenever IEMS receives a Clear from the Southbound device, for which IEMS could not identify the matching raise from its database. Hence the OSS should use this log to identify some kind of misleading log information that is being sent from the Southbound devices. NOTE: This log is not generated for MDM devices.
IEMS616	Generated when an SNMP protocol authentication failure occurs with the MS2010/MS2020. It is an INFO event.
IEMS650	Indicates that an IEMS device is changed to a managed state by the user.
IEMS Sec- urity logs	Generated for any unauthorized configuration access attempts of measurement collection jobs.
	Generated for any unauthorized configuration access attempts of measurement transfer jobs.
	Generated for any unauthorized configuration access attempts of measurement report jobs.
	Generated when a tuple is added for the IP address in the security server.
	Generated when the RADIUS secret is updated for the IP address in the security server.
	Generated when a delete operation occurs for the IP address in the security server.

CS2000 Logs/Faults available

Log/Fault	Description
	Database password change logs: successful change, invalid user, and invalid machine used. Certificate creation and change logs: fresh certificate installed, and certificate changed. ssh Key creation and change logs: ssh key change, and invalid user for ssh key change. IPSec IKE policy creation and deletion logs: • IKE rule or entry added or deleted • Problem occurred loading IPSec rules on other cluster unit • Could not Sync IPSec data • IKE rule, key, or entry could not be added or deleted • IKE configuration data or preshared key data could not be updated IPSec IKE Key Change logs: • Preshared key modified • Attempt to modify Preshared key • Could not change Preshared key • IKE preshared key data could not be updated • Problem occurred loading IPSec rules on other cluster unit IPSec IKE Key Change logs (continued): • Could not Sync IPSec data • Could not modify preshared key
IEMS Security alarms	Password expiration warning alarm (Info), relates to SPFS350 log. Password expiration alarm (Minor), relates to SPFS350 log. Account expiration warning alarm (Info), relates to SPFS350 log. Account expiration alarm (Minor), relates to SPFS350 log. Certificate expiration alarm (Minor), relates to SPFS350 log. Certificate expiration alarm clearing, relates to SPFS350 log.
logNormalizer and logNormSAF Process logs	Desc Msg: Event file <EventFileName> was not found...logNormalizer exiting Desc Msg: Event delimiter cannot be more than one character long...logNormalizer exiting Desc Msg: Event file "<<EventFileName<<" is empty..logNormalizer exiting Desc Msg: Event file "<<EventFileName<<" had errors..logNormalizer exiting Desc Msg: Mapper file "<<MapperFileName<<" was not found...logNormalizer exiting

CS2000 Logs/Faults available

Log/Fault	Description
	Desc Msg: Mapper delimiter cannot be more than one character long...logNormalizer exiting Desc Msg: Mapper file "<<MapperFileName<<" is empty..logNormalizer exiting Desc Msg: Mapper file "<<MapperFileName<<" has errors.."<<argv[0]<<"exiting Desc Msg: Mapping information parsing error for log "<<logName<<" empty information or wrong delimiter used Desc Msg: output file "<<outputFileName<<" could not be opened Desc Msg: lostLogFile "<<lostLogFileName<<" could not be opened Desc Msg: lostLogFile "<<outputFileName<<" is empty Desc Msg: lostLogFormat string is empty Desc Msg: lostLogTriggerSize is empty Desc Msg: lostLogVisibleMsg string is empty Desc Msg: lostLogVisLog string is empty Desc Msg: sdmLogList is empty Desc Msg: probeTimer string is empty Desc Msg: checkLen string is empty Desc Msg: No Lost Log Trigger message has been specified Desc Msg: Could not send events to agent. Agent removed from output list Desc Msg: Unknown log format. No mapping will be done for input
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).

CS2000 Logs/Faults available

Log/Fault	Description
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.
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.

CS2000 Logs/Faults available

Log/Fault	Description	
Media Proxy alarm	Media Proxy Communications Failure	Severity varies, based on the number of media proxies that are out of service as compared to the number of media proxies provisioned checked on a 5-minute polling period. Critical - Over 50% of media proxies disabled. Major - Over 20% of media proxies disabled. Minor - Any media proxies disabled.
MGTH logs	MGTH300	MGTH300--acBoardEvResettingBoard
	MGTH301	MGTH301--acBoardFatalError
	MGTH302	MGTH302--acBoardConfigurationError
	MGTH303	MGTH303--acBoardTemperatureAlarm
	MGTH307	MGTH307--acBoardEthernetLinkAlarm
	MGTH309	MGTH309--acActiveAlarmTableOverflow
	MGTH312	MGTH312--acOperationalStateChange
	MGTH313	MGTH313--acKeepAlive
	MGTH314	MGTH314--acNATTraversalAlarm
	MGTH500	MGTH500--acBoardEvBoardStarted
	MGTH501	MGTH501--acgwAdminStateChange
	MGTH600	MGTH600--acEnhancedBITStatus
	MGTH601	MGTH601--dsx1LineStatusChange
	MGTH800	MGTH800--acPerformanceMonitoringThresholdCrossing
NCAS logs	NCAS325	An alarm log generated when a critical alarm is raised because the NCAS Link goes down. It is also generated when the alarm is cleared when the NCAS Link comes up
	NCA501	Generated when an Out-of-Band REFER Request that has been received by the Session Server does not validate and this the request can not be accepted.
	NCAS502	Indicates Unable to Establish Connection with SCPLite.
	NCAS601	Raised when a new NCAS Link is created.
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.

CS2000 Logs/Faults available

Log/Fault	Description
NLClient logs and NLServer logs	Desc Msg: Failed to register for connection to export Server at service<service name>
	Desc Msg: Failed to register for connection to Data Server at port <port number>
	Desc Msg: Failed to register for connection to Data Server at service <service name>
	Desc Msg: Failed to register for signals
	Desc Msg: Failed to send error
	Desc Msg: Communications not initialized
	Desc Msg: Input from unknown end point
	Desc Msg: Failed to send registration message to Data Server
	Desc Msg: Failed to send deregistration message to Data Server
	Desc Msg: Invalid Message from archive
	Desc Msg: store is disconnected:deregister the connection
	Desc Msg: Receive from Archive failed
	Desc Msg: Unreadable Data Server message type
	Desc Msg: Unreadable OM report
	Desc Msg: Failed to send correlation error data to Archive
	Desc Msg: OM Registration failed
	Desc Msg: Unreadable registration response
	Desc Msg: OM DeRegistration failed
	Desc Msg: Unreadable deregistration response from Data Server
	Desc Msg: Failed to send CM info request to Data Server
	Desc Msg: Failed to send deferred registration message to Data Server
	Desc Msg: Failed to send re-registration message to Data Server
	Desc Msg: Fatal status change
	Desc Msg: Unreadable OM status received from Data Server
	Desc Msg: Could not get GroupInfo
	Desc Msg: Failed to send nlGrpInfoRsp data to Archive
	Desc Msg: Unreadable CM info message from Data Server
	Desc Msg: Could not open License File
	Desc Msg: Unexpected message type from Data Server
	Desc Msg: Lost connection to Data Server
	Desc Msg: Receive from Data Server failed
	Desc Msg: Communications not initialized

CS2000 Logs/Faults available

Log/Fault		Description
		Desc Msg: Failed to send end_of_report msg to store
		Desc Msg: Connection from unknown end point
		Desc Msg: Switch name unknown
		Desc Msg: Arithmetic overflow in correlation <correlation name>
		Desc Msg: Failed to send OM data to Archive
		Desc Msg: Error while doing a send to the Agent, discard send queue
		Desc Msg: Port for the service <NLservice name> is not available
		Desc Msg: Failed to register for connection to export Server at service <service name>
		Desc Msg: Failed to register for connection to Data Server at port <port num>
		Desc Msg: Failed to register for connection to Data Server at service <service name>
NMSS logs	NMSS115	Generated if an error occurs while sending NMS TCAP messages to SCTP.
	NMSS116	Generated if an error occurs while receiving NMS TCAP messages from SCTP.
	NMSS117	Generated if an error occurs while sending NMS REJ messages to SCTP.
	NMSS118	Generated if an error occurs while receiving NMS REJ messages from SCTP.
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.
	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.
PATC log	PATC300	Major alarm and log to indicate when a restart is required for a patch on a specific card. PATC300 is generated when a patchAlarmFault is received from an MG9000 DCC card.

CS2000 Logs/Faults available

Log/Fault	Description
PKManager Security logs and alarms	PKM300 A Major Alarm log that indicates an attempt to create and validate an X509 certificate failed. PKM300 also functions as a clear log.
	PKM301 A Major Alarm log that indicates an attempt to deliver a certificate to an application for a device failed. PKM301 also functions as a clear log.
	PKM302 A Critical Alarm log that indicates an X509 certificate has expired. PKM302 also functions as a clear log.
	PKM303 A Major Alarm log that is the last forewarning of an impending certificate expiration. PKM303 also functions as a clear log.
	PKM304 A Minor Alarm log that is the initial forewarning of an impending certificate expiration. PKM304 also functions as a clear log.
	PKM305 A Major Alarm log that indicates a certificate used for OAM&P functions has expired. PKM305 also functions as a clear log
	(TBD) Creation of a certificate request for export
	(TBD) Reception of a certificate request from integrated client applications
	(TBD) Successful creation of an X509 certificate.
	(TBD) Successful delivery of an X509 certificate
	(TBD) Invalid and rejected certificate requests
	(TBD) Revocation of certificates
	(TBD) X509 certificate replacement requests
RMGC log	When a major RMGC alarm is raised or cleared, an SNMP trap is sent from the GWC to the GWC EM.
REX logs	REX 600 Indicates the start or completion of REX on a card/card-pair.
	REX 601 Indicates the success or failure of REX on a card/card-pair.
	REX 602 Indicates that the REX for the card/card-pair under consideration has been skipped.
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.
SCAI logs	SCAI304 If the total size of the outgoing ICM message with UUI exceeds the maximum supported size of outgoing ICM message then the UUI IE will be discarded and LOG SCAI 304 will be generated.
	SCAI600 When TDM Call Recording TRNKINFO criteria is met, if the trunk information is not accessible by SCAI, the new parameter, TRNKINFO, will not be sent and SCAI600 will be generated.
SFPS log	SFPS100 Generated when a craft person enters an invalid LFPS password three times.

CS2000 Logs/Faults available

Log/Fault	Description
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.
SIPS logs	SIPS300 Generated during the alarming of dropped connection requests (due to either the threshold being crossed for throttling connections, or due to attempting to use TLS when TLS is not enabled). The severity of the alarm indicates the threshold that was crossed, 10 dropped connection requests in a minute for a MINOR, 50 dropped requests for a MAJOR, and 100 dropped requests (or more) for a critical. The alarm is raised for a minimum of 30 minutes.

CS2000 Logs/Faults available

Log/Fault	Description
SIPS301	Generated during authentication failure events. The alarmd process log indicates the level of trouble (CRIT indicates a very serious problem, MINOR may be transient or the beginning of a series of authentication failures).
SIPS302	Generated as a result of the alarm process check to ensure the Local Server certificate continues to be valid. The expiration date contained in the certificate is checked on a daily basis, and when the expiration of the certificate will occur within 31 days (MINOR), 15 days (MAJOR), or 5 days (CRIT), the alarm is raised, with this log. For certificates that have already expired, the CRIT alarm and log is generated, and authentication failures will be output for any connections that are attempted.
SIPS303	Certificate Mismatch in Server Certificate, generated if the two sets of files on the active and inactive sides do not match each other. An alarm is also raised.
SIPS305	Generated during the initialization of the Call Processing application (i.e. during the unlock). If one of these critical logs comes out, it means that there is a problem with the initialization, and the application is unable to start.
SIPS308	Failed Certificate Policy Check, generated when enough certificate policy failures have occurred to generate an alarm. An alarm is also raised.
SIPS600	Generated during the connection set up of the Call Processing application. When the 'monitor OMs' log comes out, ensure that the threshold levels set for connection throttling are reasonable for the size of the office. If the 'TLS is not enabled' message comes out, ensure that the initialization of the call processing application worked correctly.
SIPS601	Generated during authentication failure events. This INFO log indicates the reason for the authentication failures.
SIPS604	Generated during the initialization of the Call Processing application (i.e. during the unlock). This log indicates when the current local certificate will expire. The Certificate Effective Date log is added in SN09.
SIPS605	Generated during the initialization of the Call Processing application (i.e. during the unlock). This log indicates that TLS has been enabled. Expect a SIPS604 log along with this log.
SIPS606	Generated when there is a problem importing the trusted certificate provisioned via the web interface in the database.
SIPS608	TLS Certificate Policy failure, generated when the remote side of the connection presents a certificate that does not conform to the selected local certificate policy.
SIPS609	Security Parameter Changed, generated whenever a TLS Security Parameter is changed by the user.

CS2000 Logs/Faults available

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. Also generated to indicate Password, Account, or Certificate expiration warning. SPFS380 Indicates that the syslog system has failed to write logs, or that it has resumed writing logs.
SSPFS security logs	SSPFS security logs are generated whenever any security affecting parameter is changed from the CLI. They include the following events: Login Retries Limit--whenever an MSAP access threshold is changed. Login Session (User Inactivity) Timeout-- whenever an MSAP time interval that controls keyboard lockout is changed. User Termination Timeout--whenever an MSAP time interval that controls keyboard lockout is changed. User Reauthentication Disable Timeout-- whenever an MSAP time interval that controls keyboard lockout is changed. Login Session Master Server--whenever an MSAP time interval that controls keyboard lockout is changed. Socks Security Service--whenever changes to MSAP security profiles and attributes occurs. IEMS Server IP address--whenever changes to MSAP security profiles and attributes occurs. Default PAM--whenever changes to the MSAP security configuration (e.g., routing to a security server) occurs. Radius PAM--whenever changes to the MSAP security configuration (e.g., routing to a security server) occurs.
STGW log	STGW700 An INFO log that may indicate any one of these issues or problems: FCR Change, Babbling node detected, Babbling node timeout, All babbling node IPs re-enabled due to initialization, or CPU occupancy critical alarm.

CS2000 Logs/Faults available

Log/Fault	Description
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.
Syslog alarm	Major alarm to indicate that the syslog system has failed to write logs, and a clear alarm to indicate that syslog has resumed writing logs.
TLS alarms	TLS connection request comes in above the connection throttle limit (and above the threshold for the alarm - the defined thresholds are: 10 for minor, 50 for major, and 100 for critical). TLS connection handshake failures (the thresholds are: 1 for minor, 2 for major, and 5 for critical). TLS local certificate expiration (expiry in 31 days or less - minor, 15 days or less - major, and 5 days or less - critical).
TMN logs	TMN301 Application error TMN302 System error TMN303 Communication error TMN309 Data Server error TMN311 Fatal error TMN600 Information only TMN601 File IO info TMN604 Application status TMN630 DataServer OK
TOPS logs	TOPS131 Generated when problems occur in the call flow for the activity TOPS Wireless Automated Directory Assistance Call (ADACC) with Release. TOPS615 An INFO log to indicate the operator teams and the number of positions in each team with auto-compression turned on. 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.

CS2000 Logs/Faults available

Log/Fault	Description
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).
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.

CS2000 Logs/Faults available

Log/Fault	Description	
	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
	TRKT211	Vacant Code
	TRKT212	Vacant Country Code
	TRKT213	Trigger Block
UNEM and UMUX logs	UNEM or UMUX300	Generated for a minor, major, or critical communication alarm.
	UNEM or UMUX301	Generated for a minor, major, or critical equipment alarm.
	UNEM or UMUX302	Generated for a minor, major, or critical environmental alarm.
	UNEM or UMUX303	Generated for a minor, major, or critical processing error alarm.
	UNEM or UMUX304	Generated for a minor, major, or critical quality of service alarm.
	UNEM or UMUX500	Generated when a standing alarm condition has bee cleared.
	UNEM or UMUX600	INFO log generated when an alarm is acknowledged by the UNEM system.
	UMUX501	INFO is generated to indicate a change in the operational state of a UMUX NE.
	UMUX502	INFO is generated to indicate that the UNEM's polling status of the UMUX NE has been modified.
	UMUX601	INFO is generated when a UMUX NE has been added to the UNEM topology inventory.
	UMUX602	INFO is generated when a UMUX NE has been deleted from the UNEM topology inventory.
	UMUX603	INFO is generated when a UMUX NE name is changed in the UNEM.
	UMUX604	INFO is generated when a card has been added to a managed UMUX inventory.

CS2000 Logs/Faults available

Log/Fault	Description
	UMUX605 INFO is generated when a card has been deleted from a managed UMUX inventory.
USNBD logs	UNB300 Reports problems with USNBD shared resources used by PCES.
	UNB302 Reports problems with USNBD processes used by PCES
	UNB304 Reports success and failure of surveillance activation and deactivation, and problems with surveillance activation.
	UNB305 Reports problems that affect PCES administration data and reports all user creations and deletions.
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 SN08 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.

CS2000 Logs/Faults available

Log/Fault	Description
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.
XAC400	XA-Core summary report.
XAC413	REx schedule failure. Accompanied by REXSch alarm.
XAC415	Routine exercise report. SN08 added "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	AMDI link condition cleared.
XAC610	Card returned to service. Modified in SN08 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).

CS2000 Logs/Faults available

Log/Fault	Description
	XAC628 Output when provisioning or deprovisioning.
	XAC629 Loss of communication restored.
	XAC630 FWvers cleared.
	XAC631 FW soaking started. Accompanied by FWsoak alarm.
	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, 729, 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 SN08, 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. This change is also reflected in SN09.
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.

CS2000 Logs/Faults available

Log/Fault	Description
	XNET605 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.
XTS logs	XTS382 When a sensor reports a failure condition, an XTS382 alarm is raised on the Alarms panel of the NCGL Session Server unit. An XTS382 log is generated. XTS383 When one or more sensors report failure conditions with either power supply module A or B, an XTS383 alarm is raised on the Alarms panel of the NCGL Session Server unit. An XTS383 log is generated. XTS682 When XTS382 Chassis Sensor fault condition and alarm is cleared, an alarm trap and INFO log XTS682 are generated. XTS683 When XTS383 Minor/Major Power Supply Sensor Fault alarm condition clears, INFO alarm/log XTS683 is generated.
XPKT log	XPKT340 Reports a variety of Gateway, Gateway Controller, and DPTMA resource problems, including failed anchor attempts.

CS2000 Core Manager--available logs/faults

The following table lists the CS2000 Core Manager Logs/Faults available. 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 Appendix G in this document titled "IEMS Functionality." For details on the faults themselves, refer to the Fault Management section of CS 2000 FCAPS documentation, NN10082-911 and NN10275-909, *Fault Management Log Reference*.

CS2000 Core Manager Logs/Faults available

Log/Fault	Description
Network Element: CS2000 Core Manager	
	For details on previously existing Logs/Faults, refer to NN10082-911.
CBM upgrade log	The CBM upgrade log is generated for any CBM upgrade failure.
SDM267	Indicates a change in the condition of a CBM link
SDM300	The connection from the CS2000 Core Manager to the CM or operating company LAN server(s) is down.

CS2000 Core Manager Logs/Faults available

Log/Fault	Description
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. More generally, indicates that a backup requirement is present/not fulfilled or not yet fulfilled.
SDM309	Fault detected on HW device or user took HW device OOS.
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.

CS2000 Core Manager Logs/Faults available

Log/Fault	Description
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
SDM337	Indicates that the patch failed signature checking.
SDM338	Indicates that the OMDD audit finds omdata file system usage exceeds 60% (Minor) or 80% (Major).
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.
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. More generally, indicates that the backup requirement has been fulfilled or is no longer present.
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.

CS2000 Core Manager Logs/Faults available

Log/Fault	Description
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.
SDM631	An info log generated when a file in <i>closedNotSent</i> directory is deleted by audit to make more than 80% available space in the omdata file system.
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.
SDM637	Indicates that patch check status is cleared by the user.
SDM638	A clear log generated when the OMDD audit finds omdata file system usage goes below 80% or below 60%.
SDM639	Critical--indicates that the OMDD audit finds omdata file system usage exceeds 90%. All the OM files from the closedSent directory will be deleted.
SDM650	Link maintenance requests a report on a failed link maintenance action.
SDM666	This INFO log indicates there is a failure to generate cryptographic keys for the user.
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.

CS2000 Core Manager Logs/Faults available

Log/Fault	Description
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.
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.

CS2000 Core Manager Logs/Faults available

Log/Fault	Description
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.
SDM security log	An Authentication and Authorization Security Syslog, generated when a security event occurs on a SDM.
SDM patch check alarm	This minor alarm is generated under the "sdmmtc sys" level, raised upon a patch signature check failure.

CS2K Management Tools (CMT)--available logs/faults

The following table lists the CS2000 Management Tools logs available. 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 chapter in this document titled "IEMS Functionality." For details on these logs, refer to the Fault Management section of CS2K Management Tools, NN10325-900 and to NN10275-909, *Fault Management Log Reference*.

CS2K Management Tools Logs/Faults available

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.
CMT303	A Critical automatically generated log upon the raising/clearing of a CMT alarm.
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.
CMT600	Generated when an RMGC overflow condition is detected. This log is propagated to the IEMS under the "other" category.

CS2K Management Tools Logs/Faults available

Log/Fault	Description
Alarm log for Corrupt Certificate	The log lists additional detail for the Corrupt Certificate alarm.
Alarm log for Changed Certificate	The log lists additional detail for the Changed Certificate alarm.
Corrupt Certificate	Minor alarm, raised when a syntax error is recognized in a Certificate or a disallowed combination of fields is present.
Duplicate Certificate	Minor alarm, raised when more than one Certificate with the same name is detected in the Nortel or Third Party certificate directories.
Delete Certificate	Minor alarm, raised if a Certificate file is removed that has GWs associated with it.
Certificate Changed	Minor alarm, raised when an existing profile is changed and one or more of the fields that are changed are not allowed.
Missing Certificate	Minor alarm, raised when a Nortel Certificate has been removed from the Nortel directory or changed to a different name.
No Available Call Server IP	A Critical alarm, raised if the SESM cannot get any available C-Side IP address from the Core.

ERS8600 (previously Passport 8600)--available traps/faults

ERS8600 (formerly Passport 8600) supports SCC2 format through the IEMS interface. For details on the IEMS interface, refer to the chapter in this document titled "IEMS Functionality." The following table lists the Passport 8600 traps available.

ERS8600 (previously Passport 8600) Traps available

Trap Name	Description
Network Element: ERS8600 (formerly Passport 8600)	
Faults from the ERS8600 (formerly Passport 8600) are provided via an SNMP Northbound interface that is provided on the ERS8600 itself.	
risingAlarm	Minor, correlates with PP310.
fallingAlarm	Cleared, correlates with PP311.
Default Trap	Indeterminate, correlates with PP312.
coldStart	Info, correlates with PP313.
warmStart	Info, correlates with PP315.
linkDown	Major, correlates with PP317.
linkUp	Cleared, correlates with PP318.
authenticationFailure	Warning, correlates with PP319.

ERS8600 (previously Passport 8600) Traps available

Trap Name	Description
rcnChasPowerSupplyDown	Critical, correlates with PP322.
rcnChasPowerSupplyUp	Cleared, correlates with PP323.
rcnChasFanDown	Critical, correlates with PP324.
rcnChasFanUp	Cleared, correlates with PP325.
rcn2kCardDown	Critical, correlates with PP326.
rcn2kCardUp	Cleared, correlates with PP327.
rcn2kTemperature	Critical/Cleared, correlates with PP328.
rcnErrorNotification	Warning, Major, Critical, correlates with PP329.
rcnLinkOscillation	Major, correlates with PP330.
rcnMacViolation	Critical, correlates with PP331.
rcnSonetTrap	Warning, correlates with PP332.
rcnStpNewRoot	Warning, correlates with PP333.
rcnStpTopologyChange	Warning, correlates with PP334.
rcnStpTCN	Warning, correlates with PP335.
rcn2kAtmPvcLinkStateChange	Info, Minor, Major, Cleared, correlates with PP336.
rcnSmlt1stLinkUp	Cleared correlates with PP337.
rcnSmlt1stLinkDown	Major, correlates with PP338.
rcnSmltLinkUp	Cleared, correlates with PP339.
rcnSmltLinkDown	Major, correlates with PP340.
rcnPasswordChange	Warning, correlates with PP341.
rcnPcmciaCardRemoved	Critical, correlates with PP342.
rcnSmartCpldTimerFired	Major, correlates with PP343.
rcnCardCpldNotUpDate	Major, correlates with PP344.
rcnlgapLogFileFull	Major, correlates with PP345.
rcnCpLimitShutDown	Major, correlates with PP346.
rcnSshServerEnabled	Cleared, correlates with PP347.
rcnSshServerDisabled	Major, correlates with PP348.
rcnSshSessionLogin	Info, correlates with PP349.
rcnSshSessionLogout	Info, correlates with PP350.
rcnSshUnauthorizedAccess	Critical, correlates with PP351.
rcnHaCpuState	Critical, correlates with PP352.
rcnInsufficientMemory	Critical, correlates with PP353.
rcnSaveConfigAction	Info, correlates with PP354.
rcnLoopDetectOnPort	Critical, correlates with PP355.
vrrpTrapStateTransition	Critical, correlates with PP356.
rcnEmError	Warning, correlates with PP357.

ERS8600 (previously Passport 8600) Traps available

Trap Name	Description
ospfVirtIfStateChange	Warning, Cleared, correlates with PP358.
ospfNbrStateChange	Warning, Cleared, correlates with PP359.
ospfVirtNbrStateChange	Minor, Cleared, correlates with PP360.
ospfIfConfigError	Critical, correlates with PP361.
ospfVirtIfConfigError	Critical, correlates with PP362.
ospfIfAuthFailure	Critical, correlates with PP363.
ospfVirtIfAuthFailure	Critical, correlates with PP364.
ospfIfStateChange	Warning, Cleared, correlates with PP365.
rcnCardDown	Critical, correlates with PP366.
rcnCardUp	Cleared, correlates with PP367.
rcnbgpEstablished	Cleared, correlates with PP368.
rcnbgpBackwardTransition	Critical, correlates with PP369.
rcnAggLinkUp	Cleared, correlates with PP370.
rcnAggLinkDown	Major, correlates with PP371.
rcnIgmpNewGroupMember	Info, correlates with PP372.
rcnIgmpLossGroupMember	Info, correlates with PP373.
rcnIgmpNewQuerier	Info, correlates with PP374.
rcnIgmpQuerierChange	Info, correlates with PP375.
rcnDvmrplfStateChange	Info, correlates with PP376.
rcnDvmrpNewNbrChange	Info, correlates with PP377.
rcnDvmrpNbrLossChange	Info, correlates with PP378.
rcnFdbProtectViolation	Info, correlates with PP379.
rcnLogMsgControl	Info, correlates with PP380.
rcnSaveConfigFile	Info, correlates with PP381.
rcnDNSRequestResponse	Info, correlates with PP382.
pingProbeFailed	Info, correlates with PP383.
pingTestFailed	Info, correlates with PP384.
pingTestCompleted	Info, correlates with PP385.
traceRoutePathChange	Info, correlates with PP386.
traceRouteTestFailed	Info, correlates with PP387.
traceRouteTestComplete	Info, correlates with PP388.
UDPEapSessionEndTrap	Info, correlates with PP389.
UDPEapSessionStartTrap	Info, correlates with PP390.
rcnDuplicateIpAddress	Critical, correlates with PP391.
rcnLoopDetectPortDown	Critical, correlates with PP392.

ERS8600 (previously Passport 8600) Traps available

Trap Name	Description
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 the design description of feature A00002920, which supports and generates ERS8600 (formerly 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.

GWC--available logs/faults

The following table lists the GWC Logs/Faults available.

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 chapter in this document titled “IEMS Functionality.” For details on the logs/faults themselves, refer to the Fault Management section of GWC FCAPS documentation, NN10090-911 and NN10275-909, *Fault Management Log Reference*.

GWC Logs/Faults available

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 SN08 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.
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 sub0system 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.

GWC Logs/Faults available

Log/Fault	Description
Standby unit disabled	Critical; indicates a unit is out of service and not available.
Core communication lost	Major if active unit; Minor if inactive unit. No response received to Core heartbeat.
Mate unit communication lost	Minor; no response received to mate heartbeat.
Gateway communication lost	A gateway has stopped responding to heartbeat.
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.
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).

GWC Logs/Faults available

Log/Fault	Description
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.
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. Datsync 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.

GWC Logs/Faults available

Log/Fault	Description
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.
GWC314	Raised in connection with a Location Id Reporting connection failure alarm.
GWC317	An alarm log raised whenever PreSwact audit fails. An alarm will be raised with proper text which explains which component has led Preswact audit to fail. The specific problem displayed at the GWC level for the alarm raised will match with the swact failure reason at the SESM GUI.
GWC318	Associated with a critical alarm which indicates an autonomous SWACT is initiated due to a loss of communication to all the associated media gateways. Clear log is GWC399.
GWC319	Associated with a critical alarm that indicates communication with the GWC's associated gateways is down. Clear log is GWC399.
GWC321	Indicates that Auto-negotiation is disabled on the ethernet link for the GWC card.
GWC322	Indicates that GWC's SNMP message rate exceeded the recommended maximum. A minor alarm is raised on crossing the Panic Levels and a warning alarm is raised on crossing the Warning Levels.
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 of 64 or fewer endpoints.
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.
GWC603	An Info log that indicates a netfail event occurred from the GW and was reported to the connection broker. The log shows on which GWC the problem occurred, the Gateway name, IP address of the GW, the Endpoint name, the terminal ID, and the reason for the netfail event.
GWC604	An Info log that indicates a connection broker exception occurred from the GW and was reported. The log shows on which GWC the problem occurred, the Gateway name, IP address of the GW, the Endpoint name, the terminal ID, and the reason for the exception.
GWC alarms	External Host Interface Signal Loss, based on the number of gateways that are out of service as compared to the number of gateways provisioned checked on a 5 minute polling period.

GWC Logs/Faults available

Log/Fault	Description
	External Host Interface Configuration Error, based on a 5 minute polling period.
	External Host Interface Protocol Error, based on the number of USP connections that are not active but do have heartbeat messages checked on a 5 minute polling period.
GWC EM alarm	“Failure to retrieve the certificate” is a Critical Alarm when GWCEM fails to retrieve the certificates from the PKBClient.
GWC security logs	telnet connection from remote host
	serial connection
	login attempted
	login result
	authentication server unreachable
	logout (by request, force out, or idle timeout)
	local account login
	local password change/reset
	GWC restart
	GWC reload

MCS Manager Logs/Faults

The following table lists the MCS Manager Faults and Alarms available through equipment such as MAS, BCP7200, SSLines, and MCS5200. Note that only alarms are sent northbound. MCS Manager can be supported through IEMS. For details on the IEMS interface, refer to the chapter in this document titled “IEMS Functionality.” For details on the logs, refer to NN10383-900, *Fault Management Alarm and Log Reference*, NN10332-911, *Session Server Fault Management*, and NN10035-111, *MCS5200 RTP Media Portal Basics*.

MCS Manager Logs/Faults

Log/Fault	Description
AC102	Trunk Framing settings on the connected PSTN switch do not match those provisioned on the Audiocodes Mediant 2000.
AC105	The port on the gateway is unable to tell the trunk is in-service. At this point, the trunk will attempt to send an Alarm Indication Signal (AIS).
AC107	There is a physical problem in the connectivity of the trunk to the gateway. In order to receive this alarm, the far end could be offline or disconnected.
AC128	The gateway is no longer responding to SNMP polling. Either SNMP is misconfigured, the gateway is network isolated, or the gateway is not operational.
DBCM101	A network element has lost communication with the database.

MCS Manager Logs/Faults

Log/Fault	Description
DBMN101	The System Manager cannot communicate with the SNMP agent that provides the database monitoring raw data.
DBMN102	Indicates an inability of the database SNMP agent to process the requests sent by the System Manager.
DBMN103	Indicates that the operational state of the database server process is a value other than "UP".
DBMN401	Indicates that the amount disk space used by the database is approaching its limit.
EMTC401	A threshold has been crossed. The number of unreachable static clients has reached or exceeded the configured percentage of 100% ... currently there are 20000 unreachable clients. Also functions as a Clear log.
FTP703	The FTP operation of OAM records to the OSS destination failed due to the error encountered in creating directory on the base directory configured.
FTP704	Indicates the FTP operation of OAM Record to the OSS destination failed with an error message.
FTP706	Indicates the FTP operation of OAM records failed because of failure of login for the userid and password configured.
HWER701	Cooling Device Malfunction - For the BC-T platform, derived from the monitors.blowers table. The alarm is raised when one or more blowers have any state value other than "good". The alarm severity is Critical if both blowers are faulty, otherwise the severity is Major. - For the Langley platform, derived from the tCoolingDevice and tOperationalState tables. The alarm is raised when one or more cooling devices have an operational state not equal to vEnabled. The alarm severity is Critical if any of the faulty cooling devices are unspared, otherwise the severity is Major.
HWER702	Power Supply Malfunction - For the BC-T platform, derived from the powerModuleHealthTable table. The alarm is raised when one or more power modules have a state not equal to "good". The alarm severity is Critical if any of the faulty power modules are unspared, otherwise the severity is Major. - For the Langley platform, derived from the tPowerSupply and tOperationalState tables. The alarm is raised when one or more power supplies have an operational state not equal to vEnabled. The alarm severity is Critical if any of the faulty power supplies are unspared, otherwise the severity is Major.

MCS Manager Logs/Faults

Log/Fault	Description
HWER703	Temperature Threshold Exceeded - For the BC-T platform, derived from the bladeTemperaturesTable and bladeTemperatureThresholdsTable tables. The alarm is raised when one or more blade SensorNTemp probes report a value greater than the corresponding warning threshold. The sensor value table in the report text consists an inequality ("actual > expected" and the sensor name for each sensor out of spec. The alarm severity is Major. - For the Langley platform, derived from the tTemperatureProbe table. The alarm is raised when one or more temperature probes report that a55TemperatureStatus is any value other than vOk. The sensor value table in the report text consists of the a55TemperatureStatus and the a55TemperatureProbeDescription variables for each sensor out of spec. The alarm severity is Major.
HWER704	Processor Malfunction - For the BC-T platform: HWER 704 is not reported for BC-T. - For the Langley platform, derived from the tProcessor and tOperationalState tables. The alarm is raised when one or more processors have an operational state not equal to vEnabled. The alarm severity is Major.
IMDB700	Indicates an internal cache in the network element (NE) has failed to load its data from the database during system initialization.
IMDB701	Indicates an internal cache in the network element (NE) has failed to synchronize its data with the database during regular system operation.
IMDB702	Indicates an internal table of the network element (NE) that is kept in memory has reached or is nearing its capacity.
KCRE201	Indicates a license key code resource owner is unable to update the resource management tables with its new key code limit from a newly applied license key.
LKEY470	Indicates the license key limit for a resource has reached or exceeded thresholds licensable limits.
LKEY750	Indicates the System Manager is not able to retrieve the license key from the database.
LKEY751	Indicates that the license key file could not be decrypted. This can be caused by: an invalid license key file, incompatible version of the license key file, or a corrupt license key file.
LKEY752	Indicates an error occurred during validation of the license key.
LKEY753	Indicates an error occurred during validation of the license key file when a license key has keycodes that are not compatible with the installed software.
LKEY754	Indicates an error occurred validating the license key file against the target system hardware.
LKEY755	Indicates that the license key upgrade failed because the supplied license key was intended for a system with a newer software release.
LOAD801	Indicates a new load becomes available in the loads directory (/var/mcp/loads).

MCS Manager Logs/Faults

Log/Fault	Description
MAS102	Indicates the MAS Provisioning Manager is unable to communicate with the database.
MAS103	Indicates the MAS Provisioning Manager is unable to communicate with one of the Media Application Server(s) configured in the system.
MAS300	Indicates that all initial connections upon startup are being established.
MAS301	Indicates the MediaController has lost connectivity with one or more processes.
MAS302	Indicates one or more MAS system components have failed to properly initialize.
MAS303	Indicates the MediaController is having some difficulty communicating with a particular process.
MAS304	Indicates the license key provided to the MediaController was invalid.
MAS305	Indicates the MediaController could not find the MAS license key.
MAS306	Indicates that all G711 licenses have been exhausted.
MAS307	Indicates all G729 licenses have been exhausted.
MAS308	Indicates the G711 license counter is getting close to exhausted.
MAS309	Indicates the G729 license counter is getting close to exhausted.
MAS310	Indicates the primary MediaController peer connection has failed.
MAS311	Indicates the MediaController peer backup connection has failed.
MAS312	Indicates the MediaController component is in a shutdown state.
MAS313	Indicates the MediaController is in a lock-pending state.
MAS314	Indicates the MediaController is in a locked state.
MAS327	Indicates a CStore is configured with a Content Store Mirrored Peer Server but is not connected to it.
MAS328	Indicates that a synchronization is in progress and that data may still be in the process of being copied with the peer content store. Occurs upon System restart or connection reestablishment with peer Content Store.
MAS329	Indicates CStore determined the pre 3.0 data format is present in the storage root.
MAS330	Indicates the CStore has been shutdown and is not running.
MAS331	Indicates the disk containing the Storage Root is at or near capacity (less than 1073741824 bytes available).
MAS351	Indicates the lvrMP component is in a shutdown state.
MAS361	Indicates the ConfMP component is in a shutdown state.
MAS371	Indicates the StreamSource component is in a shutdown state.
MAS382	Indicates the ConferenceManager process on the MAS has been shutdown and is not running.
MAS383	Indicates the connection between the MAS and the Web Collaboration Server is down.

MCS Manager Logs/Faults

Log/Fault	Description
MAS504	Indicates the number of pending transactions in the database exceeds 100,000.
MAS701	Indicates an error was encountered during the initialization of the MAS Provisioning Manager.
MAS705	Indicates more than two Media Application Servers have been found for a given pooled entity configured in the system.
NCAS101	An NCAS link has been disconnected from a specified IP address. Also functions as a Clear log.
NECM101	Indicates the System Manager is unable to communicate with an online network element (NE) instance.
NECM102	Indicates that the Fault/Performance Manager (FPM) that is configured to manage network element (NE) has no running instance.
NED101	Local communication with NED (Network Element Daemon) lost. This normally indicates NED has died, in which case it should automatically be restarted. Also functions as a Clear log.
NIF100	Indicates a network element instance configured with a floating IP address is unable to send a gratuitous ARP to associate the IP address with a logical interface.
NIF200	The logical interface for a specified floating IP Address is not up. Also functions as a Clear log.
NIF201	Failed to down logical interface for a specified floating IP Address. Also functions as a Clear log.
OLC401	Indicates the calls will be failing as the component has gone in overload mode.
OLC402	Indicates the database has gone into overload mode.
OLC403	Indicates the memory is exhausted.
R6AS700	R6AS configuration modified while instance is not offline. Also functions as a Clear log.
RESM701	Indicates the resource management partition audit raised an alarm when the resource management partition table usage values differ from the actual usage values returned from the resource owner.
RESM702	Indicates the resource management partition audit raised an alarm when the resource management partition table usage percentage are above the alarm thresholds.
RTA101	Indicates that the status of the standard recording stream is down.
RTA201	Indicates that there is an exception occurred when recording a data record into the spool directory of the network element instance.
RTP101	Critical. Raised from alarm "Blade Out of Service." Occurs when Managed IP or MCP Service network difficulties (communication problems) are encountered when attempting to communicate with the Media Blade specified by BladeName.
RTP102	Critical or Major. Raised from alarm "RTP Media Portal Out of Service." Occurs when timer activated event checks availability of Media Blades that are currently configured or when a OutOfServiceAlarm is raised.

MCS Manager Logs/Faults

Log/Fault	Description
RTP103	Critical. Raised from alarm "Best Blade Selection." Occurs during session setup when the host attempts to determine which media blade should handle the session.
RTP104	Critical, Major, or Minor. Raised from alarm "Port Usage." Occurs when timer activated event checks to see what percentage of the configured Managed IP Network ports are in use. Alarm severity is based on the percentages configured for the parameters: "Minor Port Usage Alarm Level," "Major Port Usage Alarm Level," and "Critical Port Usage Alarm Level."
RTP105	Major. Raised from alarm "Host Interface Failure." Occurs when a timer activated event checks the status of host network interfaces.
RTP106	Major. Indicates a communications problem (e.g. network difficulties) was encountered when attempting to communicate with the Media Blade specified by Blade Name (\$1).
RTP107	Major. Indicates link issues (e.g. carrier sense fails) were encountered when attempting to communicate over a problem interface (specified by Interface Name \$2) on the identified Media Blade (specified by Blade Name \$1).
RTP108	Critical. Indicates a Session Manager does not receive responses to requests made to the only available RTP Media Portal in its media resource pool.
RTP109	Major. Indicates a Session Manager does not receive responses to requests made to an available RTP Media Portal in its media resource pool.
RTP801	Minor. Indicates there is a change made to configuration data for an in-service RTP Media Portal.
RTP802	Critical. Indicates this RTP Media Portal is not configured correctly.
RTPB804	An error occurred during initialization. test-string. The RTP Media Portal is NOT operational. Also functions as a Clear log.
RTPB805	The RTP Media Portal Blade in slot 1 is in Standby. Also functions as a Clear log.
RTPB806	Cluster is in a 1+0 configuration with 0 node(s) shutting down and should be in a 1+1 configuration. Also functions as a Clear log.
RTPB815	Live Update of Media Portal Cluster Configuration Parameters Data is NOT supported. Also functions as a Clear log.
RTPB816	Live Update of Media Portal Cluster Fault Tolerance Data is NOT supported. Also functions as a Clear log.
RTPB817	Live Update of Media Portal Cluster Gateway Controllers Data is NOT supported. Also functions as a Clear log.
RTPB818	Live Update of Media Portal Cluster Session Managers Data is NOT supported. Also functions as a Clear log.
RTPB819	Live Update of Media Portal Cluster Static Routes Data is NOT supported. Also functions as a Clear log.
RTPB820	Live Update of Media Portal Cluster Service Instance Data is NOT supported. Also functions as a Clear log.

MCS Manager Logs/Faults

Log/Fault	Description
SEC820	Minor, Major, or Critical. Indicates a certificate in the internal keystore will expire in 89 days or less.
SEC821	Minor, Major, or Critical. Indicates a certificate in the internal truststore will expire in 89 days or less.
SIP401	The number of 500 Server Internal Error responses to SIP 9273429374@47.102.244.146 requests in OM group SIP_Inbound_Response_Report exceeds the specified percentage of responses. Also functions as a Clear log.
SIP703	Raise: Message received that contained bad syntax information. Bad headers will be discarded. Also functions as a Clear log.
SMCM101	Major. Indicates an online network element (NE) instance cannot communicate with the System Manager.
SRVR101	Major. Indicates the SNMP agent on the server cannot be contacted.
SRVR102	Major. Indicates the Server Monitor encountered unexpected error responses to the SNMP queries.
SRVR401	Indicates the CPU Occupancy of the monitored Server equals or exceeds the configured threshold.
SRVR402	Indicates the RAM Utilization of the monitored Server equals or exceeds the configured threshold.
SRVR403	Indicates the disk space utilization for a partition on the monitored Server equals or exceeds the configured threshold.
SRVR404	Indicates the interface utilization for a physical interface on the monitored Server equals or exceeds the configured threshold.
SVCA801	The System Manager service address has changed. Also functions as a Clear log.
SYNC200	Indicates that the configuration data for an NE instance is out-of-sync.
SYS101	Major. Peer network element instance presumed failed.
SYS102	Major. Indicates a fault tolerant Status message was received by a network element instance when no peer is provisioned for that instance.
SYS103	Major. Indicates a fault tolerant Status message was received by a network element instance when from a peer whose IP address is different from that of the provisioned peer..
SYS104	Major. Indicates a network element is in a fault tolerant configuration and a peer instance informs an instance that it believes it to be failed. This can happen if there is one way network failure or congestion from the instance to its peer.
SYS105	Major. Indicates a network element instance is isolated from the network. This indicates a failure in all network interface cards connected to that network.
SYS106	Critical. Indicates an unusual condition where a peer network element instance believes it is network isolated but is still able to communicate the isolation condition to the local instance.

MCS Manager Logs/Faults

Log/Fault	Description
SYS703	Major. Indicates a network element instance in a fault tolerant configuration when a peer instance is in the ACTIVATING phase but fails to transition to ACTIVE within the time specified by the engineering parameter "FaultTolerance:PeerActivityTransitionTimeout".
SYS704	Major. Indicates a network element instance in a fault tolerant configuration when a peer instance is in the DEACTIVATING phase but fails to transition to SHUTDOWN within the time specified by the engineering parameter "FaultTolerance:PeerActivityTransitionTimeout".
SYS707	A request to receive synchronization from peer is rejected. Also functions as a Clear log.
TCF902	Major. Indicates a network element is in a fault tolerant configuration and a peer instance informs an instance that it believes it to be failed. This can happen if there is one way network failure or congestion from the instance to its peer.
TCF903	Critical. Indicates a failure to create a TCP server or UDP based socket.
THLD401	Indicates a generic threshold alarm provided by the OM framework.
THLD402	Indicates a generic threshold alarm provided by the OM framework.
TSVR700	Critical. Indicates the failure by the session manager to connect to the terminal server provisioned in the voicemail server configuration page on the provisioning client.
TSVR701	Major. Indicates that the session manager failed to connect to the terminal server on the specified address and port..

MG4000-available logs/faults

The following table lists the MG4000 logs available. 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 chapter in this document titled "IEMS Functionality." For detailed information on logs, refer to NN10275-909, *Fault Management Log Reference*.

MG4000 logs available

MG4I 300	Media Integrity Failure
MG4I 301	GigE Audit Failure
MG4I 320	Counter overflow in the Operational Measurement pegs
MG4I 501	SCTP Core Connection State Change
MG4I 502	SCTP Peer Connection State Change

MG9000--available logs/faults

The following table lists the MG 9000 Faults available. 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 chapter in this document titled "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, *Fault Management Log Reference*.

MG 9000 Faults available

Network Element: MG 9000	
Fault	Description
ATM50 alarm	Raised if the SSI (Signal State Interrupt) count gets too high.
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.
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.

MG 9000 Faults available

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.
ESA304	Generated by the EM in response to a Major alarm from the MG9000 (nnEsaColFault) trap. The MG9000 sends this trap when it detects communication problems to other nodes in the same community of interest.
ESA312	Generated by the EM when a failure occurs while trying to provision internodal community of interest data for a given NE (Major alarm).
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 SN08.
GIGE alarms	301 LOS Loss of Signal, Critical 302 RFI Remote Failure Indication, Critical 304 TEM Temperature Threshold Exceeded, Critical 305 POW Low power indicated, Critical 306 RxSD Receive Signal Degraded, Critical 307 Receive Excessive Error Ratio, Critical RxEED 308 TBC Transmit Bias Current, Critical 309 LINT Link Initialization, Critical 310 OPT Transmit Optical Power, Critical 311 OPR Receive Optical Power, Critical 312 GARP GARP Failure, Critical 313 LKINT Link Integrity Failure, Critical 314 Auto Negotiation Failure, Critical AUTONEG 315 NON Non-preferred Link is active, Critical PREFLINK
GIGE logs	GIGE301 Indicates a Communications Subsystem Failure, loss of signal. GIGE302 Indicates a Communications Subsystem Failure, remote failure.

MG 9000 Faults available

GIGE303	Indicates a Communications Subsystem Failure, transmit failure.
GIGE304	Indicates a Communications Subsystem Failure, temperature threshold exceeded.
GIGE306	Indicates a Communications Subsystem Failure, low power indicated.
GIGE307	Indicates a Communications Subsystem Failure, transmit excessive error ratio.
GIGE308	Indicates a Communications Subsystem Failure, transmit bias current.
GIGE309	Indicates a Communications Subsystem Failure, link initialization.
GIGE310	Indicates a Communications Subsystem Failure, transmit optical power.
GIGE311	Indicates a Communications Subsystem Failure, receive optical power.
GIGE312	Indicates a Communications Subsystem Failure, GARP failure.
GIGE313	Indicates a Communications Subsystem Failure, link integrity failure.
GIGE314	Indicates a Communications Subsystem Failure, autonegotiation failure.
GIGE315	Indicates a Communications Subsystem Failure, non-preferred link is active.

MG9K EM alarms: The following alarms are raised or cleared when the Mg9kEM receives the "nnIpsecCertifFault" trap from the gateway:

IPSC 307	Indicates certificate has expired.
IPSC 308	Indicates certificate is about to expire in 4 days.
IPSC 309	Indicates certificate has invalid from date.
IPSC 310	Indicates remote certificate verification failed.
IPSC 311	Indicates certificate is missing Subject Alt. Name.
IPSC 312	Indicates time of date not set at the gateway.
IPSC 313	Raised when the EM attempts but fails to deliver certificates to the gateway. This alarm is cleared when subsequent delivery attempt succeeds.

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.

MGAUxxx Generated when audit task starts.

MG 9000 Faults available

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.
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.

MG 9000 Faults available

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.
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 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 connect to the database has failed

MG 9000 Faults available

MGEM705	Indicates that the Database is unavailable and correction failed.
MGEM714	Raised each time the MG9K Upgrade Tool is executed.
MGEM715	An audit log that is raised whenever a user attempts to set or clear the "Use Certificate" indicator for the NE.
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.
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.

MG 9000 Faults available

NE319	The NE319 log indicates MTA alarms of any severity.
NE320	The NE320 log indicates data audit faults of any severity; data audit required.
NE606	Generated each time a user clicks on “Clear persist and discover” button in NE Discovery View.
NE609	A software image log generated whenever a user executes an image request.
OMC300	Indicates that the OM Collector failed to collect OM files from the MG9K during a particular collection interval. Also indicates that the OM Collector is able to restart collecting OM files from the MG9K.
OVL808	(Critical) Indicates that an external messaging link has closed and cannot send/receive message.
OVL809	(Major) Indicates that the message loss is high enough such that the message link is in a degraded service state.
OVL810	(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.

MG 9000 Faults available

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.
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 2High Threshold exceeded. Correlates with Minor bipCSAshf2HighThres alarm.

MG 9000 Faults available

SHLF347	Current-Sense Card A Shelf 3High Threshold exceeded. Correlates with Minor bipCSAshf3HighThres alarm.
SHLF348	Current-Sense Card BShelf 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.
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.

MG 9000 Faults available

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.
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 bipAlarmFailedLED 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.

MG 9000 Faults available

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 alarmvccTpRdi.
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.
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.
VMG313	A Major alarm log which indicates an equipment malfunction due to a DSP resource overload. During the alarm state, new requests are diverted from the overloaded DSP to the other DSPs until the overloaded DSP recovers from the overload condition.
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.

MG 9000 Faults available

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 Main-tenance 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.
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.

MG 9000 Faults available

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).
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.

MG 9000 Faults available

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.
DACV alarms	DACV at Rail is a Major alarm to indicate the ITP clock circuitry has attempted to acquire sync and has traversed the frequency range to the extreme end of its capture range.. DACV Out of Range is a Major alarm to indicate that the ITP 's DACV clock circuitry is in an invalid condition and the values are out of range.
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.
MG9K alarms	Unable to communicate with RADIUS Server. Secure link Down with GWC. Packet Discard (depends on the threshold set). Overload Controls--these alarms will now also apply to the ABI & ITP Card as well as the DCC Card.
MG9K Threshold logs	SAD: Discard Policy, or Loop failed. IKE: Main mode failed, or Mismatched PSK, or Quick mode failed, or Proposal mismatch, or NULL ESP & authentication = null, or en/decryption failures, or Packet discarded, or decryption errors, or Auth errors. IPSec Security: Decryption error or Authentication error.
MG9K security alarms	Non-responsive RADIUS Server Expired Links to Security Peers Replayed Packet threshold Packet Discard threshold
MG9K security events logs	IKE negotiation errors IP packet authentication failures Packet discard Replayed packets
IPSec Syslog messages	There is a wide variety of IKE failure messages generated to syslog. Refer to feature A00005561 in the SN07.1 OSS Guide for the complete list.

MG15000 (previously PVG) Logs/Faults

For Logs/Faults available for MG15000 (previously PVG), refer to NTP NN10600-500, *Nortel Multiservice Switch 6400/7400/15000/20000 Alarms Reference*.

Multiservice Data Manager logs/faults

For logs and faults information for the Multiservice Data Manager (MDM), refer to the following documents: 241-6001-500, *MDM Alarms Reference*, and 241-6001-011, *MDM Fault Management Tools*.

NPM--available logs/faults

The following table lists the Network Patch Manager (NPM) Logs/Faults available.

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 chapter in this document titled “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, *Fault Management Log Reference*.

NPM Logs/Faults available

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	

NPM Logs/Faults available

Log/Fault	Description
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)
PATCH_ONHOLD	Patches on hold. Minor.
DEVICE_ONHOLD	Devices on hold. Minor.
REL_GEN_NOT_APP	A Major alarm raised when a released patch has not been applied. Relates to log NPM360.
PFRSGETPATCH	A Major alarm raised when the PFRS GENREPORT task has failed. Relates to log NPM360.
PFRSGENREPORT	A Major alarm raised when the PFRS GETPATCH task has failed. Relates to log NPM360.

QCA Logs/Faults

The following table lists the QCA Faults/Alarms available. 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 chapter in this document titled “IEMS Functionality.” For details on the logs,

refer to the Fault section of the FCAPS documentation on CS 2000, NN10083-911 and NN10275-909, *Fault Management Log Reference*.

QCA Logs/Faults

Log/Fault	Description
QCA201	Warning. Qca.properties not available at QCA start-up, or other problems related to properties/qca.properties.
QCA202	No priority. Old file retention directory (today-x) is being removed, OR file found in active directory when QCA started.
QCA203	QCA cannot be stopped for one of several possible reasons. Examples: the qca.properties file may be missing, the system cannot determine the QCA port number, QCA not running on specified port, an out-of-range port number is specified, or similar issues.
QCA300	No priority. File handler or server socket could not be started.
QCA301	Minor or Major. Minor: QoS Record received with Unsupported Length or Unsupported Version. Major: 10 sequential QoS Records received with Unsupported Length or Version.
QCA302	No priority. Out of sequence QoS record received, OR problem processing binary QoS record.
QCA305	No priority. Connection to client is closed. OR, The binary QoS Record header could not be processed.
QCA310	Minor, Major, or Critical. Minor: disk space is below the minimum threshold. Major: Disk space is below 500Mb. Critical: disk space is below 100 Mb.
QCA315	No priority, or Warning. Generated for one of many possible file writing or file access problems. For the Warning level, it means that a request to get a new file name has failed, or the QCA has failed to write the footer information to the active file while attempting to close. Other reasons, for example, might be: could not get new file to write records; file <fileName> is corrupted or removed; could not write to the activefile; active file exists but cannot write records to it. In some cases, QCA will shut down.
QCA322	No priority. New GWC connection received.
QCA399	No priority. Clear log for QCA301 or QCA310.

SAM21--available logs/faults

The following table lists the SAM21 Logs/Faults available. 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 chapter in this document titled "IEMS Functionality." For details on the logs/faults themselves, refer to the Fault Management

section of SAM21 FCAPS documentation NN10089-911 and NN10275-909,
Fault Management Log Reference.

SAM21 Logs/Faults available

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

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

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.
BootServerUnavailable	Indicates that the boot server cannot be reached. Severity may vary.
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.
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

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.
Memory usage high	Major. Total free memory has fallen below 15%. Critical. Total free memory has fallen below 10%.
NFSMountsDown	Raised for any mounts that remain down after the check and attempt to re-mount.

SAM21 Logs/Faults available

Log/Fault	Description
Power supply in Sled 1/2/3 has been removed.	Major. Most likely the whole sled has been removed.
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.

SAM21 Logs/Faults available

Log/Fault	Description
Firmware Flashing failed at backing up the firmware.	Critical. The copy operation from one bank to the other failed. Possible bad memory.
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.	
UnderlyingResourceUnavailable	A minor alarm when it indicates that an application card is locked and is not available, but a major alarm when it indicates that an application card is being autorecovered.

SPM--available logs/faults

The following table lists the SPM family Logs/Faults available.

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 chapter in this document titled “IEMS Functionality.” For details on the logs/faults themselves, refer to the Fault Management section of the appropriate SPM FCAPS documentation and NN10275-909, *Fault Management Log Reference*.

- SPM: NN10075-911
- DPT-SPM: NN10079-911 (IP)
- IW-SPM: NN10077-911 (IP)

General SPM Logs/Faults available

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.
ATM50	An alarm which is reported as an NE305 log. ATM50 adds a new reason code.
ATM501	The system's ATM signaling status has changed.

General SPM Logs/Faults available

Log/Fault	Description
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.
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.

General SPM Logs/Faults available

Log/Fault	Description
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.
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.

General SPM Logs/Faults available

Log/Fault	Description
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.
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.
IWBM502	Indicates that a BSY command is being requested for a set of IW SPM bridge terminals.
IWBM503	Indicates that an RTS command is being requested for a set of IW SPM bridge terminals.
IWBM504	Indicates that an OFFL command is being requested for a set of IW SPM bridge terminals.
IWBM505	Indicates that a FRLS command is being requested for a set of IW SPM bridge terminals.
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.

General SPM Logs/Faults available

Log/Fault	Description
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.
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. SN08 added a new text reason showing that it is generated when a STS3L carrier experiences an RFI alarm. SN08 added the aestivate/status of the unit/device. SN08 added 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.

General SPM Logs/Faults available

Log/Fault	Description
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.
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.

General SPM Logs/Faults available

Log/Fault	Description
SPM399	Generated whenever an SPM enters or leaves an overload condition. SN08 added next text "SPM Overload Report" due to being triggered via resource exhaustion/overload conditions on the ATMRRM.
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	Indicates that a particular resource RM protection group is excluded by the SPMRESALIGN tool, without align RMID-PWID values.
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).

General SPM Logs/Faults available

Log/Fault	Description
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.
SPM683	Indicates the reason for CEM swact.
SPM684	Indicates that the erase flash command has initiated, is completed, has failed, or has been rejected. SN08 added the aestivate/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.

General SPM Logs/Faults available

Log/Fault	Description
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.
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

The following table lists the STM logs available. STM logs will only be present in the HLR market. For detailed information on logs, refer to NN10275-909, *Fault Management Log Reference*.

STM logs available

STM398	Indicates a raised alarm in an STM device.
STM399	Indicates a cleared alarm in an STM device.

UAS--available logs/faults

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, *Fault Management Log Reference*.

Refer to the New and Changed section of this document to see if there are SN09FF changes in UAS logs and faults.

UAS Logs/Faults available

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

- 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

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

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

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

- 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

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

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

- 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_alarm_001] %s.
- 96258 (374) REMOTE_SRVSOCK_CREATION_FAILED Major, EventServer [es_alarm_002] %s.
- 96259 (375) SYSTEM_RESOURCE_ERR Critical, EventServer [es_alarm_003].
- 96260 (376) CONFIG_ERR EventServer [es_alarm_004].
- 96261 (377) HAMODE_CHECK_FAILED Critical, EventServer [es_alarm_005].
- 96262 (378) MATE_EVTSVR_CONN_LOST Minor, EventServer [es_alarm_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

	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

For detailed information on logs, refer to NN10275-909, *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 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.

OMs/PMs collection and delivery

There are two major OM/PM interfaces used in SN09:

- For CS2K Core OMs, SDM functionality uses either OM Data Delivery (OMDD) or EADAS. The OMs are grouped into user-defined report elements, formatted into CSV (comma-separated value) format, and delivered to a customer OSS (operations support system). The OMDD application delivers OMs only for the MG 4000, IW-SPM, DPT-SPM, SPM, and XA-Core. For more complete details on the CS2K Core OMs, refer to NN10264-709, *Carrier Voice over IP Performance Management: Operational Measurements Reference*.
- The following CS2K Network Elements use the Integrated Element Management System (IEMS) single performance interface to OSS in Common Performance Record Format (CSV or XML): GWC, Storm, ERS8600 (formerly Passport 8600), MS, USP (raw format), MSS15000, MG9000, MCS, MAS, RTP Portal.

The Integrated EMS provides a centralized location for collecting, storing and forwarding performance data in a CS 2000 central office. Its performance collection sub-system provides some basic tools for viewing and graphing the collected performance attributes. In addition, it does provide interfaces to configure the generation of threshold alarms for the collected Operation Measurement data. For detailed information on the IEMS performance management features please refer to the Integrated EMS Performance Management document (NN10327-711). You may also refer to chapter one of this document, *IEMS Functionality*.

Available OMs/ PMs

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.

CS 2000 Core OMs/PMs

The following table lists the operational measurements (OMs) and performance measurements (PMs) **that are new or changed since SN04** and

that are available from the Call Server 2000 Core network element. For a complete list of Core OMs/PMs available in Carrier Voice over IP, refer to NN10264-709, *Performance Management Operational Measurements Reference*.

CS 2000 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.

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
Network Element: CS 2000 Core			
AINTRAN	AIN Transports group--new in SN08		AIN
	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 SN08 Used for register overflows from the OM group ATTAMA, only when the BAS00023 SOC is ON, and only for registers AMANS and AMUNANS.		CAIN
	QUERYSCU	Counts call attempts that are unsuccessful because switching equipment in another office handles too many calls.	
	ISCONUCC	Counts the number of times a CAIN call queries the SCU.	
AUDSRVS	--provides one tuple for each Audio Server (AUD) node. These OMs appear in the Core only.		MG9K
	ANNCINSU	Announcement port in-service usage	
	ANNCOOSU	Announcement port out-of-service usage	
	ANNCTRU	Announcement port traffic usage	
	ANNCFTRU	Announcement port fast traffic usage	
	CNF3INSU	3-port conference circuit in-service usage	
	CNF3OOSU	3-port conference circuit out-of-service usage	
	CNF3TRU	3-port conference circuit traffic usage	
	CNF3FTRU	3-port conference circuit fast traffic usage	
	CNF6INSU	6-port conference circuit in-service usage	
	CNF6OOSU	6-port conference circuit out-of-service usage	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	CNF6TRU	6-port conference circuit traffic usage	
	CNF6FTRU	6-port conference circuit fast traffic usage	
CAINTRIG	CAIN Triggers group		CAIN
	QUERYSCU	Counts call attempts that are unsuccessful because switching equipment in another office handles too many calls.	
	ISCONUCC	Counts the number of times a CAIN call queries the SCU.	
CICM QoS Statistics: The following QoS statistics are reported by the CICM at the end of each call:			
	Jitter Average	Average variation in packet arrival times due to transmission (routing, queuing delay, etc...) through the network.	
	Jitter High Water Mark	Max variation in packet arrival times due to transmission (routing, queuing delay, etc...) through the network.	
	Far End Originated Loss	Far end originated loss	
	Round Trip Average	Average RTCP packets round trip time.	
	Round Trip High Water Mark	Max RTCP packets round trip time.	
	Local Silence Suppression	Indicates if silence suppression was used.	
	Local Rx and Tx Codec Type	Codec Type	
	Local Rx and Tx Packetization Rate	Frame duration in milliseconds.	
	End System Delay	Most recently specified/calculated end system delay in milliseconds.	
	Average One Way Delay	Average one-way delay in milliseconds.	
	Maximum One Way Delay	Maximum one-way delay in milliseconds.	
	Average Noise Level	Ratio of the silent period background noise level to overflow signal power, expressed in decibels.	
	Average Signal Power	Ratio of the signal level to overflow signal level, expressed in decibels	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	Echo Return Loss	Sum of the measured echo return loss (ERL) and the echo return loss enhancement (ERLE) expressed in dB	
	Listening R factor	Direct measure of the call quality or transmission quality, and incorporate the effects of CODEC type, packet loss, discard, burstiness, delay etc.;	
	Conversational R factor	Segment of the call that is carried over a network segment, external to the RTP segment	
	Listening Quality MOS	Estimated mean opinion score for listening quality.	
	Conversational Quality MOS	Estimated mean opinion score for conversational quality.	
	Burst R factor	R factor during a burst period; a burst is defined as a longest sequence of packets bounded by lost or discarded packets.	
	Average Burst Density	Average percentage of MIU's lost or discarded during burst periods.	
	Burst count	Number of bursts that have occurred on the call	
	Average Burst Length in MS	Average length of all burst periods in milliseconds that have occurred on the call	
	Gap R factor	R factor during a gap period; a gap is defined as the period of time between two bursts.	
	Average Gap Density	Average MIU'S lost or discarded within gap periods.	
	Average Gap Length in MS	Average length in milliseconds of all gaps that have occurred on the call.	
	Average Loss Rate	Total average percentage of MIUs lost and/or discarded.	
	Average Network Loss Rate	Total average percentage of MIUs lost in the network.	
	Average Discard Rate	total average percentage of MIU's discarded.	
	MIU Duration	Duration of each MIU, in milliseconds.	
	MIU per packet	Total number of MIU's in each RTP packet.	
	MIU Loss percentage	Percentage of MIUs handled by the call channel that were lost in the network.	
	MIU Discard percentage	Percentage of MIUs handled by the call channel that were discarded by the endpoint.	
	MIU Out of order percentage	Percentage of MIUs handled by the call channel that is discarded by the endpoint.	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	MIU Duplicate percentage	Percentage of MIUs handled by the call channel that is discarded by the endpoint.	
	Number of RTP packets rx/tx	Number of RTP packets received and transmitted.	
	Number of RTP packets out of order	Number of RTP packets received out of order.	
	Octets rx/tx	Octets sent and received.	
CMR FM OMs: 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.	
CP	Call Processing Software Resources group		CS2K Core
	CPLOSZ	Counts origination messages correctly attached to a call condense block.	
	CINITC	Counts call condense blocks that were in use at the time of a cold restart.	
	WAKESZ	Counts CPWAKEUP block seizures.	
DPLOM	OM group DPLOM has 13 registers for pegs and usage measurements of the VID resource pool.		CS2K Core
	DPLUSE	Usage register (100 sec sampling, with extension register) that tracks the number of VIDs in use by call processing.	
	DPLUSE2	Extension register for DPLUSE.	
	DPLFRE	Usage register (100 sec sampling, with extension register) that tracks the number of VIDs on the resource pool free list.	
	DPLFRE2	Extension register for DPLFRE.	
	DPLNOA	Peg register (with extension) that indicates the number of allocations from the resource pool.	
	DPLNOA2	Extension register for DPLNOA.	
	DPLNOD	Peg register (with extension) that indicates the number of deallocations to the resource pool.	
	DPLNOD2	Extension register for DPLNOD.	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	DPLFNVA	Peg register that indicates the number of times that a failure to allocate a VID happened because the resource pool free list was empty.	
	DPLFBAL	Peg register that indicates the number of times that a failure to allocate a VID happened because the resource pool free list was unavailable due to rebalancing (part of the rebuild process).	
	DPLFREB	Peg register that indicates the number of times that a failure to deallocate a VID happened (resulting in a "lost" VID) because the resource pool free list was being rebuilt.	
	DPLRLOS	Peg register that indicates the number of "lost" VIDs that were recovered.	
	DPLRCAL	Peg register that indicates the number of VIDs that were in use by call processing, but were not returned to the resource pool free list.	
DPTNODE Dynamic packet trunk node type (SPM or DPT), PM #, and node # SN07 adds the following: 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.			DPT-SPM
	DPTGTAT	The number of attempts to get a DPT Terminal for a particular DPT node, pegged every time an attempt to get a DPT terminal is made within a given transfer period. For a typical SIPT call the number of pegs is in the range of 1 peg per DPT agent per call. For a typical BICC call the number of pegs is in the range of 1 to 3 pegs per DPT agent per call.	
	DPTGTAT2	Extension of DPTGTAT	
	DPTGTFL	The number of attempts to get a DPT Terminal that failed (non-optimized) for a particular DPT node, pegged every time an attempt to get a <i>non-optimized</i> DPT terminal fails within a given transfer period.	
	DPTUSAG	The number of DPT Terminals in use for a particular DPT node, pegged every one-hundred seconds within a given transfer period.	
	DPTUSAG2	Extension of DPTUSAG	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	DPTGTFLO	The number of attempts to get a DPT Terminal that failed (optimized) for a particular DPT node, pegged every time an attempt to get an <i>optimized</i> DPT terminal fails within a given transfer period. Optimized failure attempts on nodes “not DPT-enabled” are not pegged against this register. Pegs to this register do not signify call failures. The optimized failure attempt to get an optimized terminal is immediately followed by an attempt to get a non-optimized terminal instead.	
	DPTHWT	The high water mark for number of DPT Terminals in use for a particular DPT node, pegged every ten seconds within a given transfer period.	
DPTOFC	Dynamic packet trunk office events		DPT-SPM
	DPGTAT	The number of attempts to get a DPT Terminal, pegged every time an attempt to get a DPT terminal is made within a given transfer period. For a typical SIPT call the number of pegs is in the range of 1 peg per DPT agent per call. For a typical BICC call the number of pegs is in the range of 1 to 3 pegs per DPT agent per call.	
	DPGTAT2	Extension register of DPGTAT incremented when DPGTAT reaches 65,535	
	DPGTFL	The number of attempts to get a DPT Terminal that failed (non-optimized), pegged every time an attempt to get a <i>non-optimized</i> DPT terminal fails within a given transfer period.	
	DPGTFL2	Extension register of DPGTFL incremented when DPGTFL reaches 65,535	
	DPUSAG	The number of DPT Terminals in use, pegged every one-hundred seconds within a given transfer period. Since this register is an accumulator and is added to itself the register can be misleading. To interpret the usage register, divide the value by the number of slow samples to determine the average usage for a given transfer period.	
	DPUSAG2	Extension register of DPUSAG incremented when DPUSAG reaches 65,535	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	DPGTFLO	The number of attempts to get a DPT Terminal that failed (optimized), pegged every time an attempt to get an <i>optimized</i> DPT terminal fails within a given transfer period. Optimized failure attempts on nodes “not DPT-enabled” are not pegged against this register. Pegs to this register do not signify call failures. The optimized failure attempt to get an optimized terminal is immediately followed by an attempt to get a non-optimized terminal instead.	
	DPGTFLO2	Extension register of DPGTFLO incremented when DPGTFLO reaches 65,535	
	DPHWT	The high water mark for number of DPT Terminals in use, pegged every ten seconds within a given transfer period.	
	DPHWT2	Extension register of DPHWT incremented when DPHWT reaches 65,535	
	DPDPL	Number of attempts to get a DPT terminal that failed due to port depletion, pegged every time an attempt to get a DPT terminal fails due to port depletion within a given transfer period.	
	DPDPL2	Extension register of DPDPL incremented when DPDPL reaches 65,535	
DPTOFCP DPT Office Protocol group--new in SN07			DPT-SPM
This OM group measures the performance of the supported dynamic packet trunk protocols for the office. The two supported protocols are BICC and SIP-T. 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.			
DTSRPM Pegs originations and dialtone delays grouped by the type of line making the call (DP, DTMF, or Pphone).			GWC
	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.	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
ENETPLNK ENET Peripheral Side Links group. The registers listed here are the only ones supported for SPM and MG4K applications.			DPT-SPM
	ENSPCHER	NOTE: This is an existing OM group. For details on the	
	ENLKERR	registers, see NTP 297-2621-814, available on Helmsman	
	ENLKFLT	Express.	
	ENSBLKU		
	ENMBLKU		
	ENLKPARU		
	ENSLKPAR		
	ENMLKPAR		
	ENLNKISOU		
	ENSLKISO		
	ENMLKISO		
ETHERNET	OM group		CS2K Core
	Alignment Errors	The counter associated with AlignErr Collection Interval.	
	FCS Errors	The counter associated with FcsErr Collection Interval.	
	Internal MAC Receive Errors	The counter associated with Internalmacrxerr.	
	Frame Too Long	The counter associated with Frtoolongs.	
	Internal MAC TX Errors	The counter associated with Internalmactxerr.	
	Symbol Errors	The counter associated with Symbolerr.	
	Inpause Frames	The counter associated with Inpausefr.	
	Outpause Frames	The counter associated with Outpausefr.	
FCDRTM1E	(Applies only to DMS)		CS2K Core
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.			

CS 2000 Core OMs/PMs

OM Group	or PM name	Registers	Description	Applicability
FCDRTM2E		(Applies only to DMS)		CS2K Core
		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)		CS2K Core
		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..		
IOCAP		IO Capacity for messaging over HIOP and HCMIC group		CS2K Core
		IO_SERVICE_T YPE	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, RxSIZE	Report the average transmit and receive message rates and sizes through the service.	
		IOTHRESH	Pegged every time the service average utilization for one minute exceeds the value of OFCENG office parameter IO_WARNING_THRESHOLD.	
ISUPCONN		ISUP Connection group		CS2K Core
		ISCONUCC	Added to count call attempts that are unsuccessful because there are no available idle circuits in another office to handle the call.	
		ISCONUCE	Added to count call attempts that are unsuccessful because switching equipment in another office handles too many calls.	
		ISCONUCF	Added to count call attempts that are unsuccessful because of a temporary fault in the far-end network.	
IWBM		Interworking bridge manager events (associated with IW SPMs)		IW-SPM
		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	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	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%	
MediaPortalInstance Created for registers that are per-BCP. For each BCP configured to support this Session Manager, an OM Row is created. It has the following registers:			Session Manager
	sesmSuccessStr eams	The number of stream setups that were successfully processed by this Media Portal Instance.	
	sesmFailedStrea ms	The number of stream setups that were not successfully processed by this Media Portal Instance.	
	rSipReceivedCo unt	The number of RSIP messages received from this Media Portal Instance.	
	createConnectio nCount	The number of CRCX messages sent to this Media Portal Instance.	
	modifyConnectio nCount	The number of MDCX messages sent to this Media Portal Instance.	
	deleteConnectio nCount	The number of DLCX messages sent to this Media Portal Instance.	
	CRCXErrorCoun t	The number of CRCX error response messages received from this Media Portal Instance.	
	CRCXTimeOutC ount	The number of CRCX time out (no response) from this Media Portal Instance.	
	MDCXErrorCoun t	The number of MDCX error response messages received from this Media Portal Instance.	
	MDCXTimeOutC ount	The number of MDCX time out (no response) from this Media Portal Instance	
	DLCXTimeOutC ount	The number of MDCX time out (no response) from this Media Portal Instance.	
MNGEMLNK Multiservice Node Gigabit Ethernet Module Link Bandwidth Engineering provides Gigabit Ethernet Link usage statistics to assist with network bandwidth Engineering.			IW-SPM
	TXOCT	Provides count for total number of bytes transmitted on a Gigabit Ethernet Link connected to a particular MG4K-IP/IW-IP node.	
	TXOCT2	Extension of TXOCT.	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	RXOCT	Provides count for total number of bytes received on a GigE Link connected to a particular MG4K-IP/IW-IP node.	
	RXOCT2	Extension of RXOCT.	
	TXPKT	Provides count for total number of packets transmitted on a GigE Link connected to a particular MG4K-IP/IW-IP node.	
	TXPKT2	Extension of TXPKT.	
	RXPKT	Provides count for total number of packets received on a GigE Link connected to a particular MG4K-IP/IW-IP node.	
	RXPKT2	Extension of RXPKT.	
	TXEROCT	Provides count for total number of bytes transmitted in errored packets on a GigE Link connected to a particular MG4K-IP/IW-IP node.	
	TXEROCT2	Extension of TXEROCT.	
	RXEROCT	Provides count for total number of bytes received in errored packets on a GigE Link connected to a particular MG4K-IP/IW-IP node.	
	RXEROCT2	Extension of RXEROCT.	
	TXERPKT	Provides count for total number of errored packets transmitted on a GigE Link connected to a particular MG4K-IP/IW-IP node.	
	RXERPKT	Provides count for total number of errored packets received on a GigE Link connected to a particular MG4K-IP/IW-IP node.	
	CRCERPKT	Provides count for total number of packets received with Cyclic Redundancy Check (CRC) errors on a GigE Link connected to a particular MG4K-IP/IW-IP node.	
	UNDERPKT	Provides count for total number of undersize packets received on a GigE Link connected to a particular MG4K-IP/IW-IP node.	
	OVERPKT	Provides count for total number of oversize packets received on a GigE Link connected to a particular MG4K-IP/IW-IP node.	
	SHORTPKT	Provides count for total number of short packets (aka fragments) received, on a GigE Link connected to a particular MG4K-IP/IW-IP node.	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	LONGPKT	Provides count for total number of long packets (aka jabber) received on a GigE Link connected to a particular MG4K-IP/IW-IP node.	
MNGEMTRF	Multiservice Node Gigabit Ethernet Module Traffic Engineering provides statistics of Nodal traffic usage		IW-SPM
	TOTCONN	Provides count for total number connections handled by a particular MG4K-IP/IW-IP node.	
	TXRTPOCT	Provides count for total number of RTP bytes transmitted from a MG4K-IP/IW-IP node. Register TXRTPOC2 is an extension register for TXRTPOCT.	
	TXRTPOCT2	Extension of TXRTPOCT.	
	RXRTPOCT	Provides count for total number of RTP bytes received for a MG4K-IP/IW-IP node.	
	RXRTPOCT2	Extension of RXRTPOCT.	
	G711MUCN	Provides count for total number of G.711 MuLaw codec connections handled by a particular MG4K-IP/IW-IP node.	
	G711ACN	Provides count for total number of G.711 A-Law codec connections handled by a particular MG4K-IP/IW-IP node.	
	TXG711PK	Provides count for total number of RTP packets transmitted for G.711 connections handled by a particular MG4K-IP/IW-IP node.	
	TXG711PK2	Extension of TXG711PK.	
	RXG711PK	Provides count for total number of RTP packets received for G.711 connections handled by a particular MG4K-IP/IW-IP node.	
	RXG711PK	Extension of RXG711PK.	
	G729CN	Provides count for total number of G.729 connections handled by a particular MG4K-IP/IW-IP node.	
	TXG729PK	Provides count for total number of RTP packets transmitted for G.729 connections handled by a particular MG4K-IP/IW-IP node.	
	TXG729PK	Extension of TXG729PK	
	RXG729PK	Provides count for total number of RTP packets received for G.729 connections handled by a particular MG4K-IP/IW-IP node.	
	RXG729PK	Extension of RXG729PK	
	CCDCN	Provides count for total number of 64K Clear Channel Data (CCD) Connections handled by a particular MG4K-IP/IW-IP node.	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	TXCCDPK	Provides count for total number of RTP packets transmitted for Clear Channel Data connections handled by a particular MG4K-IP/IW-IP node.	
	RXCCDPK	Provides count for total number of RTP packets received for Clear Channel Data connections handled by a particular MG4K-IP/IW-IP node.	
	VBDCN	Provides count for total number of Voice Band Data (VBD) Connections handled by a particular MG4K-IP/IW-IP node.	
	TXVBDPK	Provides count for total number of packets transmitted for Voice Band Data connections handled by a particular MG4K-IP/IW-IP node.	
	RXVBDPK	Provides count for total number of packets received for Voice Band Data connections handled by a particular MG4K-IP/IW-IP node.	
	T38CN	Provides count for total number of T.38 connections handled by a particular MG4K-IP/IW-IP node.	
	TXT38PK	Provides count for total number of packets transmitted for T.38 connections handled by a particular MG4K-IP/IW-IP node.	
	RXT38PK	Provides count for total number of packets received for T.38 connections handled by a particular MG4K-IP/IW-IP node.	
	RF2833CN	Provides count for total number of RFC2833 connections handled by a particular MG4K-IP/IW-IP node.	
	SLSUPCN	Provides count for total number of Silence Suppression connections handled by a particular MG4K-IP/IW-IP node.	
NCAS_LINK	Non-call Associated Signaling (NCAS) Link OM group		NGSS
	NUM_LINK_UP	Number of times the NCAS Link is brought up.	
	NUM_LINK_DO	Number of times the link goes down.	
	WN		
	NUM_MSG_SE	Number of messages sent over the NCAS Link.	
	NT		
	NUM_MSG_RC	Number of times a response is received over the NCAS Link	
	VD		
	NUM_MSG_SE	Number of times the message send fails	
	ND_FAIL		
	NUM_MSG_RC	Number of times the message receive fails.	
	V_FAIL		

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
NGSSOM	Next Generation Session Server OM group		NGSS
	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.	
NMSNCAS	Network Message Waiting (NMS) Non-call Associated Signaling (NCAS) OM group		NGSS
	SCTPNMSS	NMS TCAP messages sent successfully over SCTP	
	SCTPNMSR	NMS TCAP messages received successfully over SCTP	
	SCTPREJS	NMS REJ messages sent successfully over SCTP	
	SCTPREJR	NMS REJ messages received successfully over SCTP	
NMTCUNIT	Node Maintenance Unit Measurements group. The registers listed here are the only ones supported for SPM and MG4K applications.		DPT-SPM
	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		
NWMFRRCT	Network Management Flexible Reroute group		CS2K Core
	FRRATTCT	Counts calls that are rerouted to a Virtual Interworking Agent (VIA) route list. Required for ACC (Automatic Congestion Control).	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	FRRFLCT	Counts rerouted calls that fail to find an idle VIA route list. Required for ACC (automatic congestion control).	
PCEM	Performance Measurements		CS2K Core
	EMSENT	Event message successfully generated.	
	EMFAIL	Failed to build event message.	
	EMSYSFL	System unable to send event message.	
	EMSENT2	Overflow register for EMSENT	
	EMFAIL2	Overflow register for EMFAIL	
	EMSYSFL2	Overflow register for EMSYSFL	
PKTMA	Packet Media Anchor group		GWC
	PMAREQST	A peg register to indicate the number of anchored call attempts..	
	PMAFLNR	A peg register to indicate the number of failed anchored call attempts due to the unavailability of resources.	
	PMAHWM	A high water mark register to indicate the maximum number of simultaneous anchored calls.	
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	
	PMFLT	registers, see NTP 297-2621-814, available on Helmsman	
	PMMSBU	Express.	
	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,	
	PMTFLT	available on Helmsman Express.	
	PMTMSBU		
	PMTUSBU		
	PMTMMBU		

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	PMTSBP PMTMBP PMTMWXFR PMTMCXFR PMTINTEG		
PORTS	This OM group is created due to the large number of registers already existing in the MPCP OM group. Two registers are moved from MPCP to Ports: "rtpMpPortUsage" and "connMapEntries"		
	sampledRtpMpPortUsage	Provides the summing of the in use ports every 100 seconds.	
	portUsageSampleCnt	The number of 100 second samples taken during this collection interval contributing to the averaged report.	
	rtpMpPortUsageHWM	Highest number of simultaneous ports detected to be in use during this collection interval.	
	rtpMpPortUsageLWM	Lowest number of simultaneous ports detected to be in use during this collection interval.	
SCMP	SCMPTRF	If an SCMP line is found Callp busy, the SCMPTRF register will be pegged for that line.	Line Provisioning
	SCMPMNT	If an SCMP line is found maintenance busy or unavailable, the SCMPTRF register will be pegged for that line.	
SIPGW	OM groups--In SN09FF, 5 spare registers were added to each of the SIPGW OM Groups listed here. NOTE: The spare OM registers and spare OM groups introduced are reserved for future use.		
	SIPGW_CALLP		
	SIPGW_SERVICES		
	SIPGW_MISC		
	SIPGW_TLS		
	SIPGW_OOB		
	SIPGW_NCAS		
	In SN09FF, 3 spare OM groups are added, each with 10 registers. NOTE: The spare OM registers and spare OM groups introduced are reserved for future use.		
	SIPGW_SPARE1		
	SIPGW_SPARE2		
	SIPGW_SPARE3		
SIPGW_OVERLOAD	OM group SIPGW_OVERLOAD is added to the Session Server to provide statistics related to the resources that are monitored to determine whether the SIP Gateway application is in overload. In SN09FF, 5 spare registers were added to this group, reserved for future use.		NGSS

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	CPU_OCCUPAN CY	The value calculated for the amount of time the CPU spent performing work as a percentage to its total running time over the last sampling period (10 seconds)	
	CPU_OCCUPAN CY_HWM	The maximum value calculated for the amount of time the CPU spent performing work as a percentage to its total running time over a 30 minute period. Reset to 0 every 30 minutes.	
	GCP_QUEUE_S IZE	The size of the GCP queue at the time the last sample was collected.	
	GCP_QUEUE_S IZE_HWM	The maximum sampled size of the GCP queue over a 30 minute period. Reset to 0 every 30 minutes.	
	SIP_QUEUE_SI ZE	The size of the SIP queue at the time the last sample was collected.	
	SIP_QUEUE_SI ZE_HWM	The maximum sampled size of the SIP queue over a 30 minute period. Reset to 0 every 30 minutes.	
SMSTOPS.	This OM group records application-level events for the TOPS short message service.		TOPS
	SMSSSENT, SMSSSENT2	SMS sent	
	SMSSSUCC, SMSSSUCC2	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	
SPMOVLD	Spectrum Overload Statistics group		SPM
	The new SPMOVL D 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).		

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
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	
	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	
TDGTHRU. TOPS Datagram Throughput. This OM group counts the number of UDP messages sent and received in each of several “buckets” or message size ranges. 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. The group consists of 14 registers and 14 extension registers, counting message sizes ranging from <= 48 bytes up to > 368 bytes.			TOPS
TONES			CS2K Core

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	TONEATT	Counts calls that the system routes to each tone generator.	
	TRKQOS records instances in which QOS threshold values have been exceeded for GWC 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.	GWC
(Checking)		The OMs 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	GWC
TRNK2	OM group to hold extension registers from TRK OM group		CS2K Core
	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	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	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	
	NPQUERY2	Extension register of NPQUERY in TRK OM group	
	NPRESP2	Extension register of NPRESP in TRK OM group	
UTR	Universal Tone Receiver group		UAS
	UTRSZRS	Counts each time that the system supplies a UTR to a call in response to a request.	
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	
	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.	
	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.	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	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.	
XACORE	XA-Core hardware-related OMs		CS2K Core
	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	
	XETHRLNK	Hardware faults on an Ethernet link	
XACSRVC	XA-Core service-related OMs		CS2K Core
	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	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	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	
	XATRAP	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	
XPMOVL Collects statistics on XPM overload conditions. This is an existing OM group that functions the same as in TDM switches.			GWC
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

The following section describes performance measurements collected and reported by the Integrated EMS for the various network elements. Pre-IEMS Performance interfaces for Network Elements, if integrated by the customer in SN07, are still supported in SN09, but are subject to the MD process that will be published for all FCAPS interfaces.

Audio codes Media Servers (AMS) Performance Measurements

Performance Measurements for the AudioCodes media servers are available through the Integrated EMS, and also through an SNMP interface. 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.

AudioCodes media servers PMs

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: AMS		
acPerfMediaGateway (new in SN08)	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.
	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.

AMS Control Protocol, RTP, packet statistics PMs

OM Group or PM Name	Name	Description
	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
	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.

AMS Control Protocol, RTP, packet statistics PMs

OM Group or PM Name	Name	Description
	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: AMS		
acPerfMediaServices (new in SN08)	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.

AMS IVR, BCT, CONF, and IT PMs

OM Group or PM Name	Name	Description
	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.
	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.

AMS IVR, BCT, CONF, and IT PMs

OM Group or PM Name	Name	Description
	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.
	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.

AMS IVR, BCT, CONF, and IT PMs

OM Group or PM Name	Name	Description
	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.
	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.

Ethernet Routing Switch 8600 (formerly Passport 8600) PMs

For information on performance measurements (PMs) available for the Media Gateway 15000 (previously PVG) network element, refer to Appendix G in this document, *Ethernet Routing Switch 8600 Trap List*.

GWC Performance Measurements

Performance Measurements for the Gateway Controller are available through the Integrated EMS. For more detailed information, refer to NN10208-711, Gateway Controller Performance Management. The following table lists the GWC performance measurements.

GWC Performance Measurements

OIDs	Description
The GWC supports collection of a subset of several MIBs. The following table entries show the OIDs that are collected in various categories.	
Host-Resources-MIB	
host(25).hrSystem(1)	
25.1.hrSystemUptime(1)	System Uptime (distinct from sysUpTime)
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.

GWC Performance Measurements

OIDS	Description
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.
RFC1213-MIB	
sysDescr	
snmpInPkts	
snmpOutPkts	
snmpInBadVersions	
snmpInBadCommunityNames	
snmpInBadCommunityUses	
snmpInASNParseErrs	
snmpInTotalReqVars	
snmpInTotalSetVars	
snmpOutTraps	
snmpSilentDrops	
Unit Status-MIB	
norUnitAdminStatus	
norUnitOperStatus	
norUnitActivity	
DPT Services PM-MIB	
dptCallAttempts	
dptCallFailResTimeout	
dptCallFailResError	
dptCallFailAccOOS	

GWC Performance Measurements

OIDs	Description
accState	
apgInsertions	
maxSimulApgCalls	
apgCallFailGWException	
apgCallFailGWLost	
raState	
totalResourceCapacity	
resourceRequestError	
GWC Performance Statistics	
The following are reported through the GWC Performance MIB:	
• Small GWs in Disabled State • Large GWs in Disabled State • Trunk GWs in Disabled State • Audio GWs in Disabled State • Total Gateways Provisioned • DNS failed GW discovery • DNS good GW discovery • RSIP used in GW discovery • Total DNS GWs to discover • USP SS7 paths disabled • USP SS7 path not Active • Peer connections failed during interval • Peer connections completed during interval • Peer connections attempted during interval	

GWC Performance Measurements

OIDs	Description
GWC Performance Statistics	
Media Proxy OMs	The following are reported through the GWC Performance MIB: • Number of provisioned Media Proxies counts the number of currently provisioned media proxies on the GWC each 5-minute period. • Media Proxy 5 minute successful calls counts the number of calls that were successfully setup using this Media Proxy on this GWC in the last 5 minute OM period. • Media Proxy 30 minute successful calls counts the number of calls that were successfully setup using this Media Proxy on this GWC in the last 30 minute period. • Media Proxy 5 minute failed calls counts the number of failed attempts to setup a call using this Media Proxy on this GWC in the last 5 minute OM period. • Media Proxy 30 minute failed calls counts the number of failed attempts to setup a call using this Media Proxy on this GWC in the last 30 minute period. • GWC 5 minute successful calls counts the number of calls that were successfully setup using any available Media Proxy on this GWC in the last 5 minute OM period. • GWC 30 minute successful calls counts the number of calls that were successfully setup using any available Media Proxy on this GWC in the last 30 minute period. • GWC 5 minute failed calls counts the number of failed attempts to setup a call on any available Media Proxy on this GWC in the last 5 minute OM period. • GWC 30 minute failed calls counts the number of failed attempts to setup a call on any available Media Proxy on this GWC in the last 30 minute period.

IEMS Performance Measurements

The following table lists the performance measurements (PMs) collected by the Integrated Element Management System.

Collection Attribute Name	Description
Network Element: IEMS	
database	usedTableSpaceInBytes
	usedTableSpaceInPercent
	numOfTableCleanUpPolicyExecutions
fault/events	numOfEvents
	numOfEventsFromUnknownCustlogDevices
	numOfEventsFromUnknownDevices
	numOfDiscardedEvents
	numOfEventsAdded
	eventQueueSize
	avgEventThroughputRate
	maxEventThroughputRate
	DeviceEventRateTable This table will have the following columns:
	- ID
	- DeviceName
	- EventRate per Second
fault/alarms	numOfActiveAlarms
	numOfCriticalAlarms
	numOfMajorAlarms
	numOfMinorAlarms
	nmOfWarningAlarms
	numOfAlarmsCleared
	numOfAlarmsAdded
MG3200	Call Processing Performance Management (10 measurements)
	RTP Performance Measurements (12 measurements)
	System Performance Measurements (2 measurements)
performance	numOfCollectionJobsProvisioned
	numOfReportJobsProvisioned
	numOfFailedReportJobs
	numOfTransferJobProvisioned
	numOfAttributesCollected
	numOfAttributesCollectedOverPreviousInterval
performance/Successful Collection Jobs	numOf5MinSuccessfulJobs
	numOf15MinSuccessfulJobs
	numOf30MinSuccessfulJobs

Collection Attribute Name	Description
performance/Partial Successful Collection Jobs	numOf60MinSuccessfulJobs
	numOf12HrSuccessfulJobs
	numOf24HrSuccessfulJobs
	numOf5MinPartialSuccessfulJobs
performance/Failed Collection Jobs	numOf15MinPartialSuccessfulJobs
	numOf30MinPartialSuccessfulJobs
	numOf60MinPartialSuccessfulJobs
	numOf12HrPartialSuccessfulJobs
	numOf24HrPartialSuccessfulJobs
	numOf5MinFailedJobs
performance/Collection Job Table	numOf15MinFailedJobs
	numOf30MinFailedJobs
	numOf60MinFailedJobs
	numOf12HrFailedJobs
	numOf24HrFailedJobs
	5MinCollectionJobTable
performance/report Job Table	This table will have the following columns - ID - JobName - Start Time - Execution Time
	15MinCollectionJobTable
	30MinCollectionJobTable
	60MinCollectionJobTable
	5MinReportJobTable
	15MinReportJobTable
performance/failedTransfer Jobs	30MinReportJobTable
	60MinReportJobTable
	numOf5MinFailedJobs
	numOf15MinFailedJobs
	numOf30MinFailedJobs
	numOf60MinFailedJobs
performance/transfer Job Table	numOf12HrFailedJobs
	numOf24HrFailedJobs
	5MinTransferJobTable
	15MinTransferJobTable
	30MinTransferJobTable
	60MinTransferJobTable

Collection	Attribute Name	Description
topology	30MinReportJobTable	
	60MinReportJobTable	
	numOfManagedObjects	
	numOfAddedManagedObjects	
	numOfDeletedManagedObjects	
	numOfThrottledDevices	
client	numOfUnManagedDevices	
	numOfUnknownDevices	
	numOfActiveClients	
	numOfSuccessfulLogins	
application memory	numOfFailedLoginAttempts	
	applicationHeapSize	
system	maxApplicationHeapSizeInAGivenInterval	
	systemRestartCount	

MCS, RTP Media Portal, and MAS Performance Measurements

For information on performance measurements (PMs) available for these network elements, refer to the following documents:

- NN10384-700, *MCS 5200 Performance Management*
- NN10367-111, *CVoIP RTP Media Portal Basics*
- NN10303-111, *MAS Meetme Basics*

The following MCS performance measurements were new in SN09.

MCS Performance Measurements

OM Group or PM Name	Registers	Description
Network Element: MCS		
StableCallCheckpointGenerated		Increments for each checkpoint generation corresponding to a new stable call on the active instance.
EndCallCheckpointGenerated		Increments when the Call terminates on the active instance and gets checkpointed for deletion.
StableCallCheckpointProcessed		Increments on the standby instance when a checkpoint indicating a new stable call or the end of an existing call is processed.
EndCallCheckpointProcessed		Increments on the standby instance when a checkpoint indicating a new stable call or the end of an existing call is processed.
CheckpointedCalls		Used on the standby instance to monitor the number of calls that would be preserved in a case of a failover.

MCS Performance Measurements

OM Group or PM Name	Registers	Description
Presence Event Report		Tracks the behavior of the various presence events that are processed by the server. For the 8 presence event types, OM registers count events Created, Processed, Optimized, Queued, and Parked.
EndCallCheckpointProcessed		Increments on the standby instance when a checkpoint indicating a new stable call or the end of an existing call is processed.
CONVERGED DESKTOP3_ SERVICE OM Group	CDC2C	Counts the number click-to-call originations that were placed from a MCD PC Client.
	CDANSPAD	Counts the number call attempts that were answered on the CD Mobile (PAD).
	CDANSPCC	Counts the number call attempts that were answered on the MCD PC Client.
	CDCOG	Counts the number call-of-grace terminations that were attempted on a MCD PC Client.
	CDPXYCALL	Counts the number call attempts that were proxied back to the CS2000.
	CDCATTEXP	Counts the number of termination attempts presented to MCD PC Client, where the call attempt timer expired.
	CDDECLINE	Counts the number of declined termination attempts that were presented to MCD PC Client.
	CDIGNORE	Counts the number of ignored termination attempts presented to MCD PC Client.
	CDHLDRT	Counts the number of hold/retrieve attempts managed by the CD3 service.
	CDXFER	Counts the number of call transfers managed by the CD3 service.
	CDCONF	Counts the number of conference calls managed by the CD3 service.
	CDREG	Counts the number of register messages that are sent by the MCD PC Client during Login, updates, and Presence state changes.
Ports OM Group	sampledRtpMpPortUsage	Provides the summing of the in use ports every 100 seconds.
	portUsageSampleCnt	The number of 100 second samples taken during this collection interval contributing to the averaged report.
	connMapEntriesHWM	Highest number of simultaneous ports detected to be in use during this collection interval.
	connMapEntriesLWM	Lowest number of simultaneous ports detected to be in use during this collection interval.

MG 3200 Performance Measurements

Performance Measurements for the MG 3200 are available through the Integrated EMS via SNMP. For more information on MG 3200 PMs, refer to LTRT-72704, *Nortel Media Gateway MG3200 H.248 User's Manual*.

MG 3200 Performance Measurements

OM Group or PM Name	Registers	Description
Network Element: MG 3200		
	Call Processing Performance Management	
	acPerfCpNumDupsForCompletedTransactions	
	acPerfCpNumDupsForOutstandingTransactions	
	acPerfCpMessageSendSuccesses	
	acPerfCpMessageSendErrors	
	acPerfCpMessageReceiveSuccesses	
	acPerfCpMessageReceiveErrors	
	acPerfCpProtocolSyntaxErrors	
	acPerfCpMessageRetransmissions	
	acPerfCpMessageMaxRetransmissionsExceeded	
	acPerfCpMessagesFromUntrustedSources	
	RTP Performance Measurements	
	acPerfRtpSenderPackets	
	acPerfRtpSenderOctets	
	acPerfRtpReceiverPackets	
	acPerfRtpReceiverOctets	
	acPerfRtpRcvrLostPackets	
	acPerfRtpFailedDueToLackOfResources	
	acPerfRtpSimplexInSessionsTotal	
	acPerfRtpSimplexInSessionsCurrent	
	acPerfRtpSimplexOutSessionsTotal	
	acPerfRtpSimplexOutSessionsCurrent	
	acPerfRtpDuplexSessionsTotal	
	acPerfRtpDuplexSessionsCurrent	
	System Performance Measurements	
	acPerfSystemPacketEndpoints	
	acPerfSystemPacketEndpointsInUse	

MG 9000 Performance Measurements

Performance Measurements for the MG 9000 are available through the Integrated EMS. For more information on MG9000 PMs, refer to NN10140-711, *MG 9000 Performance Management* and Appendix B of this document, *MG 9000 MIB OMs/PMs*. That appendix, together with the following table, list the MG 9000 performance measurements.

MG 9000 Performance Measurements

OM Group or PM Name	Registers	Description
Network Element: MG 9000		
Ethernet OMs		
	Number of Alignment Errors	
	Number of FCS Errors	
	Number of Internal MAC Receive Errors	
	Number of Frame Too Longs	
	Number of Internal MAC TX Errors	
	Number of Symbol Errors	
	Number of Inpause Frames	
	Number of Outpause Frames	
	Number of Drop Events	
	Number of Broadcast Packets	
	Number of Multicast Packets	
	Number of CRC Alignment Errors	
	Number of Undersize Packets	
	Number of Oversize Packets	
	Number of Fragments	
	Number of Jabbers	
	Number of Collisions	
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.
MG9K Performance Statistics		
	Errored Seconds	
	Severely Errored Seconds	
	Unavailable Seconds	
	Optical Power Transmit	
	Optical Power Receive	
	Transmit Bias Current	

MG 9000 Performance Measurements

OM Group or PM Name	Registers	Description
	Temperature	
	Voltage	
MG9K GIGE OM Statistics MG9K EM performance strategy where the data is collected in 15 or 5/30 minutes for 96 intervals.		
	Errored Seconds	Counter for Errored Seconds
	Severely Errored Seconds	Counter for Severely Errored Seconds
	Unavailable Seconds	Counter for Unavailable Seconds
	Optical Power Transmit	Optical Power Transmit
	Optical Power Receive	Counter for Optical Power Receive
	Transmit Bias Current	Counter for Transmit Bias Current
	Temperature	Counter for Temperature
RMON Performance Measurements		
	Drop Events	The current data associated with etherStatsDropEvents.
	Broadcast Packets	The counter data associated with etherStatsBroadcastPkts.
	Multicast Packets	The counter associated with etherStatsMulticastPkts.
	CRC Alignment Errors	The counter associated with etherStatsCRCAlignErrors.
	Undersize Packets	The counter associated with etherStatsUndersizePkts.
	Oversize Packets	The counter associated with etherStatsOversizePkts.
	Fragments	The counter associated with etherStatsFragments.
	Jabbers	The counter associated with etherStatsJabbers.
	Collisions	The counter associated with etherStatsCollisions.
RMON HC Performance Measurements		
	HC overflow packets	The counter associated with HC Overflow Packets.
	Packets received	The counter associated with number of packets received.
	Overflow octets	The counter associated with HC number of Overflow octets.
	Octets of data received	The counter associated with number of octets of data received.
	Total HC Octets	The counter associated with Total Number of HC Octets.
	Total non unicast packets	The counter associated with Total number of non unicast packets.
	Total non unicast HC octets	The counter associated with Total number of non unicast HC octets.
	Total non unicast octets	The counter associated with Total number of non unicast octets.
	Total non unicast over flow octets	The counter associated with Total number of non unicast over flow octets.

MG 9000 Performance Measurements

OM Group or PM Name	Registers	Description
SMON MIB table	Total non unicast HC octets	The counter associated with Total number of non unicast HC octets.
	smonVlanIdStatsTotalPkts	Total incoming packets.
	smonVlanIdStatsTotalHCPkts	Total outgoing packets.
	smonVlanIdStatsTotalOctets	Total incoming octets.
	smonVlanIdStatsTotalHCOctets	Total outgoing octets.
SMON Performance Measurements		
	VLAN ID	The VLAN ID.
	Total Packets	The counter associated with Total number Packets.
	Total HC Packets	The counter associated with Total Number of HC Packets.
	Create time	The Create time.
	Total Octets	The counter associated with Total Number of Octets.
	Total HC octets	Displays the total number of HC octets.
	Total overflow packets	Displays the total number of overflow packets.
	Total overflow octets	Displays the total number of overflow octets.
	Total non unicast packets	The counter associated with Total number of non unicast packets.
	Total non unicast HC octets	The counter associated with Total number of non unicast HC octets.
	Total non unicast octets	The counter associated with Total number of non unicast octets.
	Total non unicast over flow octets	The counter associated with Total number of non unicast over flow octets.
	Total non unicast HC octets	The counter associated with Total number of non unicast HC octets.
SMON Performance		
	smonVlanIdStatsTotalPkts - total incoming packets	
	smonVlanIdStatsTotalHCPkts - total outgoing packets	
	smonVlanIdStatsTotalOctets - total incoming octets	
	smonVlanIdStatsTotalHCOctets - total outgoing octets	

Media Gateway 15000 OMs/PMs and Passport 15000/Multiservice Switch OMs/PMs

Note: Starting in SN08, the terms Packet Voice Gateway (PVG) and Passport 15000 were 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, *MSS 15000, MG 15000 & MDM Performance*.

Starting in SN08, the 5- and 30-minute performance measurements (PMs) provided 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, 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 Multiservice Data Manager (MDM) servers.

On Nortel Networks 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 MDM servers transfer the NTM data directly to the OSS applications, or to the CS2000 Core Manager running on the SDM, depending on the network configuration.

Accessing files through the SDM or MDM

Note: Access via SDM is not generally available for Media Gateway 15000 (previously PVG) performance measurements.

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 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

For information on performance measurements (PMs) available for the Media Gateway 15000 (previously PVG) network element, refer to NN10158-711, *MSS 15000, MG 15000 & MDM Performance*.

MS 2000 Series Node OMs/PMs

Refer to NN10320-100, *ATM Solutions Basics*, and NN10300-100, *IP Solutions Basics*.

Session Server Manager OMs/PMs

Refer to NN10342-711, *Session Server Manager Performance Management*.

SAM21 OMs/PMs

The SAM21 EM has no operational or performance measurements.

STORM OMs/PMs

Refer to NN10054-711, *STORM Performance Management*.

UAS OMs/PMs

The following table lists the operational measurements (OMs) and performance measurements (PMs) available for the UAS network element. UAS supports CSV and XML format. For details, refer to NN10139-001, *UAS Performance*.

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
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.

OM group or PM name	Description
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.
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.

OM group or PM name	Description
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

See Appendix D

Refer to Appendix D for a complete list of the operational measurements (OMs) and performance measurements (PMs) available for the USP network element. You may also refer to NN10137-711, *USP Performance Management* and NN1038-711, *USP-Compact Performance Management*.

USP supports SSV format. For details on this format, refer to the Performance section of the FCAPS documentation on USP, NN10137-711.

Appendix A: Ethernet Routing Switch 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 SM 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
ifIndex	RFC1213-MIB	A list of the following PM ID labels contained in this table.	Every 5 and 30 mins
ifDescr	RFC1213-MIB	DisplayString. A textual string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the hardware interface."	Every 5 and 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			
etherStatusDataSource	RFC1271-MIB	A list of the following PM ID labels contained in this table.	Every 30 mins
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
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

<u>Performance Metric Identifier</u>	<u>MIB Name</u>	<u>Description</u>	<u>Default Succession</u>
			<u>IEMS Collection Interval</u>
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
etherHistoryIndex	RFC1271-MIB	A list of the following PM ID labels contained in this table.	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
historyControlDataSource	RFC1271-MIB	This object identifies the source of the data for which historical data was collected and placed in a media-specific table on behalf of this historyControlEntry. This source can be any interface on this device. In order to identify a particular interface, this object shall identify the instance of the ifIndex object, defined in [4,6], for the desired interface.	Every 30 mins
OSPF-MIB			
ospfIfIpAddress	OSPF-MIB	A list of the following PM ID labels contained in this table.	Every 30 mins
ospfAddressLessIf	OSPF-MIB	Integer32. For the purpose of easing the instancing of addressed and addressless interfaces; This variable takes the value 0 on interfaces with IP Addresses, and the corresponding value of ifIndex for interfaces having no IP Address.	Every 30 mins
ospfIfEvents	OSPF-MIB	The number of times this OSPF interface has changed its state, or an error has occurred.	Every 30 mins
OSPF-MIB			
ospfNbrAddressLessIndex	OSPF-MIB	A list of the following PM ID labels.	Every 30 mins
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			
snmpInvalidMsgs	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			
snmpInPkts	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
snmpInBadVersions	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
snmpInBadCommunityUses	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
snmpInASNParseErrs	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
snmpInTotalReqVars	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

<u>Performance Metric Identifier</u>	<u>MIB Name</u>	<u>Description</u>	<u>Default Succession IEMS Collection Interval</u>
snmpInTotalSetVars	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			
vrrpStatusIfIndex	VRRP-MIB	INTEGER. A list of the following PM ID labels contained in this table.	Every 30 mins
vrrpStatsVrId	VRRP-MIB	Integer32 (1..255). This object contains the Virtual Router Identifier (VRID).	Every 30 mins
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 (rcStat)			
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
rcStatPortIndex	RAPID-CITY	Integer32. A list of the following PM ID labels contained in this table.	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 bridging 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
rcStatGigPortIndex	RAPID-CITY	Integer32. A list of the following PM ID labels contained in this table.	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
RAPID-CITY (rc2kAtm)			
rc2kAtmPortStatsIndex	RAPID-CITY	Integer32. A list of the following PM ID labels contained in this table.	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
rc2kAtmVportStatsIfIndex	RAPID-CITY	Integer32. A list of the following PM ID labels contained in this table. Port number.	Every 5 and 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
rcStgPort	RAPID-CITY	Integer32. The port number of the port for which this entry contains Spanning Tree Protocol management information	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 SN09

Appendix B: MG 9000 MIB OMs/PMs

OM Name	Type	Description
norCarrSonetMedCurrentOpt	Unsigned32	Optical Power Transmitted. This is interpreted as a Percentage
norCarrSonetMedIntervalLBC	Unsigned32	Laser Bias Current.
nnMegacoOMDSPIntervalTable		
nnMegacoOMDSPnumToneRcvrReq	Unsigned32	The number of tone receiver requests during this interval.
nnMegacoOMDSPnumToneRcvrReqFail	Unsigned32	The number of tone receiver requests that failed during this interval.
nnMegacoOMDSPnumToneGenReq	Unsigned32	The number of tone generator requests during this interval.
nnMegacoOMDSPnumToneGenReqFail	Unsigned32	The number of tone generator requests that failed during this interval.
nnMegacoOMDSPnumCMRmodemReq	Unsigned32	The number of CMR modem requests during this interval.
nnMegacoOMDSPnumCMRmodemReqFail	Unsigned32	The number of CMR modem requests that failed during this interval.
nnMegacoOMDSPCurrentDayTotalTable		
nnMegacoOMCESnumChnlAllocIntra	Unsigned32	The total number of channel allocation requests for intra-switched calls during this interval.
nnMegacoOMCESnumChnlAllocIntraFail	Unsigned32	The total number of channel allocation requests for intra-switched calls that failed during this interval.
nnMegacoOMCESnumChnlAllocInter	Unsigned32	The total number of channel allocation requests for inter-switched calls during this interval.
nnMegacoOMCESnumChnlAllocInterFail	Unsigned32	The total number of channel allocation requests for inter-switched calls that failed during this interval.
nnMegacoOMECANIntervalTable		
nnMegacoOMECANnumResrceReq	Unsigned32	The total number of ECAN resource request attempts during this interval.
nnMegacoOMECANnumResrceReqFail	Unsigned32	The total number of ECAN resource request attempts that failed during this interval.
nnMegacoQoSIntervalTable		
nnMegacoQoSIntervalCalls	Unsigned32	total number of calls (in this 15-min interval)."
nnMegacoQoSIntervalBadCalls	Unsigned32	total number of bad calls (in this 15-min interval)."
nnMegacoQoSIntervalPktsSent	Unsigned32	number of packets sent (in this 15-min interval)."
nnMegacoQoSIntervalPktsLost	Unsigned32	number of packets lost (in this 15-min interval)."
nnMegacoQoSIntervalPktLossPct	Interger	% of packets lost (in this 15-min interval)."
nnMegacoQoSIntervalJitter	Unsigned32	average jitter (in a 15-min interval)."
nnMegacoQoSIntervalLatency	Unsigned32	average latency (in a 15-min interval)."
nnMegacoOMMedGwyIntervalTable		
nnMegacoOMMedGwyNumInMessages	Unsigned32	Number of messages received from the Gateway Controller (GWC) during this interval.
nnMegacoOMMedGwyNumInOctets	Unsigned32	Number of octets received from the Gateway Controller (GWC) during this interval.
nnMegacoOMMedGwyAvrgInMsgRate	Unsigned32	Average message rate (per minute) for messages received from the GWC during this interval.
nnMegacoOMMedGwyMaxInMsgRate	Unsigned32	Maximum message rate (per minute) for messages received from the GWC during this interval.
nnMegacoOMMedGwyNumOutMessages	Unsigned32	Number of messages sent to the Gateway Controller (GWC) during this interval.
nnMegacoOMMedGwyNumOutOctets	Unsigned32	Number of octets sent to the Gateway Controller (GWC) during this interval.
nnMegacoOMMedGwyAvrgOutMsgRate	Unsigned32	Average message rate (per minute) for messages sent to the GWC during this interval.
nnMegacoOMMedGwyMaxOutMsgRate	Unsigned32	Maximum message rate (per minute) for messages sent to the GWC during this interval.
NORTEL-UEMG-BANDWIDTH-MIB		
nnBwShelfCurrentSloaBandwResrvdTable		

nnBwShelfCapacitySloaBandwReserved	NnBwCellsPerSec	Current amount of reserved bandwidth Capacity for the aggregate of all Switched Lines over ATM VCs on This UEMG shelf.
nnBwShelfIntervalSloaBandwResrvdTable		
nnBwShelfIntervalSloaBandwReserved	NnBwCellsPerSec	ith 15-minute measure amount of reserved band width allocated for the aggregate of all Switched Lines over ATM VCs on This UEMG shelf."
nnBwIntervalBandwUtilTable		
nnBwBandwUtilIntervalInCellRate	NnBwCellsPerSec	The ith 15min measure of the inbound bandwidth utilization.
nnBwBandwUtilIntervalOutCellRate	NnBwCellsPerSec	The ith 15min measure of the outbound bandwidth utilization.
nnBwBandwUtilIntervalInDslCellRate	NnBwCellsPerSec	The ith 15min measure of the inbound dsl band width utilization.
nnBwBandwUtilIntervalOutDslCellRate	NnBwCellsPerSec	The ith 15min measure of the outbound dsl band width utilization.
nnBwIntervalQueueFillTable		
nnBwQueueFillIntervalTotal	NnBwPercent	ith 15-minute value % fill of the entire input cell queue associated with the central switching fabric.
nnBwQueueFillIntervalCbr	NnBwPercent	ith 15-minute value % fill of the entire input queue associated with the aggregate of all CBR VCs.
nnBwQueueFillIntervalRtVbr	NnBwPercent	ith 15-minute value % fill of the entire input queue associated with the aggregate of all rt-VBR VCs.
nnBwQueueFillIntervalNrtVbr	NnBwPercent	ith 15-minute value % fill of the entire input queue associated with the aggregate of all nrt-VBR VCs.
nnBwQueueFillIntervalUbr	NnBwPercent	ith 15-minute value % fill of the entire input queue associated with the aggregate of all UBR VCs.
nnBwQueueFillIntervalUbrPlus	NnBwPercent	ith 15-minute value % fill of the entire input queue associated with the aggregate of all UBR+ VCs.
nnBwQueueFillIntervalControl	NnBwPercent	ith 15-minute value % fill of the entire input queue associated with the aggregate of all Control VCs.
nnBwAbiCurrentBandwResrvdTable		
nnBwAbiCapacityBandwReserved	NnBwCellsPerSec	Current amount of reserved bandwidth Capacity for the aggregate of all ABI VCs on this ABI interface.
nnBwAbiIntervalBandwResrvdEntry		
nnBwAbiIntervalBandwReserved	NnBwCellsPerSec	ith 15-minute measure amount of reserved bandwidth allocated for the aggregate of all VCs on this ABI interface."
SNMP-MPD-MIB		
SNMP Table		
snmplInvalidMsgs	Counter32	The total number of packets received by the SNMP engine which were dropped because there were invalid or inconsistent components in the SNMP message.
SNMPv2-MIB		
snmplnBadCommunityNames	Counter32	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.
snmplnPks	Counter32	The total number of messages delivered to the SNMP entity from the transport service.
NORTEL-UEMG-CLKSYNC-MIB		
NnClkSyncRefTable		
		This table provides status information for each of the sync reference inputs associated with the ITP card. There are six references per ITP card, two ITP cards on each shelf.
nnClkSyncRefId	integer	Reference Identification... Identifies the six possible clock synchronization references on the ITP card. This field along with entPhysicalIndex defines a unique row in the nnClkSyncRefTable. 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 "
nnClkSyncRefLossOfSignalCount	Unsigned32	Contains the count of the number of onsets of timing reference signal loss. Range is from 0 - 255
nnClkSyncRefLossOfFrameCount	Unsigned32	Contains the count of the number of loss of frames. Range is from 0 - 255.
NnClkSyncSignalTable		This table provides status information on each of the six timing signals coming into the UE9KMG host shelf. There is one entry for each network timing signal (total of two), and one entry for each BITS signal (total of 4)
nnClkSyncSignalId	interger	Signal Identification... Identifies the six possible timing source signals which eventually are seen as references into the ITP card. This field defines a unique row in the nnClkSyncSignalTable. bitsA-0 (1), -- BITS A signal coming into the left ITX of -- 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"
nnClkSyncSignalLossOfFrameCount	Unsigned32	Contains the count of the number of loss of frames.
nnClkSyncSibnalLossOfSignalCount	Unsigned32	Contains the count of the number of onsets of timing source signal loss.
SONET-MIB		
sonetSectionIntervalTable		
sonetSectionIntervalESSs	PerfIntervalCount	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.
sonetSectionIntervalSESSs	PerfIntervalCount	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.
sonetSectionIntervalSEFSs	PerfIntervalCount	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.
sonetSectionIntervalCVs	PerfIntervalCount	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.
sonetLineIntervalTable		
sonetLineIntervalESSs	PerfIntervalCount	The counter associated with the number of Errored Seconds encountered by a SONET/SDH Line in a particular 15-minute interval in the past 24 hours.
sonetLineIntervalSESSs	PerfIntervalCount	The counter associated with the number of Severely Errored Seconds encountered by a SONET/SDH Line in a particular 15-minute interval in the past 24 hours.
sonetLineIntervalCVs	PerfIntervalCount	The counter associated with the number of Coding Violations encountered by a SONET/SDH Line in a particular 15-minute interval in the past 24 hours.
sonetLineIntervalUASs	PerfIntervalCount	The counter associated with the number of Unavailable Seconds encountered by a SONET/SDH Line in a particular 15-minute interval in the past 24 hours.
sonetPathIntervalTable		
sonetPathIntervalESSs	PerfIntervalCount	The counter associated with the number of Errored Seconds encountered by a SONET/SDH Path in a particular 15-minute interval in the past 24 hours.
sonetPathIntervalSESSs	PerfIntervalCount	The counter associated with the number of Severely Errored Seconds encountered by a SONET/SDH Path in a particular 15-minute interval in the past 24 hours.

sonetPathIntervalCVs	PerfIntervalCount	The counter associated with the number of Coding Violations encountered by a SONET/SDH Path in a particular 15-minute interval in the past 24 hours.
sonetPathIntervalUASs	PerfIntervalCount	The counter associated with the number of Unavailable Seconds encountered by a Path in a particular 15-minute interval in the past 24 hours.
APS-MIB		
apsChanStatusTable		
apsChanSignalDegrades	Counter32	A count of Signal Degrade conditions. This condition occurs when the line Bit Error Rate exceeds the currently configured threshold.
apsChanSignalFailures	Counter32	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.
apsChanSwitchovers	Counter32	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.
IMA-MIB (new in SN05)		
imaGroupIntervalTable		
imaGroupIntervalUnavailSecs	Gauge32	Count of one second intervals where the IMA Group Traffic State Machine is Down in one of the previous 96, individual 15 minute, intervals
imaGroupIntervalNeNumFailures	Gauge32	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
imaLinkIntervalTable		
imaLinkIntervalImaViolations	Gauge32	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
imaLinkIntervalOifAnomalies	Gauge32	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
imaLinkIntervalNeSevErroredSecs	Gauge32	Count of one second intervals containing $\geq 30\%$ of the ICP cells counted as IV-IMAs, or one or more link defects (e. g., LOS, OOF/ LOF, AIS, or LCD), LIF defects, or LODS defects, except during UAS-IMA condition, in one of the previous 96, individual 15 minute, intervals
imaLinkIntervalNeUnavailSecs	Gauge32	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
imaLinkIntervalNeTxUnusableSecs	Gauge32	Tx Unusable seconds: count of Unusable seconds at the near-end Tx LSM in one of the previous 96, individual 15 minute, intervals
imaLinkIntervalNeRxUnusableSecs	Gauge32	Rx Unusable seconds: count of Unusable seconds at the near-end Rx LSM in one of the previous 96, individual 15 minute, intervals
imaLinkIntervalNeTxNumFailures	Gauge32	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
imaLinkIntervalNeRxNumFailures	Gauge32	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
imaLinkIntervalTxStuffs	Gauge32	Count of stuff events inserted in the transmit direction in one of the previous 96, individual 15 minute, intervals. This is an optional attribute
imaLinkIntervalRxStuffs	Gauge32	Count of stuff events detected in the receive direction in one of the previous 96, individual 15 minute, intervals. This is an optional attribute

UEMG-PERFMON-MIB		
nnPmUtilOmlntervTable		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	Peak CPU Occupancy (as a percentage of usage)
nnPmUtilIntervCpuAvg	Integer	Average CPU Occupancy (as a percentage of usage)
nnPmUtilIntervRamPeak	Integer	Peak RAM Usage (as a percentage of usage)
nnPmUtilIntervRamAvg	Integer	Average RAM Usage (as a percentage of usage)
nnPmUtilIntervFlashPeak	Integer	Peak Flash Memory Usage (as a percentage of usage)
nnPmUtilIntervFlashAvg	Integer	Average Flash Memory Usage (as a percentage of usage)
nnPmUtilIntervChanPeak	Integer	Peak Channel Usage (as a percentage of usage)
nnPmUtilIntervChanAvg	Integer	Average Channel Usage (as a percentage of usage)
nnPmSnmpOmlntervTable		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.
nnPmSnmpIntervReqPeak	Interger32	The Peak number of SNMP Requests/PDUs in the most Recent 15 mins. These are accumulated on 1-minute cycles.
nnPmSnmpIntervReqAvg	Interger32	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
nnPmSnmpIntervNotifPeak	Interger32	The Peak number of SNMP Notifications in the most Recent 15 mins. These are accumulated on 1-minute cycles.
nnPmSnmpIntervNotifAvg	Interger32	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 cycles. Precision is tenths, thus 816 is 81.6
nnPmOvldRscIntervTable		
nnPmOvldRscIntervPduRatePeak	Interger32	Peak # received AAI5 PDUs per sec for this 15 minute interval
nnPmOvldRscIntervPduRateAvg	Interger32	Avg num recvd AAL5 PDUs per sec for this 15 minute interval
nnPmOvldRscIntervCbvMsgRPeak	NnPerfMonHundredths	Peak recvd conn request msgs per sec for this 15 minute interval
nnPmOvldRscIntervCbvMsgRAvg	NnPerfMonHundredths	Avg conn request msgs per sec for this 15 minute interval
nnPmOvldRscIntervConQDelPeak	NnPerfMonHundredths	Milliseconds...peak time a connRequest is pending in its queue for this 15 minute interval
nnPmOvldRscIntervConQDelAvg	NnPerfMonHundredths	Milliseconds...Avg time a connRequest is pending in its queue for this 15 minute interval
nnPmOvldRscIntervCpuUtilPeak	NnPerfMonPercent	Peak cpu occupancy for this 15 minute interval
nnPmOvldRscIntervCpuUtilAvg	NnPerfMonPercent	Avg cpu occupancy this 15 minute interval
nnPmOvldConnDenyIntervTable		
nnPmOvldConnDenyIntervCount	Interger32	Count of the number of Connection requests Denied for this 15 minute interval
NORTEL-UEMG-RELMSGING-MIB		
nnRelMsgSctpAssocOmCurrTable		
nnRelMsgSctpAscCurrClosed	Unsigned32	number of times that this association closed (both aborts and shutdowns)
nnRelMsgSctpAscCurrAbort	Unsigned32	number of times that this association aborted.
nnRelMsgSctpAssocOmlntervTable		
nnRelMsgSctpAscIntervClosed	Unsigned32	number of times that this association closed (both aborts and shutdowns)
nnRelMsgSctpAscIntervAbort	Unsigned32	number of times that this association aborted.
nnRelMsgSctpAscIntervOutPacks	Unsigned32	number of packets transmitted
nnRelMsgSctpAscIntervInPacks	Unsigned32	number of packets received, this association
nnRelMsgSctpAscIntervDiscPacks	Unsigned32	number of packets discarded by this association.
nnRelMsgSctpAscIntervRetranPacks	Unsigned32	number of packets retransmitted by this association, this interval
nnRelMsgSctpAscIntervT1expires	Unsigned32	number of T1 Expires
nnRelMsgSctpAscIntervT2expires	Unsigned32	number of T2 expires.
nnRelMsgSctpAscIntervT3expires	Unsigned32	number of T3 expires
nnRelMsgSctpAscIntervCongCount	Unsigned32	number of times this assoc entered congestion.

nnRelMsgSctpAscIntervCongCleared	Unsigned32	number of times congestion cleared by audit.
NORTEL-UEMG-GIGE_mib		
nnGLinkOmIntervTable		
nnGLinkIntervESs	Unsigned32	history, nth interval Errored Seconds
nnGLinkIntervSESSs	Unsigned32	history, nth interval Severely Errored Seconds
nnGLinkIntervUASs	Unsigned32	history, nth interval Unavailable Seconds
nnGLinkIntervOPT	Unsigned32	history, nth interval Optical Transmit Current
nnGLinkIntervOPR	Unsigned32	history, nth interval Optical Power Receive
nnGLinkIntervTBC	Unsigned32	history, nth interval Transmit Bus Current
nnGLinkIntervVCC	Unsigned32	history, nth interval Voltage
nnGLinkIntervTEMP	Unsigned32	history, nth interval Temperature
nnGLinkIntervTxFifoOverruns	Counter64	history, nth interval Transmit Fifo Overruns
nnGLinkIntervTxFifoUnderruns	Counter64	history, nth interval Transmit Fifo Underruns
nnGLinkIntervTxBytesOverflow	Unsigned32	history, nth interval Transmit Bytes, Overflow
nnGLinkIntervTxBytes	Counter64	history, nth interval Transmit Bytes
nnGLinkIntervRxFcsFail	Counter64	history, nth interval Receive Fcs Failures
nnGLinkIntervRxLenTypeFail	Counter64	history, nth interval Receive LEN Type Failures
nnGLinkIntervRxGoodPause	Counter64	history, nth interval Receive Good Pause
nnGLinkIntervRxBadOpCntlFrames	Counter64	history, nth interval Receive Bad Opcode Control Frames
nnGLinkIntervRxControlFrames	Counter64	history, nth interval Receive Control Frames
Remote Network Monitoring MIB		
etherHistoryTable		
etherHistoryDropEvents	Counter32	The total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. Note that this numbe is not necessarily the number of packets dropped, it is just the number of times this condition has been detected.
etherHistoryBroadcastPkts	Counter32	The number of good packets received during this sampling interval that were directed to the broadcast address.
etherHistoryMulticastPkts	Counter32	The number of good packets received during this sampling interval that were directed to a multicast address. Note that this number does not include packets addressed to the broadcast address.
etherHistoryCRCAAlignErrors	Counter32	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 had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherHistoryUndersizePkts	Counter32	The number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
etherHistoryOversizePkts	Counter32	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.
etherHistoryFragments	Counter32	The total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error)
etherHistoryJabbers	Counter32	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error)
etherHistoryCollisions	Counter32	The best estimate of the total number of collisions on this Ethernet segment during this sampling interval.
etherHistoryUtilization	Counter32	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
HC-RMON-MIB		
etherHistoryHighCapacityTable		

etherHistoryHighCapacityOverflowPkts	Gauge32	The number of times the associated etherHistoryPkts Gauge overflowed during this sampling interval.
etherHistoryHighCapacityPkts	CounterBasedGauge64	The total number of packets (including bad packets, broadcast packets, and multicast packets) received during this sampling interval.
etherHistoryHighCapacityOverflowOctets	Gauge32	The number of times the associated etherHistoryOctets counter has overflowed during this sampling interval.
etherHistoryHighCapacityOctets	CounterBasedGauge64	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets) during this sampling interval.
NORTEL-UEMG-IPSEC-MIB		
nnIpsecOmIntervalTable		
nnIpsecOmIntervalPacketsTx	Integer32	Number of Transmitted Packets this 15min interval
nnIpsecOmIntervalPacketsRx	Integer32	Number of Received Packets this 15min interval
nnIpsecOmIntervalPacketsDiscardedOut	Integer32	Number of Dropped Outbound Packets this 15min interval
nnIpsecOmIntervalPacketsDiscardedIn	Integer32	Number of Dropped Inbound Packets this 15min interval

Appendix C: VoA/IP MSS15000, MG15000, and MDM Alarm Log Summary

1. Introduction

This document provides a list of Multiservice Switch 15000 (MSS15000), Media Gateway 15000 (MG15000) (formerly known as PVG) and Multiservice Data Manager (MDM) alarm logs applicable to up to Succession SN08 for Voice over ATM (VOA) and Voice over IP (VOIP) solutions.

The purpose of this document includes:

- It provides a Carrier VOIP customer (and more specifically an OSS Fault application writer) a summarized subset of the possible alarms that can appear when MSS15000/MG15000 and MDM are configured for the Carrier VOIP application. The descriptions of the alarms are found in [3] and [1].
- When configured to receive MSS15000/MG15000/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.

2. SCC2 Log Format

The SCC2 log report for MSS15000, MG15000, 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:

```
aabbccdddeeffgghhijjj
```

Each field, as applicable for MSS15000/MG15000 and MDM alarms, is described in Table 1.

Table 1 MSS15000/MG15000 and MDM SCC2 Header Field Description

Field	Description	Applicable Log Values
aa	Alarm severity MSS15000/MG15000/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 MSS15000/MG15000 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 MSS15000/MG15000 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 MSS15000/MG15000 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 MSS15000/MG15000 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 MSS15000/MG15000 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.

3. MSS15000/MG15000 Alarm Logs

Table 2 presents the list of MSS15000 and MG15000 set/clear alarm logs that are applicable for Carrier VOIP.

Table 2 does not explicitly state all MSS15000/MG15000 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 MSS15000/MG15000 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 [1] and [3] for further information.

Table 2 MSS15000 Set/Clear Alarms Supported for Succession

MSS15000 Index Group	Component Name	MSS15000/MG15000 configuration (N/A)	MSS15000 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 MSS15000 components.		0000		bb CA eee gghh TBL where: eee = 302, 303, 306
	This alarm can apply to many MSS15000 components.		1000		aabb CA eee gghh TBL where: aa = “*C”, “**”, “* ” eee = 300, 306
	This alarm can apply to many MSS15000 components.		1001		aabb CA 303 gghh TBL where: aa = “*C”, “**”, “* ”
	This alarm can apply to many MSS15000 components.		3000		aabb CA eee gghh TBL where: aa = “*C”, “**”, “* ” eee = 300, 302
	This alarm can apply to many MSS15000 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. Card instance range (<n>): 0-15 LP instance range (<m>): 0-15				

MSS15000 Index Group	Component Name	MSS15000/MG 15000 configuration (N/A)	MSS15000 Subindex	Importance Category (N/A)	SCC2 Header
	Prov		0007		aabb PPEM306 gghh TBL where: aa = “*C”, “**”, “*”
	This alarm can apply to many MSS15000 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 or *Cbb PPEM306 gghh TBL
	Prov CriticalAttributeActivation		0042		* bb PPEM306 gghh TBL for warning/clear or *Cbb PPEM306 gghh TBL for set/clear
	Prov ActivationMode		0043		* bb PPEM306 gghh TBL
	Shelf Card/<x> Lp/<m>		0044		*Cbb PPEM302 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		*Cbb PPEM304 gghh TBL
	Shelf FabricCard/<i>		0004		*Cbb PPEM304 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

MSS15000 Index Group	Component Name	MSS15000/MG 15000 configuration (N/A)	MSS15000 Subindex	Importance Category (N/A)	SCC2 Header
	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
7006	Radius security alarms.				
	Ac Radius		0100		*Cbb PPEM305 gghh TBL
7008	File system alarms. Disk instance range (<n>): 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

MSS15000 Index Group	Component Name	MSS15000/MG 15000 configuration (N/A)	MSS15000 Subindex	Importance Category (N/A)	SCC2 Header
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-n, where n is 1 less than the number of ports Sts instance range (<n2>): 0-11 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
	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/0 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/0 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

MSS15000 Index Group	Component Name	MSS15000/MG 15000 configuration (N/A)	MSS15000 Subindex	Importance Category (N/A)	SCC2 Header
	LP/0 EDS1/<n2> Lp/<n> Sdh/0 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/0 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
	LP/0 EDS1/<n2>		5050		aabb PPEM303 gghh TBL where: aa = “*C”, “* “
	LP/<n> DS3/<n2>		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

MSS15000 Index Group	Component Name	MSS15000/MG 15000 configuration (N/A)	MSS15000 SubIndex	Importance Category (N/A)	SCC2 Header
			5120		TBL
			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
	LP/<n> Sonet/<n2> Sts/0 Lp/<n> Sdh/<n2> Vc4/0 LAPS/<n> Sts/0 LAPS/<n> Vc4/0 Pbg/<n> Sts/0		5254		*Cbb PPEM300 gghh TBL
Lp/<n> Sonet/<n2> Path/<n2> Lp/<n> Sonet/<n2> Sts/<n2> Lp/<n> Sonet/<n2> Vc4/<n2> Lp/<n> Sdh/<n2> Path/0 Lp/<n> Sdh/<n2> Sts/0 Lp/<n> Sdh/<n2> Vc4/0 LAPS/<n> Path/0 LAPS/<n> Sts/0 LAPS/<n> Vc4/0 Pbg/<n> Sts/0		5255		*Cbb PPEM300 gghh TBL	

MSS15000 Index Group	Component Name	MSS15000/MG 15000 configuration (N/A)	MSS15000 Subindex	Importance Category (N/A)	SCC2 Header
	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
	LAPS/<n> CrossConnect		5281		*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		*Cbb PPEM303 gghh TBL
			5291		
			5292		
			5293		
			5294		
	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		*Cbb PPEM303 gghh TBL
			5296		

MSS15000 Index Group	Component Name	MSS15000/MG 15000 configuration (N/A)	MSS15000 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}		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		*Cbb PPEM300 gghh TBL
	LP/<n> DS3/<n2>		5601		* bb PPEM300 gghh TBL
			5602		
	LP/<n> DS3/<n2>		5603		**bb PPEM300 gghh TBL
			5604		
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 = “*C”, “**”	
Shelf Shelf FabricCard/<i>		0052		aabb PPEM303 gghh TBL	
Shelf		0053		**bb PPEM303 gghh TBL where: aa = “*C”, “**”, “* “	
Shelf		0055		aabb PPEM303 gghh TBL where: aa = “**”, “* ”	

MSS15000 Index Group	Component Name	MSS15000/MG 15000 configuration (N/A)	MSS15000 Subindex	Importance Category (N/A)	SCC2 Header
	Shelf		0056		* bb PPEM303 gghh TBL
	Shelf		0057		**bb PPEM303 gghh TBL
			0058		
	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
			0104		
	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		
			0011		
	LP/<n>		0021		**bb PPEM301 gghh TBL
	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 TBL
			0002		
	Time Server/<n>		0010		* bb PPEM300 gghh TBL
			0011		
	Time Server/<n>		0012		* bb PPEM300 gghh TBL
7017	Network clock synchronization alarms				

MSS15000 Index Group	Component Name	MSS15000/MG 15000 configuration (N/A)	MSS15000 Subindex	Importance Category (N/A)	SCC2 Header
	NS		1000		*Cbb 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 Protocol Port Id (<ppld>) VirtualIfEntry identifier (<virtIfId>)				
	Vr/<i> Ip Cache/<n>		0006		**bb PPEM302 gghh TBL
	Vr/<i> Ip Cpp IsolatedDa/<ipaddress>, <lpnum>		0013		* bb PPEM305 gghh TBL
	Rtr/<i> Cpp IsolatedDa/<ipaddress>, <lpnum>		0014		**bb PPEM305 gghh TBL
	Rtr/<i> Vrf/<y> Cpp IsolatedDa/<ipaddress>, <lpnum>				
	Vr/<i> Pp/<ppld> IpPort logicalIf/<ipaddress>		1002		**bb PPEM305 gghh TBL
	OspfIf				
	Rtr/<i> Interface/<ipaddress>				
	OspfIf				
	Vr/<i> Ip Ospf		1003		**bb PPEM305 gghh TBL
	VirtIfEntry/<virtIfId>				
	VR/<i> Ip OSPF		1017		* 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

MSS15000 Index Group	Component Name	MSS15000/MG 15000 configuration (N/A)	MSS15000 Subindex	Importance Category (N/A)	SCC2 Header
	Atmif/<n>, Atmif/<n> Ca Cbr/0, Atmif/<n> Ca rtVbr/0, Atmif/<n> Ca nrtVbr/0, Atmif/<n> Ca Ubr/0		1001		* bb PPEM301 gghh TBL
			1002		
			1003		
			1004		
	Atmif/<n> Vcc/<n2.n3>		2000		**bb PPEM302 gghh TBL
			2003		
	Atmif/<n> Vpt/<n2>		3000		* bb PPEM300 gghh TBL
7041	Atmif/<n>		4001		**bb PPEM300 gghh TBL
	Atmif/<n>		5000		*Cbb PPEM300 gghh TBL
	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 Ilmi		0052		*Cbb PPEM300 gghh TBL
	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		* bb PPEM302 gghh TBL
			0601		
	Artg Pnni CfgNode /<n>		0700		**bb PPEM300 gghh TBL
	Atmif/<n> Pnni Rcc		0701		**bb PPEM300 gghh TBL

MSS15000 Index Group	Component Name	MSS15000/MG15000 configuration (N/A)	MSS15000 SubIndex	Importance Category (N/A)	SCC2 Header
	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		**bb PPEM303 gghh TBL
			0101		
			0102		
			0103		
			0104		
			0105		
7056	Voice Services Processor (VSP) / Narrowband Service Trunk over ATM (Nsta) This group is specific to MG15000 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 Security policy database name (<spd_name>): string				
	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

MSS15000 Index Group	Component Name	MSS15000/MG 15000 configuration (N/A)	MSS15000 Subindex	Importance Category (N/A)	SCC2 Header
	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				
	Nsta/<i> Vgs Control/<n> MediaGataway Aap Nsta/<i> Vgs Control/<n> Signalingateway 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
	Nsta/<x> Vgs Ctrl/<n> Spd/<spd_name> IkePolicy/1		1219		** bb PPEM300 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
7082	Routine Exercise alarms.				
	Rex		0001		* bb PPEM302 gghh TBL

MSS15000 Index Group	Component Name	MSS15000/MG 15000 configuration (N/A)	MSS15000 Subindex	Importance Category (N/A)	SCC2 Header
	Rex		0002		* bb PPEM306 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 MSS15000 Message Alarms Supported for Succession VOA/VOIP

MSS15000 Index Group	Component Name	Solution Notes	MSS15000 Subindex	Importance Category	SCC2 Header
0000	OSI administrative state changes, general engineering and memory alarms, etc.				
	These alarms can apply to many MSS15000 components. Often, it is: EM/<nodename>		9000		* bb CA eee gghh
			9001		TBL
			9002		where:
			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

MSS15000 Index Group	Component Name	Solution Notes	MSS15000 Subindex	Importance Category	SCC2 Header
	Prov		0032		* bb PPEM30? gghh TBL
	This alarm can apply to many MSS15000 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
	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/log Spooler		0008		* bb PPEM306 gghh TBL
7006	Network Management Interface system alarms and Radius security 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) Radius Server instance range (<m>): 0-1				
	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
	Ac		0009		* bb PPEM300 gghh TBL or * bb PPEM305 gghh TBL
	Ac Radius Server/<m>		0101		**bb PPEM305 gghh TBL

MSS150 00 Index Group	Component Name	Solution Notes	MSS1 5000 Subin dex	Impor tance Categ ory	SCC2 Header
	Ac Radius Server/<m>		0102		**bb PPEM305 gghh TBL
	Ac Radius		0103		**bb PPEM305 gghh TBL
	Ac Radius		0104		**bb PPEM305 gghh TBL
	Ac Radius Server/<m>		0105		**bb PPEM305 gghh TBL
7008	File system alarms. Disk instance range (<n>): 0-1 Card instance range (<x>): 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)				
	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 0152		**bb PPEM302 gghh TBL

MSS150 00 Index Group	Component Name	Solution Notes	MSS1 5000 Subin dex	Impor tance Categ ory	SCC2 Header
			0153		
	Shelf Card/<n>		0154		**bb PPEM303 gghh TBL
			0155		
			0156		
			0201		
	LP/<n>		0203		* bb PPEM306 gghh TBL
	LP/0		0204		* bb PPEM303 gghh TBL
7015	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 PPEM302 gghh TBL
			1000		
			1001		
	VR/<i> Ip OSPF				
			1011		
	VR/<i> Ip OSPF		1016		**bb PPEM302 gghh TBL
	VR/<i> Ip OSPF		1100		* bb PPEM300 gghh TBL
	Vr/<i>		1021		**bb PPEM302 gghh TBL
	Vr/<i> Ip Ospf		1101		* bb PPEM302 gghh TBL
	Vr/<i> Ip Ospf		1103		* 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.				

MSS15000 Index Group	Component Name	Solution Notes	MSS15000 Subindex	Importance Category	SCC2 Header
	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
	Artg		0603		**bb PPEM303 gghh TBL
7056	Voice Services Processor (VSP) / Narrowband Service Trunk over ATM (Nsta) This group is specific to MG15000 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				
	<Any MSS15000 component>		0000		* bb PPEM302 gghh TBL
	Lp/<x> Vsp PModule/<y>		0006		* bb PPEM303 gghh TBL

MSS15000 Index Group	Component Name	Solution Notes	MSS15000 Subindex	Importance Category	SCC2 Header
	Nsta/<i> Conn/<l> Brag/<d> Ccst		1101		* bb PPEM300 gghh TBL
	Nsta/<i> Vgs H248/0		1206		* 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 LP/<n> Eng LP/<n> Eng LP/<n> Eng LP/<n> Eng		1200		* bb PPEM301 gghh TBL
			1300		
			1400		
			1500		
			1600		
7061	Security policy violation alarms. VR instance range (<i>): any string, but often specified simply as a digit. <spd_name>: name of the security policy database <pol_id>: instance number of the Policy component <ip_addr,esp,spi>: IP address of the peer with which this SecurityAssociation component is established, the security protocol (ESP), and the Security Parameter Index (SPI) value				
	Vr/<i> Ip Spd/<spd_name> Pol/<pol_id> Sa/<ip_addr,esp,spi>		0001		**bb PPEM305 gghh TBL
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
7082	Routine Exercise alarms.				
	Rex		0003		**bb PPEM303 gghh TBL
7083	Flash burning alarms. Card instance range (<x>): 0-15				
	Shelf Card/<x> Fpga		0100		**bb PPEM302 gghh TBL
	Shelf Card/<x> Fpga		0101		**bb PPEM303 gghh TBL

Reference [3] provides detailed descriptions of MSS15000 alarm logs, of which only a portion are applicable for Succession VOA/VOIP.

4. MDM Alarm Logs

Table 4 presents the list of MDM and MDM proxy set/clear alarm logs that are applicable for Succession VOA/VOIP. Table 5 presents the list of MDM and MDM proxy message 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 MSS15000 (for a number of reasons) and injects into the MSS15000 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 MSS15000 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 MSS15000				
	EM/<nodename>		0001		*Cbb MDM 303 gghh TBL
0999	MDM Proxy-alarm. MDM-originated alarm sent on behalf of the MSS15000, either due to a state walk or a state-change notification.				
	This alarm can apply to many MSS15000 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 Autopatch nodes (<nodes parameter>): typically, this is the name of an HGDS group or a node name or file name containing a list of node names. EM node name (<node name>): the name of the MSS15000 or MG15000 shelf				

MDM Index Group	Component Name	N/A	MDM SubIndex	Importance category (N/A)	SCC2 Header
	NMS/<x> APP/<a>		0000		**bb MDM 302 gghh TBL
	NMS/<x> APP/PPAUTOPATCH		0801		*bb MDM 306 gghh TBL
	NMS/<x> APP/PPAUTOPATCH NODES/<nodes parameter>		0802		*bb MDM 302 gghh TBL
	NMS/<x> APP/PPAUTOPATCH NODES/<nodes parameter>		0803		**bb MDM 302 gghh TBL
	NMS/<x> APP/PPAUTOPATCH EM/<node name>		0820		**bb MDM 302 gghh TBL
	NMS/<x> APP/PPAUTOPATCH EM/<node name>		0821		**bb MDM 302 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. The alarms 3011 xxFF (where xx can be 01,02,03,04,05,06, or 07) are clear alarms only. A single 3011xxFF alarm clears all outstanding alarms from 3011xx00 through 3011xx99. 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”, “***”
	NMS/<x>		01FF		bb MDM 303 gghh TBL

MDM Index Group	Component Name	N/A	MDM SubIndex	Importance category (N/A)	SCC2 Header
			02FF		bb MDM 303 gghh TBL
			03FF		bb MDM 303 gghh TBL
			04FF		bb MDM 303 gghh TBL
			05FF		bb MDM 303 gghh TBL
			06FF		bb MDM 303 gghh TBL
			07FF		bb MDM 303 gghh TBL
3012	Template configuration audit alarms. Indicates problems with MSS configuration, detected by audit tool. EM node name (<node name>): the name of the MSS15000 or MG15000 shelf				
	NMS_APP/CFGAUDIT		0001		**bb MDM 302 gghh TBL
	EM/<node name>		0002		

Reference [4] provides detailed descriptions of MDM and MDM proxy alarm logs, of which only a portion are applicable for Succession VOA/VOIP.

Table 5 MDM Message Alarms Supported for Succession VOA/VOIP

MDM Index Group	Component Name	N/A	MDM SubIndex	Importance category (N/A)	SCC2 Header
0999	MDM proxy-alarm. Issued when a loss of redundancy of alarm feed occurs. The MDM has lost its direct network alarm feed, but is still collecting them from its mate MDM. Note that this message alarm will not be issued for all conditions that could lead to a loss of redundancy, nor is it “cleared” when the problem is resolved. Thus, we do not recommend that this alarm be keyed upon, but include it here because it is likely to be seen. <deviceType> is any IP-enabled device, such as “EM” or “PP8600”. <nodeName> is the name of the device or shelf.				
	<deviceType>/<nodeName>		0100		* bb MDM 303 gghh TBL
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 GROUP instance range (<g>): a string, which is the HGDS group name for a set of MSS15000s PP instance range (<nodename>): a string, typically the CLLI identifier for the MSS15000				
	NMS/<x> GROUP/<g>		0700		* bb MDM 305 gghh TBL
	NMS/<x> PP/<nodename>		0701		* bb MDM 300 gghh TBL
	NMS/<x> PP/<nodename>		0702		* bb MDM 300 gghh TBL
	NMS/<x> APPL/TODCHANGEORVER		0703		* bb MDM 304 gghh TBL

MDM Index Group	Component Name	N/A	MDM SubIndex	Importance category (N/A)	SCC2 Header
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", "C", "C"

5. SN06(VOA)-to-SN06.2(VOA/VOIP) Delta Summary

The following table captures the SN06.2 (VOA/VOIP) alarm log delta that includes MG15000 application as compared with SN06 (VOA) documentation that did not include any MG15000 application specifics

Table 6 SN06 (non MG15000 content) -to-SN06.2 (including MG15000 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

6. 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 7 SN06.2-to-SN07 Change Summary Description

Fault Code	Description of Change
SET ALARMS	
7000 0041	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
0999 0004	New
3011 01FF	New
3011 02FF	New
3011 03FF	New
3011 04FF	New

3011 05FF	New
3011 06FF	New
3011 07FF	New
MESSAGE Alarms	
7003 0008	New
7008 1021	New
7021 1021	New
7021 1101	New
7041 0151	New
7056 0006	New
7080 0100	New

7. SN07-to-SN08 (VOA/VOIP) Delta Summary

The following table captures the SN08 (VOA/VOIP) alarm log delta as compared with SN07 (VOA/VOIP) documentation.

Table 8 SN07-to-SN08 Change Summary Description

Fault Code	Description of Change
SET ALARMS	
7000 0041	Changed
7002 0003	Changed
7002 0004	New
7006 0100	New
7021 1002	Changed
7021 1003	Changed
7041 0052	New
7056 1219	New
0999 0004	Removed (applies only to PP8600 and other DCD managed devices)
3010 0801	New
3010 0802	New
3010 0803	New
3010 0820	New
3010 0821	New
MESSAGE Alarms	
0999 0100	New
7006 0009	New
7006 0101	New
7006 0102	New
7006 0103	New
7006 0104	New
7006 0105	New
7061 0001	New

8. SN08-to-SN09 (VOA/VOIP) Delta Summary

The following table captures the SN09 (VOA/VOIP) alarm log delta as compared with SN08 (VOA/VOIP) documentation.

Table 9 SN08-to-SN09 Change Summary Description

Fault Code	Description of Change
SET Alarms	
3012 0001	New
3012 0002	New
7000 0042	New
7000 0043	New
7000 0044	New
7011 5281	New
7011 5501	Changed
7011 5290	Changed
7011 5291	Changed
7011 5292	Changed
7011 5293	Changed
7011 5294	Changed
7039 1001	New
7039 1002	New
7039 1003	New
7039 1004	New
7039 2000	Changed
7039 2003	Changed
7082 0001	New
7082 0002	New
MESSAGE Alarms	
7021 1103	New
7056 0000	New
7056 1206	New
7082 0003	New
7083 0100	New
7083 0101	New

9. SN09-to-SN09FF (VOA/VOIP) Delta Summary

The following table captures the SN09FF (VOA/VOIP) alarm log delta as compared with SN09 (VOA/VOIP) documentation.

Table 10 SN08-to-SN09 Change Summary Description

Fault Code	Description of Change
SET Alarms	
7008 1005	Changed
7012 0053	Changed
7017 1000	Changed

10. References

1. NTP 241-6001-501 Nortel Networks Multiservice Data Manager Alarms Reference, 15.3D2, June 2005.
2. NTP 241-6001-309 Preside MDM Management Data Provider User Guide, 14.3RSUP, 2003.
3. NTP NN10600-500 Multiservice Switch 7400/15000/20000 Alarms Reference, 7.1M1, June 2005
4. NTP NN10092-911 Nortel Networks Multiservice Switch 15000 Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Overview PT-AAL1/UA-AAL1/UA-IP, SN07S1, Dec 2004

Appendix D: USP Logs

LOG TYPE	LOG TITLE	DESCRIPTION	PROBABLE CAUSE	INFORMATION AND DATA SPECIFICS	CORRECTIVE ACTION
LOG_SWERR	AA1 Driver, 01: Get Buffer Error	The system generates this log when an attempt to get a system data buffer failed.	There are insufficient buffers in the SAR buffer pool.	The Information field describes the pool on which the attempt was made. The Data field provides the return code from the pool_get_buffer routine.	Contact your next level of support.
LOG_CLEAR_ALL	System Node Maintenance, 05: Off-line State	This log documents the clearing of all outstanding alarms against an RTC, CC, or application system node.	The user has requested an off-line operation on the RTC, CC, or application system node.	The Information field indicates the clearing of the outstanding alarms.	No action is required.
LOG_CRITICAL	Application DB Manager, 05: NPAC Data Lost	The Application database on an application database controller system node has determined that it has lost NPAC data.	A multiple application database system node failure occurred and recovery of the failed nodes occurred in an order that caused NPAC data to be lost.	No additional information is provided.	Perform a bulk load operation to reload the Application database with fresh NPAC data from the LSMS.

LOG_CRITICAL	Application DB Manager, 07: <Application> Database is Corrupted	The Application database manager has detected corruption in the Application database. The manager is initiating recovery by attempting to reload from the existing disk image or transferring a valid database from another application database system node.	1. There is a disk error 2. NPE is corrupt & can't communicate with NPC/NPS 3. Inactive application database controller became active due to more current birthdate 4. An application database system node has out of date or invalid birthdate 5. An application database system node has a sequence number behind or invalid 6. Failed to load the application database from disk 7. NPC/NPS received unexpected msg from NPE & msg indicates db change on NPE 8. NPC/NPS didn't receive an expected msg from NPE that would've caused db change on NPE 9. NPC/NPS received expected msg from NPE but msg is corrupted 10. Disk write error on an application database system node 11. Record count mismatch between active application database controller & other application database system nodes 12. Error in propagation of updates to other application database system nodes 13. Checksum of an index element or record element is invalid	No additional information is provided. A traceback log may accompany the corruption log which is provided for Nortel support personnel to trace the source of the corruption.	If another application database system node contains a valid database, the system will automatically transfer that copy to the affected node. Otherwise, a bulk load operation should be performed to reload the database from the LSMS.

LOG_CRITICAL	Application DB Manager, 27: <Application> database timestamp is invalid	The creation timestamp for the Application Database on the affected node references a date/time that is in the future. Since the creation timestamp is used in the synchronization of the Application DB between Application system nodes, and the timestamp value cannot be trusted, the Application DB has been declared invalid by the Application database manager.	The date/time on the USP has been set back to a time that is before the creation timestamp on the Application DB.	The date/time displayed in the data area of the log gives the creation timestamp of the Application DB.	If the date/time on the USP is incorrect, use the "Set Date/Time" button in the Administration panel to correct the date/time on the USP. If the date/time on the USP is correct and there is at least one application database controller system node not displaying this alarm, then the system should automatically correct itself on all affected application database system nodes. If the date/time on the USP is correct and all application database system nodes are displaying this alarm, then the Application database must be bulkloaded or the date/time on the USP must be changed to be beyond the creation timestamp of the Application DB.
LOG_CRITICAL	ASM Interworking, 01: GSO Critical Condition	The Core is in SS7 Overload and the USP has decreased the traffic level to the minimum allowed.	Either the minimum threshold is too high or the Core is in excessive overload.	The Information and Data fields indicate the ASM name.	Investigate the Core to determine why it is in overload.

LOG_CRITICAL	Buffer Manager, 07: Critical Buffer Depletion	This log is generated when the percentage of buffers in one of the buffer pools that are free or have been allocated for less than the office parameter SS7_BUFFER_ALLOCATE_MINS is less than the office parameter SS7_CNTL_BUF_CRITICAL_PRCNT_REM	Memory leak.	The Information field indicates the pool that is affected and the percentage of the pool buffers allocated for more than the specified allocation time.	If active NPC or LLC raised the alarm, perform SWACT. If SWACT succeeds then lock, load, and unlock the inactive NPC or LLC node immediately. If a LINK or an RTC raised the alarm, then lock, load, and unlock troubled node in immediately.
LOG_CRITICAL	Data Audit, 09: Net Appear Data Audit Alarm	This log is generated when a data audit between the AS Master and the USP detects a network appearance data mismatch.	A data update was not performed on the USP or AS Master.	The Information and Data fields indicate the type of alarm.	Contact your next level of support.
LOG_CRITICAL	Data Audit, 10: Routeset Data Audit Alarm	This log is generated when a data audit between the AS Master and the USP detects a routeset data mismatch.	A data update was not performed on the USP or AS Master.	The Information and Data fields indicate the type of alarm.	Contact your next level of support.
LOG_CRITICAL	Data Audit, 30: MHD table capacity exceeds 600K	This log is generated	This log is caused by the MHD table capacity exceeds 600K on PP4 cards	The Information and Data fields indicate the MHD capacity is full or not	This log is not expected to come during software upgrade. As the periodic data auditing facility is not running during software upgrade, perform a load operation on the affected RTC system node or application system node.
LOG_CRITICAL	Event Records, 01: Event Records No Connection	The system generates this log when Event Records are enabled on a system node but no connection to a downstream processor exists.	A downstream processor has not established a connection after the node has been reloaded, or an existing connection has been terminated by the downstream processor.	N/A	Connect a downstream processor to the system node.

LOG_CRITICAL	Event Records, 02: Event Records Overflow	The system generates this log when the Event Records queue has overflowed. Event Records that are not already in the queue will be discarded until the overflow is cleared.	The Event Records system is generating more data than can be transmitted to the downstream processor. This can happen when there is congestion on the network between the system node and the downstream processor or when users of the Event Record facility are requesting generation of records at rate greater than the facility's engineered limit.	N/A	Verify that there are no problems with the connection between the system node and the downstream processor, and that the system node is operating within engineered tolerances. If there are no problems with either, please contact your next level of support.
LOG_CRITICAL	Processor Exception, 08: Card not providing service	The system generates this log when a card has encountered a service affecting fault and is taking itself out of service. The card remains ENABLED, but will not be functional by means of providing service.	An internal error has occurred.	No additional data is included in this log.	Contact your next level of support.
LOG_CRITICAL	System Node Maintenance, 40: Isolation	The extension shelf of the CC node associated with this log has become isolated from the control shelf.	There is a problem with the fiber-optic cables, a problem with the CCs, or a combination of fiber-optic cable and CC problems. Check logs for fiber optic cable failures and/or CC card failures.	The data associated with this log contains the cfgIDNumber of the node that sent the isolation statechange message. Example Control Shelf CC1: 0101 0101 where 3rd digits is the shelf number (0) and the 5th digit is the slot number.	Please refer to the Alarm section of the USP Fault Management Manual for Isolation recovery procedures.

LOG_CRITICAL, LOG_CLEAR_CRITICAL	System Node Maintenance, 12: Locked Active RTC	This alarm indicates that an RTC system node in a locked state has been forced to the active state for the mated RTC system node pair. The clearing of this alarm indicates that the active RTC system node is no longer locked.	The active RTC system node failed while the mate RTC system node was in a locked state, and the locked RTC system node became active. When the alarm is cleared it means that the user has performed an unlock operation on the active RTC system node or an unlocked RTC system node has recently been enabled and the system has automatically switched activity to the unlocked RTC system node.	The Information field indicates that the active RTC system node is locked. When the alarm is cleared it indicates that the active RTC is no longer locked.	Refer to the Performing an Unlock Operation subsection in the RTC System Node Provisioning and Maintenance section of the USP User Guide for the steps necessary to unlock the active RTC system node. When the alarm is cleared no action is required.
LOG_CRITICAL, LOG_CLEAR_CRITICAL	System Node Maintenance, 32: Dual CC Failure	A critical alarm is raised when both of the CC system nodes on the CAM shelf have failed.	The CC system nodes have encountered an internal failure.	The Information field indicates either that a dual CC system node failure condition has occurred or that the condition has been cleared.	The system automatically attempts to recover the CC system nodes. No action is required.
LOG_INFO	Application Audit, 02: <Application> DB Audit Successful	The Application Audit task has completed an audit of the Application database and has found no problems.	The Application database audit completed without error.	No additional information is provided.	No action is required.
LOG_INFO	Application Audit, 03: <Application> DB audit has detected errors	The Application audit has identified one or more records in the Application Database that contain data inconsistencies.	In an Application local subsystem, an indirect routing method has been selected and one or more records have been found in the database with a ported status value of "ported across" or "not known to be ported".	The Data field contains a summary of the scope of the problem, including the number of affected records and the total number of records in the database. More detailed information can be obtained by requesting the Application Database Audit Report from the OAM&P workstation.	Review USP and LSMS datafill for correctness.

LOG_INFO	Application Database, 13: Record Duplicates	When loading records (from disk or bulk load file) records with the same Directory Number Key were found with identical data. The second identical records were deleted.	The bulk load data file has records with the same key.	(n) Duplicate Record(s) deleted, where (n) is the number of records deleted	This problem is self-correcting.
LOG_INFO	Application Database, 20: <Application> database created - no records	The Application DB database has been created with no Application DB records	This is a new system, with no previously existing database. A bulkload or SMI requests are required to load the records into the database.	No additional information is provided.	Perform a bulkload or use the SMI request system to load the records into the database
LOG_INFO	Application Database, 21: Duplicate returned record in NPDB	The system generates this log when the LLCNPDB search finds out there are two "matched" records in the database. It informs the user so that they could take the appropriate corrective action (delete the duplicate "matched" entry if required).	During a NPDB database search, there are two "matched" result records that could lead to ambiguous result. (e.g. DB with entries 0123 and 012345, key 01234 could return either 0123 - matched record or 012345 (required more info).	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred. The duplicated entries info could allow the user to determine whether they need to make any change in the DB to remove the ambiguity. The info are stored in the Data section with the following format (first 12 bytes - matched record, next 12 bytes - overlap record and all unused bytes are initialized to 0xFF). The data is in BCD format and so should be interrupted as below: data "0119" == key 1091.	Use the duplicated "matched" entries info to find out whether you need to make any change in the DB. Also, this LOG is throttled to 1 every 30 secs.

LOG_INFO	Application DB Manager, 01: Beginning <Application> Database Load	The Application Database Manager has started loading the Application database from disk into memory. The time required to load the database will depend on the number of records it contains. An informational log will be generated when the database load is completed. This log also occurs following the transfer of the Application database from another application database system node.	The Application database manager has begun loading the Application database as part of normal system startup or following transfer of the Application database from another application database system node.	No additional information is provided.	No action is required.
LOG_INFO	Application DB Manager, 02: Completed Loading <Application> database	The Application Database Manager has finished loading the Application database from disk into memory. This log also occurs following the transfer of the Application database from another application database system node.	The Application database manager has finished loading the Application database as part of normal system startup or following transfer of the Application database from another application database system node.	The Information field contains a count of the number of records in None.	No action is required.
LOG_INFO	Application DB Manager, 03: <Application> Database Load Failed	A failure occurred when the Application Database Manager attempted to load the Application database from disk into memory. A previous log should have been generated which will give more specifics regarding the cause of the error.	- One or more of the Application DB files is corrupted, or - There is a problem with the disk on this application database system node.	<Application> database load failed, code = (error) The (error) text in the log information field is the internal error code returned by the npdbLoadDatabase function.	The system will attempt to automatically recover from this condition by transferring a good copy of the database from another application database system node. If the automatic recovery is successful, no action is required. Otherwise, contact your next level of support.
LOG_INFO	Application DB Manager, 04: <Application> Database Load Interrupted	The loading of the Application database was interrupted by a lock or load user maintenance request or by a bulk load request.	The user initiated a lock or load user maintenance request or initiated a bulk load of the Application database.	No additional information is provided.	No action is required.

LOG_INFO	Application DB Manager, 08: <Application> DB is Operational	The Application database is now in an operational state. The database is now capable of handling updates and/or queries provided the local subsystem administrative state is set to "activated".	The Application database manager has successfully synchronized the Application database on this application database system node.	The log data contains a count of the number of records in the Application database.	No action is required.
LOG_INFO	Application DB Manager, 10: Bulk Load File Transfer Begun	This log indicates that the Application database manager has started the FTP transfer of the bulk load schema or data file from the LSMS system to the application database system node. Two files must be loaded from the LSMS a schema file and a data file. The schema file is the first to be transferred. It defines the format and location of the data file. The data file contains the NPAC data to be loaded into the Application database. The data file can be very large (hundreds of megabytes).	A bulk load operation was initiated from the OAM&P workstation.	Bulk load file transfer started: (type), where: (type) is either SCHEMA or DATA	No action is required.
LOG_INFO	Application DB Manager, 11: Bulk Load File Transfer Complete	This log indicates that the Application database manager has successfully transferred one of the files required to perform the Application bulk load operation.	The bulk load file transfer of the specified file completed successfully.	Bulk load file transfer complete: (type), where: (type) is either SCHEMA or DATA	No action is required.
LOG_INFO	Application DB Manager, 12: Bulk Load File Transfer Failed	This log indicates that a failure occurred when the Application database manager attempted to transfer one of the bulk load files from the LSMS system to the application database system node.	There are several possible causes: - Incorrect parameters specified by craftsman in the bulk load screen at the OAM&P workstation. - Input file missing on LSMS system. - Network error occurred during transfer. - Disk on the application database system node is full.	Bulk load file transfer failed: (type), where: (type) is either SCHEMA or DATA	Check the parameters used to initiate the bulk load operation. Verify the existence of specified files on the LSMS. Verify the network connectivity between the application database system node and the LSMS system. Check available disk space on the affected application database system node. If a problem is found, correct the problem and try again.

LOG_INFO	Application DB Manager, 13: Bulk Load Import Started	This log indicates that the Application database manager has successfully transferred the required bulk load files from the LSMS and has begun to import the bulk load data into the Application database.	A bulk load operation was initiated from the OAM&P workstation and the required data files have completed transfer from the LSMS.	No additional information is provided.	No action is required.
LOG_INFO	Application DB Manager, 14: Bulk Load Import Complete	This log indicates that the Application database manager has successfully imported the bulk load data into the Application database.	The bulk load operation has completed successfully.	No additional information is provided.	No action is required.
LOG_INFO	Application DB Manager, 15: Bulk Load Import Failed	This log indicates that an error occurred when the Application database manager was attempting to import the bulk load data into the Application database.	One or both of the bulk load data files contains a syntax error.	Bulk load import failed: (code), where: (code) is the internal failure code	Contact your next level of support.
LOG_INFO	Application DB Manager, 16: Bulk Load Aborted	This log indicates that the bulk load operation was aborted by the user from the OAM&P workstation.	The bulk load operation was aborted by the user from the OAM&P workstation.	No additional information is provided.	No action is required.
LOG_INFO	Application DB Manager, 17: Database Reload Initiated	This log indicates that the application database server system node has begun the transfer of the Application database from another application database system node due to the successful completion of a bulk load operation.	A bulk load operation was successfully completed on an application database controller system node. The propagation of the new database is starting.	No additional information is provided.	No action is required.
LOG_INFO	Application DB Manager, 18: Update Acknowledgment Timeout	An update message sent out to the other Application nodes in the system has not been acknowledged within the acknowledgment timeout period.	Problems with other Application and RTC system nodes in the system are preventing update messages from being responded to.	No additional information is provided.	Contact your next level of support.

LOG_INFO	Application DB Manager, 21: Beginning <Application> Database Transfer	The Application Database Manager has started transferring the Application database from another application database system node within the USP in order to recover from database corruption. The time required to transfer the database will depend on the number of records it contains. An informational log will be generated when the database transfer is completed. Transfer of the Application database also occurs when a new application database system node is added to the system.	The Application database manager has begun transfer the Application database to recover from database corruption or to bring a new application database system node into service.	The Data field identifies the application database system node from which the database is being transferred.	No action is required.
LOG_INFO	Application DB Manager, 22: <Application> Database Transfer Complete	The Application Database Manager has finished transferring the Application database from another application database system node.	The Application database manager has finished transferring the Application database.	The Data field identifies the application database system node from which the database was transferred.	No action is required.
LOG_INFO	Application DB Manager, 23: <Application> Database Transfer Failed	A failure occurred when the Application Database Manager attempted to transfer the Application database from another application database system node.	- The system node from which the transfer was occurring failed or was reset. - The disk on either of the application database system nodes involved in the transfer has gone bad.	The Data field identifies the application database system node from which the database transfer attempt was made and a code for the type of error which occurred.	The system will attempt to automatically recover from this condition by retrying the transfer from another application database system node. If the automatic recovery is successful, no action is required. Otherwise, contact your next level of support.
LOG_INFO	Application DB Manager, 24: <Application> Database Transfer Interrupted	Transfer of the Application database from another application database system node was interrupted by a lock or load user maintenance request or by a bulk load request.	The user initiated a lock or load user maintenance request or initiated a bulk load of the Application database.	The Data field identifies the application database system node from which the database transfer was being attempted.	No action is required.

LOG_INFO	Application DB Manager, 25: Searching for Valid <Application> Database	The application database system node is trying to locate another application database system node within the USP that contains a valid Application database. Once found, the database will be transferred and loaded into the application database system node. The search will continue until a valid copy is located or some other situation occurs which alters the state of the application database system node.	The node is attempting to recover from a corrupted or missing Application database and no valid copy of the database can currently be located.	No additional information is provided.	If there is no valid Application database on any application database system node, the Application Local Subsystem will need to be bulk-loaded. Otherwise, take the necessary steps to bring the affected application database system node online with a known good copy of the database.
LOG_INFO	Application DB Manager, 28: NPA Split created	This log indicates that an NPA Split has been created within the Application Database as a result of receiving an NPA Split creation request from the LSMS. This occurs at the start of the permissive dialing period (PDP) that was defined for the NPA Split when the NPA Split record was created on the LSMS. Using background audit cycles, the Application subsystem will proceed to migrate all ported DN records affected by the split from the old NPA to the new NPA. During the permissive dialing period, the Application DB will allow Application queries to use either the old or the new NPA value to access the affected ported DN records in the Application DB.	An NPA Split creation request was received from the LSMS to trigger the start of the permissive dialing period (PDP).	The old and new NPAs will be displayed in the text of the log.	No action is required.

LOG_INFO	Application DB Manager, 29: NPA Split deleted	This log indicates that an NPA Split has been deleted from the Application Database as a result of receiving an NPA Split deletion request from the LSMS. This occurs at the end of the permissive dialing period (PDP) that was defined for the NPA Split when the NPA Split record was created on the LSMS. At this point, queries made to the Application DB using the old NPA will not find a ported DN record, unless the telephone number in the old NPA is reassigned to a new customer and the customer subsequently ports his number to another service provider.	An NPA Split deletion request was received from the LSMS to signal the end of the permissive dialing period (PDP).	The old and new NPAs will be displayed in the text of the log.	No action is required.
LOG_INFO	Application DB Manager, 30: NPX Database Transaction Manager	This log indicates that a problem has occurred during communication with the NPE expanded database cards. Additional logs and alarms will follow indicating the action taken to clear the problem.	Timeout has occurred waiting for a response from one of the NPE expanded database cards.	None	No action is required.
LOG_INFO	Application DB Manager, 32: <Application> Database Disk Write Failed	A failure occurred when the Application Database Manager attempted to write to the disk files.	- Disk files closed by another application - Disk itself is no longer functioning		The system will attempt to automatically recover from this condition by trying to reload from the existing disk files, Failing that it will try to transfer a new database over from another application database system node. Failing that it will try to reload the application database system node to reinitialize the disk access. Failing that the disk card should be replaced with a new disk.

LOG_INFO	Application DB Manager, 33: bulk-output-services-db file creation started	This log indicates that the execution of a bulk-output services-db command has been started.	A bulk output operation was initiated from the OAM&P workstation.	The data field contains the user-id and user-ip-address of the user that initiated the bulk output as well as remote-server-user-id, remote-server-ip-address, and sub-system.	No action is required.
LOG_INFO	Application DB Manager, 34: bulk-output-services-db file creation completed	This log indicates that the Application database manager has successfully exported the Application database to file.	The bulk output file creation operation has completed successfully.	The data field contains the user-id and user-ip-address of the user that initiated the bulk output as well as remote-server-user-id, remote-server-ip-address, and sub-system.	No action is required.
LOG_INFO	Application DB Manager, 35: bulk-output-services-db file creation failed	This log indicates that an error occurred when the Application database manager was attempting to create the bulk output files from the Application database.	There are several possible causes: - insufficient disk space to create the bulk output file - write IO error occurred during bulk output file creation - errors encountered during record export (contact next level of support).	The data field contains the user-id and user-ip-address of the user that initiated the bulk output as well as remote-server-user-id, remote-server-ip-address, sub-system. See journal log for details of error response.	If the problem persists, contact your next level of support.
LOG_INFO	Application DB Manager, 36: bulk-output-services-db file transfer started	This log indicates that the Application database manager has started the FTP transfer of the bulk data file and load schema from the application database controller system node to the LSMS. Two files must be transferred from the application database controller node, a schema file and a data file. The data file contains the NPAC data to be loaded into the Application database. The data file can be very large (hundreds of megabytes). The schema file is the last to be transferred. It defines the format and location of the data file.	A bulk output operation was initiated from the OAM&P workstation.	The data field contains the user-id, user-ip-address, remote-server-user-id, remote-server-ip-address, subsystem-name	No action is required.
LOG_INFO	Application DB Manager, 37: bulk-output-services-db file transfer completed	This log indicates that the Application database manager has successfully transferred the bulk output files created during the export operation.	The bulk load file transfer of the specified file completed successfully.	The data field contains the user-id, user-ip-address, remote-server-user-id, remote-server-ip-address, subsystem-name	No action is required.

LOG_INFO	Application DB Manager, 38: bulk-output-services-db file transfer	This log indicates that a failure occurred when the Application database manager attempted to transfer one of the bulk output files from the application database controller system node to the LSMS.	There are several possible causes: - problems with accessing the server - problems with the ftp connection - the server disk quota for the remote-server-user-id has exceeded	The data field contains the user-id, user-ip-address, remote-server-user-id, remote-server-ip-address, subsystem-name.	Ensure that the remote-server-user-id, remote-server-user-password, and the remote-server-ip-address specified in the bulk-output command is correct. If this information is correct, verify the network connectivity between the application database controller system node and the FTP server by attempting to FTP to the server. If FTP action is successful, check the write permissions on the server. Ensure that the disk quota for the user is not exceeded on the server. If a problem is found with any of the above, correct the problem and try again. If the problems persist, contact your next level of support.
LOG_INFO	Application DB Manager, 39: bulk-input-services-db processing error	This log indicates that an error occurred during bulk-input processing.	There are several possible causes: - Incompatible or incorrect schema file - Incompatible or incorrect data file - Incomplete or missing provisioning data	The data field contains detail error information	Correct the problem based on the error information.

LOG_INFO	Application DB Manager, 40: bulk-input-services-db client rtc failure	This log indicates that the client rtc node that requested the bulk input has failed.	The rtc has been reloaded by the user or by the system.	The data field contains the user id of the client and the node id of the failed rtc.	No corrective action is required. The bulk-input process runs to completion on the application database controller system node, even after the rtc failure. However, no journaling log is issued at the completion of the bulk-input process.
LOG_INFO	Application DB Manager, 41: bulk-output-services-db file create abort	This log indicates that the Application database manager is aborting the bulk output services db file creation of the Application database.	The card executing the bulk-output-services-db has been unlocked to return the application database to service.		No action is required.
LOG_INFO	Application DB Manager, 42: Birthdate ahead - Move In-Service	The active NPC has been trying to come up for 10 minutes, but the birthdate of the RTC database is ahead of the birthdate of the active NPC database. However, since there is only one active NPC it will try to come up regardless. The RTC database will then sync up with the NPC database.	The birthdate of the RTC database is ahead of the NPC database.		After the sync check that NPC database is up to date and that it also has all the updates from external interfaces.
LOG_INFO	Application DB Manager, 43: Sync Achieved SeqNum <Sequence Number>	NPC or NPS node came up correctly and synced with other databases in the system.			No action is required.
LOG_INFO	Application DB Manager, 44: SeqNum Behind <Sequence Number>	This log indicates that the Application database manager is aborting the bulk output services db file creation of the Application database.			No action is required.
LOG_INFO	Application DB Manager, 45: SeqNum Wrong Sync <Sequence Number - Sequence Number>	The card and database came up but is missing updates from external interfaces. Therefore it will query local NPC or NPS cards to get the missing information.			After the sync check that NPC database is up to date and that it also has all the updates from external interfaces.

LOG_INFO	Application DB Transfer, 01: Socket Write Failed	A write operation on a TCP socket used to transfer Application database files between application database system nodes encountered an error.	Loss of communication between the application database system nodes involved in the file transfer.	Socket write failed: errno = (ee) (ee) is the internal operating system error code	If the problem occurs on an otherwise normal system report this problem to your next level of support. The problem is self-correcting the system will continue to attempt the data transfer automatically.
LOG_INFO	Application DB Transfer, 02: Socket Read Failed	A read operation on a TCP socket used to transfer Application database files between Application system nodes encountered an error.	Loss of communication between the Application system nodes involved in the file transfer.	Socket read failed: errno = (ee), where: (ee) is the internal operating system error code	If the problem occurs on an otherwise normal system report this problem to your next level of support. The problem is self-correcting the system will continue to attempt the data transfer automatically.
LOG_INFO	Application SMI, 03: Socket Write Failed	A write operation on a TCP socket used to communicate with the LSMS encountered an error.	There is a loss of communication between the application database controller system node and the LSMS.	Socket write failed: errno = (ee), where: (ee) is the internal operating system error code	Check the LAN connectivity between the application database controller system node and the LSMS. Make sure the LSMS is operational.
LOG_INFO	Application SMI, 04: Socket Read Failed	A read operation on a TCP socket used to communicate with the LSMS encountered an error.	There is a loss of communication between the application database controller system node and the LSMS.	Socket read failed: errno = (ee), where: (ee) is the internal operating system error code	Check the LAN connectivity between the application database controller system node and the LSMS. Make sure the LSMS is operational.
LOG_INFO	Application SMI, 08: LSMS Connection Established	The Application SMI subsystem has accepted a login request from an LSMS.	An LSMS has attempted a login to the SMI subsystem.	LSMS connection established: (nnn.nnn.nnn.nnn), (userid), where: (nnn.nnn.nnn.nnn) is the IP address of the LSMS. (userid) is the user ID used to log in.	No action is required.

LOG_INFO	Application SMI, 09: LSMS Connection Dropped	The Application SMI subsystem has lost a connection to an LSMS.	The LSMS has disconnected the connection to the SMI subsystem, or a network problem has occurred.	LSMS connection dropped: (nnn.nnn.nnn.nnn), (userid), where: (nnn.nnn.nnn.nnn) is the IP address of the LSMS. (userid) is the user ID associated with the dropped connection. The Data field contains the reason for dropping the connection.	Check the status of the LSMS. If the session was not dropped intentionally from the LSMS side, check network connectivity for problems.
LOG_INFO	Application SMI, 10: SMI Congestion Increased	The Application SMI subsystem has detected an increase in its internal congestion level.	The LSMS is sending updates to the SMI subsystem at a rate that exceeds the rated maximum.	SMI congestion level increased to (level), where: (level) is the new congestion level (low, medium, or high).	This problem is self correcting. The SMI subsystem will drop incoming messages according to the message priority value and the current congestion level until the internal congestion decreases.
LOG_INFO	Application SMI, 11: SMI Congestion Decreased	The Application SMI subsystem has detected a decrease in its internal congestion level.	The LSMS has reduced the rate at which it is sending updates to the SMI subsystem such that the backlog of requests has been reduced and congestion is abating.	SMI congestion level decreased to (level), where: (level) is the new congestion level (medium, low, or none).	No action is required.
LOG_INFO	Application SMI, 13: Repeated Invalid Msgs	An LSMS is sending a stream of SMI messages that are incorrectly formatted. This log will be repeated periodically during the period that the problem persists.	The LSMS is not sending correctly formatted SMI messages.	Repeated msgs from (n.n.n.n) invalid - total: (nn), where: (n.n.n.n) is the IP address of the LSMS that is sending invalid messages (nn) is the number of consecutive invalid messages received from this LSMS	Check with the LSMS vendor to ensure that the software is written to support the Nortel Networks SMI protocol.

LOG_INFO	Application SMI, 14: <Application>DB Operation Timeout	The SMI subsystem is encountering operation timeouts when attempting to perform an operation on the Application database. This log is throttled to prevent an excessive number of these logs from swamping the logging subsystem.	There is internal Application database congestion.	<Application>DB timeout on session (n.n.n.n) - total: (nn), where: (n.n.n.n) is the IP address of the LSMS encountering timeout errors (nn) is the number of database timeouts that have occurred on this LSMS session	Contact your next level of support.
LOG_INFO	ASM Interworking, 04: GSO SOC State Change	The GSM SS7 Overload functionality is enabled or disabled based on messages received from the Core. This log indicates that the enabled state has changed for one of the Cores the USP is connected to.	GSM SS7 Overload functionality has been enabled/disabled.	The Information and Data fields indicate the ASM name and the new SOC/enabled state.	None.
LOG_INFO	ASM Interworking, 05: GSO Restart	A Core the USP is connected to has gone through a restart.	The Core has gone through a restart.	The Information and Data fields indicate the ASM name.	None.
LOG_INFO	ASM Interworking, 06: GSO SSN Change	The GSM SS7 Overload functionality performs congestion control for two SCCP subsystems, RANAP and BSSAP. This log indicates that the SSN for one of these subsystems has changed.	The BSSAP or RANAP SSN on the Core has changed.	The Information and Data fields indicate the ASM name, the subsystem changed and the subsystem number.	None.
LOG_INFO	ASM Interworking, 07: TTP State Change	The GSM TCAP TRID Peeking functionality is enabled or disabled based on messages received from the Core. This log indicates that the enabled state has changed for one of the Cores the USP is connected to.	GSM TCAP TRID Peeking functionality has been enabled/disabled.	The Information and Data fields indicate the ASM name and the new enabled state.	None.
LOG_INFO	ASM Interworking, 08: TTP SSN Change	The GSM TCAP TRID Peeking functionality performs message pre-processing for four SCCP subsystems on the Core. Two of these SSNs can be changed by the Core, GSMINAP and GSMCAP. This log indicates that the SSN for one of these subsystems has changed	The GSMINAP or GSMCAP SSN on the Core has changed.	The Information and Data fields indicate the ASM name, the subsystem changed and the subsystem number.	None.

LOG_INFO	ATM Device Driver, 03: Mux Memory Error	This log indicates that the IgT WAC-185 mux had an error on the memory test. The system will not initialize.	There may be a hardware problem.	The Information and Data fields provide the address of the memory location that failed, as well as the value written and the value read from that location.	Contact your next level of support.
LOG_INFO	ATM Device Driver, 05: RT Memory Error	This log indicates that the IgT WAC-187 routing table or the PMC QRT-PM73487 routing table had an error on the memory test. The system will not initialize.	There may be a hardware problem.	The Information and Data fields provide the address of memory location that failed, as well as the value written and the value read from that location.	Contact your next level of support.
LOG_INFO	Boot, 02: Boot Error	An error was encountered during booting of an RTC, CC, or application system node.	This log occurs if a reset of the system node timed out, if the system node failed to request its load, or if the system node failed to become enabled.	The Information field indicates which error occurred.	No action is required. The system will continue attempting to recover the affected system node.
LOG_INFO	Boot, 03: Configuration Error	The boot manager has detected a configuration error.	There is an error accessing a database, or database records do not match expected values in the system, or Image not found on disk.	The Information field indicates the reason that the specific error occurred.	If the error is Image not found on disk, verify the configured software image is properly installed on the SCSI disks of both RTC system nodes. For other errors, contact your next level of support.

LOG_INFO	Boot, 06: No Boot Path	The booting of a CC or application system node has not been attempted because there is no communication path. Booting will be re-attempted when the communication path is restored.	There is no communication path between the RTCs and the system node to be booted.	No additional information is provided.	Make sure that at least one communication path exists between the RTCs and the system node you are trying to boot. Verify the following: - CC on the control self is enabled If trying to boot an extension shelf system node, verify that: - The fiber-optic cable directly connected to that control shelf CC. - The enabled extension shelf CC directly connected to that fiber-optic cable. See the USP Fault Management Manual for more information.
LOG_INFO	Buffer Manager, 08: Buffer Audit Active	This log is generated to report the activity of buffer audit.	Buffer Audit is active.	No additional information is provided.	No action is required.
LOG_INFO	Call Gap, 02: Call Gap audit mismatch	The system generates this log when the Call Gap audit detects a difference in the number of records call gap has and should have.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	No action is required. The audit has fixed the record counts. If however this log is seen continuously, you should contact your next level of support.
LOG_INFO	Call Gap, 03: Call Gap message received	The system generates this log when the SCP Call Gap procedure receives an incoming CallGap message	CallGap message has been received	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred. note: this is a throttled log	No action is required.

LOG_INFO	Call Gap, 04: Call Gap message sent	The system generates this log when the SSP Call Gap procedure sends a CallGap message	CallGap message has been sent	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred. note: this is a throttled log	No action is required.
LOG_INFO	Call Gap, 05: Global BHCA Overload	The system generates this log when a Global BHCA overload condition is triggered within the SSP Call Gap procedure -- meaning the total IDP count has exceeded the global "fall-back" BHCA value. (This is a normal part of the operation of the BHCA processing function).	Global BHCA overload condition triggered	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred. note: this is a throttled log	No action is required.
LOG_INFO	Call Gap, 06: BHCA Overload	The system generates this log when a BHCA overload condition is triggered within the SSP Call Gap procedure. (This is a normal part of the operation of the BHCA processing function).	BHCA overload condition triggered	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred. note: this is a throttled log	No action is required.
LOG_INFO	Carrier, 00: Carrier State Change	This log records the carrier state changes for T1 or E1 carriers.	One of the following state changes occurred from the carrier : LOS - Loss of Signal LOF - Loss of Frame AIS - Alarm Indication Signal RAI - Remote Alarm Indication	The Information field indicates the state change and whether it has been declared or cleared.	No action is required.

LOG_INFO	Command Line Interface, 02: bulk-input-system-db bulk file transfer started	This log indicates that the transfer of the bulk-input command file from the server has been started.	The bulk-input command has been issued by a CLI user.	The data field contains the user-id, user-ip-address, remote-server-user-id, remote-server-ip-address and the bulk command file name.	No action is required.
LOG_INFO	Command Line Interface, 03: bulk-input-system-db bulk file transfer completed	This log indicates that the transfer of the bulk-input command file from the server has been completed.	The bulk-input command has been issued by a CLI user.	The data field contains the user-id, user-ip-address, remote-server-user-id, remote-server-ip-address and the bulk command file name.	No action is required.
LOG_INFO	Command Line Interface, 04: bulk-input-system-db bulk file transfer aborted	This log indicates that a failure occurred during the bulk-input command file transfer from the server.	There are several possible causes: - problems with accessing the server - problems with the ftp connection - command file has exceeded the maximum allowed size - the server disk quota for the remote-server-user-id has exceeded	The data field contains the user-id, user-ip-address, remote-server-user-id, remote-server-ip-address and the command file name.	Ensure that the remote-server-user-id, remote-server-user-password, and the remote-server-ip-address specified in the bulk-input command is correct. If this information is correct, verify the network connectivity between the RTC system node and the FTP server by attempting to FTP to the server. If FTP action is successful, check the command file on the server. Ensure that the disk quota for the user is not exceeded on the server. If a problem is found with any of the above, correct the problem and try again. If the problems persist, contact your next level of support.

LOG_INFO	Command Line Interface, 05: bulk-input-system-db command execution started	This log indicates that the execution of a bulk-input command file has been started.	The bulk-input command has been issued by a CLI user.	The data field contains the user-id, user-ip-address, remote-server-user-id, remote-server-ip-address, the bulk command file name and the start time	No action is required.
LOG_INFO	Command Line Interface, 06: bulk-input-system-db command execution completed	This log indicates that the execution of a bulk-input command file has been completed.	The bulk-input command has been issued by a CLI user.	The data field contains the user-id, user-ip-address, remote-server-user-id, remote-server-ip-address, the bulk command file name, the start time, number of commands executed, and the number of command failed	No action is required.
LOG_INFO	Command Line Interface, 07: bulk-input-system-db command aborted	This log indicates that the bulk-input command execution has been aborted.	The bulk-input operation was aborted by a user or by the system due to the reason listed in the log data.	The data field contains the user-id, user-ip-address, remote-server-user-id, remote-server-ip-address, the bulk command file name, the start time, number of commands executed, number of command failed, and the abort reason	Check the abort reason listed in log data. Take action based on the abort reason.
LOG_INFO	Command Line Interface, 08: Insufficient disk space	This log indicates that there is insufficient disk space in the SCSI disk for the bulk-input file and/or bulk-input log file.	There is not enough space on the SCSI disk associated with the RTC system node. Most likely there are too many data snapshots or old loads resident on the disk.	The Information field indicates that there is not enough disk space to create transfer the bulk-input file or create bulk-input log file.	Delete the older snapshots and/or loads on the SCSI disk associated with the RTC system node and try again to execute the bulk-input. Refer to the Backup section of the USP User Guide for more information.

LOG_INFO	Command Line Interface, 09: Scheduler	This log indicated Scheduler related information	It provides details when user has add/delete/modify commands completed unsuccessfully	The data field indicates an error text when an OAM command has attempted to be scheduled and failed.	Validate command syntax and/or parameters values.
LOG_INFO	Command Line Interface, 10: bulk-input-system-db log file transfer started	This log indicates that the transfer of the bulk-input log file to the server has been started	The bulk-input command processing has ended, causing the log file to be transferred.	The data field contains user-id, user-ip-address, remote-server-user-id, remote-server-ip-address and the log file name.	No action is required.
LOG_INFO	Command Line Interface, 11: bulk-input-system-db log file transfer completed	This log indicates that the bulk input log file has been transferred successfully to the server.	The bulk-input command processing has ended, causing the log file to be transferred.	The data field contains user-id, user-ip-address, remote-server-user-id, remote-server-ip-address and the log file name.	No action is required.

LOG_INFO	Command Line Interface, 12: bulk-input-system-db log file transfer aborted	This log indicates that a failure occurred during the bulk-input log file transfer to the server.	There are several possible causes: - problems with accessing the server - problems with the ftp connection - log file has exceeded the maximum allowed size - the server disk quota for the remote-server-user-id has exceeded	The data field contains user-id, user-ip-address, remote-server-user-id, remote-server-ip-address and the log file name.	Ensure that the remote-server-user-id, remote-server-user-password, and the remote-server-ip-address specified in the bulk-input command is correct. If this information is correct, verify the network connectivity between the RTC system node and the FTP server by attempting to FTP to the server. If FTP action is successful, check the log file on the server. Ensure that the disk quota for the user is not exceeded on the server. If the log file is found, validate the creation date, time and the content. If log file is not found or the file content is incorrect, contact your next level of support before starting another bulk-input.
LOG_INFO	Command Line Interface, 13: bulk-output-system-db started	This log indicates that the execution of a bulk-output system-db command has been started.	The bulk-output system-db command has been issued by a CLI user.	The data field contains the user-id, user-ip-address, remote-server-user-id, remote-server-ip-address, subsystem-name, table-name, output-format	No action is required.
LOG_INFO	Command Line Interface, 14: bulk-output-system-db completed	This log indicates that the execution of a bulk-output system-db command has been completed.	The bulk-output system-db command has ended.	The data field contains the user-id, user-ip-address, remote-server-user-id, remote-server-ip-address, subsystem-name, table-name, output-format	No action is required.

LOG_INFO	Configuration, 01: Semaphore Unavailable	The system generates this log when two users at different OAM&P workstations try to access the same set of configuration management data simultaneously.	The semaphore that controls access to the data is unavailable.	The Information and Data fields describe the inaccessible data.	No action is required.
LOG_INFO	Configuration, 02: Shelf Added	The system generates this log when an extension CAM shelf is successfully added.	A user has added an extension CAM shelf.	The Information and Data fields show the shelf the user added.	No action is required.
LOG_INFO	Configuration, 03: Shelf Modified	The system generates this log when a CAM shelf is successfully modified.	The user modified a CAM shelf.	The Information and Data fields show the CAM shelf the user modified.	No action is required.
LOG_INFO	Configuration, 04: Shelf Deleted	The system generates this log when an extension CAM shelf is successfully deleted.	The user deleted a shelf.	The Information and Data fields show the extension CAM shelf the user deleted.	No action is required.
LOG_INFO	Configuration, 05: System Node Added or Modified	The system generates this log when an RTC, CC, or application system node is added or modified.	The user added or modified a system node.	The Information and Data fields describe the system node the user added or modified.	No action is required.
LOG_INFO	Configuration, 06: System Node Deleted	The system generates this log when an RTC, CC, or application system node is deleted.	The user deleted a system node.	The text describes the system node deleted.	No action is required.
LOG_INFO	Configuration, 24: System Node Modified	The system generates this log when an RTC, CC or application system node is modified successfully.	The user modified an RTC, CC, or application system node.	The Information and Data fields describe the RTC, CC, or application system node that was modified.	No action is required.
LOG_INFO	Configuration, 25: System Modified	The system generates this log when system parameters are modified successfully.	The user modified system parameters.	The Information and Data fields describe which system parameters have been modified.	No action is required.

LOG_INFO	Data Audit, 03: Database File Access Failure	This log is generated when a failure occurs while the system is trying to write or read from a database stored on a SCSI disk associated with an RTC system node.	This occurs when the indicated database is not on the SCSI disk, the SCSI disk is full, or the indicated directory path is not on the SCSI disk.	The Information and Data fields indicate the name of the affected database and the internal code that identifies the reason for the failure.	Contact your next level of support.
LOG_INFO	Data Audit, 04: Minor Corrective Action	This log is generated when the data audit reveals data corruption. The system takes corrective action by pushing the state of the related link or path into the next state.	This log occurs when a message is lost or timer buffers are not available.	The Information and Data fields indicate the internal ID of the link or path and the internal ID for the state.	Contact your next level of support.
LOG_INFO	Data Audit, 05: Congestion Update Message Lost	This log is generated when a local link congestion update message is lost.	This log occurs when an internal control message is lost.	The Information and Data fields indicate the internal ID for the affected SS7 link.	No action is required.
LOG_INFO	Data Audit, 07: Database Update Lost	This log is generated when a database update message is lost and the database on the application system node is now out of sync with the databases stored on the RTC system node and, potentially, other application system nodes.	This log occurs when the system is so busy that the message was lost.	The Information and Data fields indicate the name of the database associated with the lost message and the steps being taken by the system to correct the problem.	The system tries to correct the problem by downloading the database from the active RTC system node to the affected application system node. If this does not correct the problem, deactivate the SS7 link or bring down the IP path provisioned for the affected application system node and perform a load operation. Refer to the USP User Guide for more information. If loading the affected application system node does not correct the problem, contact your next level of support.
LOG_INFO	Data Audit, 11: Net Appear Index Failed Audit	This log is generated when a data audit between the AS Master and the USP detects an error with the network appearance index.	A data update was not performed on the USP or AS Master.	The Information and Data fields indicate the reason for the audit failure, the network appearance index, and the network name.	Contact your next level of support.

LOG_INFO	Data Audit, 12: Net App Elem Type Failed Audit	This log is generated when a data audit between the AS Master and the USP detects an error with the network appearance element type.	A data update was not performed on the USP or AS Master.	The Information and Data fields indicate the reason for the audit failure, the network appearance index, and the network name.	Contact your next level of support.
LOG_INFO	Data Audit, 13: Net App Net Id Failed Audit	This log is generated when a data audit between the AS Master and the USP detects an error with the network appearance network identifier.	A data update was not performed on the USP or AS Master.	The Information and Data fields indicate the reason for the audit failure, the network appearance index, and the network name.	Contact your next level of support.
LOG_INFO	Data Audit, 14: Net App Cnty Var Failed Audit	This log is generated when a data audit between the AS Master and the USP detects an error with the network appearance country variance.	A data update was not performed on the USP or AS Master.	The Information and Data fields indicate the reason for the audit failure, the network appearance index, and the network name.	Contact your next level of support.
LOG_INFO	Data Audit, 15: Net App CLLI Failed Audit	This log is generated when a data audit between the AS Master and the USP detects an error with the network appearance CLLI.	A data update was not performed on the USP or AS Master.	The Information and Data fields indicate the reason for the audit failure, the network appearance index, and the network name.	Contact your next level of support.
LOG_INFO	Data Audit, 16: Net Appear PC Failed Audit	This log is generated when a data audit between the AS Master and the USP detects an error with the network appearance pointcode.	A data update was not performed on the USP or AS Master.	The Information and Data fields indicate the reason for the audit failure, the network appearance index, and the network name.	Contact your next level of support.
LOG_INFO	Data Audit, 17: Routeset Index Failed Audit	This log is generated when a data audit between the AS Master and the USP detects an error with the routeset index.	A data update was not performed on the USP or AS Master.	The Information and Data fields indicate the reason for the audit failure, the routeset index, and the routeset name.	Contact your next level of support.
LOG_INFO	Data Audit, 18: Routeset Net App Failed Audit	This log is generated when a data audit between the AS Master and the USP detects an error with the routeset's network appearance.	A data update was not performed on the USP or AS Master.	The Information and Data fields indicate the reason for the audit failure, the routeset index, and the routeset name.	Contact your next level of support.

LOG_INFO	Data Audit, 19: Routeset Cnty Var Failed Audit	This log is generated when a data audit between the AS Master and the USP detects an error with the routeset's country variance.	A data update was not performed on the USP or AS Master.	The Information and Data fields indicate the reason for the audit failure, the routeset index, and the routeset name.	Contact your next level of support.
LOG_INFO	Data Audit, 20: Routeset CLLI Failed Audit	This log is generated when a data audit between the AS Master and the USP detects an error with the routeset's CLLI.	A data update was not performed on the USP or AS Master.	The Information and Data fields indicate the reason for the audit failure, the routeset index, and the routeset name.	Contact your next level of support.
LOG_INFO	Data Audit, 21: Routeset DPC Failed Audit	This log is generated when a data audit between the AS Master and the USP detects an error with the routeset's destination pointcode.	A data update was not performed on the USP or AS Master.	The Information and Data fields indicate the reason for the audit failure, the routeset index, and the routeset name.	Contact your next level of support.
LOG_INFO	Data Audit, 22: ISUP MHD Audit Information	This log is generated when an ISUP MHD data audit detects and error. This can be a mismatch between the AS Master and the USP or a mismatch between the active RTC and the other nodes.	A data update was not performed on the USP or AS Master.	The Information and Data fields indicate if the data mismatch has been corrected.	If the mismatch was corrected then no action is necessary. If the mismatch was detected but not corrected, contact your next level of support.
LOG_INFO	Data Audit, 28: Xlist Audit Correction	This log provides information for Nortel Networks technical support.	Various activities are reported.	The Information and Data fields provide MTP event information.	No action is required.
LOG_INFO	Disk Maintenance, 03: SCSI Disk Failure	An RTC system node is not able to access its SCSI disk.	There is a hardware failure or the SCSI disk has failed to respond within a specified time.	The Information field describes the error.	Contact your next level of support.
LOG_INFO	Disk Maintenance, 06: Format Failed	The system generates this log when disk formatting fails due to inability to access a device or a fatal disk hardware failure.	Poor connection or faulty disk hardware: SCSI disk, SCSI connector, TM, or RTC.	No additional information is available.	Reseat or replace the disk hardware.

LOG_INFO	Disk Maintenance, 07: Disk Access Failed	The disk audit on an NP node is not able to access its disk.	Poor connection or faulty disk hardware: SCSI disk, SCSI connector, TM, or RTC. Or disk audit task is being blocked out by another task that requires prolonged access to the disk.	No additional information is available.	Reseat or replace disk hardware.
LOG_INFO	Disk Manager, 02: File Renamed	This log is generated when a corrupted file is opened. The system renames the file with the same file name plus the timestamp of when the renaming occurred.	This log occurs when a corrupted file was opened.	The Information and Data fields indicate the original file name, the new file name, and whether the renaming operation was successful.	No action is required.
LOG_INFO	Disk Manager, 11: Files Being Synchronized	This log is generated during system initialization when files are being synchronized between the mated RTC system nodes. This log is used only by Nortel Networks technical support.	This log occurs as part of a request to sync files between the mated RTC system nodes.	The Information field lists the name of the file being synchronized. The Data field lists the name of the database associated with the file.	No action is required.
LOG_INFO	Disk Manager, 12: Data Being Synchronized	This log is generated when data is being synchronized between the mated RTC system nodes or between an application system node and the RTC system nodes. This log is only used by Nortel Networks technical support.	This log occurs as part of a request to sync data between the mated RTC system nodes or between an application system node and the RTC system nodes.	If the data transfer failed, the Information and Data fields indicate that the data transfer failed, the name of the database with the problem, and the reason for the failure (database semaphore unavailable, failure of data transfer mechanism, or database size mismatch). If the data transfer is successful, the Information and Data fields indicate the progress of the data transfer process.	If the data transfer has failed, contact your next level of support. Otherwise, no action is required.
LOG_INFO	Disk Manager, 13: Directories	This log is generated during system initialization to indicate the names of the SS7 directories. This log is used only by Nortel Networks technical support.	This log occurs as part of system initialization.	The Information and Data fields indicate the directory paths for the SS7 directories.	No action is required.

LOG_INFO	EDP Messaging Layer, 07: Connection Audit	This log indicates that an EDP connection was found to be disabled.	A system error has occurred.	An audit checks the status of every EDP connection. The log indicates that at least one of these connections was unexpectedly found to be disabled. Corrective action was taken by the audit to re-establish the disabled connection(s).	Corrective action was taken by the audit to recover the connection. Should this log continue to be generated by a card or system for an extended period of time contact your next level of support.
LOG_INFO	Event Records, 03: Event Records Lost	The system generates this log when event records were generated but discarded before they could be transmitted. The log indicates how many logs were discarded.	A connection to a downstream processor was not established when event records were generated, or the Event Record facility was in an overflow state.	N/A	N/A
LOG_INFO	External Transaction Facility, 02: Failure During Message Receive	This log is generated when a failure is detected while receiving an HMI transaction message.	The OAM&P workstation may be down, or the network connection between the OAM&P workstation and the USP may have failed.	The Information field describes the failure condition.	Determine the status of the OAM&P workstation and network components. If no components are determined to be faulty, report this log to your next level of support.
LOG_INFO	File Purge, 10: stat call problem	File purge task could not get file information present in "sd0/tmp" dir.	File might have already been deleted.	The Information field describes the information about the status of a file	No action is required.
LOG_INFO	FTP Server, 01: FTP full access enabled	This log indicates that the FTP server access privileges for a given user have been changed from secure to full access.	A user, such as the Nortel Networks technical support, has changed the FTP server access privileges for a given user.	The specified user has the complete read/write access to the file system via FTP. Please refer to the Secure FTP Server documentation for details on enabling and disabling full access.	No action is required, unless the specified user should not be granted FTP full access.

LOG_INFO	FTP Server, 02: FTP full access disabled	This log indicates that the FTP server access privileges for a given user have been changed from full access to secure access.	A user, such as the Nortel Networks technical support, has changed the FTP server access privileges for a given user.	The specified user has secure (normal) access to the file system via FTP. This is the normal mode of operation. Please refer to the Secure FTP Server documentation for details on enabling and disabling full access.	No action is required.
LOG_INFO	FTP Server, 03: FTP server event	This log provides the information about certain FTP sever events.	A FTP server event that worth capturing in a log has occurred,	None.	No action is required.
LOG_INFO	Gateway Screening, 01: MSU Rejected by GWS	This log is issued when an MSU has been filtered by the GWS function (removed from the payload path due to GWS criteria rules).	The MSU contained a value in one of the screening fields that prevented it from passing the screening.	The Information and Data fields display the following information: MSU Rejected: Screen Set = ss name, MSU = xxxx xxxx xxxx ... where: name = name of the incoming link or path. ss = name of the GWS screening set that rejected the MSU. xxxx = raw MSU in hexadecimal dump format.	No action is required, the MSU was properly rejected by the GWS function. This is normally expected when a screened MSU arrives. However, you may want to look at the screened MSU to ensure that it is in fact an MSU that should be screened, particularly if several of these logs appear unexpectedly. You also may want to update the GWS criteria to remedy unexpected rejections.

LOG_INFO	Gateway Screening, 02: MSU Ignored by GWS	This log is generated when an MSU is filtered by the GWS function (removed from the payload path due to GWS criteria rules). Specifically, the MSU satisfied the Ignore criterion. This log is only used by Nortel Networks technical support.	The MSU contained a value in one of the screening fields that prevented it from passing the screening.	The Information and Data fields display the following information: MSU Ignored: Screen Set = ss name, MSU = xxxx xxxx xxxx ... where: name = name of the incoming link or path. ss = name of the GWS screening set that ignored the MSU. xxxx = raw MSU in hexadecimal dump format.	No action is required, the MSU was properly ignored by the GWS function. This is normally expected when a screened MSU arrives. However, you may want to look at the screened MSU to ensure that it is in fact an MSU that should be screened, particularly if several of these logs appear unexpectedly.
LOG_INFO	Global Title Translations, 06: Route on Global Title	This log is generated to indicate that the message was route on Global Title.	The Global Title Identifier was set to route on Global Title.	The Information and Data fields indicate the MSU was a route on Global Title	No action is required.
LOG_INFO	Global Title Translations, 07: Address Indicator shows GTI Type NOT 2	This log was generated to indicate that the Address Indicator shows that GTI type is NOT 2	The Global Title Indicator was invalid.	The Information and Data fields indicate the MSU had an invalid Global Title Indicator.	No action is required.
LOG_INFO	Global Title Translations, 08: Address Indicator shows GTI Type is 2	This log was generated to indicate that the Address Indicator shows that GTI type IS 2	A valid Global Title Indicator was used.	The Information and Data fields indicate the MSU has a valid Global Title Indicator.	No action is required.
LOG_INFO	Global Title Translations, 09: GTT Network Failure	This log was generated to indicate a GTT Network Failure.	There is no available Remote Point Code.	The Information and Data fields indicate there was no available RPC.	No action is required.

LOG_INFO	Global Title Translations, 10: GTT Failure	This log was generated to indicate GTT Failure.	There was a possible provisioning error or received a global title not provisioned.	The Information and Data fields indicate that the GTT was not able to be translated.	No action is required.
LOG_INFO	Global Title Translations, 12: Network Congestion	This log is generated when global title translation is unable to be performed due to network congestion.	There is high traffic volume and or one or more link(s) are down.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	Global Title Translations, 13: Address Indicator shows GTI Type is 1	This log was generated to indicate that the Address Indicator contains a GTI of 1 (0001).	A valid Global Title Indicator was used.	The Information and Data fields indicate the MSU was a valid Global Title Indicator.	No action is required.
LOG_INFO	Global Title Translations, 14: Address Indicator shows GTI Type is 3	This log was generated to indicate that the Address Indicator contains a GTI of 3 (0011).	A valid Global Title Indicator was used.	The Information and Data fields indicate the MSU was a valid Global Title Indicator.	No action is required.
LOG_INFO	Global Title Translations, 15: Address Indicator shows GTI Type is 4	This log was generated to indicate that the Address Indicator contains a GTI of 4 (0100).	A valid Global Title Indicator was used.	The Information and Data fields indicate the MSU was a valid Global Title Indicator.	No action is required.
LOG_INFO	Global Title Translations, 16: Remote subsystem is unavailable	This log was generated to indicate that the remote subsystem found as a result of the GTT translation is unavailable.	Remote subsystem is unavailable	The Information and Data fields indicate a remote subsystem failure	No action is required.
LOG_INFO	HMI Server, 10: Mate Fail	The system generates this log when an HMI server is unable to replicate a transaction to the mate RTC system node.	The communication to the mate RTC system node via the internal ATM network is not available. The HMI server is unable to replicate a transaction to the mate as required.	The text field indicates the condition.	If the mate RTC system node or both CC system nodes are disabled, recover them by following the appropriate actions in the USP Fault Management Manual.
LOG_INFO	HMI Server, 20: Max Servers	This log indicates that the maximum number of supported USP GUI sessions are active.	There are multiple logins from OAM&P workstations.	The Information field indicates the condition.	No action is required.
LOG_INFO	HMI Server, 27: Communication Failure	The HMI server task generates this log when it detects an abnormal termination of a USP GUI session.	An error has occurred with the interface to the USP application session.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.

LOG_INFO	HMI Server, 30: Incompatible Version	This log indicates that the an incompatible USP GUI has attempted to log into the STP.	The STP is running a newer version than the GUI.	The Information field indicates the version of the USP GUI.	Upgrade USP GUI.
LOG_INFO	HMI Server, 31: Invalid User Id	This log indicates that a user tried to log into the USP GUI with an invalid userid.	A user entered an invalid user id.	The Information field indicates the name of the user id attempting to log in.	Enter a valid user id.
LOG_INFO	HMI Server, 32: User Locked Out	This log indicates that a user who is attempting to log in is been locked out.	The system administrator has locked out some or all other users.	The Information field indicates the user id of the user who is attempting to log in.	No action is required.
LOG_INFO	HMI Server, 34: Hmisvr Task Killed	This log indicates that the Hmisvr task is killed because a callback function failed to return.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	No action is required.

LOG_INFO	HSL SAAL Event, 01: Link Failure	This log is generated to report the reasons for a HSL (SAAL) signaling link failure.	The Remote Release, Protocol Error, and Too long without credit errors indicate hardware or software problems on the far end. The Stop Received from MTP3 indicate that the cause comes from the levels above SAAL Level 2.	The following information is displayed: L2 Signaling Link Failure link_name, failure_reason: ss where: ss = internal ID for link The failure_reason variable has the following valid values: - Stop Received from MTP3 - Release received from SAAL = The local SAAL stack has failed the link. - Processor Outage - Protocol Error = SAAL L2 stack has detected a protocol error - Remote Release = Remote Release Management Initiated - LM Error Rate Monitor = link error rate has exceeded defined limits - Too long without credit - Alignment not successful - Proving not successful - Remote Release - Protocol Error = The link at the far end was failed due to non management events.	??
LOG_INFO	HSL SAAL Event, 02: Link Congestion	This log is generated when congestion events are present in an SS7 SAAL link.	This log occurred due to facility errors or over-engineering of traffic.	The Information and Data fields indicate the name of the affected link, an internal link ID, and a congestion indication (Onset of Congestion, Abatement of Congestion, or MSU Discard due to Congestion).	Verify that the associated application system node running SS7 and its related equipment are functioning properly.

LOG_INFO	HSL SAAL Event, 03: Link State Change	This log is generated to inform you of the SAAL (Level 2) state of a link, especially concerning link alignment. This log is used only by Nortel Networks technical support.	SAAL link activity state changes respond to any Level 2 events including facility failure, manual activation, and deactivation.	The Information and Data fields indicate the name of the link that changed its state, and the new SAAL state.	Verify that the associated application system node running SS7 and its related hardware are functioning properly.
LOG_INFO	IPS7, 02: IPS7 Protocol Violation	There is a IPS7 protocol error involving a message received from, or transmitted to, the Application Server Processor.	An error has occurred while processing a message received from, or sent to, an ASP. - There is a local or remote facility problem. - There is a message corruption. - The USP does not support the given version of the protocol used to deliver the message.	The Information and Data fields describe the error.	There is a local or remote facility problem contact the remote facility. Contact your next level of support.
LOG_INFO	IPS7, 03: IPS7 Path State Change	This log indicates that an Application Server Processor Path has changed states.	A path changed from one state to another.	The Information and Data fields indicate the path that changed state. Information about the state transition is also included.	No action is required.
LOG_INFO	IPS7, 04: IPS7 Event Information	This log provides information for Nortel Networks technical support.	Various activities are reported.	The Information and Data fields provide Application Server Processor event information.	No action is required.
LOG_INFO	IPS7, 05: IPS7 ASP Activity Change	This log provides information for Nortel Networks technical support.	Various activities are reported.	The Information and Data fields provide Application Server Processor activity information.	No action is required.

LOG_INFO	IPS7, 06: IPS7 Protocol Violation	This log indicates that some messages sent from the Application Server were discarded by the USP	The messages received from the Application Server were discarded because of one of the following reasons: - The Network ID sent from the AS is not datafilled on the USP. - No Network ID was sent from the AS and the USP cannot further route the message without the Network ID.	The Information and Data fields give the count of the total number of messages that were discarded per IP link card in the last 5 minutes	Ensure that the Application Servers are sending messages with correct Network ID's which are datafilled on the USP. Contact your next level of support.
LOG_INFO	IPS7, 07: IPS7 AS Activity Change	This log provides information for Nortel Networks technical support.	Various activities are reported.	The Information and Data fields provide Application Server activity information.	No action is required.
LOG_INFO	Journal Files, 01: Journal File Entry	This log reports any OAM provisioning command execution. This log is used only by Nortel Networks technical support.	OAM provisioning was done.	The Information and Data fields indicate specifics to the provisioning: -ip address and id of the user doing the provisioning	-provisioning command including parameters values
LOG_INFO	Journal Files, 01: Journal File Entry	This log reports any SS7 provisioning. This log is used only by Nortel Networks technical support.	SS7 provisioning was done.	The Information and Data fields indicate specifics to the provisioning: -ip address and id of the user doing the provisioning - provisioning command -any error messages generated	No action is required.
LOG_INFO	Log Facility, 07: New Log Period Begun	The log facility generates this log when a new log collection period starts.	A new period starts for the following reasons: A user requested a new log collection period. A time of day change was made. The current log collection period reached its expected end time. The current log collection period reached its maximum log capacity.	The Information field indicates that a new log collection period was started, and the specific event that caused it.	No action is required.

LOG_INFO	Log Facility, 08: Log Loss	The log facility generates this log when one or more log messages were generated but lost in the system.	There were more log events generated than the log subsystem could handle.	The Information field indicates the number of logs lost by the system (2 bytes), the system node that sent the log (4 bytes), the received sequence number (2 bytes) and the expected sequence number (2 bytes.)	No action is required.
LOG_INFO	Log Facility, 09: Some Alarms Resent	The log facility generates this log after isolation is cleared and some alarms had been generated prior to isolation.	Alarm logs can be lost between the time an extension CAM shelf becomes isolated, and the time isolation is detected.	The Information field indicates the number of alarm logs resent.	No action is required.
LOG_INFO	Log Facility, 10: Traceback Generated	The log facility generates this when a software error has occurred.	An internal error has occurred.	In some instances, several logs are generated with information split over each of the logs. The text field indicates the sequence number of the log for each instance. The data area of this log captures debugging information to help determine the route cause of the error.	Contact your next level of support.
LOG_INFO	Log Facility, 11: System Log Generated	The Application audit has identified one or more records in the Application Database that contain data inconsistencies. An audit report has been generated and may be found in the directory specified in the data portion of the log.	In an application local subsystem, an indirect routing method has been selected and one or more records have been found in the database with a ported status value of "ported across" or "not known to be ported".	The data field contains the location in which the audit report can be obtained on any enabled RTC.	Review USP and LSMS datafill for correctness.
LOG_INFO	M2PA, 01: M2PA Info	This log provides information for Support	Report of an activity.	The information and DATA fields report the information.	No action is required.

LOG_INFO	M2PA, 02: M2PA State Change	This log is generated to inform you of the M2PA state of a link.	M2PA state changes respond to any events that it may experience such as link failure, activation and deactivation.	The Information and Data fields indicate the name of the link that changed its state, and the M2PA state.	Verify that the associated application system node running SS7 and its related hardware are functioning properly.
LOG_INFO	M2UA, 01: M2UA Info	This log provides information for Support	Report of an activity.	The information and Data fields report the information.	No action is required.
LOG_INFO	M2UA, 02: M2UA State Change	This log is generated to inform you of the M2UA state of a link.	M2UA state changes respond to any events that it may experience such as link failure, activation and deactivation.	The Information and Data fields indicate the name of the link that changed its state, and the M2UA state.	Verify that the associated application system node running SS7 and its related hardware are functioning properly.
LOG_INFO	MSU Trapping, 01: Facility State Change	The system generates this log when the MSU Trace facility experiences a state change.	A user initiated a state change, or a subsequent RTC system node state change required MSU Trace be deactivated.	The Information and Data fields provide the new MSU Trace state - active or inactive.	No action is required.
LOG_INFO	MSU Trapping, 02: OAM&P Workstation Disconnect	The system generates this log when an OAM&P workstation running MSU Trace is unexpectedly disconnected from the USP.	An OAM&P workstation was disconnected from the USP.	The Information and Data fields provide the IP address of the disconnected OAM&P workstation and the connection ID that the OAM&P workstation held on the USP.	No action is required.

LOG_INFO	MTP Level 2, 01: Link Failure	This log is generated to report the MTP Level 2 reasons for a signaling link failure.	The Excessive Delay of Ack, Excessive Error Rate (SUERM), and Excessive L2 Congestion errors indicate problems with the associated Link system node. The Abnormal FIB/BSN Received, Unexpected SIO received, Unexpected SIN received, and Unexpected SIE received errors indicate software or hardware problems on the far end. The Stop Received from L3 and SIOS received errors indicate that the cause comes from the levels above MTP Level 2.	The Information and Data fields display the failure reason, and the linkset name, linkset pointcode and SLC of the failed link.	If the failure reason is Excessive Delay of Ack, Excessive Error Rate (SUERM), or Excessive L2 Congestion, verify that the associated Link system node and its related equipment are functioning properly. Otherwise the error is related to MTP Level 3 or the far end.
LOG_INFO	MTP Level 2, 02: Link Congestion	This log is generated when congestion events are present in MTP Level 2.	This log occurred due to facility errors or over-engineering of traffic.	The Information and Data fields indicate the name of the affected link, an internal link ID, and a congestion indication (Onset of Congestion, Abatement of Congestion, or MSU Discard due to Congestion).	Verify that the associated application system node running SS7 and its related equipment are functioning properly.
LOG_INFO	MTP Level 2, 03: Buffer Congestion	This log is generated when there are buffer congestion events in MTP Level 2.	This log occurred because of facility errors.	The Information and Data fields display a congestion indication (Onset of Congestion or Abatement of Congestion).	Verify that the associated application system node running SS7 and its related hardware are functioning properly.

LOG_INFO	MTP Level 2, 04: Link State Change	This log is generated to inform you of the MTP Level 2 state of a link, especially concerning link alignment. This log is used only by Nortel Networks technical support.	MTP Level 2 activity state changes respond to any events at MTP Level 2, including facility failure, manual activation, and deactivation.	The Information and Data fields indicate the name of the link that changed its state, and the new MTP Level 2 state.	Verify that the associated application system node running SS7 and its related hardware are functioning properly.
LOG_INFO	MTP Level 3 Event, 01: Changeover	An MTP link changeover has occurred. The signaling link has stopped carrying traffic.	Several conditions can cause this log: The link lost alignment. (MTP Level 2 detect failure) The link was inhibited by either the local or the remote end. The link was deactivated locally. There is a loss of the host Link system node/shelf/CC system node.	The Information and Data fields indicate the signaling link ID.	Take action according to the specific cause.
LOG_INFO	MTP Level 3 Event, 02: Changeback	There was a signaling link changeback. The link is now able to carry signaling traffic.	The problem that caused the corresponding changeover was repaired. For more information, see the causes for the corresponding changeover log.	The Information and Data fields indicate the signaling link ID.	No action is required.
LOG_INFO	MTP Level 3 Event, 03: Restoration	A changeback to a previously failed linkset has occurred.	The problem that caused the corresponding changeover was repaired.	The Information and Data fields indicate the name of the link coming back into service.	No action is required.
LOG_INFO	MTP Level 3 Event, 04: Remote Processor Outage	The link is aligned, but is experiencing remote processor outage. The far end of the link is unable to handle the traffic received, so the traffic is blocked at both ends.	The traffic-processing modules at the far end office of this link have failed.	The Information and Data fields indicate the link name.	No action is required.
LOG_INFO	MTP Level 3 Event, 05: Remote Processor Outage Cleared	The remote processor outage has been cleared and the link is aligned. The link can now carry traffic.	Traffic processing at the far end of the link has recovered.	The Information and Data fields indicate the link name.	No action is required.

LOG_INFO	MTP Level 3 Event, 06: Signaling Link Congestion	A signaling link is congested.	There are several possible causes: There is a local or remote link failure. Signaling resources are insufficient. The link is experiencing a lot of retransmission. There is an unexpected brief traffic surge.	The Information and Data fields indicate the signaling link ID of the congested link and the level of congestion, which is 1, 2, or 3. The system will discard messages with priorities lower than the current level.	Recover any local link failures, or provision additional link resources.
LOG_INFO	MTP Level 3 Event, 07: Congestion Cleared	A previously congested link has become uncongested.	Traffic has been reduced, or resources have been restored or augmented.	The Information and Data fields indicate the signaling link ID of the congested link.	No action is required.
LOG_INFO	MTP Level 3 Event, 08: MSU Discarded - Congestion	The system has discarded an MSU because of congestion.	A specific signaling link transmit buffer is full.	The Information and Data fields indicate the ID of the signaling link where the congestion is.	No action is required.
LOG_INFO	MTP Level 3 Event, 09: Restoration Commenced	A linkset is no longer available to carry SS7 traffic.	All links on the linkset are unavailable.	The Information and Data fields indicate the linkset name. The following information is also displayed: dd routesets are no longer available Where: dd = the number of routesets that have failed due to the loss of this linkset.	Determine the status of the individual links, and take appropriate action to recover them.

LOG_INFO	MTP Level 3 Event, 10: Linkset Recovered	The linkset has recovered.	A linkset has become available for traffic.	The Information and Data fields indicate the linkset name. The following information is also displayed: dd routesets have become available Where: dd = the number of routesets that have recovered due to the recovery of this linkset.	No action is required.
LOG_INFO	MTP Level 3 Event, 13: Destination Lost	A routeset can no longer carry traffic.	No links are available in the linkset group of the routeset. No paths are available in the application server assignment.	The Information and Data fields indicate the destination routeset that is unavailable. The following information is also provided: Network Appearance = nn PC = point code, where: point code = the full or partial point code (member, cluster, or network)	Restore the links. Restore the paths.
LOG_INFO	MTP Level 3 Event, 14: Destination OK	The routeset is now available to carry traffic. The system generates this log only when the routeset is first provisioned and its links or paths are available for traffic.	A link in the linkset group of the routeset has been recovered. A path in the ASP routeset assignment has been recovered.	The Information and Data fields indicate the destination routeset that is available. The following information is also provided: Network Appearance = nn PC = point code Where point code = the full or partial point code (member, cluster, or network)	No action is required.

LOG_INFO	MTP Level 3 Event, 15: Adjacent SP Lost	Traffic access to the adjacent signaling point is not available.	A linkset has failed.	The Information and Data fields indicate the linkset name.	Recover the linksets the adjacent signaling point uses.
LOG_INFO	MTP Level 3 Event, 16: Adjacent SP Recovered	Traffic access is now available to the adjacent signaling point.	The linkset has been recovered.	The Information and Data fields indicate the linkset name.	No action is required.
LOG_INFO	MTP Level 3 Event, 18: Link Activity State	This log indicates a transition of states for link activation or restoration.	The link state has changed because of activity changes.	The Information and Data fields indicate the signaling link ID, and the current and previous activity states of the link.	No action is required.

LOG_INFO	MTP Level 3 Event, 19: MTP Level 3 Error	An error occurred during MTP Level 3 operations.	Each error is associated with a specific problem. In general, MTP Level 3 has suffered a performance or functional problem. Some problems may be related to difficulties in the local site, while others are related to problems in the SS7 network.	The Information and Data fields indicate which MTP Level 3 error occurred. The following list are the possible error messages and definitions. MTP_BAD_PRIM MTP Level 3 configuration tasks are unable to accept a configuration request. MTP_POOL_EMPTY The system is out of buffers. MTP_TX_FAIL The system is unable to transmit a message to MTP Level 2. MTP_LEN_ERR A request has been rejected because a configuration message is of unexpected length. MTP_SLT_FAIL A signaling link test (SLT) failed. The link will be taken out of service. MTP_BAD_DPC Signaling message handling is unable to deliver an MSU to its requested destination. The MSU is discarded, and a TFP message is sent to the originator of the MSU. MTP_TALLOC_ERR The system is unable to allocate TFrames. MTP_BAD_ID The system does not recognize the resource ID in the request. The request	Contact your next level of support

LOG_INFO	MTP Level 3 Event, 20: TFA Received	A destination routeset route has changed to the allowed state.	A TFA/TCA message was received from the far end, indicating reliable transfer capability is available.	The Information and Data fields indicate: The destination route marked as transfer allowed. The adjacent STP (Linkset name) The destination routeset ID The following information is also provided: rr routesets have become available Where: rr = the number of routesets recovered with this TFA.	No action is required.
LOG_INFO	MTP Level 3 Event, 21: TFP Received	A destination routeset route has changed to the prohibited state.	A TFP/TCP message was received from the far end, indicating reliable transfer capability is not available.	The Information and Data fields indicate: - The destination route marked transfer prohibited - The adjacent STP (linkset name) - The destination routeset ID The following information is also provided: rr routesets are no longer available, where: rr = the number of routesets failed with this TFP.	The problem is at the far end. If the destination no longer has routing, then return local resources to service, or provision additional resources.

LOG_INFO	MTP Level 3 Event, 22: TFR Received	A destination routeset route has changed to the restricted state.	A TFR/TCR message was received from the far end, indicating reliable transfer capability is degraded.	The Information and Data fields indicate: The destination route marked transfer restricted The adjacent STP (linkset name) The destination routeset ID The following information is also provided: rr routesets have become available Where: rr = the number of routesets recovered with this TFR.	The problem is at the far end. If the destination no longer has routing, return local resources to service, or provision additional resources.
LOG_INFO	MTP Level 3 Event, 24: MSU With Unknown SP	An MSU was received for an unknown signaling point.	The system received an MSU for an unknown destination.	The Information and Data fields indicate the point code of the unknown destination.	Monitor and contact the originating point code if this log persists.
LOG_INFO	MTP Level 3 Event, 25: Link Uninhibit Failed	This log indicates a link uninhibit failure.	There is no reply from the far end.	The Information and Data fields indicate the link uninhibit failure and the signaling link ID.	Confirm that routing resources are available to reach the far end. If local resources are available, contact the far end.
LOG_INFO	MTP Level 3 Event, 26: Link Inhibit Denied	This log indicates that a link inhibit request was denied. The system was unable to inhibit a signaling link.	Either the far end or the local end denied the request because it would lose routing to destinations.	The Information and Data fields indicate the link inhibit that was denied and the signaling link ID.	Ensure that alternate routing resources are available for the signaling link users (other links in linkset).
LOG_INFO	MTP Level 3 Event, 27: Link Uninhibited	This log indicates that a signaling link was uninhibited.	A link was successfully uninhibited.	The Information and Data fields indicate the link that was uninhibited and the signaling link ID.	No action is required.

LOG_INFO	MTP Level 3 Event, 28: Link Inhibited	This log indicates that a signaling link has been inhibited.	There was an inhibit request from management at either the local or the remote end of the link.	The Information and Data fields indicate the link that was inhibited and the signaling link ID.	No action is required.
LOG_INFO	MTP Level 3 Event, 29: MTP Event Information	This log provides information for Nortel Networks technical support.	Various activities are reported.	The Information and Data fields provide MTP event information.	No action is required.
LOG_INFO	MTP Level 3 Event, 30: MSU Routing Failure	This log indicates an MSU routing failure. This log is used only by Nortel Networks technical support.	An MSU is routed to a DPC that is inaccessible.	The Information and Data fields provide the following information: send MSU: Unable to route MSU DPC = 0x (hhhhhh) (MSU content) (hhhhhh) = DPC in hexadecimal data (MSU content) = the entire MSU in hexadecimal data.	No action is required.
LOG_INFO	MTP Level 3 Event, 40: Protocol violation	An SNM msg has been received on a network whose protocol does not recognize the msg.	An SNM message was received from the far end, this msg is not expected in this scenario for our network's protocol.	The Information and Data fields indicate: The type of message received and the nature of the violation. The linkset on which the message was received. Hex dump of SNM msg	Verify protocol with far end. Invalid SNM messages should not be received when networks have the same protocol.
LOG_INFO	MTP Level 3 Event, 41: Local Processor Outage	The link is aligned, but is experiencing local processor outage. The link is unable to handle the traffic received, so the traffic is blocked at both ends.	All paths to the AS Master are unavailable.	The Information and Data fields indicate the link name.	Bring one path to the AS Master in service.
LOG_INFO	MTP Level 3 Event, 42: Local Processor Outage Cleared	The local processor outage has been cleared and the link is aligned. The link can now carry traffic.	One or more paths to the AS Master became available.	The Information and Data fields indicate the link name.	No action is required.
LOG_INFO	MTP Level 3 Event, 43: Activated Routeset	Traffic access to the destination has been activated.	The routeset was activated	The Information and Data fields indicate the routeset name.	No action is required.

LOG_INFO	MTP Level 3 Event, 44: Deactivated Routeset	Traffic access to the destination has been deactivated.	The routeset was deactivated.	The Information and Data fields indicate the routeset name.	No action is required.
LOG_INFO	MTP Level 3 Event, 47: Xlist Block Shortage	It is not possible to add a new block to Xlist table to keep a cluster/network routeset member information.	Xlist Table is full.		No action is required.
LOG_INFO	MTP Level 3 OMs, 10: Network Appearance Not Found	This log indicates the network appearance in question is not yet configured. This log is used only by Nortel Networks technical support.	The network appearance is not configured.	The Information and Data fields indicate that NA = nn not found, where: nn = the network appearance number.	No action is required.
LOG_INFO	MTP Level 3 OMs, 11: Record Not Written	This log indicates an SS7 OM application does not write the OM values to the database in the current OM collection cycle, because certain information is not yet available. This log is used only by Nortel Networks technical support.	OM collection is in progress, but the network appearance of the system is not yet configured. Some SS7 OM server callbacks need this information to write OM records to the database. Since information is not yet available, no record will be written in the current collection cycle.	The Information and Data fields indicate that NA = nn not found, where: nn = the network appearance number	No action is required.
LOG_INFO	MTP Level 3 OMs, 12: Data Out Of Sequence	This log indicates the received UDP message from the OM server to the server callback is out of sequence. This log is used only by Nortel Networks technical support.	An internal error has occurred.	The Information and Data fields indicate the message out of sequence. The system expects nn, but gets mm, where: nn = the expected sequence number, and mm = the received sequence number	No action is required.
LOG_INFO	MTP Restart, 12:	MTP Restart Timer T22 expired	T22 conditions not satisfied	Time of expiry. MTP Restart will continue with next phase	None. Network Dependent.
LOG_INFO	MTP Restart, 13:	MTP Restart Timer T23 expired	T23 conditions not satisfied	Time of expiry. MTP Restart will continue with next phase	None. Network Dependent.

LOG_INFO	MTP Restart, 14:	MTP Restart Timer T24 expired	T24 conditions not satisfied	Time of expiry. MTP Restart will continue with next phase	None. Network Dependent.
LOG_INFO	MTP Restart, 15:	MTP Restart Timer T25 expired	T25 conditions not satisfied	Time of expiry. MTP Restart will continue with next phase	None. Network Dependent.
LOG_INFO	MTP Restart, 16:	MTP Restart Timer T26 expired	T26 conditions not satisfied	Time of expiry. MTP Restart will continue with next phase	None. Network Dependent.
LOG_INFO	MTP Restart, 17:	MTP Restart Timer T28 expired	T28 conditions not satisfied	Time of expiry. MTP Restart will continue with next phase	None. Network Dependent.
LOG_INFO	MTP Restart, 18:	MTP Restart Timer T29 expired	T29 conditions not satisfied	Time of expiry. MTP Restart will continue with next phase	None. Network Dependent.
LOG_INFO	MTP Restart, 19:	MTP Restart Timer T30 expired	T30 conditions not satisfied	Time of expiry. MTP Restart will continue with next phase	None. Network Dependent.
LOG_INFO	MTP Restart, 20:	MTP Restart Timer T18 expired	T18 conditions not satisfied	Time of expiry. MTP Restart will continue with next phase	None. Network Dependent.
LOG_INFO	MTP Restart, 21:	MTP Restart Timer T19 expired	T19 conditions not satisfied	Time of expiry. MTP Restart will continue with next phase	None. Network Dependent.
LOG_INFO	MTP Restart, 22:	MTP Restart Timer T20 expired	T20 conditions not satisfied	Time of expiry. MTP Restart will continue with next phase	None. Network Dependent.
LOG_INFO	MTP Restart, 23:	MTP Restart Timer T21 expired	T21 conditions not satisfied	Time of expiry. MTP Restart will continue with next phase	None. Network Dependent.

LOG_INFO	MTP Restart, 24:	MTP Restart Timer T27 has been invoked	None.	Time of forced isolation. MTP Restart isolation option is executing.	None. Provisionable.
LOG_INFO	MTP Restart, 25:	MTP Restart Timer T27 has expired	None.	Stop time of forced isolation. MTP Restart isolation option has completed.	None. Provisionable.
LOG_INFO	MTP Restart, 26:	Full MTP Restart has started	Node isolation.	Timestamp.	None.
LOG_INFO	MTP Restart, 27:	Adjacent MTP Restart has started	Adjacent node isolation.	Timestamp.	None.
LOG_INFO	MTP Restart, 28:	Partial MTP Restart has started	Not Supported.	Timestamp.	None.
LOG_INFO	MTP Restart, 29:	Signaling Point has received a TRM message outside of the MTP Restart time frame	A TRM message has been received while there are no MTP Restart procedures executing and/or T29/T19 have expired.	Timestamp. Link Set.	None.
LOG_INFO	MTP Restart, 31:	Full MTP Restart has ended	All MTP Restart conditions have been satisfied.	Timestamp.	None.
LOG_INFO	MTP Restart, 32:	Adjacent MTP Restart has ended	None.	Timestamp.	None.
LOG_INFO	MTP Restart, 33:	Partial MTP Restart has ended	Not Supported.	Timestamp.	Not Supported.
LOG_INFO	MTP Restart, 34:	Full MTP Restart has achieved sufficient links	ANSI - More than 50% of links have recovered within T22. ITU - More than 50% of links have recovered.	Timestamp.	None.
LOG_INFO	MTP Restart, 35:	Full MTP Restart has achieved sufficient TRAs	all TRAs have been received from adjacent nodes	Timestamp.	None.
LOG_INFO	MTP Restart, 36:	MTP Restart has received a TRA	FE has sent a TRA	Timestamp.	None.

LOG_INFO	MTP Restart, 37:	MTP Restart cannot process the received TRA	Internal error.	Timestamp. LinkSet. Link.	Contact next level support.
LOG_INFO	MTP Restart, 38:	TRW received on an ITU network	Possible error in FE.	Timestamp. LinkSet. NA.	None.
LOG_INFO	Network, 16: Audit Successful	This log indicates that all steps of the network audit have passed	All external network configuration requirements have been met.	No additional information is required.	None
LOG_INFO	Network, 17: Improper File Access Permissions	This log indicates that the NFS server may not have the proper file access permissions set	NFS server may not have the proper file access permissions set	No additional information is required.	Correct NFS server file access permissions
LOG_INFO	Network, 18: RTC Subnet Mask Mismatch	This log indicates that the rtc has a different subnet mask provisioned than the one obtained from the alternate boot server	Mismatch between alternate boot server and rtc provisioning	No additional information is required.	Correct the mismatch in the bootp of the alternate boot server or by modifying the rtc and reloading it.
LOG_INFO	Network, 19: RTC Gateway Mismatch	This log indicates that the rtc has a different gateway provisioned than the one obtained from the alternate boot server	Mismatch between alternate boot server and rtc provisioning	No additional information is required.	Correct the mismatch in the bootp of the alternate boot server or by modifying the rtc and reloading it.
LOG_INFO	Network, 20: RTC IP mismatch	This log indicates that the ABS has a different RTC IP provisioned than the actual RTC IP address	Mismatch between alternate boot server and rtc provisioning	No additional information is required.	Correct the mismatch in the bootp of the alternate boot server or by modifying the rtc and reloading it.
LOG_INFO	OM RDM Utilities, 01: Information	This log is generated when the OM RDM Database Utilities encounter a condition/event of which you should be aware.	A condition/event occurred under normal operating conditions.	The Information and Data fields contain information about the condition/event that occurred.	No action is required.
LOG_INFO	OMs, 02: Information	This log is generated when the OM subsystem encounters a condition/event of which the user should be aware.	A condition/event occurred under normal operating conditions.	The Information and Data fields contain information about the condition/event that occurred.	No action is required.

LOG_INFO	Processor Exception, 04: Initialization Error	The system generates this log during node initialization if an error occurs that will prevent the RTC, CC, or application system node from performing its required functions.	An initialization error has occurred on a system node. The system will attempt to reload the system node.	The Information and Data fields contain information about the problem that occurred, and state that the system will attempt to reload the system node.	No action is required.
LOG_INFO	Processor Exception, 06: Previous exception record	The system generates this log when it recovers from a failure caused by a hardware or software exception. The information contained in this log is a summary of the information captured and generated when the exception occurred originally.	Previously, an internal error had occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_INFO	Processor Exception, 07: Watchdog timeout	The system generates this log when the failsafe timer on a board expires. Typically, this is caused by a runaway task stuck in an endless loop, or some similar software problem. If possible, the system will automatically reload the faulted RTC, CC, or application system node. The logs contain information about tasks that were active at the timer expiry so that the problem can be identified.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_INFO	RDM Utilities, 05: Database Recovery	This log is generated when the RDM utility starts a database recovery operation.	The RDM utility detected an inconsistency in the database during system startup. This error can occur when the USP, or any of its software processes, terminates processing abnormally (for example, a power outage).	The Information and Data fields display the RDM utility error number and return codes. Additional details are also displayed.	No action is required.
LOG_INFO	SCCP Management, 01: Unknown Remote Subsystem	This log is generated when an SSP message sent to the local node contains an unknown remote subsystem.	Either the incorrect remote subsystem or the incorrect concerned point code has been provisioned.	The Information and Data fields indicate the affected point code and subsystem number.	Check the provisioned remote subsystem and concerned point code. If you are unable to determine the problem, contact your next level of support.

LOG_INFO	SCCP Management, 02: SCCP Msg Syntax Error	This log is generated because the message contains a syntax error. (For LLCP, the data length must be 6 bytes and the received message had a length other than 6 bytes).	The originator of the message did not format the message correctly.	No additional information is provided.	No action is required.
LOG_INFO	SCCP Management, 03: LSS Allowed	A local subsystem availability state has changed to allowed.	Enough local subsystem instances have become allowed to meet or exceed the minimum instance rule provisioned for the local subsystem.	The Information and Data fields display an SSID number that indicates which local subsystem has become allowed.	No action is required.
LOG_INFO	SCCP Management, 04: LSS Prohibited	A local subsystem availability state has changed to prohibited.	No local subsystem instances are available, so the local subsystem availability state is set to prohibited.	The Information and Data fields display an SSID number that indicates which local subsystem has become prohibited.	No action is required.
LOG_INFO	SCCP Management, 05: LSS Instance Activated	A local subsystem instance's administrative state has been set to activate.	The user has initiated a manual activation of the local subsystem instance or the auto recovery sequence has re-asserted the administrative state after an application node has recovered from a reset.	An instance number will be in the log to indicate which local subsystem instance has been activated.	No action is required.
LOG_INFO	SCCP Management, 06: LSS Instance Deactivated	A local subsystem instance administrative state has been set to deactivate.	The user has initiated a manual deactivation of the local subsystem instance or the auto recovery sequence has re-asserted the administrative state after an application node has recovered from a reset.	The Information and Data fields display an instance number that indicates which local subsystem instance has been deactivated.	No action is required.
LOG_INFO	SCCP Management, 07: LSS Offline	A local subsystem instance's administrative state has been set to offline.	The user has initiated a lock of the application system node or the auto recovery sequence has re-asserted the administrative state after an application system node has recovered from a reset.	The Information and Data fields display an instance number that indicates which local subsystem instance has been offlined.	No action is required.

LOG_INFO	SCCP Management, 08: LSS Prohibited for Routing	An attempt was made to route a SCCP message to a Local Subsystem that is in prohibited state.	The originator of the message has not yet updated the availability state of the localsubsystem residing on this node.	The Information and Data fields display a local subsystem ID to identify the local subsystem instance.	No action is required.
LOG_INFO	SCCP Management, 09: LSS Instance Not Allowed	An attempt was made to route an SCCP message to a Local Subsystem Instance that is not in allowed state.	The instance was deactivated but the distribution table was not updated yet.	The Information and Data fields display a local subsystem instance index that identifies the local subsystem instance.	No action is required.
LOG_INFO	SCCP Management, 10: SCRC No Buffer	An attempt was made to allocate a buffer for SCRC.	The destination local subsystem instance is temporarily in congested state.	No additional information is provided.	No action is required.
LOG_INFO	SCCP Management, 11: Wrong Address Indicator	A wrong address indicator was detected in Cdpa field.	An internal error has occurred.	The Information and Data fields contain the value of the wrong address indicator.	Contact your next level of support.
LOG_INFO	SCCP Management, 14: LSS Instance Prohibited	A local subsystem instance availability state has changed to prohibited.	A deactivate command has been received by the local subsystem instance and the normal availability state is prohibited.	The Information and Data fields contain a subsystem number and instance number that indicate which local subsystem instance has become prohibited.	No action is required.
LOG_INFO	SCCP Management, 15: LSS Instance Allowed	A local subsystem instance availability state has changed to prohibited.	An activate command has been received by the local subsystem instance and the normal availability state is allowed.	The Information and Data fields contain the subsystem number and instance number that indicate which local subsystem instance has become allowed.	No action is required.
LOG_INFO	SCCP Management, 16: LSS Instance Congestion	A local subsystem instance availability state has changed to congestion.	SCCP Routing has informed SCCP Management that the local subsystem instance is experiencing internal congestion.	The Information and Data fields contain the subsystem number and instance number that indicate which local subsystem instance has become congested.	No action is required.

LOG_INFO	SCCP Management, 17: LSS Instance Abatement	A local subsystem instance availability state has changed to available.	SCCP Routing has informed SCCP Management that the local subsystem instance congestion has abated.	The Information and Data fields contain the subsystem number and instance number that indicate which local subsystem instance congestion has abated.	No action is required.
LOG_INFO	SCCP Management, 18: LSS Instance Not Initialized	A local subsystem instance availability state is not initialized.	This availability state usually exists when a local subsystem instance is first provisioned since no data or database exist on the instance.	The Information and Data fields contain the subsystem number and instance number that indicate which local subsystem instance is not initialized.	No action is required.
LOG_INFO	SCCP Management, 19: LSS Instance Initializing	A local subsystem instance availability state has changed to initializing.	The application resident on the local subsystem instance is initializing data, databases, etc.	The Information and Data fields contain a subsystem number and instance number that indicate which local subsystem instance has become allowed.	No action is required.
LOG_INFO	SCCP Management, 20: LSS Instance Suspended	A local subsystem instance availability state has changed to suspended.	The application resident on the local subsystem instance has changed the availability state to suspended to indicate that it is no longer able to carry traffic. After automatic corrective action, the application will bring itself back to allowed.	The Information and Data fields contain the subsystem number and instance number that indicate which local subsystem instance has become suspended.	No action is required.
LOG_INFO	SCCP Management, 21: LSS Instance Failed	A local subsystem instance availability state has changed to failed.	The node has become disabled and SCMG has marked the node as failed. The node should recover without user intervention.	The Information and Data fields contain the subsystem number and instance number that indicate which local subsystem instance has changed state to failed.	No action is required unless the node does not recover. If the node does not recover, contact your next level of support.

LOG_INFO	SCCP Management, 22: LSS Not Provisioned	The local subsystem is not provisioned.	The SS7 network setup is not correct, or the local subsystem is not yet provisioned.	A SCCP message cannot be delivered to a local subsystem because the local subsystem is not provisioned on the USP.	Check the network configuration in order to detect the node(s) sending messages to a local subsystem that is not provisioned, then correct the network setup or provision the required system on the USP.
LOG_INFO	SCCP Management, 23: SCMG Local Subsystem Instance Isolated	A local subsystem instance's availability state has been set to isolated.	A local subsystem instance availability state has been set to isolated since the extension shelf where it resides is isolated. Once the extension shelf isolation clears, the lssi state will go back to its previous availability state.	An instance number will be in the log to indicate which local subsystem instance has been offlined.	No action is required. Note: This log is not used in SSR2.1. (Nodes on an isolated shelf are taken down and then rebooted when isolation clears. This log may be used in future versions.)
LOG_INFO	SCCP Management, 24: SCMG Remote Point Code Congestion	The Congestion level of an ITU SCCP RPC has changed.	There are two probable causes for the congestion level of a Remote Point Code to be increased, remote (network) congestion, or local congestion. In the case of remote (network) congestion, a network message (TFC) was received about the concerned point code, indicating that the remote node has gone into congestion.	The affected Remote Point Code, the direction in which congestion is progressing, and the associated internal congestion level will be reported in the log.	No action is required. Note: This log should only be seen in ITU networks. These congestion levels represent an internally calculated congestion status.
LOG_INFO	SCCP Management, 26: RSS Prohibited	A RSS availability state has changed to prohibited because of receiving an SSP.	RSS failure in the far end.	The Information and Data fields display that which RSS has become prohibited.	Correct RSS far end failure condition.

LOG_INFO	SCCP Management, 27: RSS Allowed	A remote subsystem availability state has changed to allowed.		The Information and Data fields display an SSID number that indicates which remote subsystem has become allowed. No action is required.	
LOG_INFO	SCCP Management, 28: LSS Activated	A local subsystem administration state has changed to ACTIVATED.	The Local Subsystem has been manually put into the activation state.	The Information and Data fields display an SSID number and a network appearance number that indicates which local subsystem has become activated.	No action is required.
LOG_INFO	SCCP Management, 29: LSS Deactivated	A local subsystem administration state has changed to DEACTIVATED.	The Local Subsystem has been manually put into the activation state.	The Information and Data fields display an SSID number and a network appearance number that indicates which local subsystem has become deactivated.	No action is required.
LOG_INFO	SCCP Management, 30: Remote User Part Unavailable	The system generates this log when it detects that the SCCP user part on a far end office has become unavailable.	The SCCP user part on the far end office has failed.	The data will contain the affected pointcode, and the cause.	No action is required.
LOG_INFO	SCCP Management, 31: Remote User Part Available	The system generates this log when it detects that the SCCP user part on a far end office has become available.	The SCCP user part on the far end office has returned to service.	The data will contain the affected pointcode.	No action is required.
LOG_INFO	SCCP Management, 32: SCCP Routing not supported for message type	The USP does not support SCCP routing of certain message types, LUDT for example. If an unsupported message type is received which requires SCCP routing, the message will be discarded and this log produced. This is a throttled log to protect system resources.	SCCP Routing not supported for message type.	The data will contain the first 255 bytes of the message.	Determine who sent the message and correct the routing scenario.
LOG_INFO	SCCP OMs, 09: Network Appearance Not Found	Indicates the network appearance in question is not yet configured. This log is used only by Nortel Networks technical support.	The network appearance is not configured.	The Information and Data specifics indicate that NA = nn not found, where: nn = the network appearance number.	No action is required.

LOG_INFO	SCCP OMs, 10: Data Out Of Sequence	This log indicates the Received UDP message from the OM server to the server callback is out of sequence. This log is used only by Nortel Networks technical support.	An internal error has occurred.	The Information and Data fields provide the message that is out of sequence. The system expects nn but receives mm, where: nn = the expected sequence number mm = the received sequence number	No action is required.
LOG_INFO	SCCP OMs, 11: Record Not Written	This log indicates the SS7 OM application has not written the OM values to the database in the current OM collection cycle, because certain information is not yet available. This log is used only by Nortel Networks technical support.	OM collection is in progress, but the system network appearance is not configured. Some SS7 OM server callbacks need this information to write OM records to the database. Since the information is not yet available, no record will be written in the current collection cycle.	The Information and Data fields indicate that NA = nn was not found, where: nn = the network appearance number.	No action is required.
LOG_INFO	SCCP OMs, 13: SCCP LSS Version Mis-match	This log indicates that the Local Subsystem OM application parser received a message with an unexpected version number. This log is used only by Nortel Networks technical support.	An internal error has occurred.	The Information and Data fields provide the expected and received version number. The system expects nn but receives mm, where: nn = the expected version number mm = the received version number	No action is required.

LOG_INFO	SCTP, 01: SCTP Link Failure	This log is generated to report the cause of a link failure in SCTP.	> Shutdown message received - Source and destination endpoint are the same - Abort message received - Unacked list is too big - No free port available - Port already in use - Dual instance Name - Received abort from application - Maximum of consecutive heartbeat misses - Multiple timeouts on the same data message - Passed the number of retransmits	The Information and Data fields display the following information: - Reason of association failure - Association ID - Previous SCTP state	- Verify the provisioning - Verify the network utilization
LOG_INFO	SCTP, 02: SCTP Link Congestion	This log is generated when congestion is present in the network.	The network is running into congestion - A sudden network outage for a short period of time - Physical connection has been lost for a short period of time	The Information and Data fields display the following information: - Reason of association congestion - Association ID	- Verify the physical portion of the network - Verify the traffic load of the network
LOG_INFO	SCTP, 03: SCTP Buffer Congestion	This log is generated when there are buffer congestion events in SCTP. NOTE: This log is reserved for future use.	This log occurred because of facility errors.	The Information and Data fields display a congestion indication (Onset of Congestion or Abatement of Congestion).	Verify that the associated application system node running SS7 and its related hardware are functioning properly.
LOG_INFO	SCTP, 04: SCTP State Change	This log is generated to inform you of an SCTP state change of a association. This log is used only by Nortel Networks technical support.	SCTP state changes respond to any events that SCTP may experience like link failures, application messages or other special events.	The Information and Data fields display the following information: - Reason of association state change - Association ID - Previous SCTP state	Verify that the associated application system node running SS7 and its related hardware are functioning properly.
LOG_INFO	SCTP, 05: SCTP Info	This log provides information for Nortel Networks technical support.	Various activities are reported.	The Information and Data fields display the following information: - Association ID	No action is required.

LOG_INFO	Signaling Network Management, 01: Link or Path Suspension	Signaling link or path restoration is suspended for the time period associated with the T34 timer because of link or path alignment oscillation. The link or path has been in and out of service for an interval less than T33.	A recently aligned link or restored path has failed.	The Information and Data fields indicate the link or path suspension, and provide the signaling link ID or path ID.	Wait for time interval T34 to expire. Restoration attempts will resume.
LOG_INFO	Signaling Network Management, 02: False Link Congestion	This log indicates false link congestion, or a link in congestion for a long period of time T31. The link is taken out of alignment.	There could be hardware problems at the local end of the link, there could be true congestion. Long-term congestion can be caused by insufficient signaling resources, or a continuous overload of traffic.	The Information and Data fields provide the signaling link ID and indicate that the system detects false link congestion.	The USP will resume link restoration after some diagnostics. If congestion persists, align more resources or reduce the traffic load.
LOG_INFO	Signaling Network Management, 03: Repeated Link or Path Activation Failure	This log indicates a repeated link activation or path restoration failure. A link or path has failed to align despite repeated attempts to restore it, for a time period of T19.	There is a facility failure, or the far end is not attempting to align.	The Information and Data fields indicate repeated activation failure and provide the signaling link ID or path ID.	The link or path will continue to attempt to restore and align. Test facilities for quality. Contact the far end for alignment status.
LOG_INFO	Signaling Network Management, 04: SLT Passed	This log indicates a signaling link test (SLT) was successfully completed.	The system has completed the test protocol with the far end.	The Information and Data fields indicate the SLT passed and provide the signaling link ID.	No action is required.
LOG_INFO	Signaling Network Management, 05: SLT Failed	This log indicates a signaling link test (SLT) failed. The signaling link will fail, and the system will attempt to restore it.	There are several possible causes: The link is provisioned incorrectly either locally or remotely. There are facility errors. An overload at processing elements is preventing the exchange of test messages.	The Information and Data fields indicate the SLT failed, and provide the signaling link ID.	Verify provisioning of the link and the linkset with the far end. Confirm the facility quality and processor capacity.

LOG_INFO	Signaling Network Management, 06: Link or Path Audit	These logs are associated with the discovery and correction of link or path state problems.	Depend on specific link/path state problem, but in general, the system is experiencing resource exhaustion. Causes for some of problems	Link State Audit Problems: No Timer Buffer: Unable to start the wait timer. Forced Inactive: Incorrect state and is forced to an inactive state. Please Deactivate: Incorrect state, and the system failed to send the correction. Mission Slice Failed: No host card is available. SLM: Sent AuditLinkState Qry: Link/Path has a working card. Permission to be active CurrLink: Message reply was received, but not for the correct link or path. SLM Audit Problems: Sent OUT_SVC: State mismatch. SLM successfully sent SS7_MSG_OUT_SVC message. Sent RPO: An RPO is not asserted. SS7_MSG_REM_PR_OUT is successfully sent. Sent StopL2: State mismatch. Stopped MTP Level 2. Unexpected state: The Level 2 state is unexpected.	Provide details about the problem and the action the system has taken, as well as the associated signaling link/path ID. The information provided may include the followings: Link/Path State Audit Problem: No Timer Buffer Forced Inactive Please Deactivate Mission Slice Failed SLM: Sent AuditLinkState Qry, Link/Path = nn, where: nn = the current link/path ID SLM: AuditState, CurrLink/Path = nn, RcvdLk/Path = mm, where: nn = expected link/path ID mm = received link/path ID SLM Audit Problem: OUT_SVC Send failed, RC = ss, where: ss = the return code. RPO_OK Send failed, RC = ss, where: ss = the return code Unexpected state = hh, where hh = the unexpected Level 2 state value in hexadecimal. SLM: AuditLinkStateTimeout: CurrLink/Path = nn, RcvdLk/Path = mm, where: nn = the expected link/path mm = the
LOG_INFO	Signaling Network Management, 08: LS SLS Distribution	This log reports uneven 5-bit or 8-bit SLS distribution for linksets. This log is used only by Nortel Networks technical support.	The system is experiencing uneven 5-bit or 8-bit SLS distribution.	The Information and Data fields indicate 5-bit or 8-bit SLS distribution, and provide the signaling linkset ID.	No action is required.

LOG_INFO	Signaling Network Management, 09: CLS SLS Distribution	This log reports uneven 5-bit or 8-bit SLS distribution for combined linksets. This log is used only by Nortel Networks technical support.	The system is experiencing uneven 5-bit or 8-bit SLS distribution.	The Information and Data fields indicate 5-bit or 8-bit SLS distribution, and provide the signaling combined linkset ID.	No action is required.
LOG_INFO	Signaling Network Management, 10: SNM Information	This log provides signaling network management information.	The last signaling network management message received concerning one of the routesets of the combined route was not used to update the routing data of the concerned combined route.	An internal mismatch between the TSRC (Signaling Routing Control) flag and the combined route of a routeset has been detected. There is a conflict between routesets of a combined route. The routeset data of the combined route could not be used to determine the appropriate routeset for sending a message to a remote point code. The TSRC Audit has corrected the incorrect routeset data. The appropriate routeset has been determined and the message has been sent successfully.	No action is required. nn = the link ID or path ID. nn = the incoming link ID or path ID. nn = the incoming link ID or path ID. nn = link ID or path ID. nn = the incoming link ID or path ID. nn = the link ID or path ID. nn = the link ID or path ID. nn = the link ID or path ID. for the link or path of the received message is SMH_L_BUFFER. MSU sequence monitoring start was requested on the Link or Path card. than the Link or Path card. nn = the incoming link ID or path ID.
LOG_INFO	Signaling Network Management, 11: SNM 5->8 bit SLS conversion active on a link	This log provides an indication that the link has detected reception of 5-bit SLS values and that internal 5 to 8 bit SLS conversion is now active for the link.	The Cause of this log is reception on 5 bit SLS values from far end. The Log will only be issued following link activation if 5 bit values are detected in the received messages.	Included in the log are the NodeID of the node hosting the link and the link ID.	If the far end office should be sending 8 bit SLS values than operators should double check the configuration at the far end. No local action is required.
LOG_INFO	SIP Application Group, 01: SIP Appl Congestion	the SIP protocol receives a 503 SIP response msg and trigger congestion.	A 503 message is received from the SIP application AS.	The Information and Data fields describe the congestion.	Contact your next level of support.
LOG_INFO	SIP Application Group, 02: SIP Appl UnExpected Msg	the USP receives an Unexpected SIP/AIN msg	A Unexpected message is received from the SIP application AS.	The Information and Data fields describe the unexpected msg.	Contact your next level of support.

LOG_INFO	Software Upgrade, 01: Backlevel load	This log is generated when the user reboots a system node and it is now running the backlevel software load after all system nodes had been previously upgraded. It is not possible to successfully abort the software upgrade after all system nodes have been upgraded.	The user rebooted a system node with the backlevel software load after all system nodes had been upgraded.	The information field indicates that a system node has been booted with the backlevel software release after all system nodes have been upgraded.	Reboot the system node with the upgraded software load.
LOG_INFO	Software Upgrade, 02: Upgrade Started	This log is generated when the user starts the software upgrade process.	The user started the software upgrade process.	The information field indicates that the user has started the upgrade process.	No action is required.
LOG_INFO	Software Upgrade, 03: Upgrade Cleaned Up	This log is generated when the user cleans up the software upgrade process.	The user cleaned up the software upgrade process.	The information field indicates that the user has cleaned up the upgrade process.	No action required.
LOG_INFO	Software Upgrade, 04: Upgrade Completed	This log is generated when the user completes the software upgrade process.	The user completed the software upgrade process.	The information field indicates that the user has completed the upgrade process.	No action required.
LOG_INFO	Software Upgrade, 05: Upgrade Activated	This log is generated when the user activates the new release features during the software upgrade process.	The user activated the new release features during the software upgrade process.	The information field indicates that the user has activated the new release features during the upgrade process.	No action required.
LOG_INFO	Software Upgrade, 06: Upgrade Deactivated	This log is generated when the user deactivates the new release features during the software upgrade process.	The user deactivated the new release features during the software upgrade process.	The information field indicates that the user has deactivated the new release features during the upgrade process.	No action required.
LOG_INFO	Software Upgrade, 07: Upgrade Information	These logs do not indicate a problem, they are used for tracing the flow of execution of the software. No action is required.	System generated information.	The Information and Data fields contain information regarding the program flow of the Software Upgrade subsystem.	No action required.

LOG_INFO	SS7 Atomic Buffer, 03: Entry ID	This log is generated when an atomic buffer is constructed successfully. It provides internal data on the characteristics of an atomic buffer. This log is used only by Nortel Networks technical support.	The system created an atomic buffer for management of SS7 link or IP path status changes.	The Information field contains the following information: Atomic Buffer: Packed & sent nn entries. Atomic buffer message entry ID = '0x%xx' where: nn = number of logical entries in the buffer xx = internal buffer ID	No action is required.
LOG_INFO	SS7 Data, 02: Database Access Error	This log is generated when the Data subsystem encounters an unexpected database access error condition or message.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.

LOG_INFO	SS7 Messaging, 01: Message Send Error	This log indicates a failure to send a message. It is used only by Nortel Networks technical support.	An internal error has occurred.	The Information and Data fields provide the following information: Msg_Send Send Error: nn (num_msg_not_sent = mm) Data in hexadecimal data, where: nn = the return code from edpSend() mm = the total number of messages not sent Msg_UDP_Send Send Error: rcode = nn Data in hexadecimal data, where: nn = the return code send_msg_to_RTC mt = message type (hexadecimal) nd = destination node (hexadecimal) dt = destination task (decimal) rc = return code from called send procedure (decimal)	Contact your next level of support.

LOG_INFO	SS7 OM Trace, 01: Five-minute Write Request	This log reports 5-minute OM write request.	The system is processing 5-minute OMs.	The Information field contains the following information: 5Min OM write request: Element=e (e_hex) where: e=OM element ID in decimal e_hex = OM element ID in hex 5Min OM write request: Element=e (e_hex), Subelement=s (s_hex) where: e=OM element ID in decimal e_hex = OM element ID in hex s=OM subelement ID in decimal s_hex=OM subelement ID in hex The Data field contains the following information: Link/Path=l, ElId=e, Appld=a, RegId=r, RegVal=v, OpCode=o where: l=link ID or path ID a=OM application ID r=OM register ID v=value of OM register r o = OM opcode	No action is required.
LOG_INFO	SS7 STP Provisioning, 01: L3 User Provisioning	This log is generated when the user adds a system identity.	The user provisioned a System Identity.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 02: Add Linkset or ASP Success	This log is generated when the user adds a new linkset or ASP.	The user provisioned a linkset or ASP.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 03: Add Combined Linkset Success	This log is generated when the user adds a new combined linkset.	The user provisioned a combined linkset.	The Information and Data fields provide additional system status information to the user.	No action is required.

LOG_INFO	SS7 STP Provisioning, 04: Add LSG or AS Success	This log is generated when the user adds a new linkset group or application server.	The user provisioned a linkset group or application server.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 05: Link Added, Odd Number	This log is generated when the user adds a new link to a linkset. This linkset is a part of a combined linkset which has an odd number of links set as its maximum number links. (One of the linksets has an odd number of links for its maximum number and the other has an even number.)	The user provisioned a link, but not all links have been provisioned for the linkset and there is an odd number of links.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 06: Link Added, Even Number	This log is generated when the user adds a new link to a linkset or path to application server process, but not all links or paths have been provisioned. In this case there is an even number of links or paths provisioned.	The user provisioned a link, but not all links have been provisioned for the linkset and there is an even number of links. The user provisioned a path, but not all paths have been provisioned for the application server process and there is an even number of paths.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 07: Combined LS Has Odd Links	This log is generated when the user adds a new link to a linkset. In this case the linkset is a part of a combined linkset which has an odd number of links set as its maximum and the linkset still does not have all links provisioned.	The user provisioned a link, but not all links have been provisioned for the linkset and there is an odd number of links in the combined linkset.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 08: Add Link or Path Success	This log is generated when the user adds the last link for a linkset or the last path for a application server process.	The user provisioned the link or path.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 09: Change System Identity Success	This log is generated when the user changes a System Identity.	The user provisioned the network appearance change.	The Information and Data fields provide additional system status information to the user.	No action is required.

LOG_INFO	SS7 STP Provisioning, 10: Change Linkset or ASP Success	This log is generated when the user changes a linkset or application server process.	The user provisioned the linkset or application server process change.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 11: Combined Linkset Changed	This log is generated when the user changes the combined linkset.	The user provisioned the combined linkset change.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 12: Change LSG or AS Success	This log is generated when the user changes the linkset group or application server.	The user provisioned the linkset group or application server change.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 13: Change Link/Path Success	This log is generated when the user changes a link or path.	The user provisioned the link or path change.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 14: Change RS, ASC or ASA Success	This log is generated when the user changes the routeset or Application Server Cluster or Assignment.	The user provisioned the routeset change. The user provisioned an application server cluster change. The user provisioned an application server assignment change.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 15: Add RS, ASC or ASA Success	This log is generated when the user adds a routeset or Application Server Cluster or Assignment.	The user provisioned a new routeset. The user provisioned a new ASC. The user provisioned a new ASA.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 16: Delete RS, ASC or ASA Success	This log is generated when the user deletes a routeset or Application Server Cluster or Assignment.	The user provisioned the routeset deletion. The user provisioned the ASC deletion. The user provisioned the ASA deletion.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 17: Delete Linkset or ASP Success	This log is generated when the user deletes a linkset or application server process.	The user provisioned the linkset or application server process deletion.	The Information and Data fields provide additional system status information to the user.	No action is required.

LOG_INFO	SS7 STP Provisioning, 18: Delete Link/Path Success	This log is generated when the user deletes a link or path.	The user provisioned the link deletion. The user provisioned the path deletion.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 19: Delete Combined LS Success	This log is generated when the SS7 Data Provisioning deletes a combined linkset.	The user provisioned the combined linkset deletion.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 20: Delete LSG or AS Success	This log is generated when the user deletes a linkset group or application server.	The user provisioned the linkset group or application server deletion.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 21: Delete System Identity Success	This log is generated when the user deletes an System Identity.	The user provisioned the System Identity deletion.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 22: Add MTP L2 Timer Success	This log is generated when the user adds an MTP Level 2 Timer Set.	The user provisioned the addition of an MTP L2 Timer Set.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 23: Delete MTP L2 Timer Success	This log is generated when the user deletes an MTP Level 2 timer set	The user provisioned the deletion of an MTP L2 timer set.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 24: Add MTP L3 Timer Success	This log is generated when the user adds an MTP Level 3 timer set.	The user provisioned the addition of an MTP L3 timer set.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 25: Delete MTP L2 Timer Success	This log is generated when the user deletes an MTP Level 3 timer set.	The user provisioned the deletion of an MTP L3 timer set.	The Information and Data fields provide additional system status information to the user.	No action is required.

LOG_INFO	SS7 STP Provisioning, 26: Add SAAL Timer Success	This log is generated when the user adds a SAAL timer set.	The user provisioned the addition of a SAAL timer set.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 27: Add SAAL Timer Success	This log is generated when the user deletes a SAAL timer set.	The user provisioned the deletion of a SAAL timer set.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 28: Add SAAL Parameter Set Success	This log is generated when the user adds a SAAL parameter set.	The user provisioned the addition of a SAAL parameter set.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 29: Delete SAAL Parameter Set Success	This log is generated when the user deletes a SAAL parameter set.	The user provisioned the deletion of a SAAL parameter set.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 30: Add MTP SLT Timer Set Success	This log is generated when the user adds an MTP SLT Timer Set.	The user provisioned the addition of an MTP SLT Timer Set.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 31: Delete MTP SLT Timer Set Success	This log is generated when the user deletes an MTP SLT timer set	The user provisioned the deletion of an MTP SLT timer set.	The Information and Data fields provide additional system status information to the user.	No action is required.
LOG_INFO	SS7 STP Provisioning, 32: Add SCTP Parameter Set Success	This log is generated when the user adds a SCTP parameter set.	The user provisioned the addition of a SCTP parameter set.		No action is required.
LOG_INFO	SS7 STP Provisioning, 33: Del SCTP Parameter Set Success	This log is generated when the user deletes a SCTP parameter set.	The user provisioned the deletion of a SCTP parameter set.		No action is required.
LOG_INFO	SS7 TCAP Decode, 01: Invalid TCAP Message	This log reports an error in TCAP decoding due to an invalid formatted TCAP message being received.	An incorrectly formatted TCAP message.	The Information and Data fields describe the error.	Contact your next level of support.

LOG_INFO	SS7 TCAP Decode, 02: Unknown TCAP Package Type	This log reports an error in TCAP decoding due to an unknown Package Type being found in the received TCAP message.	An incorrectly formatted TCAP message.	The Information and Data fields describe the error.	Contact your next level of support.
LOG_INFO	SS7 TCAP Decode, 03: Invalid TRID Length	This log reports an error in TCAP decoding due to an invalid Transaction Id Length value being found in the received TCAP message.	An incorrectly formatted TCAP message.	The Information and Data fields describe the error.	Contact your next level of support.
LOG_INFO	SS7 TCAP Decode, 04: Invalid TRID Identifier	This log reports an error in TCAP decoding due to an invalid Transaction Id Identifier being found in the received TCAP message.	An incorrectly formatted TCAP message.	The Information and Data fields describe the error.	Contact your next level of support.
LOG_INFO	SS7 TCAP Decode, 05: Invalid TCAP Length Field	This log reports an error in TCAP decoding due to an invalid TCAP Length value being found in the received TCAP message.	An incorrectly formatted SCCP message. An incorrectly formatted TCAP message.	The Information and Data fields describe the error.	Contact your next level of support.
LOG_INFO	SS7 TCAP Decode, 06: OPC TCAP failure	This log reports an error in OPC TCAP Distribution.		The Information and Data fields describe the error and probable cause Contact your next level of support.	
LOG_INFO	SS7 TCAP Tagging, 01: Incorrect TRID field format	This log reports an error in TCAP decoding due to an invalid formatted TCAP message being received.	A TRID of a TCAP message is invalid. An incorrectly formatted TCAP message.	The Information and Data fields describe the error.	Contact your next level of support.
LOG_INFO	SS7 TCAP Tagging, 03: Unsupported Protocol and/or Variant	This log reports an error in TCAP decoding due to an unsupported Package Type being found in the received TCAP message.	A message from an unsupported protocol is received. An incorrectly formatted TCAP message.	The Information and Data fields describe the error.	Contact your next level of support.

LOG_INFO	SS7 User Part, 02: ISUP Distribution	This log reports the events related to ISUP message distribution.	An abnormal ISUP distribution event has occurred.	The Information and Data fields contain the failure reason, the incoming link (linkset, DCP, SLC), the originating point code (OPC), the circuit identification code (CIC) and the ISUP message type.	The following are some common failure reasons and recommended corrective actions. MHD Data not found for OPC/CIC: The reason could be that the far end office (OPC) is messaging to a trunk that is not provisioned or in incorrect state. The corrective action is one of the following. These actions must be performed at the AS Master. - If the trunk is not provisioned, provision the trunk and change the trunk state to MB - If the trunk is in INB state, change the state to MB - If the trunk is in a state other than INB, change the trunk state to INB and back to MB. - If the far end office has an invalid trunk provisioned, take appropriate action to remove the trunk from the far end office AS Path not found: AS Master Path not found: Check the path-state of the application-server-process-path. Ensure that the path-state is up.

LOG_INFO	SS7 User Part, 03: TUP Distribution	This log reports the events related to TUP message distribution.	An abnormal TUP distribution event has occurred.	The Information and Data fields contain the failure reason, the incoming link (linkset, DCP, SLC), the originating point code (OPC), the circuit identification code (CIC) and the TUP message type.	The following are some common failure reasons and recommended corrective actions. MHD Data not found for OPC/CIC: The reason could be that the far end office (OPC) is messaging to a trunk that is not provisioned or in incorrect state. The corrective action is one of the following. These actions must be performed at the AS Master. - If the trunk is not provisioned, provision the trunk and change the trunk state to MB - If the trunk is in INB state, change the state to MB - If the trunk is in a state other than INB, change the trunk state to INB and back to MB. - If the far end office has an invalid trunk provisioned, take appropriate action to remove the trunk from the far end office AS Path not found: AS Master Path not found: Check the path-state of the application-server-process-path. Ensure that the path-state is up.

LOG_INFO	SS7 User Part, 04: BICC Distribution	This log reports the events related to BICC message distribution.	An abnormal BICC distribution event has occurred.	The Information and Data fields contain the failure reason, the incoming link (linkset, DCP, SLC), the originating point code (OPC), and the BICC message type.	The following are some common failure reasons and recommended corrective actions. AS Path not found: AS Master Path not found: Check the path-state of the application-server-process-path. Ensure that the path-state is up. ASP not in service: Check the path-state of the application-server-process path. Ensure that the path-state is up. If the problem still exists, delete and re-provision the associated application-server.
LOG_INFO	SSCS Messaging Layer, 06: Mapped from SSCS SME_LOG_INFO	This log is generated when the connection to an RTC, CC, or application system node has failed.	An RTC, CC, or application system node has failed and the connection to that RTC, CC, or application system node has failed as a result. System Node Maintenance logs will indicate the location of the failed RTC, CC, or application system node.	The Information field describes the error.	Contact your next level of support.
LOG_INFO	System Administration, 01: Semaphore Unavailable	This log is generated by the HMI server task when two USP GUI sessions are trying to access the same set of system administration data at the same time. This is not considered an error condition, but you will have to try again.	Two USP GUI sessions are attempting to access the same set of system administration data at the same time. The semaphore controlling access to the data is unavailable at this time.	The Information field indicates that the system administration data is inaccessible to the user.	Make another attempt to access the system administration data.

LOG_INFO	System Administration, 03: User ID Exists	This log is generated by the HMI server task when the user tries to add a user ID to the system that already exists. This is not an error condition. The system does not support multiple users with identical user IDs.	A user attempted to add a new user ID to the system, and the user ID already exists.	The Information field indicates that the user ID already exists.	Try to add the user again with a different user ID. If you were trying to modify the user account information, click the Modify button instead of the Add button.
LOG_INFO	System Administration, 04: User Information Invalid	This log is generated by the System Administration subsystem when a user login request has been denied by a system interface.	A user trying to log into the system has entered an incorrect user ID and password combination.	The Information field indicates that the input user ID and password combination are invalid. login failed (gui) = graphical user interface login failed (cli) = command line interface	Try to log into the system again using the correct user ID and password combination.
LOG_INFO	System Administration, 05: User Account Added Successfully	This log is generated by the HMI server task when a user account is successfully added to the system. This occurs when a user with system administration authority adds a new user account to the system using the USP GUI.	A user account was added to the system.	The Information field indicates that the user account was added to the system.	No action is required.
LOG_INFO	System Administration, 06: User Account Deleted Successfully	This log is generated by the HMI server task when a user account is successfully deleted from the system. This occurs when a user with system administration authority deletes a user account from the system using the USP GUI.	A user account was deleted from the system.	The Information field indicates that the user was deleted from the system.	No action is required.
LOG_INFO	System Administration, 16: Only One User Account - Deletion Aborted	The system generates this log when a user tries to delete a user account from the system when there is only one user account available. The system will prohibit the deletion.	The user has attempted to delete the last user account from the system.	The Information field indicates that the last user account cannot be deleted.	Do not attempt to delete the last user account in the system.
LOG_INFO	System Administration, 18: Cannot Delete Active Load Image File	This log is generated by the System Administration subsystem when the user tries to delete a load image file from the system that is either active or will be used to boot an RTC, CC, or application system node the next time it is reset.	A user has tried to delete a load image file that has been designated as the boot image file.	The Information field indicates that the load image file cannot be deleted.	Do not try to delete the specified load image file until it is no longer designated as the boot image file.

LOG_INFO	System Administration, 23: Cannot Delete Boot Data Snapshot	This log is generated by the System Administration subsystem when the user tries to delete a data snapshot from the system that is either active or will be used as the boot data snapshot by the system the next time it is reset.	A user has tried to delete a data snapshot that is active or has been designated as the boot data snapshot.	The Information field indicates that the specified data snapshot cannot be deleted.	Do not attempt to delete the specified data snapshot until it is no longer active or designated as the boot data snapshot.
LOG_INFO	System Administration, 25: snapshot created	This log is generated by the System Administration subsystem when a data snapshot has been successfully created on the SCSI disk associated with the active RTC system node.	A data snapshot was successfully created.	The information field contains the name of the snapshot.	No action is required.
LOG_INFO	System Administration, 27: Not Enough Disk Space For New Data Snapshot	This log is generated by the System Administration subsystem when there is not enough disk space available to create a data snapshot.	There is not enough space on the SCSI disk associated with the active RTC system node to store another data snapshot. Most likely there are too many data snapshots already resident on the disk.	The Information field indicates that there is not enough disk space to create a data snapshot.	Delete the older snapshots on the SCSI disk associated with the active RTC system node and try again to create a data snapshot. Refer to the Backup section of the USP User Guide for more information.
LOG_INFO	System Administration, 29: Matching Data Snapshot Exists	This log is generated by the System Administration subsystem when a data snapshot creation fails because another data snapshot with the same name already exists.	The name of a snapshot is based on several variables and is automatically generated by the system. One of the variables is date and time. Therefore, it is possible to see this log if you are changing the time one the system and you try to create a snapshot at exactly the right moment.	The Information indicates that a data snapshot with that name already exists.	Wait 5 minutes and retry. If the problem persists, contact your next level of support.
LOG_INFO	System Administration, 31: Data Snapshot Deleted	This log is generated by the System Administration subsystem when a data snapshot is successfully deleted from the SCSI disk associated with an RTC system node.	The user initiated a data snapshot deletion operation.	The Information field indicates that a data snapshot was deleted.	No action is required.
LOG_INFO	System Administration, 35: Load Image File Deleted	This log is generated by the System Administration subsystem when a load image file is successfully deleted from the SCSI disk associated with an RTC system node.	The user initiated a load image file deletion operation.	The Information field indicates that a load image file was deleted.	No action is required.

LOG_INFO	System Administration, 36: User Login Successful	This log is generated by the System Administration subsystem when a user has successfully logged into a system interface.	A user successfully logged into a system interface.	The Information field indicates that a user logged into a system interface. login (gui) = graphical user interface login (cli) = command line interface login (les) = log export server	No action is required.
LOG_INFO	System Administration, 37: User Logout Successful	This log is generated by the System Administration subsystem when a user has successfully logged out of a system interface.	A user has successfully logged out of a system interface.	The Information field indicates that a user logged out of a system interface. logout (gui) = graphical user interface logout (cli) = command line interface logout (les) = log export server	No action is required.
LOG_INFO	System Administration, 38: Load Image File Exists	This log is generated by the system administration subsystem when an attempt to copy a load image file from the OAM&P workstation to the SCSI disk on the selected RTC system node fails because a number of duplicates of the load image file already exist on the SCSI disk.	This occurs when the maximum number of duplicate load image files on disk threshold has been reached. It is not possible to create another duplicate because the names are numerically generated.	The Information field indicates that the maximum number of duplicate load image files already exists on the SCSI disk.	Delete some of the existing duplicate load image files residing on the SCSI disk associated with the selected RTC system node and try again to copy the load image file. Refer to the Backup section of the USP User Guide for more information.
LOG_INFO	System Administration, 39: Maximum Data Snapshots Exist	This log is generated by the system administration subsystem when a data snapshot creation function fails because the maximum number of data snapshots already exists on the SCSI disk associated with an RTC system node.	This occurs when the maximum number of snapshots allowed already exists on the SCSI disk associated with an RTC system node. It is not possible to create another data snapshot until one is deleted.	The Information field indicates that the maximum number of data snapshots already exists on the SCSI disk associated with an RTC system node.	Delete some of the existing data snapshots from the SCSI disk associated with the RTC system node and try again to create a data snapshot.

LOG_INFO	System Administration, 40: Successful Load Image File Copy	This log is generated by the System Administration subsystem when a load image file is successfully copied from the OAM&P workstation to the SCSI disk associated with an RTC system node.	A load image file has been copied to the SCSI disk associated with an RTC system node.	The Information indicates that a load image file has been copied.	No action is required.
LOG_INFO	System Administration, 41: Successful Data Snapshot Copy	This log is generated by the system administration subsystem when a data snapshot is successfully copied from the OAM&P workstation to the SCSI disk associated with an RTC system node.	A data snapshot has been copied to the SCSI disk associated with an RTC system node.	The Information field indicates that a data snapshot has been copied.	No action is required.
LOG_INFO	System Administration, 42: Maximum Load Image Files Exist	This log is generated by the system administration subsystem when a load image file copy function fails because the maximum number of load image files already exists on the SCSI disk associated with a specified RTC system node.	This occurs when the maximum number of load image files allowed on disk threshold has been reached. It is not possible to copy another load image file to the SCSI disk until one is deleted.	The Information field indicates that the maximum number of load image files already exists on the SCSI disk associated with the specified RTC system node.	Delete some of the existing load image files from the SCSI disk associated with the RTC system node and try again to copy the load image file.
LOG_INFO	System Administration, 43: Maximum User Accounts Exist	This log is generated by the HMI server task when the user tries add a user account when the maximum number of user accounts threshold has already been reached.	The number of user accounts already registered is at its maximum.	The Information field indicates that the maximum number of user accounts has been exceeded.	Delete an existing user account before adding another user account. Refer to the Getting Started section of the USP User Guide for more information.
LOG_INFO	System Administration, 50: User Session Timeout	The system generates this log when a user session has been inactive for too long, typically 5 minutes.	user is no longer active.	user name and ip address is provided	re-establish user session if required
LOG_INFO	System Administration, 51: User Session Force Out	The system generates this log when a user session has been forced-out by another user	another user has executed the force-out command.	user name and ip address is provided	re-establish user session if required
LOG_INFO	System Administration, 55: Authentication server response string parse error	This log is generated by the Authentication routine that is used to authenticate users when they login to the system. It is generated when communicating with the Remote Authentication server and the response for the server does not follow the prearranged format.	Messaging version between the USP and Remote Authentication server has changed.	N/A	Contact your next level of support.

LOG_INFO	System Administration, 58: Max CLI Sessions Reached	The system generates this log when the maximum number of concurrent CLI sessions has been reached on the specified RTC.	Maximum number of concurrent CLI sessions has been reached	The system-node in the log will indicate which RTC has reached the maximum.	Attempt to connect to the mate RTC or ask an existing user to log out of the system to free up an additional session.
LOG_INFO	System Administration, 59: oldest snapshot on abs deleted	The system generates this log when the oldest snapshot on the alternate boot server is deleted as a result of taking a backup.	The user has selected the "delete oldest snapshot on alternate boot server" option when taking a backup and the maximum number of snapshots on the server has been reached.	The log description contains the name of the deleted snapshot.	No corrective action is required
LOG_INFO	System Administration, 60: oldest snapshot on rtc deleted	The system generates this log when the oldest snapshot on the RTC is deleted as a result of taking a backup.	The user has selected the "delete oldest snapshot on rtc" option when taking a backup and the maximum number of snapshots on the RTC has been reached.	The log description contains the name of the deleted snapshot.	No corrective action is required
LOG_INFO	System Administration, 61: snapshot transferred to abs	The system generates this log when the snapshot is transferred to the alternate boot server.	The user has selected the "transfer snapshot to alternate boot server" option when taking a backup.	The log description contains the name of the snapshot.	No corrective action is required
LOG_INFO	System Administration, 62: active snapshot set	The system generates this log when the active snapshot is set on the alternate boot server.	The user has selected the "set as active snapshot on alternate boot server" option when taking a backup.	The log description contains the name of the snapshot.	No corrective action is required
LOG_INFO	System Administration, 63: backup create command in progress	The system generates this log when at the start of creating a snapshot.	The user has issued the backup command.	None	No corrective action is required
LOG_INFO	System Administration, 64: password expired	The system generates this log when user's password expires in USP.	The user has not changed the password within the allowed days of password expiration.	The information field indicates the input userid whose password is expired. It also indicates the user's password must be changed before account gets locked.	Change the password for your account.

LOG_INFO	System Administration, 65: account locked	The system generates this log when user's password and grace period expires in USP.	The user has not changed the password within the allowed days of password expiration and has exhausted all the grace period logins.	The information field indicates the input userid and the reason for locking the account.	Contact your next level of support to activate your account.
LOG_INFO	System Node Maintenance, 01: Lock State Transition	This log records an RTC, CC, or application system node administrative state transition from an unlocked state to a locked state.	The user has requested a lock operation on the specified RTC, CC, or application system node.	The Information field indicates the transition to the locked administrative state.	No action is required.
LOG_INFO	System Node Maintenance, 02: Unlock State Transition	This log records an RTC, CC, or application system node administrative state transition from a locked state to an unlocked state.	The user has requested a unlock operation on the specified RTC, CC, or application system node.	The Information field indicates the transition to the unlocked administrative state.	No action is required.
LOG_INFO	System Node Maintenance, 04: Enable State Transition	This log records an RTC, CC, or application system node operational state transition from a disabled state to an enabled state.	The RTC, CC, or application system node has transitioned to an enabled state.	The Information field indicates the transition to the enabled operational state.	No action is required.
LOG_INFO	System Node Maintenance, 06: RTC Activity Gain	This log records that a particular RTC system node has assumed activity for the mated RTC system node pair.	The switch of activity has occurred for one of the following reasons: The user has performed a manual SWACT operation or another manual action which resulted in a switch of activity. The system has determined that a newly active RTC system node is better suited to have activity for the mated RTC system node pair.	The Information field indicates that the particular RTC system node is now the active RTC system node.	No action is required.

LOG_INFO	System Node Maintenance, 07: RTC Activity Drop	This log records that a particular RTC system node has released activity for the mated RTC system node pair.	The switch of activity has occurred for one of the following reasons: The user has performed a manual SWACT operation or another manual action which resulted in a switch of activity. The system has determined that a newly active RTC system node is better suited to have activity for the mated RTC system node pair.	The Information field indicates that activity was released for the RTC system node.	No action is required.
LOG_INFO	System Node Maintenance, 08: Diagnostic Result	This log records the results of a diagnostic test performed on an RTC, CC, or application system node.	A user-initiated diagnostic test has completed.	The Information field indicates the results of the diagnostic test.	No action is required.
LOG_INFO	System Node Maintenance, 09: RTC, CC, or Application System Node Addition	This log indicates that a new RTC, CC, or application system node has been configured in the system.	A user has provisioned a new RTC, CC, or application system node.	The Information field indicates that an RTC, CC, or application system node has been added to the system.	No action is required.
LOG_INFO	System Node Maintenance, 10: RTC, CC, or Application System Node Deletion	This log indicates that an RTC, CC, or application system node has been removed from the system.	A user has deleted an RTC, CC, or application system node.	The Information field identifies the RTC, CC, or application system node that has been deleted.	No action is required.
LOG_INFO	System Node Maintenance, 11: BERT Statistics	A BERT operation has completed.	A user has run a BERT operation. The test was either terminated by the user, or the system has terminated the test automatically.	The Information field indicates whether the test was stopped by the user, or automatically by the system. The Data field provides some statistical information about the BERT operation.	No action is required.

LOG_INFO	System Node Maintenance, 13: Lock Request Denied	This log indicates that a request to lock an RTC or CC system node has been denied due to the administrative and operational states of other RTC, CC, or application system nodes.	This log is caused by one of the following reasons: User has attempted to lock the active RTC system node when its mate could not assume activity. User has attempted to lock the only enabled and unlocked RTC system node when at least one CC system node is unlocked. User has attempted to lock a CC system node when the other CC system node on that shelf could not assume activity. User has attempted to lock any CC system node while at least one application system node on that shelf is unlocked.	The Information field indicates the reason that the lock request was denied.	If you are trying to lock an RTC system node for the purpose of maintenance on that RTC system node, ensure that the mate RTC system node is unlocked and enabled. If you are trying to lock an RTC system node for the purpose of taking the system down, ensure that all of the CC system nodes are locked. If you are trying to lock a CC system node for the purpose of maintenance on that CC system node, ensure that the other CC system node on that shelf is unlocked and enabled. If you are trying to lock a CC system node for the purpose of taking the system down, ensure that all of the application system nodes on that shelf are locked.

LOG_INFO	System Node Maintenance, 14: Unlock Request Denied	This log indicates that a request to unlock a CC or application system node has been denied due to the administrative and operational states of other RTC or CC system nodes in the system.	This log is caused by one of the following reasons: User is trying to unlock a CC system node when there are no unlocked and enabled RTC system nodes. User is trying to unlock an application system node when there are no unlocked and enabled CC system nodes on that shelf.	The Information field indicates that the CC or application system node could not be unlocked.	If you are trying to unlock a CC system node, ensure that at least one RTC system node is unlocked and enabled. If you are trying to unlock an application system node, ensure that at least one CC system node on that shelf is unlocked and enabled.
LOG_INFO	System Node Maintenance, 15: Locked Active CC	This log indicates that a locked CC system node has become active for the mated pair.	The active unlocked CC system node transitioned to disabled while its mate was in a locked state.	The Information field indicates that the active CC system node is locked.	Unlock the CC system node identified by this log.
LOG_INFO	System Node Maintenance, 16: RTC, CC, or Application System Node Failure	This log indicates that an RTC, CC, or application system node failure has occurred.	If an application system node is affected, that application system node has stopped responding to audits from the CC system nodes on that shelf. If a CC system node is affected, that CC system node has stopped responding to audits from the RTC system nodes. If an RTC system node is affected, that RTC system node is unable to communicate with its mated RTC system node.	The Information field indicates that an RTC, CC, or application system node failure has occurred.	The system automatically transitions the affected RTC, CC, or application system node to a disabled state and initiates recovery. No action is required unless this failure is seen repeatedly. If the failure is repetitive the card should be replaced.

LOG_INFO	System Node Maintenance, 17: HA Failure	This log indicates that an HA hardware or software failure has occurred.	The HA hardware or software stopped responding to ping requests from the Link system node.	The Information field indicates that an HA hardware or software failure has occurred.	The system automatically transitions the Link system node to a disabled state and initiates recovery. No action is required.
LOG_INFO	System Node Maintenance, 18: SWACT Request Denied	This log indicates that a request to switch activity from one RTC system node to its mate has been denied due to a mismatch in administrative or operational states for the RTC system nodes.	This log is caused by one of the following reasons: User is trying a SWACT operation when the RTC system nodes are not in the same administrative state (that is, both RTC system nodes must be either locked or unlocked). User is trying a SWACT operation when the RTC system nodes are not in the same operational state (that is, both RTC system nodes must be enabled).	The Information field indicates that the switch activity request has been denied.	Refer to the Maintenance Procedures for an RTC System Node section of the USP User Guide for the steps necessary to change both RTC system nodes to the same administrative or operational states, so that the SWACT operation can be processed.
LOG_INFO	System Node Maintenance, 19: Task Trap	This log indicates that a software exception (trap) has occurred on an RTC, CC, or application system node in the system. The system may automatically reboot the affected RTC, CC, or application system node.	A task has trapped due to a run-time error.	The Information field indicates that a trap has occurred.	Read the Information field to determine whether intervention is required. If the system could not automatically recover, the user should take the steps necessary to manually reload the affected RTC, CC, or application system node as soon as possible.
LOG_INFO	System Node Maintenance, 21: Lock Initiated	This log records that a manual lock has been initiated.	An RTC, CC, or application system node lock has been requested by the user.	The Information field indicates which user requested the lock.	No action is required.
LOG_INFO	System Node Maintenance, 22: Unlock Initiated	This log records that a manual unlock has been initiated.	An RTC, CC, or application system node unlock has been requested by the user.	The Information field indicates which user requested the unlock.	No action is required.

LOG_INFO	System Node Maintenance, 23: Diagnostic Initiated	This log records that a diagnostic test has been initiated.	An RTC, CC, or application system node diagnostic test has been requested by the user.	The Information field indicates which user requested the diagnostic test.	No action is required.
LOG_INFO	System Node Maintenance, 24: Loading Initiated	This log records that an RTC, CC, or application system node loading operation has been initiated.	Loading of an RTC, CC, or application system node has been requested by the user.	The Information field indicates which user requested the load.	No action is required.
LOG_INFO	System Node Maintenance, 25: Off-line Initiated	This log records that a manual off-line operation has been initiated.	An RTC, CC, or application system node off-line operation has been requested by the user.	The Information field indicates which user requested the off-line operation.	No action is required.
LOG_INFO	System Node Maintenance, 26: RTC Switch of Activity Initiated	This log records that an RTC system node switch of activity has been initiated.	An RTC system node SWACT operation has been requested by the user.	The Information field indicates which user requested the SWACT operation.	No action is required.
LOG_INFO	System Node Maintenance, 27: BERT Start Requested	This log records that a BERT start has been requested for a port.	A BERT start has been requested by the user.	The Information field indicates which user requested the BERT start. The Data field indicates the port for which the request was made.	No action is required.
LOG_INFO	System Node Maintenance, 28: BERT Stop Requested	This log records that a BERT stop has been requested for a port.	A BERT stop has been requested by the user.	The Information field indicates which user requested the BERT stop. The Data field indicates the port for which the request was made.	No action is required.
LOG_INFO	System Node Maintenance, 29: Loopback Set Requested	This log records that a remote loopback set has been requested for a port.	A remote loopback set has been requested by the user.	The Information field indicates which user requested the loopback set. The Data field indicates the port for which the request was made.	No action is required.

LOG_INFO	System Node Maintenance, 30: Loopback Clear Requested	This log records that a remote loopback clear has been requested for a port.	A remote loopback clear has been requested by the user.	The Information field indicates which user requested the loopback clear. The Data field indicates the port for which the request was made.	No action is required.
LOG_INFO	System Node Maintenance, 31: RTC Rebooted Due To Disk Failure	A disk failure fault was reported by the disk auditor. The fault causes the affected RTC system node to be rebooted.	The SCSI disk drive associated with the RTC system node is corrupted or inaccessible.	No additional information is provided.	Check SCSI cables and connectors to ensure that connections are clean and tight. If that does not clear the symptom, replace the SCSI disk drive.
LOG_INFO	System Node Maintenance, 33: RTC Reset To Sync Data	An RTC system node has reset itself to force a data synch with the mated RTC system node following a dual CC system node failure condition. By synchronizing the RTC system node, data integrity can be assured between the RTC system nodes.	The system has recovered from a dual CC system node failure condition.	The Information field indicates that the RTC system node is being reset to synchronize data between the RTC system nodes.	The system automatically tries to recover the RTC system node. No action is required.
LOG_INFO	System Node Maintenance, 34: RTC Reboot To Recover Database	A database error has been seen by the RTC system node. The RTC system node will be rebooted to recover from the problem.	A database memory corruption has occurred.	The Information field indicates that the RTC system node is being reset to recover the database files.	The system automatically tries to recover the RTC system node. No action is required.
LOG_INFO	System Node Maintenance, 35: Rule Rejection of Action	This log indicates that the system has rejected a user's request for a specific action.	This log is generated when the user requests a maintenance action (lock, unlock, or SWACT) when the system is not in a state that allows the action.	The Information and Data fields indicate the exact reason the system rejected the action.	Open a detailed view of the log to determine the exact reason for the rejection. Refer to the appropriate section of the USP User Guide for the rules governing the attempted action and the steps necessary to allow it.

LOG_INFO	System Node Maintenance, 36: Unknown State Change Opcode	This log indicates that a state change received from a different node was not one that this node knows how to process.	This log is probably caused when nodes in the system are at different release levels. During upgrade an node at a higher release level may generate state changes that back level nodes may not be able to interpret.	The Information field contains the state change operational code that was provided in the state change message. The Data field contains the actual state change message that was received.	If this log is seen during upgrade then no corrective actions are necessary. Once upgrade is completed this log should no longer be generated.
LOG_INFO	System Node Maintenance, 37: Port Mode Mismatch	This log indicates that the port mode reported by the TM during initialization is different than the information in the database at that time.	This can happen the first time a Link system node containing a V.35 TM initializes if there are ports on the TM configured in DCE mode. The database is updated during initialization with the value reported by the TM, so the next time the node initializes or loads, this log will not be generated. However, if the node is offlined and any of the port's modes are changed, the system will generate this log again the first time the node initializes after the change.	No additional information is available.	No action is necessary unless it is determined that the value to which the database was set, i.e., the value reported by the TM, is not the correct value. In that case, the card should be offlined and the appropriate port mode set.
LOG_INFO	System Node Maintenance, 39: Loss Of Communication Redundancy	The extension shelf of the CC node associated with this log experienced a Loss Of Communication Redundancy (LOCR) with the control shelf. However, there is still one viable communication path.	There is either a problem with a fiber optic cable or a problem with one of the CCs or an ATM switch problem if in multishelf configuration. NOTE: This log is indicative of a problem with a node or physical link.	There is no data associated with this log.	Please refer to the Alarm section of the USP Fault Management Manual for Loss Of Communication Redundancy recovery procedures.

LOG_INFO	System Node Maintenance, 41: Port Speed Modified	This log indicates that the port speed for a TM has been modified.	Port speed of a link system node has been modified successfully.	There will be no data section for this log.	No corrective action is necessary.
LOG_INFO	System Node Maintenance, 42: Platform State Changed	This log indicates that the platform state has changed to either PLATFORM READY or PLATFORM NOT READY. The platform state is used to prohibit (when necessary) application recovery (SS7 link, etc) so that recovery of system nodes can be given priority in the instance of multiple node failures. When the USP transitions to the PLATFORM READY state, application recovery begins. An example of such a recovery is the alignment of SS7 links. When the USP transitions to the PLATFORM NOT READY state, existing applications (SS7 link, etc) that are inservice continue to run. Applications that are not inservice will not fully recover until the USP transitions to the PLATFORM READY state. Note: As long as the USP is in the PLATFORM NOT READY state, link system nodes that go ENABLED will not automatically align their ports or process traffic.	The USP transitions to the PLATFORM NOT READY state whenever the USP recovers from a Complete Office Recovery, or whenever a certain percentage of non-offlined nodes become DISABLED. The USP transitions to PLATFORM READY when a certain percentage of the mission nodes go enabled or the USP has been in the PLATFORM NOT READY state for up to 20 minutes.	There is no data associated with this log.	No corrective action is necessary.

LOG_INFO	System Node Maintenance, 43: Software Upgrade Back Out Denied.	This log indicates that a request to back out of software upgrade was denied. The reasons that the request may be denied are: The user has attempted to back out of software upgrade with both RTCs not upgraded. The user has attempted to back out of software upgrade while RTC 15 is not Offline.	The USP was not configured properly to back out of software upgrade.	The Information field indicates the reason why the request to back out of upgrade was rejected.	Please refer to the Software Upgrade section of the USP Manual the appropriate process to use when backing out of software upgrade.
LOG_INFO	System Node Maintenance, 44: Message Timeout	This log records the receipt of a node maintenance Timeout Message on the RTC.	The RTC sent node maintenance message to a system node that was unable to respond to the request in the time allotted.	The Information field indicates the card that the original message was intended for, and any system actions taken as a result.	No action is required.
LOG_INFO	System Node Maintenance, 45: Information	This log is generated by the system node maintenance subsystem to communicate general non-error related information.	Not applicable.	Nortel Networks may use the information in the Information and Data fields to determine the status of your system when the informational log occurred.	No action is required.

LOG_INFO	System Node Maintenance, 46: Pulse Shape Mismatch	This log indicates that the pulse shape reported by the TM during initialization is different than the information in the database at that time.	This can happen the first time a Link system node containing a T1 E1 TM initializes if there are ports on the TM configured in DCE mode. The database is updated during initialization with the value reported by the TM, so the next time the node initializes or loads, this log will not be generated. However, if the node is offlined and any of the pulse shapes are changed, the system will generate this log again the first time the node initializes after the change.	No additional information is available.	No action is necessary unless it is determined that the value to which the database was set, i.e., the value reported by the TM, is not the correct value. In that case, the card should be offlined and the appropriate port mode set.
LOG_INFO	System Node Maintenance, 47: Clock Sync Mismatch	This log indicates that the port mode reported by the TM during initialization is different than the information in the database at that time.	This can happen the first time a Link system node containing a Channelized TM initializes if there are ports on the TM configured. The database is updated during initialization with the value reported by the TM, so the next time the node initializes or loads, this log will not be generated. However, if the node is offlined and any of the clock syncs are changed, the system will generate this log again the first time the node initializes after the change.	No additional information is available.	No action is necessary unless it is determined that the value to which the database was set, i.e., the value reported by the TM, is not the correct value. In that case, the card should be offlined and the appropriate port mode set.

LOG_INFO	System Node Maintenance, 48: Channel Mapping Mismatch	This log indicates that the channel mapping reported by the TM during initialization is different than the information in the database at that time.	This can happen the first time a Link system node containing a Channelized TM initializes if there are ports on the TM configured. The database is updated during initialization with the value reported by the TM, so the next time the node initializes or loads, this log will not be generated. However, if the node is offlined and any of the clock syncs are changed, the system will generate this log again the first time the node initializes after the change.	No additional information is available.	No action is necessary unless it is determined that the value to which the database was set, i.e., the value reported by the TM, is not the correct value. In that case, the card should be offlined and the appropriate port mode set.
LOG_INFO	System Node Maintenance, 49: Port Config Modified	This log indicates that the port config for a TM has been modified.	Port config of a link system node has been modified successfully.	There will be no data section for this log.	No corrective action is necessary.
LOG_INFO	System Node Maintenance, 61: FOC State OK	The specified CC nodes fiber optic cable has no faults detected.	Not Applicable	The data associated with this log contains the cfgIDNumber of the node that sent the FOC statechange message and the internal FOC fault type value. Example Control Shelf CC1: 0101 0101 0002 where the 3rd digit is the shelf number the 5th digit is the slot number and last digit is the Int. FOC fault type.	None

LOG_INFO	System Node Maintenance, 63: Isolation between extension shelves	This log indicates that the system forced a CC node to a disabled operational state. This transition was triggered to prevent message loss due to isolation occurring between extension shelves. Isolation between extension shelves occurs when communication faults (CC or fibre cable) on one extension shelf exist on one plane and communication faults on another extension shelf exist on the opposite plane. To prevent black holing of messages between these two shelves, the last shelf to experience a fault is isolated. This isolation is achieved by disabling both CC nodes on that shelf.	Refer to Description.	Not Applicable.	To recover the isolated shelf fix the faults (CC or fibre cable) which triggered this event. It may also be necessary to perform a manual load of a CC if the maximum number of system initiated boot attempts for a CC has been exceeded.
LOG_INFO	System Node Maintenance, 64: REX status	This log indicates the stage of the REX process	Refer to Description.	Not Applicable.	No action needed
LOG_INFO	Task Management, 07: Task Stack Margin Low	This log is generated when the Task Audit subsystem detects that a task is running with a low stack margin condition. An error has not occurred, but is possible and a corrective software solution is required.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_INFO	Task Management, 08: Task error has occurred	This log is generated when the Task Audit subsystem detects that a task is running in an error condition. Sample error conditions included a suspended task or a stack overflow condition.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	The system automatically initiates recovery of the affected system node. No manual action is required. Collected logs from the time period should be sent to your next level of support.

LOG_INFO	Task Management, 10: Unable to communicate with OAM Server. Attempting RTC recovery	This log is generated when the system detects that the OAM server on the active RTC is not responding. If the mate RTC is enabled the system will perform a switch of activity and attempt to recover the RTC that is not responding. An earlier log will indicate what command was currently being processed when the OAM server stopped responding.	A system command has not returned in the expected time limit and is preventing the OAM server from processing further user requests.	No additional information.	Contact your next level of support.
LOG_INFO	Time of Day, 02: Change in System Time of Day	This log is generated when there is a major change in the time of day of in the system.	The user at the USP GUI requested to change the system time of day, either manually or via SNTP.	The Information field indicates the time immediately before the time change and the name of the user who made the change.	No action is required.
LOG_INFO	Trace, 01: Trace Message	This log reports an MTP Level 3 trace event. This log is used only by Nortel Networks technical support.	An MTP Level 3 management event has occurred.	The Information and Data fields indicate the event content.	No action is required.
LOG_INFO, LOG_MINOR, LOG_MAJOR, LOG_CRITICAL	Network, 00: Network Connectivity Error	This log indicates that connectivity to an to an external network element has been lost	This log is caused by one of the following reasons: A network fault has occurred, such as a disconnected cable. A network element has been powered down or disconnected from the network. A fault in a network element has occurred.	The Information and Data fields indicate the name and IP address of the external network element.	Correct the network problem. Check the Ethernet hubs, cables, and the affected element.
LOG_MAJOR	Application DB Manager, 31: <Application> Database Failure	This log indicates that the database manager has detected a failure scenario from which it can not recover without craftsperson intervention.	User has changed the LSS type while an application database system node is in-service, or there has been a fatal error trying to access the disk files.	None	The card raising the alarm must be re-loaded.

LOG_MAJOR	ASM Interworking, 02: GSO Major Condition	The GSM SS7 Overload functionality is enabled but the Core missed sending us a heartbeat. This indicates that the Core is in Overload and the USP is starting to throttle traffic to help alleviate Core congestion.	Core is in overload.	The Information and Data fields indicate the ASM name.	Investigate the Core to determine why it is in overload.
LOG_MAJOR	ATM Device Driver, 08: Physical Device Excessive Interrupts	This log indicates that the IDT 77/105, 77106, or 77V1254 physical device generated excessive interrupts to the processor.	The physical device is detecting conditions on the ATM-25 backplane, or is exhibiting behavior itself, which warrants interrupting the processor. Interrupts are normal, however, this log indicates that the physical device is generating an inordinate number of interrupts, which is detrimental to system performance. Conditions include: Received Cell Symbol Error, Transmit Parity Error, Short Cell Received, Receive FIFO Overrun, and several others.	The Information and Data fields indicate that the physical device generated excessive interrupts to the processor.	Contact your next level of support.
LOG_MAJOR	Buffer Manager, 06: Major Buffer Depletion	This log is generated when the percentage of buffers in one of the buffer pools that are free or have been allocated for less than the office parameter SS7_BUFFER_ALLOCATE_MINS is less than the office parameter SS7_CNTL_BUF_MAJOR_PRCNT_REM	Memory leak.	The Information field indicates the pool that is affected and the percentage of the pool buffers allocated for more than the specified allocation time.	If active NPC or LLC raised alarm, perform SWACT. If SWACT succeeds then lock, load, and unlock the inactive NPC or LLC node immediately. If inactive RTC raised alarm, then lock, load, and unlock the inactive RTC immediately. If a LINK or active RTC raised alarm, then lock, load, and unlock troubled node in the next maintenance window.

LOG_Major	Configuration, 29: Missing Mate Node	The system generates this log when only one of a mated-pair system node is found on the same shelf in the system.	Either as a result of system node provisioning activity, or when one of a mated-pair system node is removed from the system.	No additional information is provided.	Make sure there are even number (ie, 0 or 2) of the mated-pair system node provisioned on the same shelf in the system.
LOG_MAJOR	Database Sync, 13: NFS Mount Daemon Exited	This alarm indicates that the NFS mount daemon on the problem RTC system node has unexpectedly exited. Recovery of an inactive RTC will be impossible if a corrective action is not taken.	An internal error has occurred.	There is no specific data.	The problem RTC system node needs to be rebooted. Contact your next level of support.
LOG_MAJOR	Disk Maintenance, 04: SCSI Disk Free Space Low	A high-water mark for available space on the SCSI disk has been passed. Space is limited. If the disk should be filled completely, it will become unavailable, causing the RTC system node to fail.	There are probably old data files and data snapshots on the disk that are no longer needed.	The Information field describes the error.	Delete unnecessary files from the disk to create more free space.
LOG_MAJOR	Disk Maintenance, 05: Disk Formatting	This log indicates that disk formatting is in progress.	A system node was unable to read information off the disk during initialization. Either the disk is corrupted or the disk was not formatted when it was installed.	The Information and Data fields indicate the amount of time the formatting is expected to take.	No action is required.
LOG_MAJOR	IPS7, 12: ASP alarm	If the ASP can not be mated, the alarm arise.	The asp is not mated with another asp	None.	Check the asp statics
LOG_MAJOR	Network Clock, 03: No Clock Error	This log is generated when the Network Clock subsystem determines that oscillators A and B are out of synch on a particular shelf in the system. This is a major alarm that is generated when both CC system nodes are disabled, or when the external clock sources are not available.	Both CC system nodes are disabled or the network clock cables are not connected properly.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Ensure that both CC system nodes are not disabled, and that the network clock cable connectors are attached properly.

LOG_MAJOR	Network, 03: Response to Bootp Request	The system did not receive a response to the bootp request.	The bootp server is not running - the bootp server it is not configured with the RTC MAC Address - if the bootp server and the system are not on the same subnet, bootp forwarding may not be configured on the intermediate routers.	The Information and Data fields may provide additional information	#NAME?
LOG_MAJOR	Network, 04: to Ping Alternate Boot Server	There was no response to a network ping of the alternate boot server ip address that was indicated in the bootp response	The bootp server may be configured with an incorrect ip address for the alternate boot server (Note: if the Distinct Bootp server that is shipped with the system is used, this ip address is not configurable, so this will not be the probable cause) - there is a network connectivity issue between the system and the alternate boot server.	The data field will contain the ip address for the alternate boot server that was indicated by the bootp response.	- verify that the bootp server is configured with the correct ip address for the alternate boot server - verify that there are no network connectivity issues between the system and the alternate boot server
LOG_MAJOR	Network, 05: to FTP to Alternate Boot Server	The system was unable to establish a FTP connection to the alternate boot server	The ftp server is not running - the userid and password is not setup on the ftp server.	The data field will indicate the reason for the failure	Verify that the ftp server is running - verify that the userid and password is setup on the ftp server.
LOG_MAJOR	Network, 06: to NFS Mount Alternate Boot Server			The Information and Data fields may provide additional information.	

LOG_MAJOR	Network, 07: Unable to Locate rtcboot file	The system was not able to locate the rtcboot file that was indicated in the bootp response.	- the ftp server is not exporting the directory that contains the rtcboot file - the bootp server is configured with the wrong rtcboot load location - the rtcboot file has been deleted	The Information and Data fields may provide additional information	Verify that the ftp server is exporting the directory that contains the rtcboot file (for example from a external ftp client) - verify that the bootp server is configured with the correct rtcboot file location - verify that the rtcboot file exists on the alternate boot server. if it missing, Reset the alternate boot server configuration for this system via the CLI/GUI or local alternate boot server configuration Manager application. this will rebuild the missing file.
LOG_MAJOR	Network, 08: Unable to Locate bootinfo file	The system was not able to locate the bootinfo file that should be present in the same directory as the rtcboot file.	The file has been deleted or renamed	The Information and Data fields may provide additional information	Reset the alternate boot server configuration for this system via the CLI/GUI or local Alternate Boot Server Configuration Manager application. This will rebuild the missing file.
LOG_MAJOR	Network, 09: Unable to Locate sysconf file	The system was not able to locate the sysconf file that should be present in the same directory as the rtcboot file.	The file has been deleted or renamed	The Information and Data fields may provide additional information	Reset the alternate boot server configuration for this system via the CLI/GUI or local Alternate Boot Server Configuration Manager application. This will rebuild the missing file.

LOG_MAJOR	Network, 10: ABS Unable to Parse bootinfo file	The system was not able to parse the bootinfo file	The file has been corrupted	The Information and Data fields may provide additional information	Reset the alternate boot server configuration for this system via the CLI/GUI or local Alternate Boot Server Configuration Manager application. This will rebuild the corrupted file.
LOG_MAJOR	Network, 11: Unable to Parse sysconf file	The system was not able to parse the sysconf file	The file has been corrupted	The Information and Data fields may provide additional information	Reset the alternate boot server configuration for this system via the CLI/GUI or local Alternate Boot Server Configuration Manager application. This will rebuild the corrupted file.
LOG_MAJOR	Network, 12: ABS Unable to Locate RTC Load	The load directory or rtc load was not found on the alternate boot server	- the load directory indicated in the bootinfo file was not found - the load file indicated in the sysconf file was not found - the release directory may have been uninstalled (deleted) - the bootinfo file may have been corrupted - the sysconf file may have been corrupted	The information field will indicate if the entire load directory was not found or just the rtc load itself	- Reinstall the release if it has been deleted in error - Reset the alternate boot server configuration for this system via the CLI/GUI or local Alternate Boot Server Configuration Manager application. This will rebuild the bootinfo and sysconf files to point to valid directory and rtc load
LOG_MAJOR	Network, 13: Unable to Locate RTC Snapshot	The snapshot directory was not found on the alternate boot server	- the snapshot directory indicated in the bootinfo file was not found - the snapshot directory may have been deleted - the bootinfo file may have been corrupted	The Information and Data fields may provide additional information	Reset the alternate boot server configuration for this system via the CLI/GUI or local Alternate Boot Server Configuration Manager application. This will rebuild the bootinfo file to point to valid snapshot directory.

LOG_MAJOR	Network, 14: RTC Load may be Invalid	The rtcboot load may be corrupted	The rtcboot file size does not match the file size of the rtc load indicated in the sysconf file. This may be the result of an incomplete file copy.	The Information and Data fields may provide additional information	Reset the alternate boot server configuration for this system via the CLI/GUI or local Alternate Boot Server Configuration Manager application. This will rebuild the rtcboot file.
LOG_MAJOR	Network, 15: RTC Snapshot may be Invalid	The snapshot directory may be corrupted	- the snapshot.des file is missing - the bootinfo file may be corrupted and be pointing to an invalid snapshot directory. - the snapshot may have been partially deleted	The Information and Data fields may provide additional information	Reset the alternate boot server configuration for this system via the CLI/GUI or local Alternate Boot Server Configuration Manager application. This will rebuild the rtcboot file.
LOG_MAJOR	SCCP Management, 33: LSS Congestion	A local subsystem instance availability state has changed to congestion, hence a congestion alarm is raised against the LSS itself as traffic destined for the congested instance will be UDTSED.	SCCP Routing has informed SCCP Management that the local subsystem instance is experiencing internal congestion.	No additional information is provided.	No action is required. Traffic rate is very high, and as a result some traffic is being UDTSED. Once traffic rate subsides, congestion will clear.
LOG_MAJOR	System Administration, 52: Emergency Access Account Active	The system generates this log when the connection to a remote authentication server is down and a user is logged in using the configured emergency access user-account.	User is logged in to debug an remote authentication issue.	none	none
LOG_MAJOR	System Administration, 56: Connection to Authentication server was lost	This log is generated by the audit routine that checks connections with the Remote Authentication server (two if two are provisioned) and updates the alarms. If one Remote Authentication IP is provisioned and it is not functioning or two are provisioned and both are not functioning this Alarm will be active.	Ethernet cable was pulled from the RTC, network connection was disrupted or the Remote Authentication server was deactivated.	none	Check connections, contact Remote Authentication server administrator. Lastly contact your next level of support.

LOG_MAJOR	System Node Maintenance, 38: Loss Of Signal	The specified CC node has experienced a Loss Of Signal (LOS) through its fiber-optic cable, as specified by GR-1248-CORE "Generic Requirements for Operation of ATM Network Elements". NOTE: In the USP LOS failure is cleared after 8 seconds where LOS defect is absent.	There is either a problem with the fiber-optic cable or a problem with the far-end CC's transmit hardware.	The data associated with this log contains the cfgIDNumber of the node that sent the FOC statechange message and the internal FOC fault type value. Example Control Shelf CC1: 0101 0101 0002 where 3rd digit is the shelf number (0) the 5th digit is the slot number (0) and the last digit is the Int. FOC fault type.	Please refer to the Alarm section of the USP Fault Management Manual for Loss Of Signal recovery procedures.
LOG_MAJOR	System Node Maintenance, 50: Loss Of Frame	The specified CC node has detected a Loss Of Frame (LOF) on its Rx fiber-optic cable as specified by GR-253-CORE: "Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria"	A persistent LOF fault in the USP would most likely indicate transmit hardware problems with the device at the far-end of the SONET segment(cable).	The data associated with this log contains the cfgIDNumber of the node that sent the FOC statechange message and the internal FOC fault type value. Example Control Shelf CC1: 0101 0101 0002 where the 3rd digit is the shelf number the 5th digit is the slot number and last digit is the Int. FOC fault type.	Please refer to the Alarm section of the USP Fault Management Manual for Loss Of Frame recovery procedures.
LOG_MAJOR	System Node Maintenance, 51: Loss Of Pointer	The specified CC node has detected a Loss Of Pointer (LOP) on its Rx fiber-optic cable as specified by GR-253-CORE: "Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria" NOTE: In the USP LOP failure is cleared when the LOP defect is absent for 8 seconds.	A persistent LOP failure in the USP would most likely indicate transmit hardware problems with the device at the far-end of the SONET segment(cable).	The data associated with this log contains the cfgIDNumber of the node that sent the FOC statechange message and the internal FOC fault type value. Example Control Shelf CC1: 0101 0101 0002 where the 3rd digit is the shelf number the 5th digit is the slot number and last digit is the Int. FOC fault type.	Please refer to the Alarm section of the USP Fault Management Manual for Loss Of Path recovery procedures.

LOG_MAJOR	System Node Maintenance, 52: Loss Of Cell Delineation	The specified CC node has detected a Loss of Cell Delineation on its Rx fiber-optic cable as specified by GR-1248-CORE: "Generic Requirements for Operation of ATM NE's" NOTE: In the USP system LCD failures are reported when an LCD defect persists for 750 milliseconds and LCD failures are cleared when and LCD defect is absent for 8 seconds.	A persistent LCD failure in the USP would most likely indicate transmit hardware problems with the device at the far-end of the SONET segment(cable).	The data associated with this log contains the cfgIDNumber of the node that sent the FOC statechange message and the internal FOC fault type value. Example Control Shelf CC1: 0101 0101 0002 where the 3rd digit is the shelf number the 5th digit is the slot number and last digit is the Int. FOC fault type.	Please refer to the Alarm section of the USP Fault Management Manual for Loss Of Cell Delineation recovery procedures.
LOG_MAJOR	System Node Maintenance, 53: Path Label Mismatch	The specified CC node has experienced a Path Label Mismatch (PLM) through its fiber-optic cable as specified by GR-253-CORE: "Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria" The path label is basically a byte in the SONET path overhead that is set by PTE (path terminating equipment) CC's and ATM switch in USP system that specifies the type of payload in the SONET payload envelope. For the USP system this payload type is ATM cells. NOTE: In the USP system PLM failure is cleared after 8 seconds where PLM defect is absent.	The far end device is not configured properly. I.e. The payload mapping is not configured for ATM cells.	The data associated with this log contains the cfgIDNumber of the node that sent the FOC statechange message and the internal FOC fault type value. Example Control Shelf CC1: 0101 0101 0002 where the 3rd digit is the shelf number the 5th digit is the slot number and last digit is the Int. FOC fault type.	Please refer to the Alarm section of the USP Fault Management Manual for Path Label Mismatch recovery procedures.
LOG_MAJOR	System Node Maintenance, 54: Alarm Indication Signal - Defect type maps to LOS	The specified CC node has detected loss of signal on a remote SONET segment via reception of ATM AIS cells with defect type that can be mapped to LOS. NOTE: ATM AIS cells can only be received in multishelf configuration where an ATM switch is present. It is the ATM switch which generates the ATM AIS cells. Currently all defect types received in ATM AIS cells are mapped to fault type ndShelfState::FOC_AISP_UNKNOWN and therefore this log will not currently be generated.	A persistent failure indicates either a failure on this reported CC's transmit cable or a transmit hardware failure on the reported CC node. Check the logs/alarms on the ATM switch.	The data associated with this log contains the cfgIDNumber of the node that sent the FOC statechange message and the internal FOC fault type value. Example Control Shelf CC1: 0101 0101 0002 where the 3rd digit is the shelf number the 5th digit is the slot number and last digit is the Int. FOC fault type.	Please refer to the Alarm section of the USP Fault Management Manual for Alarm Indication Signal Path - Loss Of Signal recovery procedures.

LOG_MAJOR	System Node Maintenance, 55: Alarm Indication Signal Path - Defect type maps to LOF	The specified CC node has detected loss of frame on a remote SONET segment via reception of ATM AIS cells with defect type that can be mapped to LOF. NOTE: ATM AIS cells can only be received in multishelf configuration where an ATM switch is present. It is the ATM switch which generates the ATM AIS cells. Currently all defect types received in ATM AIS cells are mapped to fault type ndShelfState::FOC_AISP_UNKNOWN and therefore this log will not currently be generated.	A persistent failure indicates a transmit hardware failure on the reported CC node. Check the log/alarms on the ATM switch.	The data associated with this log contains the cfgIDNumber of the node that sent the FOC statechange message and the internal FOC fault type value. Example Control Shelf CC1: 0101 0101 0002 where the 3rd digit is the shelf number the 5th digit is the slot number and last digit is the Int. FOC fault type.	Please refer to the Alarm section of the USP Fault Management Manual for Alarm Indication Signal Path - Loss Of Frame recovery procedures.
LOG_MAJOR	System Node Maintenance, 56: Alarm Indication Signal - Defect type maps to LOP	The specified CC node has detected loss of pointer on a remote SONET segment via reception of ATM AIS cells with defect type that can be mapped to LOF. NOTE: ATM AIS cells can only be received in multishelf configuration where an ATM switch is present. It is the ATM switch which generates the ATM AIS cells. Currently all defect types received in ATM AIS cells are mapped to fault type ndShelfState::FOC_AISP_UNKNOWN and therefore this log will not currently be generated.	A persistent failure indicates a transmit hardware failure on the reported CC node. Check the log/alarms on the ATM switch.	The data associated with this log contains the cfgIDNumber of the node that sent the FOC statechange message and the internal FOC fault type value. Example Control Shelf CC1: 0101 0101 0002 where the 3rd digit is the shelf number the 5th digit is the slot number and last digit is the Int. FOC fault type.	Please refer to the Alarm section of the USP Fault Management Manual for Alarm Indication Signal Path - Loss Of Path recovery procedures.
LOG_MAJOR	System Node Maintenance, 57: Alarm Indication Signal - Defect type maps to LCD	The specified CC node has detected loss of cell delineation on a remote SONET segment via reception of ATM AIS cells with defect type that can be mapped to LCD. NOTE: ATM AIS cells can only be received in multishelf configuration where an ATM switch is present. It is the ATM switch which generates the ATM AIS cells. Currently all defect types received in ATM AIS cells are mapped to fault type ndShelfState::FOC_AISP_UNKNOWN and therefore this log will not currently be generated.	A persistent failure indicates a transmit hardware failure on the reported CC node. Check the log/alarms on the ATM switch.	The data associated with this log contains the cfgIDNumber of the node that sent the FOC statechange message and the internal FOC fault type value. Example Control Shelf CC1: 0101 0101 0002 where the 3rd digit is the shelf number the 5th digit is the slot number and last digit is the Int. FOC fault type.	Please refer to the Alarm section of the USP Fault Management Manual for Alarm Indication Signal Path - Loss Of Path recovery procedures.

LOG_MAJOR	System Node Maintenance, 58: Alarm Indication Signal Path - Defect type maps to PLM	The specified CC node has detected path label mismatch on a remote SONET segment via reception of ATM AIS cells with defect type that can be mapped to LCD. NOTE: ATM AIS cells can only be received in multishelf configuration where an ATM switch is present. It is the ATM switch which generates the ATM AIS cells. Currently all defect types received in ATM AIS cells are mapped to fault type ndShelfState::FOC_AISP_UNKNOWN and therefore this log will not currently be generated.	A persistent failure indicates a transmit hardware failure on the reported CC node. Check the log/alarms on the ATM switch.	The data associated with this log contains the cfgIDNumber of the node that sent the FOC statechange message and the internal FOC fault type value. Example Control Shelf CC1: 0101 0101 0002 where the 3rd digit is the shelf number the 5th digit is the slot number and last digit is the Int. FOC fault type.	Please refer to the Alarm section of the USP Fault Management Manual for Alarm Indication Signal Path - Loss Of Path recovery procedures.
LOG_MAJOR	System Node Maintenance, 59: Alarm Indication Signal - Unknown Defect Type	The specified CC node has detected a fault on a remote SONET segment via reception of ATM AIS cells with defect type that cannot be mapped. NOTE: ATM AIS cells can only be received in multishelf configuration where an ATM switch is present. It is the ATM switch which generates the ATM AIS cells. Currently all defect types received in ATM AIS cells are mapped to fault type ndShelfState::FOC_AISP_UNKNOWN.	A persistent failure indicates a transmit hardware failure on the reported CC node. Check the log/alarms on the ATM switch.	The data associated with this log contains the cfgIDNumber of the node that sent the FOC statechange message and the internal FOC fault type value. Example Control Shelf CC1: 0101 0101 0002 where the 3rd digit is the shelf number the 5th digit is the slot number and last digit is the Int. FOC fault type.	Please refer to the Alarm section of the USP Fault Management Manual for Alarm Indication Signal Path - Loss Of Path recovery procedures.

LOG_MAJOR	System Node Maintenance, 60: RFI_L FOC STATE	The specified CC node has detected RFI_L on its fiber-optic cable. as specified by GR-253-CORE: "Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria" RFI_L is an indication that the device at the far-end of the SONET segment has detected a receive fault. NOTE: In the USP system RFI-L failure is cleared when RDI-L defect is absent for 8 seconds.	In dual shelf (directly connected CC's) configuration check the FOC logs/alarms on the other connected CC. If LOS log type then the CC node generating the RFI log has either a bad transmit cable or faulty transmit hardware, otherwise the CC generating the RFI most likely has a transmit hardware problem. In multishelf configuration involving an ATM switch check the logs/alarms on the ATM switch and if LOS log type then the CC node generating the RFI log has either a bad transmit cable or faulty transmit hardware, otherwise the CC generating the RFI most likely has a transmit hardware problem.	The data associated with this log contains the cfgIDNumber of the node that sent the FOC statechange message and the internal FOC fault type value. Example Control Shelf CC1: 0101 0101 0002 where the 3rd digit is the shelf number the 5th digit is the slot number and last digit is the Int. FOC fault type.	Please refer to the Alarm section of the USP Fault Management Manual for RFI FOC State recovery procedures.
LOG_MAJOR	TXMGR, 02: TXMGR TCB Memory very Low	The memory resources available for managing TCAP conversations is getting very low.	The rate of queries that require a TCAP conversation is too high.	A MAJOR alarm is raised and traffic to the congested local subsystem instance will be throttled.	No action is required.

LOG_MAJOR, LOG_CLEAR_MAJ OR	Power, 01: Status Change	A loss of one of the two -48V power feeds for this RTC, CC, or application system node has occurred. LOG_CLEAR indicates that fault with one of the two -48v power feeds has been corrected.	The loss of a shelf power feed could be the result of a pulled or cut shelf power cable. The loss of power to an individual RTC, CC, or application system node could be the result of a blown fuse on the TM. LOG_CLEAR means that shelf power feed has been fixed, and/or a TM with a blown fuse has been replaced.	No additional information is provided.	If similar power status alarms are received for each RTC, CC, and application system node on a shelf, it is likely that one of the power sources for the shelf has been interrupted, possibly through a pulled or cut cable, or through the loss of the power source. Perform the corrective action steps identified for this alarm in the USP Fault Management Manual. If a power status alarm is only received for one RTC, CC, or application system node on a shelf, perform the corrective action steps identified for this alarm in the USP Fault Management Manual. In case of LOG_CLEAR no action is required.

LOG_MAJOR, LOG_CLEAR_MAJ OR	System Node Maintenance, 65: REX did not complete	This alarm is raised when an RTC Routine Exercise Test has been aborted for one of the following reasons: - user request - mated nodes are not unlocked and enabled - a critical alarm is unresolved - unexpected RTC state change may have occurred (i.e. by another user) - alternate boot audit did not pass (this test is performed at the start of the rex cycle only) - a CLI bulk input is in progress	Refer to Description.	Not Applicable.	This alarm may indicates that REX aborted while one of the RTCs was locked. The state of RTC 12 and 15 needs to be verified and the RTC must be recovered (if required). If both RTC are in-service then no action is required. This alarm will clear on the next Successful REX cycle (either the next scheduled REX or a manually initiated REX cycle).
LOG_MAJOR, LOG_CLEAR_MAJ OR, LOG_INFO	System Node Maintenance, 03: Disable State Transition	This log occurs when RTC, CC, or application system node operational state transitions from enabled to disabled. LOG_CLEAR indicates that the alarm is cleared and RTC, CC or application system node state is enabled. LOG_INFO records the state transition from enabled to disabled.	The RTC, CC, or application system node has encountered an internal failure. In the case of LOG_CLEAR the RTC, CC or application system node has been recovered from a disabled state to enabled. LOG_INFO is caused when user requests an off-line operation on the RTC, CC, or application node.	The Information field indicates the transition to the disabled operational state, this also applies to LOG_INFO. In case of LOG_CLEAR the Information field indicates that the alarm for a disabled state is being cleared.	The system automatically initiates recovery of the affected RTC, CC, or application system node. No action is required. In case of LOG_CLEAR and LOG_INFO also no action is required.
LOG_MAJOR, LOG_NONE	SCCP Management, 25: RSS Alarm	An alarm will be asserted against a remote subsystem (RSS) when a Subsystem Prohibited (SSP) message is received from the far end. It will be only one alarm more than one RSS failure. LOG_MAJOR: At least one RSS is prohibited. LOG_NONE: All RSSs are available.	RSS failure in the far end.	The log will indicate the severity of the alarm.	Search from Alarm Status field on the RSS Record of the RSS GUI to find out which RSS/RSSs is/are prohibited.

LOG_MINOR	Application DB Manager, 06: <Application> Database is Full	An attempt was made to add another record to the Number Portability database when it already contained the maximum number of records. This alarm will clear if a record is deleted from the database.	Too many records were received from the LSMS.	No additional information is available.	Change the LSMS filtering criteria for this STP to be more restrictive in selecting which Application records are to be forwarded from the LSMS.
LOG_MINOR	Application DB Manager, 19: LSS on Active NPC is Deactivated	The Application local subsystem instance running on the active NPC system node is in the "deactivated" local subsystem administrative state. This situation prevents any updates received from the LSMS from being processed.	Both NPC system nodes are deactivated or a manual SWACT has been performed to make the deactivated NPC system node active.	No additional information is provided.	Make sure that at least one NPC system node is in the "activated" local subsystem administrative state and/or perform a SWACT to make the "activated" NPC system node active.
LOG_MINOR	Application DB Manager, 20: <Application> Database Lost Synchronization	The Application database on an application database system node has lost synchronization with the databases on other application database system nodes. During the time that the database is unsynchronized, the Application subsystem instance will be unavailable to handle Application query traffic. The system will attempt to retrieve the missed updates from the Application database on another application database system node. Once the database is resynchronized, the Application subsystem instance will automatically return to the "allowed" state if the local subsystem administrative state for this instance is "activated".	An update message sent between application database system nodes was missed.	No additional information is provided.	No action is required.
LOG_MINOR	Application DB Manager, 46: LSS on Active LLC is Deactivated	The Application local subsystem instance running on the active LLC system node is in the "deactivated" local subsystem administrative state. This situation prevents any updates received from the LSMS from being processed.	Both LLC system nodes are deactivated or a manual SWACT has been performed to make the deactivated LLC system node active.	No additional information is provided.	Make sure that at least one LLC system node is in the "activated" local subsystem administrative state and/or perform a SWACT to make the "activated" LLC system node active.

LOG_MINOR	ASM Interworking, 03: GSO Minor Condition	The GSM SS7 Overload functionality is enabled and the Core has notified the USP that it is near maximum capacity. A minor alarm is raised as messages may be discarded if traffic is higher than current allowed level.	Core is near maximum capacity.	The Information and Data fields indicate the ASM name.	Investigate the Core as it may shortly go into overload.
LOG_MINOR	Boot, 01: Hardware Mismatch	The boot manager has detected a mismatch between configured and installed hardware.	The installed mission card is different than the card that has been configured for this slot.	The Information field includes the PEC and serial number the system reads from the installed card.	Compare the configuration data with the actual card in the slot. If the incorrect card is installed, take the affected RTC, CC, or application system node off-line. Replace the incorrect card with the correct one and initiate loading of the system node. If the card information has been configured incorrectly, take the affected RTC, CC, or application system node off-line. Correct the information and initiate loading of the node.

LOG_MINOR	Buffer Manager, 05: Minor Buffer Depletion	This log is generated when the percentage of buffers in one of the buffer pools that are free or have been allocated for less than the office parameter SS7_BUFFER_ALLOCATE_MINS is less than the office parameter SS7_CNTL_BUF_MINOR_PRCNT_REM	Memory leak.	The Information field indicates the pool that is affected and the percentage of the pool buffers allocated for more than the specified allocation time.	If active NPC or LLC raised alarm, perform SWACT. If SWACT succeeds then lock, load, and unlock the inactive NPC or LLC node immediately. If inactive RTC raised alarm, then lock, load, and unlock the inactive RTC immediately. If a LINK or active RTC raised alarm, then lock, load, and unlock troubled node in the next maintenance window.
LOG_MINOR	Configuration, 27: Data Boot Pointer Mismatch	The system generates this log when the data boot pointer on an RTC system node is changed to a data snapshot other than the running data snapshot.	It is a step in the process of restoring a data snapshot database.	No additional information is provided.	Consult the USP documentation for information on restarting the system after changing the data boot pointer, or set the data boot pointer back to the running data snapshot.
LOG_MINOR	Configuration, 28: Boot Image Mismatch	The system generates this log when the boot image on an RTC system node is changed to an image other than the running image.	It is a step in the process of changing the boot image.	No additional information is provided.	Consult the USP documentation for information on restarting the system after changing the boot image, or set the boot image back to the running image.
LOG_MINOR	Configuration, 37: Running image does not match mate.	This log is generated by the configuration management subsystem when the running image on an RTC, CC, NPC or LLC does not match its mate's. The check is performed whenever a node transitions to ENABLED. A CC is only required to match its mate (on same shelf). There is no requirement for CCs to match those on a different shelf.	Both mates were not updated to match each other.	None	Set the boot image to match between all RTCs, CCs, NPCs or LLCs

LOG_MINOR	Data Audit, 01: Database Synchronization Lost	This log is generated when a database loses synchronization on the specified RTC system node or application system node.	This log is caused by a lost database update message and/or a failed database reload.	The Information and Data fields indicate the name of the database that has lost synchronization and note that the associated RTC system node or application system node should be reset.	The periodic data auditing facility should automatically re-load the affected RTC system node or application system node within approximately six minutes. If this does not happen, perform a load operation on the affected RTC system node or application system node. Refer to the System Management section of the User Guide for more information. If loading the affected RTC system node or application system node does not correct the problem, contact your next level of support.
LOG_MINOR	IPS7, 09: AS destination deactivated alarm	At least one ASP destination is manually deactivated.	If the alarm is LOG_MINOR: At least one ASP destination was manually deactivated.	None.	Activate all ASP destinations which were manually deactivated.
LOG_MINOR	IPS7, 10: ASP deactivated alarm	At least one ASP is manually deactivated.	If the alarm is LOG_MINOR: At least one ASP was manually deactivated.	None.	Activate all ASPs which were manually deactivated.
LOG_MINOR	IPS7, 11: ASP path deactivated alarm	At least one ASP path is manually deactivated.	If the alarm is LOG_MINOR: At least one ASP path was manually deactivated.	None.	Activate all ASP paths which were manually deactivated.
LOG_MINOR	MTP Level 3 Event, 48: Routeset Deactivated Alarm	At least one routeset is manually deactivated.	If the alarm is LOG_MINOR: At least one routeset was manually deactivated.	None.	Activate all the routesets which were manually deactivated.

LOG_MINOR	MTP Level 3 Event, 49: Linkset Deactivated Alarm	At least one linkset is manually deactivated.	If the alarm is LOG_MINOR: At least one linkset was manually deactivated.	None.	Activate all the linksets which were manually deactivated.
LOG_MINOR	MTP Level 3 Event, 50: Link Deactivated Alarm	At least one link is manually deactivated.	If the alarm is LOG_MINOR: At least one link was manually deactivated.	None.	Activate all the links which were manually deactivated.
LOG_MINOR	Network Clock, 01: Oscillator A Error	This log is generated when the Network Clock subsystem determines that oscillator A is out of synch on a particular shelf in the system. This is a minor alarm that is generated when the CC system node in slot 1 is disabled, or when the external clock source is not available.	The CC system node in slot 1 is disabled or the network clock cable is not connected properly.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Ensure that the CC system node in slot 1 is not disabled and that the network clock cable connector is attached properly.
LOG_MINOR	Network Clock, 02: Oscillator B Error	This log is generated when the Network Clock subsystem determines that oscillator B is out of synch on a particular shelf in the system. This is a minor alarm that is generated when the CC system node in slot 18 is disabled, or when the external clock source is not available.	The CC system node in slot 18 is disabled or the network clock cable is not connected properly.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Ensure that the CC system node in slot 18 is not disabled, and that the network clock cable connector is attached properly.
LOG_MINOR	System Administration, 44: Maximum Snapshots Exist	This log is generated by the snapshot audit function after RTC initialization if the number of data snapshots that exists on the SCSI disk associated with an RTC system node is greater than 5.	This occurs when the maximum number of snapshots on the SCSI disk associated with an RTC system node is greater than five.	The Information field indicates the maximum number of data snapshots already exists on the SCSI disk associated with an RTC system node.	Delete some of the existing data snapshots from the SCSI disk associated with the RTC system node.
LOG_MINOR	System Administration, 57: Connection to Authentication server was compromised	This log is generated by the audit routine that checks connections with the Remote Authentication server (two if two are provisioned) and updates the alarms. If two Remote Authentication IP's are provisioned and one is not functioning then this Alarm will be active.	Network connection was disrupted or the Remote Authentication server was deactivated.	The IP of the Remote Authentication server to which the connection was lost.	Check connections, contact Remote Authentication server administrator. Lastly contact your next level of support.

LOG_MINOR	System Node Maintenance, 62: Information	This log is generated by the system node maintenance subsystem when lock timeout can not be cleared	If the timeout had previously been canceled.	There is no data associated with this log.	No action is required. The system always allows a node to LOCK once the timeout has occurred.
LOG_MINOR	Time of Day, 03: Timeout while waiting for SNTP server reply	This log is generated when the sntp client times out while waiting for a reply from the server.	The IP address of the SNTP server supplied to the USP GUI is incorrect or the SNTP server is not responding.	The Information field indicates the IP address of the server that failed to respond.	Supply the IP address of a working SNTP server. When the system receives a response to its queries, the alarm will be cleared.
LOG_MINOR	Time of Day, 04: Problem with received SNTP packet	This log is generated when the SNTP client receives invalid data from the SNTP server.	The IP address of the SNTP server supplied to the USP GUI points to a device that is not a synchronized SNTP server , or another machine sent data to the client.	The information field indicates if the alarm was raised due to the IP address supplied points to a SNTP device that is not synchronized or not a server, or if another machine sent the data.	Supply the IP address of a working SNTP server. When the system receives a response to its queries, the alarm will be cleared.
LOG_MINOR	TXMGR, 01: TXMGR TCB Memory Low	The memory resources available for managing TCAP conversations is getting low.	The rate of queries that require a TCAP conversation is too high.	A MINOR alarm is raised.	No action is required.
LOG_MINOR or LOG_MAJOR or LOG_CRITICAL	AA1 Driver, 09: CRC Err Count Threshold Reached	The system generates this log when CRC Error Count crosses the defined value of threshold.	number of Plane 1 CRC errors or Plane 2 CRC errors become greater than the threshold value.		Contact your next level of support.
LOG_MINOR or LOG_MAJOR or LOG_CRITICAL	AA1 Driver, 10: Plane Msg Count Threshold Reached	The system generates this log when Plane Msg Count crosses the defined value of threshold.	The difference of Plane 1 Msg Count and Plane2 Msg Count becomes greater than the threshold value.		Contact your next level of support.
LOG_MINOR or LOG_MAJOR or LOG_CRITICAL	AA1 Driver, 11: Raw Cell Count Threshold Reached	The system generates this log when Raw Cell Count crosses the defined value of threshold.	The number of ATM raw cells become greater than the threshold value.		Contact your next level of support.
LOG_MINOR or LOG_MAJOR or LOG_CRITICAL	AA1 Driver, 12: Raw Msg Count Threshold Reached	The system generates this log when Raw Msg Count crosses the defined value of threshold.	The number of ATM raw messages become greater than the threshold value.		Contact your next level of support.

LOG_MINOR or LOG_MAJOR or LOG_CRITICAL	AA1 Driver, 13: Seq.No.Reset Count Threshold Reached	The system generates this log when Sequence Number Reset Count crosses the defined value of threshold.	The number of number of times the sequence numbers are reset due to the receipt of five consecutive duplicate cells become greater than the threshold value.		Contact your next level of support.
LOG_MINOR or LOG_MAJOR or LOG_CRITICAL	Audit Facility, 02: RTC Sanity Threshold Reached	The system generates this log when RTC Sanity Count crosses the defined value of threshold.	Either RTC12 Passive Audit Count or RTC15 Passive Audit Count become greater than the defined threshold value, i.e., RTC12 or RTC15 does not receive audit request for defined number of times.		Contact your next level of support.
LOG_MINOR or LOG_MAJOR or LOG_CRITICAL	MTP Level 3 Event, 45: Link Utilization Threshold Reached	The system generates this log when Link Utilization OM crosses the defined value of threshold.	The present configuration is not enough to handle traffic.		To adjust the traffic or number of links as given in the technical specifications.
LOG_MINOR or LOG_MAJOR or LOG_CRITICAL	Processor Exception, 10: SWERR received Threshold Reached	The system generates this log when Swerr received count OM exceeds the defined value of threshold in the latest 5 mins.	Swerr received threshold reached		Contact your next level of support.
LOG_MINOR or LOG_MAJOR or LOG_CRITICAL	Processor Exception, 11: TRAP received Threshold Reached	The system generates this log when Trap received count OM exceeds the defined value of threshold in the latest 5 mins.	Trap received threshold reached		Contact your next level of support.
LOG_MINOR or LOG_MAJOR or LOG_CRITICAL	SCTP, 07: SCTP re- xmit Threshold Reached	The system generates this log when SCTP retransmitted chunks OM crosses the defined value of threshold.	Network problem.		Contact your next level of support.
LOG_MINOR or LOG_MAJOR or LOG_CRITICAL	Task Management, 09: Idle Task Starvation Threshold Reached	The system generates this log when Idle Task Duration crosses the defined value of threshold.	Idle Task Duration OM attains a value less than the defined threshold value, i.e., system is too busy.		Contact your next level of support.

LOG_MINOR, LOG_CLEAR_MIN OR	AA1 Driver, 08: ATM backplane failure	This log indicates an ATM-25 backplane failure for a system node or alleviation of that failure.	There is a hardware problem. The plane fault audit detected an idle backplane. The audit is scheduled to run every 30 seconds. Both ATM-25 backplanes are checked. If no messages have been received since the last audit and there is a hardware fault present on the physical device, the alarm is raised.	The Information field describes the failure or that the condition has been cleared. The data field contains the contents of the ISR (Interrupt Status Register) for each IDT77105 PHY device. The IDT77105 PHY is the physical device interfacing to the ATM-25 backplane. PHY_0 is connected to the backplane provided by CC Slot 1. PHY_1 is connected to the backplane provided by CC Slot 18.	If similar alarms are received for each application system node on a shelf, it is likely that one of the CC has a hardware problem. If the alarm is received for one system node possibly the fault is located on that system node. Perform the corrective action steps identified for this alarm in the USP Fault Management Manual. If LOG_CLEAR is received no action is required.
LOG_MINOR, LOG_CLEAR_MIN OR	Application SMI, 12: No LSMS Connections Active	This alarm is raised when there are no logged in connections from the LSMS to the application database controller system node. Upon system startup, this alarm will be raised if no connection exists 60 seconds after the application subsystem on the application database controller system node goes into the "allowed" local subsystem state.	The LSMS is down, an invalid user ID and/or password has been datafilled in the LSMS, or there is no network connectivity between the application database controller system node and the LSMS.	LOG_MINOR: No LSMS connections are active LOG_CLEAR_MINOR: No LSMS connections condition cleared	Check network connectivity and the LSMS functional state. Also check that the user ID and password used by the LSMS is correct.

LOG_MINOR, LOG_CLEAR_MIN OR	Application SMI, 15: Session unsynchronized	This alarm is raised when the SMI session goes to unsynchronize, that is: the SMI message Header of the SMI messages is missing.	A network transmit problem causing the lost of data, or the LSMS is not sending correct format SMI message.	LOG_MINOR: Session unsynchronized - resynchronize ongoing LOG_CLEAR_MINOR: Session resynchronize success	No specific action is needed, the USP is trying resynchronize itself. And the result will be reported. There is 4 possible results: 1. When searching fails: after searching the whole SMI buffer (default size: 8k), report the log-swerr "Session unsynchronized - terminating" and terminate the session. The "NP SMI SESSION UNSYN" alarm will be cleared after session terminated. 2. When search success, the alarm is cleared, then reread the buffer and process the SMI updates. 3. When no more data is in the SMI buffer before the re-syn function find the SMI HEADER, it will just wait for more data from the LSMS. 4. If the user re-establish the SMI session when he/she sees the alarm, also clears the alarm. And because the resyn action is on-going, the user's re-establish action will cause the buffer reading error, a log-info indicating "Socket read failed" will be generated.

LOG_MINOR, LOG_CLEAR_MIN OR	Boot, 04: Boot Failure	The booting of an RTC, CC, or application system node has been aborted. The system node will not recover without manual intervention. LOG_CLEAR means the system node has recovered after booting of that node has been aborted.	The system was unable to recover the system node within the maximum number of booting attempts. LOG_CLEAR means that user corrected the problem causing the boot error and manually loaded the system node, which recovered and became enabled.	No additional information is provided.	Make sure at least one CC system node on the same shelf as the affected system node is enabled. Verify that the front and rear cards of the system node are both seated properly. Check for any logs from the node that may indicate booting or initialization errors. If you are unable to determine the cause of the failure through other logs, replace front and rear cards and initiate loading. See the USP Fault Management Manual for more information. LOG_CLEAR indicates that no action is required.
LOG_MINOR, LOG_CLEAR_MIN OR	System Node Maintenance, 66: Node manually locked	This log is generated by the system when a node is manually locked	A node in the system gets manually locked	The Information field indicates the shelf and the node that is manually locked	Unlock the node as indicated by the information field.

LOG_MINOR, LOG_MAJOR, LOG_CLEAR_MIN OR, LOG_CLEAR_MAJ OR	Shelf, 02: Fan Status	A fault in the fan unit for a shelf has occurred. LOG_CLEAR means that the fault in the fan unit of a shelf has been corrected.	An individual fan has failed. In case of LOG_MAJOR the entire fan unit may have been removed and individual fans may have failed. LOG_CLEAR_MINOR indicates that an individual fan has been replaced. While LOG_CLEAR_MAJOR indicates that individual fans have been replaced, or the entire fan unit has been replaced.	The Information field indicates whether the status has changed for an individual fan, or for the entire fan unit. The Data field indicates which fans are not operating, if applicable. In case of LOG_CLEAR no additional information is provided.	The shelf cooling system is not operating as efficiently as it should. Rectify this problem as soon as possible. Refer to the USP Fault Management Manual for more information. In case of LOG_MAJOR if the log indicates that the fan unit is not present, the entire fan shelf has been removed. This is a serious fault. Replace the fan unit immediately to prevent overheating of the equipment in the shelf. If the log indicates that more than one fan has failed, this is a serious fault that will result in overheating of equipment on the shelf. Rectify this situation immediately. Refer to the USP Fault Management Manual for more information. In case of LOG_CLEAR no action is required.

LOG_MINOR, LOG_MAJOR, LOG_CLEAR_MIN OR, LOG_CLEAR_MAJ OR	Shelf, 03: Temperature Fault	A temperature fault has been detected. In case of LOG_CLEAR the temperature fault has been cleared.	The temperature has fallen below the minimum operating temperature. Operating the system below recommended temperatures can cause permanent damage to system components. In case of LOG_MAJOR the temperature has exceeded the maximum operating temperature. Operating the system at above recommended temperatures can permanently damage system components. LOG_CLEAR_MINOR indicates that the temperature has risen above the minimum operating temperature while LOG_CLEAR_MAJOR means that the temperature has fallen below the maximum operating temperature.	No additional information is provided.	Ensure that the ambient temperature in the room where the system is located is acceptable. In case of LOG_MAJOR check for fan alarms to determine whether one or more of the fans for the shelf has failed. If there are no fan alarms, ensure that the ambient temperature in the room where the system is located is acceptable. In case of LOG_CLEAR no action is required.
LOG_MINOR, LOG_MAJOR, LOG_CRITICAL	IPS7, 01: IPS7 Path Alarm	The path is not up, it is restoring, and the node is enabled and unlocked.	The Path is attempting to go up, but has not succeeded. There are several possible causes: There is a facility problem. The far end is not acknowledging path up messages. There is a software error.	The Information and Data fields indicate the Application Server Processor Path ID.	See the USP Fault Management manual.

LOG_MINOR, LOG_MAJOR, LOG_CRITICAL	IPS7, 08: IPS7 AS Alarm	At least one AS internal routeset is in less than the "ideal" state.	If the alarm is LOG_MINOR: None. If the alarm is LOG_MAJOR: At least one AS is not able to use its primary route. if the alarm is LOG_CRITICAL: At least one AS is inactive where the ASP(s) is/are restoring.		See the USP Fault Management manual.
LOG_MINOR, LOG_MAJOR, LOG_CRITICAL	MTP Level 3 Event, 17: Link Alarm	The link is not aligned but it is activated, and the node is enabled and unlocked.	The link is attempting to activate, but not succeeding. There are several possible causes: There is a facility problem. The far end is not attempting to align. There is a software error.	The Information and Data fields indicate the signaling link ID.	See the USP Fault Management manual.
LOG_MINOR, LOG_MAJOR, LOG_CRITICAL	MTP Level 3 Event, 39: Routeset Alarm	At least one routeset is in less than the "ideal" state.	If the alarm is LOG_MINOR: At least one link to a destination is unavailable (as long as it is not the last link in the linkset). If the alarm is LOG_MAJOR: At least one of the routes to a destination is unavailable. if the alarm is LOG_CRITICAL: All routes to a destination are unavailable.	None.	See the USP Fault Management manual.

LOG_MINOR, LOG_MAJOR, LOG_CRITICAL	MTP Level 3 Event, 46: Xlist Alarm	At least one routeset is in less than the "ideal" state on the Xlist Table.	If the alarm is LOG_MINOR: At least one link to a destination is unavailable (as long as it is not the last link in the linkset). If the alarm is LOG_MAJOR: At least one of the routes to a destination is unavailable. if the alarm is LOG_CRITICAL: All routes to a destination are unavailable.	None.	See the USP Fault Management manual.
LOG_MINOR, LOG_MAJOR, LOG_CRITICAL	SS7 Data, 05: table is almost full	This log is generated when raise alarms when MHD table is almost full	MHD table is almost full	Raise alarms when MHD table is almost full.	Contact your next level support.
LOG_NONE, LOG_MINOR, LOG_MAJOR, LOG_CRITICAL	SCCP Management, 13: LSS Alarm	An alarm will be asserted against a local subsystem when the availability status of the local subsystem instances indicates a service affecting condition. LOG_CRITICAL: No instances are allowed or congested. LOG_MAJOR: Only one instance is allowed or congested and the required instance value provisioned on the LSS form is 2 or higher. LOG_MINOR: The number of allowed and congested instances is below required value.	Alarms can be caused by instance node failure, or application suspending routing.	The log will indicate the severity and the local subsystem number.	See the USP Fault Management Manual.
LOG_SWERR	AA1 Driver, 02: Release Buffer Error	The system generates this log when an attempt to release a system data buffer fails.	There is a bad buffer pointer.	The Information field describes the failure. The Data field contain the return code from the pool_release_buffer routine.	Contact your next level of support.

LOG_SWERR	AA1 Driver, 03: Driver Resource Error	This log indicates an AA1 driver resource failure.	The AA1 driver resource is exhausted.	The Information field describes which specific resource was exhausted. The Data field contains the failure parameter in hexadecimal data.	Contact your next level of support.
LOG_SWERR	AA1 Driver, 04: Driver Transmit Error	This log indicates an AA1 driver PDU transmit failure.	A transmit buffer descriptor error occurred.	The Information field describes the failure. The Data field contains the failure parameter in hexadecimal data.	Contact your next level of support.
LOG_SWERR	AA1 Driver, 05: Driver PCI Error	This log indicates an AA1 driver PCI failure.	An AA1 module is missing or has failed.	The Information field describes the failure. The Data field contains the failure parameter in hexadecimal data.	Contact your next level of support.
LOG_SWERR	AA1 Driver, 06: Driver Protocol Error	This log indicates an AA1 driver protocol failure.	There is an invalid protocol type in the message, probably due to a corrupted message.	The Information field describes the failure. The Data field contains the failure parameter in hexadecimal data.	Contact your next level of support.
LOG_SWERR	AA1 Driver, 07: AA1 OM Collection Error	This log indicates an AA1 OM collection failure.	Database or software errors occurred during collection of AA1 driver OMs.	The Information field describes the failure. The Data field contains the failure parameter in hexadecimal data.	Contact your next level of support.
LOG_SWERR	Activity, 00: Callback Resources Exhausting	The number of applications using the activity facility is approaching its capacity.	This log allows you to track the use of the activity facility. It does not indicate a problem.	The Information and Data fields indicate the remaining available slots.	Contact your next level of support.
LOG_SWERR	Activity, 02: UDP Error Encountered	The task encountered an error involving an incoming UDP message.	The UDP resources are exhausted.	The Information and Data fields indicate the received socket address.	Contact your next level of support.
LOG_SWERR	Activity, 03: Invalid Activity State	The task attempted to enter an invalid state.	Memory is corrupted or there is another software problem.	No additional information is provided.	Contact your next level of support.

LOG_SWERR	Activity, 04: Invalid Message Received	The task received an invalid message.	Memory is corrupted or there is another software problem.	The Information and Data fields indicate the invalid message received.	Contact your next level of support.
LOG_SWERR	Activity, 05: Could Not Open UDP Socket	The task could not open a UDP socket.	There is a UDP resource problem.	The text shows the task was unable to allocate a socket and/or unable to get the host IP address.	Contact your next level of support.
LOG_SWERR	Activity, 07: Activity Mate Not Set	The system generates this log when a node cannot find its mate's IP address during initialization.	The system attempts to get the mate IP of a non-RTC mated node prior to the mate IP address being set.	No additional information is available.	Contact your next level of support.
LOG_SWERR	Activity, 08: Activity Timed Out Resolution	During initialization, the node did not resolve activity within a specified time limit.	A UDP message was lost, which triggers activity resolution, or the activity task ran into unexpected complications.	No additional information is available.	The system will automatically attempt to recover the node. If the node continues to fail, contact your next level of support.
LOG_SWERR	Application Audit, 00: <Application> Audit Software Error	The system generates this log when the Application Audit task encounters an unexpected condition. You should report this error to Nortel Networks technical support.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	Application Database, 01: File Create Failed	A file could not be created by the operating system.	No file descriptors may be available or the driver returned an error.	File create failed (ee): (fn) (ee) Internal error code (fn) The name of the file	Contact your next level of support.
LOG_SWERR	Application Database, 02: File Open Failed	A file is not available.	Probably a hardware problem.	File open failed (ee): (fn) (ee) Internal error code (fn) The name of the file	Contact your next level of support.
LOG_SWERR	Application Database, 03: File Close Failed	A file did not close correctly.	There is probably a hardware problem.	File close failed (ee): (fn) (ee) Internal error code (fn) The name of the file	Contact your next level of support.
LOG_SWERR	Application Database, 04: File Read Failed	The system encountered a failure while reading a file.	There is probably a hardware problem.	File read failed (ee): (fn), where: (ee) is the internal error code (fn) is the name of the file	Contact your next level of support.

LOG_SWERR	Application Database, 05: File Write Failed	The system encountered a failure while writing to a file.	There may be a hardware problem, or the disk may be full.	File write failed (ee): (fn), where: (ee) is the internal error code (fn) is the name of the file	Contact your next level of support.
LOG_SWERR	Application Database, 06: File Seek Failed	An Lseek system call failed.	There is probably a hardware problem.	File seek failed (ee): (fn), where: (ee) is the internal error code (fn) is the name of the file	Contact your next level of support.
LOG_SWERR	Application Database, 07: File Flush Failed	The system was unable to sync file contents to the physical disk. An ioctl system call to flush to the disk failed.	There is probably a hardware problem.	File flush failed (ee): (fn), where: (ee) is the internal error code (fn) is the name of the file	Contact your next level of support.
LOG_SWERR	Application Database, 08: File Delete Failed	The system was unable to delete a database file from disk.	There is probably a hardware problem.	File delete failed (ee): (fn), where: (ee) is the internal error code (fn) is the name of the file	Contact your next level of support.
LOG_SWERR	Application Database, 09: File Integrity - Wrong File Signature	The file does not have the correct file signature value in its header. This log is used only by Nortel Networks technical support.	An incorrect version of a file was used.	Invalid file signature (sig): (fn), where: (sig) is the invalid signature value found in the file header (fn) is the name of the file The Data field will contain the full contents of the file header. The file does not have the correct file signature value in its header. Its contents have not been used.	This problem is self-correcting if another Application system node contains a valid Application database. In this case, the database will be transferred from an Application node that has a good database. Contact your next level of support.

LOG_SWERR	Application Database, 10: File Integrity - Wrong Version Number	The file does not have the correct version number value in its header.	An incorrect version of the file was used.	Invalid file version (ver): (fn), where: (ver) is the invalid version value found in the file header (fn) is the name of the file The Data field will contain the full contents of the file header. The file does not have the correct version number value in its header. Its contents have not been used.	This problem is self-correcting if another Application system node contains a valid Application database. In this case the database will be transferred from an Application node that has a valid database. Contact your next level of support.
LOG_SWERR	Application Database, 11: File Missing	A database file is missing. This log is used only by Nortel Networks technical support.	A database file has been deleted or corrupted.	Database file missing or invalid (rc): (fn), where: (rc) is the internal return code (fn) is the name of the file A necessary database file is missing or has an invalid format.	This problem is self-correcting if another Application system node contains a valid Application database. In this case the database will be transferred from an Application node that has a valid database. Contact your next level of support.
LOG_SWERR	Application Database, 14: Record Exists	When loading records (from disk or bulk load file) two records with the same Directory Number Key were found with different data.	The bulk load data file has two records with the same key.	DN (dn) in Record (rn) and (rn), where: (dn) is the Directory Number Key (rn) is the Record number (1 based)	Correct the records in the bulk load data file.
LOG_SWERR	Application Database, 15: Record Not Loaded	When loading records (from disk or bulk load file) the index memory block became full. Additional records were not loaded.	The Index Memory Block is set too small.	Index Full (n) Record(s) not loaded, where: (n) is the number of records not loaded	Contact your next level of support.

LOG_SWERR	Application Database, 16: Index Node in Record Memory	When loading records (from disk or bulk load file) an Index type node was found in the Record memory.	The Record Memory Block is corrupted. The Data field will contain the full contents of the index node.	Index Node (rn) found in Record Memory, where: (rn) is the record number (1 based) where index node was found	This problem is self-correcting if another Application system node contains a valid Application database. In this case the database will be transferred from an Application node that has a valid database. Contact your next level of support.
LOG_SWERR	Application Database, 17: Node Invalid	A Record or Index Node with an invalid type was found or the node failed a check sum.	The Record or Index Memory Block is corrupted. The Data field will contain the full contents of the node.	Record (rn) Invalid, where: (rn) is the Record number (1 based) Or Index (rn) Invalid, where: (rn) is the Index number (1 based)	This problem is self-correcting if another Application system node contains a valid Application database. In this case the database will be transferred from an Application node that has a good database. Contact your next level of support.
LOG_SWERR	Application Database, 18: <Application>DB Semaphore Operation Failed	An operation on an Application database semaphore failed.	An internal error has occurred.	<Application>DB semaphore (op) operation failed (ee), where: (op) is the operation type (ee) is the internal error code.	Contact your next level of support.
LOG_SWERR	Application Database, 19: <Application>DB Truncated to nn Records	During loading of the Application database from the disk, the size of the on-disk database exceeded the maximum size specified in the system's office parameters file. Any records in the file beyond the specified maximum database size have been discarded.	The OP_NPDB_RECORDS_MAX parameter in the office parameters file was changed to a value less than the current size of the Application database.	<Application>DB truncated to (mm) records: (nn) not read, where: (mm) is the maximum number of records in the ApplicationDB memory buffer. (nn) is the number of records not read from disk into memory.	Contact your next level of support.
LOG_SWERR	Application DB Manager, 00: <Application> DB Manager Software Error	The system generates this log when the Application Database Manager task encounters an unexpected condition. You should report this error to Nortel Networks technical support.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.

LOG_SWERR	Application DB Manager, 26: <Application> Directory Create Failed	The Application database manager subsystem could not create a directory.	No file descriptors are available or the disk device driver returned an error.	Directory create failed (ee): (fn), where: (ee) is the internal error code (n) is the name of the directory .	Contact your next level of support.
LOG_SWERR	Application DB Transfer, 00: Socket Create Failed	A socket could not be created by the operating system.	No file descriptors may be available or the socket driver returned an error.	Socket create failed: errno = (ee), where: (ee) is the internal operating system error code	Contact your next level of support.
LOG_SWERR	Application DB Transfer, 03: Socket Bind Failed	The Application database transfer server was unable to bind the well-known address for this service to the listen socket it created. This socket allows the transfer server to listen for connection requests from other application database system nodes.	The address is already in use or the driver returned an error.	Socket bind failed: errno = (ee), where: (ee) is the internal operating system error code The Data field also contains the socket address structure.	Contact your next level of support.
LOG_SWERR	Application DB Transfer, 04: Socket Listen Failed	The Application database transfer server was unable to set up the listen queue on the listen socket it created. This socket allows the transfer server to listen for connection requests from other application database system nodes.	An internal error has occurred.	Socket listen failed: errno = (ee), where: (ee) is the internal operating system error code	Contact your next level of support.
LOG_SWERR	Application DB Transfer, 05: Socket Accept Failed	The Application database transfer server encountered an error when attempting to accept a connection request from another application database system node.	An internal error has occurred.	Socket accept failed: errno = (ee), where: (ee) is the internal operating system error code	Contact your next level of support.
LOG_SWERR	Application DB Transfer, 06: Invalid Message Type	An invalid message type was received by the Application database transfer server or client during an established conversation.	An internal error has occurred.	Invalid message type received: type = (nn), where: (nn) is the bad message type value The Data field also contains the DB transfer message header.	Contact your next level of support.

LOG_SWERR	Application DB Transfer, 07: Invalid Fileset Type	An invalid fileset type was received in a message by the Application database transfer server or client during an established conversation.	This error is most likely caused by an internal system error.	Invalid fileset type received: type = (nn), where: (nn) is the bad fileset type value The Data field also contains the DB transfer message header.	Contact your next level of support.
LOG_SWERR	Application DB Transfer, 08: Message Too Large	The body of a message received by the Application database transfer client exceeded the maximum size that the client could handle.	An internal software error or mismatch in the office parameters file between application database system nodes.	Message body size (nn) bytes exceeds maximum, where: (nn) is the size of the message body	Contact your next level of support.
LOG_SWERR	Application DB Transfer, 09: Transfer State Error	A message was received by the Application database transfer client that was not expected at the current time.	An internal error has occurred.	Data transfer state error: (explanation), where: (explanation) is the type of state error encountered .	Contact your next level of support.
LOG_SWERR	Application Journaling, 00: File Create Failed	A file could not be created by the Application journaling subsystem.	No file descriptors are available, or the disk device driver returned an error.	File create failed (ee): (fn), where: (ee) Internal error code (fn) The name of the file	Contact your next level of support.
LOG_SWERR	Application Journaling, 01: File Open Failed	A journal file is not available.	There is probably a hardware problem.	File open failed (ee): (fn), where: (ee) is the internal error code (fn) is the name of the file	Contact your next level of support.
LOG_SWERR	Application Journaling, 02: File Read Failed	A failure was encountered while reading a file.	There is probably a hardware problem.	File read failed (ee): (fn), where: (ee) is the internal error code (fn) is the name of the file	Contact your next level of support.
LOG_SWERR	Application Journaling, 03: File Write Failed	A failure was encountered while writing to a file.	Probably a hardware problem. May also be caused due to a disk full condition.	File write failed (ee): (fn), where: (ee) is the internal error code (fn) is the name of the file	Contact your next level of support.
LOG_SWERR	Application Journaling, 04: File Seek Failed	An error occurred while seeking to a specific location within a file.	There is probably a hardware problem.	File seek failed (ee): (fn), where: (ee) is the internal error code (fn) is the name of the file	Contact your next level of support.

LOG_SWERR	Application Journalling, 05: File Flush Failed	Unable to sync file contents to the physical disk. An ioctl system call to flush to the disk failed.	There is probably a hardware problem.	File flush failed (ee): (fn), where: (ee) is the internal error code (fn) is the name of the file	Contact your next level of support.
LOG_SWERR	Application Journalling, 06: File Delete Failed	Unable to delete a journal file from disk.	Probably a hardware problem.	File delete failed (ee): (fn), where: (ee) is the internal error code (fn) is the name of the file	Contact your next level of support.
LOG_SWERR	Application Journalling, 07: Wrong File Signature	The journal file identified in the log does not have the correct file signature value in its header. Its contents have not been used.	A failure occurred during software upgrade.	Invalid file signature: file = (fn), sig = (sig), where: (fn) is a journal file name (sig) is the invalid signature value found in the file header The Data field contains the full contents of the file header.	This problem is self-correcting if another application database system node contains a valid Application database. In this case, the database will be transferred from an application database system node that contains a valid database. Otherwise, contact your next level of support.
LOG_SWERR	Application Journalling, 08: Wrong Version Number	The journal file identified in the log does not have the correct version number value in its header. Its contents have not been used.	A failure occurred during software upgrade.	Invalid file version: file = (fn), ver = (ver), where: (fn) is a journal file name (ver) is the invalid version value found in the file header The Data field contains the full contents of the file header.	This problem is self-correcting if another application database system node contains a valid Application database. In this case the database will be transferred from an application database system node that contains a valid database. Otherwise, contact your next level of support.

LOG_SWERR	Application Journalling, 09: Wrong Sequence Number	The journal file does not contain the correct starting sequence number in the file header.	Another journal file was renamed or copied onto the specified journal file.	Invalid file sequence: file = (fn), seq = (seq), where: (fn) is a journal file name (seq) is the invalid sequence number value found in the file header The Data field contains the full contents of the file header.	This problem is self- correcting if another application database system node contains a valid Application database. In this case the database will be transferred from an application database system node that contains a valid database. Otherwise, contact your next level of support.
LOG_SWERR	Application Journalling, 10: Wrong File Size	The journal file size is not correct. The file is either too large or it contains a partial journal entry.	The file is corrupted from sudden system failure.	File size inconsistent (reason): file = (fn), where: (reason) is the reason the file is being declared inconsistent (either "too large" or "partial entry") (fn) is a journal file name	This problem is self- correcting if another application database system node contains a valid Application database. In this case the database will be transferred from an application database system node that contains a valid database. Otherwise, contact your next level of support.

LOG_SWERR	Application Journalling, 11: Journal File Missing	A necessary journal file is missing or has an invalid format.	A journal file has been deleted or corrupted.	Journal file missing or invalid: file = (fn), rc = (rc), where: (fn) is a journal file name (rc) is the internal return code	This problem is self-correcting if another application database system node contains a valid Application database. In this case the database will be transferred from an application database system node that contains a valid database. Otherwise, contact your next level of support.
LOG_SWERR	Application Messaging, 00: Local Send Failed	A message could not be sent between Application tasks on the same system node.	Memory has become corrupted or a software error has occurred.	Local message send failed: taskid = (tid), error = (error), where: (tid) is the task ID of the destination task (error) is the return code from itc_send_msg() The Data field contains the message header.	Contact your next level of support.
LOG_SWERR	Application Messaging, 01: Remote Send Failed	A message could not be sent to an Application task on another system node.	Most likely due to a failure of the remote system node. It could also be caused by a CC failure.	Remote send failed node = (node), EDP error = (error) (node) is the destination node ID (error) is the return code from edpSend The Data field contains the message header and the total number of messages that encountered a remote send failure.	Contact your next level of support.
LOG_SWERR	Application Messaging, 02: <Application> Software Error	The Application messaging layer detected a software error.	An internal error has occurred.	The Information field describes the event. The Data field contains related data.	Contact your next level of support.

LOG_SWERR	Application OMs, 00: <Application> OM Software Error	The system generates this log when the Application Operational Measurement interface encounters an unexpected condition. You should report this error to Nortel Networks technical support.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	Application Qry Process, 00: <Application> Qry Process Software Error	The system generates this log when the Application Query Processing subsystem encounters an unexpected condition. You should report this error to Nortel Networks technical support.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	Application SMI, 01: <Application> SMI Software Error	The system generates this log when the Application Service Management Interface (SMI) subsystem encounters an unexpected condition. You should report this error to Nortel Networks technical support.	An internal software error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	Application SMI, 02: Socket Create Failed	A socket could not be created by the Service Management Interface subsystem.	No file descriptors are available or the socket driver returned an error.	Socket create failed: errno = (ee), where: (ee) is the internal operating system error code	Contact your next level of support.
LOG_SWERR	Application SMI, 05: Socket Bind Failed	The Application SMI subsystem was unable to bind the well-known address for this service to the socket it created to listen for connection requests from the LSMS.	The address is already in use or the driver returned an error.	Socket bind failed: errno = (ee), where: (ee) is the internal operating system error code The Data field contains the socket address structure.	Contact your next level of support.
LOG_SWERR	Application SMI, 06: Socket Listen Failed	The Application SMI subsystem was unable to set up the listen queue on the socket it created to listen for connection requests from the LSMS.	An internal error has occurred.	Socket listen failed: errno = (ee), where: (ee) is the internal operating system error code	Contact your next level of support.

LOG_SWERR	Application SMI, 07: Socket Accept Failed	The Application SMI subsystem encountered an error when attempting to accept a connection request from an LSMS.	An internal error has occurred.	Socket accept failed: errno = (ee), where: (ee) is the internal operating system error code	Contact your next level of support.
LOG_SWERR	ASM Interworking, 00: ASM Interworking Software Error	There is a software error involving the AS Master interworking functionality.	An internal error has occurred.	The Information and Data fields describe the error.	Contact your next level of support.
LOG_SWERR	ATM Device Driver, 01: Switch Initialize Failed	This log indicates that the IgT WAC-188 switching element had an error during initialization. The system will not initialize.	Either the device was already initialized or there is a hardware problem.	The Information field indicates that the ATM switching element initialization failed.	Contact your next level of support.
LOG_SWERR	ATM Device Driver, 02: Mux Initialize Failed	This log indicates that the IgT WAC-185 mux had an error during initialization of the CC system node. The system will not initialize.	Either the device was already initialized or there is a hardware problem.	The Information field indicates that the ATM mux initialization failed.	Contact your next level of support.
LOG_SWERR	ATM Device Driver, 04: RT Initialize Failed	This log indicates that the IgT WAC-187 routing table or the PMC QRT-PM73487 routing table had an error during initialization. The system will not initialize.	Either the device was already initialized or there is a hardware problem.	The Information and Data fields indicate that the ATM routing table initialization failed.	Contact your next level of support.
LOG_SWERR	ATM Device Driver, 06: CC Spurious Interrupt	This log indicates that the CC system node received a spurious interrupt.	There is a hardware or a configuration problem.	No additional information is provided.	No action is required.
LOG_SWERR	ATM Device Driver, 07: Physical Device Initialize Fail	This log indicates that the IDT 77/105, 77106, or 77V1254 physical device had an error during initialization. The system will not initialize.	Either the device was already initialized or there is a hardware problem.	The Information and Data fields indicate that the physical device initialization failed.	Contact your next level of support.
LOG_SWERR	Audit Facility, 00: Callback Resources Exhausting	The number of applications using the audit facility is approaching the facility's capacity.	This log tracks the use of the audit facility. It does not indicate a problem.	The Information and Data fields indicate the number of clients approaching capacity.	No action is required.
LOG_SWERR	Audit Facility, 01: No Memory Resources	The audit facility could not allocate the required memory resources to run.	There is a system memory management problem.	The Information and Data fields indicate the audit facility failed to allocate memory resources.	Contact your next level of support.

LOG_SWERR	Boot, 00: Boot Manager Software Error	The system generates this log when the boot subsystem encounters unexpected conditions or messages.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	Buffer Manager, 01: Cannot Release Buffer	This log is generated when the system cannot release an internal buffer.	An internal error has occurred.	The Information and Data fields contain the following information: unable to release a buffer: return code from platform = rc buffer type = '0xbb' buffer size = '0xss' task id = tt where: rc = return code of release operation bb = internal buffer type ss = size of internal buffer tt = internal ID of task attempting release	Contact your next level of support.

LOG_SWERR	Buffer Manager, 02: Buffer Pool Exhausted	This log is generated when the buffer pool is out of free buffers.	This log is generated as a result of an internal error or a combination of high traffic conditions and congested links or linksets, which results in the queuing of messages in the system, which would result in a large number of outstanding buffers.	The Information field indicates that a buffer could not be allocated. The requested buffer pool was empty. Information field variations: 1) ss7_alarm_reassert msg, Cannot allocate buffer 2) No msg buf: bt = buffer type (decimal) s = size of the request (decimal) mt = message type (hexadecimal) st = source task (decimal) nd = destination node (hexadecimal) dt = destination task (decimal)	Determine whether there are high system traffic loads. If there are high system traffic loads, adjust the traffic loads. Otherwise, contact your next level of support.
LOG_SWERR	Buffer Manager, 03: Buffer Initialization Error	This log is generated when the system cannot allocate memory for buffer pools.	An internal error has occurred.	The Information and Data fields contain the following information: unable to initialize a buffer pool = mm where: mm = the internal pool identifier	Contact your next level of support.
LOG_SWERR	Buffer Manager, 09: Incorrect Pointer Reference	This log is generated during a swerr and dumps the buffer pointer as well as all the memory regions of SS7 buffer pools.	1. Someone referenced a pointer that does not belong to him/her. 2. Buffer corruption (buf_info was null, mem_index out of range,...)	No additional information is provided.	It could be a good idea to reload the card.
LOG_SWERR	Buffer Manager, 10: Incorrect Local Pointer Reference	This log is generated during a swerr and dumps the buffer pointer as well as the memory region (buffer pool region) in which it resides. This occurs when we are in a valid pool, but don't start at a valid location (byte-wise).	1. Someone referenced a pointer that does not belong to him/her. 2. Buffer corruption	No additional information is provided.	It could be a good idea to reload the card.

LOG_SWERR	Buffer Manager, 11: Incorrect pointer reference - Contents dumped	This log is generated during a swerr and dumps the buffer pointer as well as the contents of this buffer.	1. Someone referenced a pointer that does not belong to him/her. 2. Buffer corruption .	No additional information is provided.	It could be a good idea to reload the card.
LOG_SWERR	Buffer Manager, 12: Incorrect pointer reference - Header Dumped	This log is generated during a swerr and dumps the buffer header.	1. Someone referenced a pointer that does not belong to him/her. 2. Buffer corruption .	No additional information is provided.	It could be a good idea to reload the card.
LOG_SWERR	Buffer Manager, 13: Buffer software error	Generic Swerr id.	A software error occurred.	No additional information is provided.	Report to Nortel Networks technical support.
LOG_SWERR	Call Gap, 00: CallGap Software Error	The system generates this log when Call Gap encounters an unexpected condition. You should report this error to Nortel Networks technical support.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	Command Line Interface, 01: CLI Software Error	The system generates this log when the Command Line Interface (CLI) task encounters an unexpected condition. You should report this error to Nortel Networks technical support.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	Configuration, 07: System Database Error	The system generates this log when it is not possible to get or set the USP system-specific data.	An internal error has occurred.	The Information and Data fields indicate which attempt to get or set system-specific data has failed.	Contact your next level of support.
LOG_SWERR	Configuration, 08: Get Shelf Failed	The system generates this log when it is not possible to get shelf data.	An internal error has occurred.	The Information and Data fields describe which attempt to get the shelf data has failed.	Contact your next level of support.
LOG_SWERR	Configuration, 09: Set Shelf Failed	The system generates this log when it is not possible to set shelf configuration data in the database.	An internal error has occurred.	The Information and Data fields indicate which attempt to set shelf data has failed.	Contact your next level of support.

LOG_SWERR	Configuration, 10: Get Shelf Templates Failed	The system generates this log when it is not possible to get CAM shelf templates.	An internal error has occurred.	The Information and Data fields indicate which attempt to get CAM shelf templates failed.	Contact your next level of support.
LOG_SWERR	Configuration, 11: Find Shelf Failed	The system generates this log when it is not possible to find an existing CAM shelf.	An internal error has occurred.	The Information and Data fields indicate which attempt to locate an existing CAM shelf has failed.	Contact your next level of support.
LOG_SWERR	Configuration, 12: Add Shelf Failed	The system generates this log when it is not possible to add or modify a CAM shelf.	An internal error has occurred.	The Information and Data fields indicate which attempt to add or modify a CAM shelf has failed.	Contact your next level of support.
LOG_SWERR	Configuration, 13: Delete Shelf Failed	The system generates this log when it is not possible to delete an extension CAM shelf.	An internal error has occurred.	The Information and Data fields indicate which attempt to delete an extension CAM shelf has occurred.	Contact your next level of support.
LOG_SWERR	Configuration, 14: Get Slot Failed	The system generates this log when it is not possible to get slot data.	An internal error has occurred.	The Information and Data fields indicate which attempt to get slot data failed.	Contact your next level of support.
LOG_SWERR	Configuration, 15: Set Slot Failed	The system generates this log when it is not possible to set slot data.	An internal error has occurred.	The Information and Data fields indicate which attempt to set slot data failed.	Contact your next level of support.
LOG_SWERR	Configuration, 16: Find Slot Failed	The system generates this log when it is not possible to find a slot in a shelf.	An internal error has occurred.	The Information and Data fields indicate which attempt to find a slot failed.	Contact your next level of support.
LOG_SWERR	Configuration, 17: Get System Node Failed	The system generates this log when it is not possible to get RTC, CC, or application system node data.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	Configuration, 18: Set System Node Failed	The system generates this log when it is not possible to set RTC, CC, or application system node data.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	Configuration, 19: System Node Template Failed	The system generates this log when it is not possible to get an RTC, CC, or application system node template.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.

LOG_SWERR	Configuration, 20: Software Failed	The system generates this log when it is not possible to get a software version or to build a list of software loads.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	Configuration, 21: Delete System Node Failed	The system generates this log when it is not possible to delete an RTC, CC, or application system node.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	Configuration, 22: Event Failed	The system generates this log when it is not possible to generate an event when configuration data changes.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	Configuration, 23: Set Sysconf File Error	The system generates this log when it is not possible to set the sysconf file with either the new next bootable RTC system node load file or the next bootable data snapshot.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	Configuration, 26: Snapshot Restore Failed	The system generates this log when an attempt to restore a data snapshot fails.	Either the snapshot with the specified name does not exist, or there is no more room on the disk.	The Information and Data fields indicate which attempt to restore a data snapshot failed.	Contact your next level of support.
LOG_SWERR	Configuration, 30: Delete Mate Info Failed	The system generates this log when it is not possible to delete the mate information of a mate node.	An internal error has occurred.	The Information and Data fields indicate which attempt to delete the mate information of a mate node has occurred.	Contact your next level of support.
LOG_SWERR	Configuration, 31: Delete SCSI Failed	The system generates this log when it is not possible to delete the storage media of a node.	An internal error has occurred.	The Information and Data fields indicate which attempt to delete the storage media of a mate node has occurred.	Contact your next level of support.
LOG_SWERR	Configuration, 32: Get CFG Bitmap Failed	The system generates this log when it is not possible to get the configuration bitmap of a node.	An internal error has occurred.	The Information and Data fields indicate the attempt to get the configuration bitmap of a node has occurred.	Contact your next level of support.
LOG_SWERR	Configuration, 33: Set Mate Failed	The system generates this log when it is not possible to get the configuration bitmap of a node.	An internal error has occurred.	The Information and Data fields indicate the attempt to get the configuration bitmap of a node has occurred.	Contact your next level of support.

LOG_SWERR	Configuration, 34: Set Ethernet Failed	The system generates this log when it is not possible to get the configuration bitmap of a node.	An internal error has occurred.	The Information and Data fields indicate the attempt to get the configuration bitmap of a node has occurred.	Contact your next level of support.
LOG_SWERR	Configuration, 35: Rule Failure	The system generates this log when it is not possible to get the configuration bitmap of a node.	An internal error has occurred.	The Information and Data fields indicate the attempt to get the configuration bitmap of a node has occurred.	Contact your next level of support.
LOG_SWERR	Configuration, 36: Get Node Operational State Failed	The system generates this log when it is not possible to get the operational state of a node.	An internal error has occurred.	The Information and Data fields indicate the attempt to get the operational state of a node has occurred.	Contact your next level of support.
LOG_SWERR	Data Audit, 02: Alarm Callback Bind Failed	This log can be generated when the system is initializing. The system has tried to register a Reasserting Alarms data audit callback and failed. As a result, alarms will not be reasserted if the active RTC system node resets and becomes enabled.	An internal error has occurred.	The Information and Data fields indicate the name of the affected database and the internal return code for the operation.	Contact your next level of support. If there are any traffic problems associated with specific application system nodes, load those nodes. Refer to the System Management section of the User Guide for more information.
LOG_SWERR	Data Audit, 08: Routeset Alarm Count Wrong	This log is generated when the application audit system determines that the count of alarmed routesets is incorrect.	An internal error has occurred.	The Information and Data fields indicate the type of alarm, the 'current' count, and the 'corrected' count.	The system automatically corrects the problem.
LOG_SWERR	Data Audit, 23: Routeset Alarm State Wrong	This log is generated when the application audit system determines that the alarmed state of a routeset is incorrect.	An internal error has occurred.	The Information and Data fields indicate the affected routeset	The system automatically corrects the problem.

LOG_SWERR	Data Audit, 24: Routeset Alarm Database SSR2.0 Format	This log is generated when the application audit system determines that the alarm subsystem contains routeset alarms of a previous format. The format of routeset alarms was changed in SSR3.0. The audit is responsible for locating and clearing any old routeset alarms and replacing them with the new format.	Software upgrade from pre SSR3.0.	none	none.
LOG_SWERR	Data Audit, 25: Routeset Alarm Database Count Wrong	This log is generated when the application audit system determines that the alarm subsystem is out of sync with respect to the MTP Routeset database.	An internal error has occurred.	The Information and Data fields indicate the severity of the alarm	The system automatically corrects the problem.
LOG_SWERR	Data Audit, 26: Routeset Alarm Audit Return Code Invalid	This log is generated when the application audit system returns and invalid return code.	An internal error has occurred.	The Information and Data fields indicate the return code	Contact your next level of support.
LOG_SWERR	Data Audit, 27: DTX Failed - Rebooting Card	If a database mismatch is encountered we attempt to transfer, by DTX, down an up to date version from the RTC. If DTX fails, the link card is rebooted to minimize impact to the system.	An internal error has occurred.	The information field indicates which database failed DTX	If the card fails to reboot, or this failure is seen multiple times please contact your next level of support.
LOG_SWERR	Data Audit, 29: Database Synchronization Lost	This log is generated when a database loses synchronization on the specified RTC system node or application system node.	This log is caused by a lost database update message and/or a failed database reload.	The Information and Data fields indicate the name of the database that has lost synchronization and note that the associated RTC system node or application system node should be reset.	This log is not expected to come during software upgrade. As the periodic data auditing facility is not running during software upgrade, perform a load operation on the affected RTC system node or application system node. If loading the affected RTC system node or application system node does not correct the problem, contact your next level of support.

LOG_SWERR	Data Journaling, 01: Journaling Error	The log is reported when any problem occurs with the internal data journaling subsystem. Typically these problems are related to subsystem initialization or a software error for users of the subsystem.	An unexpected software condition has occurred.	The information in each log is dependent on the situation in which it is generated. The Information and Data fields change to match the data required to properly debug the cause of the problem.	Contact your next level of support.
LOG_SWERR	Data Transfer, 00: Software Error	This log is generated when the data transfer subsystem encounters unexpected conditions or messages. This is an internal error that you should report to Nortel Networks technical support.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	Database Sync, 01: Creation of Server Socket Failed	This log is generated when a server socket could not be created for the datasync controller. As a result, data synchronization will not be possible.	The address for the socket is already in use.	The Information field displays the task that caused the error and the protocol error number.	Performing a load operation on the affected RTC system node may clear the problem. Refer to the USP User Guide for more information. If this does not clear the problem, contact your next level of support.
LOG_SWERR	Database Sync, 02: Creation of Controller Semaphore Failed	This log indicates that the operating system returned an error when a semaphore for the datasync controller was created. As a result, data synchronization will not be possible.	The operating system limit has been exceeded.	The Information field displays the task that caused the error and the error code returned by the operating system.	Contact your next level of support.
LOG_SWERR	Database Sync, 03: RTC Communication Problem	This log indicates that a software communication error occurred between the mated RTC system nodes during data synchronization.	An RTC system node is disabled, or the communication link between the mates is malfunctioning. The system attempts to communicate with the affected RTC system node several times.	The Information field displays the task that caused the exception and the error code returned by the operating system.	Ensure that the affected RTC system node is enabled. Data synchronization will be aborted, and the local RTC system node becomes active automatically. The database may not be up-to-date.

LOG_SWERR	Database Sync, 04: Data Sync Failure	This log indicates that the attempt to synchronize data between the mated RTC system nodes failed.	A lower-level problem occurred in locking, unlocking or copying the database.	The Information field displays the task that caused the exception and the name of the database that could not be synchronized.	Perform a load operation on the affected RTC system node as described in the USP User Guide.
LOG_SWERR	Database Sync, 05: Server Select Error	This log indicates that an error occurred while the data synchronization server task was waiting for a message from an RTC system node.	A TCP/IP stack error occurred.	The Information field displays what task caused the exception. The underlying operation system error is logged.	Contact your next level of support.
LOG_SWERR	Database Sync, 06: Server Event Unknown	This log records a software error in the data synchronization subsystem.	An internal error has occurred.	The Information field displays what task caused the exception. The unknown event is recorded.	Contact your next level of support.
LOG_SWERR	Database Sync, 07: Copy Failed	This log indicates that an operating system error occurred when files were being copied. As a result, data synchronization will fail.	This error is caused by an NFS Server problem, a corrupt database, or incorrect file permissions.	The Information field displays the name of the task that caused the exception, the operating system error number, and the name of the file.	Contact your next level of support.
LOG_SWERR	Database Sync, 08: Client-Server Protocol Error	This log indicates that a datasync application protocol error occurred.	The problem is caused by version mismatch, RTC system node failure during data synchronization, or an internal error.	The Information field indicates the nature of the error.	Contact your next level of support.
LOG_SWERR	Database Sync, 09: Client-Server Message Length Error	This log indicates that the datasync application tried to send a message that was too long for the internal buffers.	An internal error has occurred.	The Information field displays the task that caused the exception.	Contact your next level of support.
LOG_SWERR	Database Sync, 10: Database Access Error	This log indicates that the datasync application encountered a database error.	An internal error has occurred.	The Information field displays the task that caused the exception.	Contact your next level of support.
LOG_SWERR	Database Sync, 11: System Status Object Error	This log indicates that the datasync application encountered an error when accessing the system status object instance. This object is necessary for tracking the local system state.	An internal error has occurred.	The Information field displays the task that caused the exception.	Contact your next level of support.

LOG_SWERR	Database Sync, 12: File Name Too Long	This log indicates that the datasync application received a file name that exceeds allowable length limitations. The datasync application was unable to process the request.	An internal error has occurred.	The Information field displays the task that caused the exception.	Contact your next level of support.
LOG_SWERR	Database Sync, 14: Snapshot Purge Failed	The purge facility failed to open the old temporary snapshot directories.	An internal error has occurred.	The Information field describes the error.	Contact your next level of support.
LOG_SWERR	Debug Utility, 00: Debug Utility Software Error	The system generates this log when the debug facility encounters unexpected conditions or messages.	An internal error has occurred.	The Information and Data fields indicate the module involved.	Contact your next level of support.
LOG_SWERR	Disk Maintenance, 00: NFS Export Failed	This log indicates the system failed to export the SCSI disk.	There is a connectivity failure or a hardware failure.	The Information field describes the error.	Contact your next level of support.
LOG_SWERR	Disk Maintenance, 01: NFS Mount Mate Failed	This log indicates the system was unable to NFS mount its mate disk.	There is a connectivity or hardware failure.	The Information field describes the error.	Contact your next level of support.
LOG_SWERR	Disk Maintenance, 02: NFS Unmount Mate Failed	This log indicates the system was unable to NFS unmount its mate disk.	There is a connectivity or hardware failure.	The Information field describes the error.	Contact your next level of support.
LOG_SWERR	Disk Manager, 00: Software Error	This log is generated when a software error is detected in the disk management/data area.	An internal error has occurred.	The Information field contains information that describes the event. The Data field contains a dump of the data related to the error.	Contact your next level of support.
LOG_SWERR	Disk Manager, 01: File Integrity	This log is generated when a size of a database stored on the SCSI disk associated with an RTC system node is not correct. As a result, the file size of the database is set to zero and its contents are not used.	This log occurs when the version of the database expected by the system is not present.	The Information and Data fields indicate the name of the database and its internal version number.	If this log is not generated as part of a software upgrade, contact your next level of support.
LOG_SWERR	Disk Manager, 03: File Create Failed	This log is generated when the Disk Manager subsystem could not create a file.	This log occurs when no file descriptors are available or the related driver returned an error.	The Information and Data fields indicate the name of the file that could not be created, the internal ID for the subsystem in which the error occurred, and the internal code for the error.	Contact your next level of support.

LOG_SWERR	Disk Manager, 04: Open File Failed	This log is generated when a database stored on the SCSI disk associated with an RTC system node cannot be opened.	This log can occur when there is a problem with the SCSI disk associated with an RTC system node.	The Information and Data fields indicate the name of the file that could not be opened, the internal ID for the subsystem in which the error occurred, and the internal code for the error.	Contact your next level of support.
LOG_SWERR	Disk Manager, 05: File Read Failed	This log is generated when the system tries to read a database and fails.	This log can occur when there is a problem with the SCSI disk associated with an RTC system node.	The Information and Data fields indicate the name of the database that could not be read, the internal ID for the subsystem in which the error occurred, and the internal code for the error.	Contact your next level of support.
LOG_SWERR	Disk Manager, 06: File Write Failed	This log is generated when the system tries to write to a database and fails.	This log can occur when there is a problem with the SCSI disk associated with an RTC system node.	The Information and Data fields indicate the name of the database that could not be written to, the internal ID for the subsystem in which the error occurred, and the internal code for the error.	Contact your next level of support.
LOG_SWERR	Disk Manager, 07: File LSeek Failed	This log is generated when the system tries to point to a particular location in a file, and fails.	This log can occur when there is a problem with the SCSI disk associated with an RTC system node.	The Information and Data fields indicate the name of the affected file, the internal ID for the subsystem in which the error occurred, and the internal code for the error.	Contact your next level of support.
LOG_SWERR	Disk Manager, 08: File Flush Failed	This log is generated when the system tries to move the contents of I/O buffers to the SCSI disk associated with an RTC system node, and fails.	This log can occur when there is a problem with the SCSI disk associated with an RTC system node.	The Information and Data fields indicate the internal ID for the subsystem in which the error occurred, and the internal code for the error.	Contact your next level of support.

LOG_SWERR	Disk Manager, 09: SS7 Directory Could Not Be Created	This log is generated when the system could not create an SS7 directory.	This log can occur when there is a problem with the SCSI disk associated with an RTC system node.	The Information and Data fields indicate the directory path name that could not be created, the internal ID for the subsystem in which the error occurred, and the internal code for the error.	Contact your next level of support.
LOG_SWERR	Disk Manager, 10: Unable to Register Database	This log is generated when the system tries to perform a data transfer and fails. This error occurs when the system is unable to register the name of a database.	An internal error has occurred.	The Information and Data fields indicate the name of the affected database and the internal ID of the error.	Contact your next level of support.
LOG_SWERR	Disk Manager, 15: File Write In Progress	This log is generated when the system tries to open a file that was being written to the last time that the file was saved. Part of the file has been updated, but not the entire file, which means that there could be data integrity problems within the file. This file will be renamed. As a result, the file size of the database is set to zero and its contents are not used.	The system aborted during the last write process to this file. The system most likely suffered a system failure while it was attempting to satisfy a provisioning request.	The Information and Data fields indicate the name of the affected file.	Contact your next level of support. Verify the results of the last provisioning request. If information is missing, enter the provisioning information again. In the unlikely event that both of the database copies are damaged on both RTC system nodes, then the affected database can be restored from the backup tape for the OAM&P workstation. Refer to the on-line documentation for the tape backup system for information on restoring individual files.
LOG_SWERR	Disk Manager, 16: File Integrity - Wrong File Type	This log is generated when the system tries to open a database and finds an unexpected file type in its header. As a result, the contents of the database are not used.	A file was renamed incorrectly or the file is corrupt.	The Information and Data fields indicate the name of the affected database and the unexpected file type value.	Contact your next level of support.

LOG_SWERR	Disk Manager, 17: File Integrity - Wrong Version Number	This log is generated when the system tries to open a database and finds an unexpected version number in its header. As a result, the contents of this database are not used.	The system expected a different version number of the database.	The Information and Data fields indicate the name of the affected database and the unexpected version value.	Contact your next level of support.
LOG_SWERR	Disk Manager, 18: DTX opcode bad	This log is generated when the application Data Manager subsystem got an unexpected opcode from the underlying platform Data Transfer subsystem.	An internal error has occurred.	The Information and Data fields indicate the name of the file that was being used when the error occurred, and the internal code for the error.	Contact your next level of support.
LOG_SWERR	EDP Messaging Layer, 01: Buffer or Memory Alloc Fail	An attempt to get a buffer from a buffer pool or a memory allocation failed.	There is not enough memory available, or the system is out of buffers.	The Information field indicates the calling function and, in parentheses, the object of allocation.	Contact your next level of support.
LOG_SWERR	EDP Messaging Layer, 02: Function Call Failed	This log indicates a function call failed.	The called function failed.	The Information field indicates the calling function and the called function that returned a failure indication. The Information field may also contain, in parentheses, additional information that distinguishes between multiple logs of the same type. The Data field indicates the return code received from the called function.	Contact your next level of support.
LOG_SWERR	EDP Messaging Layer, 03: Null Pointer Encountered	This log indicates the system encountered an unexpected null pointer.	An internal error has occurred.	The Information field indicates the calling function or pointer found to be null.	Contact your next level of support.
LOG_SWERR	EDP Messaging Layer, 04: Multiple Segments Buffer	This log indicates the system encountered an SSCS buffer with multiple segments.	An SSCS buffer with multiple segments has been created.	The Information field indicates the calling function and error.	Contact your next level of support.

LOG_SWERR	EDP Messaging Layer, 05: Unsatisfied Precondition	This log indicates a necessary precondition for the attempted action is not satisfied.	There has been a prior failure.	The Information field indicates the calling function and unsatisfied precondition.	Contact your next level of support.
LOG_SWERR	EDP Messaging Layer, 06: User Error Detected	An EDP user error was detected.	There was an EDP user error.	The Information field indicates the calling function and detected user error.	Contact your next level of support.
LOG_SWERR	Event Manager, 01: Socket Fail	The system generates this log when a task fails to open an interface for reporting system notification events.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	Event Manager, 02: ioctl Fail	The system generates this log when an attempt to retrieve a system notification event fails because there is an initialization error in the notification interface.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred and provide the communication socket where the failure occurred.	Contact your next level of support.
LOG_SWERR	Event Manager, 03: UDP Receive Fail	The system generates this log when an attempt to retrieve a system notification event fails because there is an access error in the notification interface.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	Event Manager, 04: Unknown Source	The system generates this log when the source of a published system notification event is not the system event manager.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	Event Manager, 05: Invalid Message Length	The system generates this log when the length of an event notification message received does not match the expected length.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred and provide the number of bytes received for the event message.	Contact your next level of support.
LOG_SWERR	Event Manager, 06: Invalid Opcode	The system generates this log when it receives an event notification message with an invalid operation code.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	Event Manager, 07: IP Fail	The system generates this log when a failure occurs in initializing the IP address of the event notification interface.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.

LOG_SWERR	Event Manager, 08: Report Fail	The system generates this log when a failure occurs while attempting to report an event message to the system event manager.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	Event Manager, 09: Invalid Event ID	The system generates this log when a task attempts to register for notification of an undefined event.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	Event Manager, 10: Invalid Registration Flag	The system generates this log when a task registering for an event receives an invalid registration flag.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	Event Manager, 11: Select Failed	The system generates this log when it encounters an internal communication error while receiving a system notification event. The event interface has been notified of a pending message, but no data are available.	An internal error has occurred.	The Information and Data fields describe the error.	Contact your next level of support.
LOG_SWERR	Event Manager, 12: Socket Open Failed	The system generates this log when the event manager fails to open an interface for receiving and publishing system events.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	Event Manager, 13: Bind Failed	The system generates this log when an error occurs while initializing the event manager on the RTC system node. A failure occurred while attempting to initialize the communication interface.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	Event Manager, 14: Resource Allocation Failed	The system generates this log if the event manager fails to properly allocate resources for monitoring system events.	An internal error has occurred.	Describes the context where the error occurred.	Contact your next level of support.
LOG_SWERR	Event Manager, 15: Notification Failed	The system generates this log when the event manager fails to properly publish an event notification to the entire system.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	Event Manager, 16: Registration Failed	The system generates this log when an error occurs while a task attempts to register or unregister an event identifier with the event manager.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred. The log context identifier indicates whether a subscribe or an unsubscribe action was requested.	Contact your next level of support.

LOG_SWERR	Event Manager, 17: Invalid Event Request	The system generates this log when the event manager receives an invalid event operation code from an event report.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred. The log context identifier indicates the invalid event operation code.	Contact your next level of support.
LOG_SWERR	Event Manager, 18: Callback Failed	The system generates this log when a callback registered with the event manager returns a failure code from processing the published event.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred. The log context identifier contains the task identifier of the task that registered the failed callback.	Contact your next level of support.
LOG_SWERR	Event Manager, 19: Subscribing Task Failed	The system generates this log when a failure occurs in initializing the IP address of the subscribing task during publication of a system event.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	Event Manager, 20: Unregister Non-existing Event	The system generates this log when a task attempts to unregister an event that does not exist with the event manager.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred and indicate the event identifier that caused the failure.	Contact your next level of support.
LOG_SWERR	Event Manager, 21: Unregister Failed	The system generates this log when the event manager is unable to unregister an event.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred and indicate the reason for the failure.	Contact your next level of support.
LOG_SWERR	Event Manager, 22: Duplicate Registration	The system generates this log when a task attempts to register for an event that is already registered with the event manager.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred and indicate the event identifier that caused the failure.	Contact your next level of support.
LOG_SWERR	Event Manager, 23: Resize Failed	The system generates this log when the event manager is unable to resize the event subscription table as required by system demands.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred and indicate the event identifier that triggered the resizing action.	Contact your next level of support.

LOG_SWERR	Event Manager, 24: Task Terminated	The system generates this log when the system event manager task on the RTC system node terminates.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	Event Manager, 25: Bad User Parameter Received	The system generates this log when a user of the event manager tries to report an event with a bad parameter.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	Event Records, 00: Event Records Software Error	The system generates this log when the Event Records facility encounters an unexpected condition. You should report this error to Nortel Networks technical support.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	External Transaction Facility, 01: I/O Control Function Failed	This log is generated when a socket control error occurs during the initialization process for receiving a transaction message.	An internal error has occurred.	The Information field describes the context in which the error occurred.	Contact your next level of support.
LOG_SWERR	External Transaction Facility, 03: Receive Buffer Truncated	This log is generated to indicate that an HMI transaction has been received that is larger than the internal buffer provided by the destination task. The resulting message buffer is truncated.	Size constants are out of sync between the current USP GUI software version and the current USP application software version. This is an internal error.	The Information field describes the context in which the error occurred.	No action is required.
LOG_SWERR	File Purge, 01: Unable to Reschedule	A bind of the file purge rescheduling callback (upon time of day change) failed.	An internal error has occurred.	The Information field describes the error.	Contact your next level of support.
LOG_SWERR	File Purge, 02: File Purge Status Failed	The file purge status function did not return the desired file information.	An internal error has occurred.	The Information field describes the error.	Contact your next level of support.
LOG_SWERR	File Purge, 03: Old File Purge Failed	The file purge facility failed to open the directory for purging old files.	An internal error has occurred.	The Information field describes the error.	Contact your next level of support.
LOG_SWERR	File Purge, 04: Snapshot Purge Failed	The file purge facility failed to open the directory for purging data snapshots.	An internal error has occurred.	The Information field describes the error.	Contact your next level of support.
LOG_SWERR	File Purge, 05: Failed to Get Host IP	The file purge facility failed to get the host IP address.	An internal error has occurred.	The Information field describes the error.	Contact your next level of support.

LOG_SWERR	File Purge, 06: Failed to Open UDP Socket	The file purge facility failed to open a UDP socket.	An internal error has occurred.	The Information field describes the error.	Contact your next level of support.
LOG_SWERR	File Purge, 07: Failed to Receive UDP Buffer	The file purge facility failed to receive a UDP buffer.	An internal error has occurred.	The Information field describes the error.	Contact your next level of support.
LOG_SWERR	File Purge, 08: Failed to Close Socket	The file purge facility failed to close the socket after sending a purge message.	An internal error has occurred.	The Information field describes the error.	Contact your next level of support.
LOG_SWERR	File Purge, 09: Failed to Send Purge Message	The file purge facility failed to send a purge message to the socket.	An internal error has occurred.	The Information field describes the error.	Contact your next level of support.
LOG_SWERR	FTP Server, 00: FTP Software Error	The system generates this log when the FTP Server encounters an unexpected condition. You should report this error to Nortel Networks technical support.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	Global Title Translations, 00: Software Error	This log is generated to record occurrences of software errors related to GTT operations.	An internal error has occurred.	The Information and Data fields indicate the nature of the error.	Contact your next level of support.
LOG_SWERR	Global Title Translations, 01: Non-Existent Global Title Address	This log is generated when the GTA in the received message does not exist in the global title database.	The GTA in question was not configured locally or at the sending site.	The Information and Data fields indicate the called party address, starting with the length field.	No action is required.
LOG_SWERR	Global Title Translations, 03: Could Not Get a Buffer	This log is generated when the system tries to obtain a new buffer for new GTA results from GTT, and no buffers are available.	An internal error has occurred.	No additional information is provided.	Contact your next level of support.
LOG_SWERR	Global Title Translations, 11: GTT SCCP Unqualified RC	This log is generated when an invalid GTT result type occurs.	This is a software error.	The Information and Data fields indicate that the called party address is missing a subsystem number.	No action is required.

LOG_SWERR	HMI Server, 01: Send Failed	The system generates this log when the HMI server task on the RTC system node is unable to send a transaction message to the USP GUI on the OAM&P workstation.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred and indicate the transaction operation code for the failed transaction.	Contact your next level of support.
LOG_SWERR	HMI Server, 02: Receive Fail	The system generates this log when the HMI server task on the RTC system node is unable to receive a transaction message from the USP GUI on the OAM&P workstation.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	HMI Server, 03: RDM Initialization Failed	The system generates this log when the HMI server is unable to initialize access to the system configuration database.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred	Contact your next level of support.
LOG_SWERR	HMI Server, 04: Event Registration Failed	The system generates this log when an HMI server is unable to register or unregister for system event notifications.	An internal error has occurred.	The Information and Data fields indicate the event registration failure condition and the event identifier.	Contact your next level of support.
LOG_SWERR	HMI Server, 05: Select Failed	The system generates this log when the HMI server encounters an internal communication error. The HMI server has been notified of a pending message to receive, but no data are available.	An internal error has occurred.	The Information and Data fields provide the error indication returned from the operating system.	Contact your next level of support.
LOG_SWERR	HMI Server, 06: Invalid Opcode	The system generates this log when an invalid operation code is detected in a message transaction received from the OAM&P workstation.	An internal error has occurred.	The Information and Data fields provide the invalid operation code received and the remaining payload data in the message.	Contact your next level of support.
LOG_SWERR	HMI Server, 07: Invalid Function	The system generates this log when a transaction message is received, but no processing callback is registered with the HMI server.	An internal error has occurred.	The Information and Data fields provide the operation code of the transaction and the payload data in the message.	Contact your next level of support.

LOG_SWERR	HMI Server, 08: Callback Error	The system generates this log when a system error occurs while processing an HMI transaction message.	An internal error has occurred.	The Information and Data fields provide the operation code of the transaction and the payload data in the message.	Contact your next level of support.
LOG_SWERR	HMI Server, 09: Mate IP Fail	The system generates this log when an HMI server is unable to determine the IP address of the mate RTC system node for replication.	An error has occurred with the interface to the activity subsystem.	The Information and Data fields describe the context where the error occurred and provide the mate RTC system node IP address as a 32-bit word.	Contact your next level of support.
LOG_SWERR	HMI Server, 11: Invalid Return Opcode	The system generates this log when an invalid operation code results during transaction processing for a response message to the OAM&P workstation.	An internal error has occurred.	The Information and Data fields provide the invalid operation code and the remaining payload data in the transaction message.	Contact your next level of support.
LOG_SWERR	HMI Server, 12: Inactive RTC Down Fail	The system generates this log when the active HMI server is unable to report a system event notification while the inactive RTC system node becomes disabled.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	HMI Server, 13: Inactive RTC Up Fail	The system generates this log when the active HMI server is unable to report a system event notification while the inactive RTC system node becomes enabled.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	HMI Server, 14: Active RTC Down Fail	The system generates this log when the inactive HMI server is unable to report a system event notification while it assumes activity.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	HMI Server, 15: Socket Fail	The system generates this log when an error occurs while initializing the TCP connection between the USP GUI and the application on the RTC system node. A failure occurred during the attempt to open the communication interface with the USP GUI on the OAM&P workstation.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.

LOG_SWERR	HMI Server, 16: Bind Fail	The system generates this log when an error occurs while initializing the TCP connection between the USP GUI and the application on the RTC system node. A failure occurred during the attempt to open the communication interface with the USP GUI on the OAM&P workstation.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	HMI Server, 17: Listen Fail	The system generates this log when an error occurs while initializing the TCP connection between the USP GUI and the application on the RTC system node. A failure occurred during the attempt to open the communication interface with the USP GUI on the OAM&P workstation.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	HMI Server, 18: Accept Fail	The system generates this log when an error occurs while initializing the TCP connection between the USP GUI and the application on the RTC system node. A failure occurred during the attempt to open the communication interface with the USP GUI on the OAM&P workstation.	An internal error has occurred.	The Information and Data fields describes the context where the error occurred.	Contact your next level of support.
LOG_SWERR	HMI Server, 19: Task Spawn Fail	The system generates this log when an error occurs on the RTC system node while the system is creating an HMI server task to handle USP application communication.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	HMI Server, 21: Unable to Release Resources	This log is generated when an HMI server terminates but is unable to release resources to allow for additional USP GUI OAM&P workstation connections.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	HMI Server, 22: Event Failed	The HMI server task generates this log when it fails to generate a system notification event.	An internal error has occurred.	The Information and Data fields describe the failure condition and contain the event identifier.	Contact your next level of support.
LOG_SWERR	HMI Server, 23: Invalid Event Code	The HMI server task generates this log when it receives a system notification event with an invalid event operation code.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred and indicate the invalid event operation code.	Contact your next level of support.

LOG_SWERR	HMI Server, 24: System Node Access	The HMI server task generates this log when it is unable to access RTC, CC, or Link system node status information to determine the operational or administrative state of a system node.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	HMI Server, 25: BERT Error	The HMI server task generates this log when an error occurs during execution of the BERT command.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	HMI Server, 26: Loopback Error	The HMI server task generates this log when an error occurs during execution of the Loopback test command.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	HMI Server, 28: Lockout Read Fail	The HMI server task is unable to read the user lockout information.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	HMI Server, 29: Lockout Write fail	The HMI server task is unable to write the user lockout information.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	HMI Server, 33: Callback Timer Error	This log indicates that an error occurred while invoking the system timer functions.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	No action is required.
LOG_SWERR	HMI Server, 35: Hmisvr Task Kill Failed	This log indicates that an error occurred while trying to kill Hmisvr task.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	No action is required.
LOG_SWERR	HMI Server, 36: HMI/OAM-API Software Error	The system generates this log when the HMI server task on the RTC system node is encounters an error when interacting with the OAM API.	An internal error has occurred.	The Information and Data fields describe the context where the error occurred.	Contact your next level of support.
LOG_SWERR	HSL SAAL Event, 00: Software Errors	This log is generated when software errors are detected that pertain to the SAAL stack.	An internal error has occurred.	The Information and Data fields report the error. If a data dump is generated by the error, the Information and Data fields include a hexadecimal data dump.	Contact your next level of support.

LOG_SWERR	IPS7, 00: IPS7 Software Error	There is a software error involving the IPS7 protocol subsystem.	An internal error has occurred.	The Information and Data fields describe the error.	Contact your next level of support.
LOG_SWERR	Log Facility, 00: Log Facility Software Error	The system generates this log when the log facility encounters unexpected conditions or messages.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	Log Facility, 01: Callback Resources Exhausting	The number of applications using the log facility is approaching its capacity.	This log tracks the use of the log facility. It does not indicate a problem.	The Information and Data fields indicate the remaining available slots.	Contact your next level of support.
LOG_SWERR	Log Facility, 02: UDP Error Encountered	The log facility encountered an error while trying to receive a UDP message.	UDP resources are exhausted.	The Information and Data fields indicate a UDP receive failure.	Contact your next level of support.
LOG_SWERR	Log Facility, 03: Invalid Message Received	The log facility received an invalid message.	Memory is corrupted or the application is faulty.	The Information and Data fields indicate the invalid message received and the invalid group ID in the message received.	Contact your next level of support.
LOG_SWERR	Log Facility, 04: Could Not Open a UDP Socket	The log facility could not open a UDP socket.	There is a UDP resource problem.	The Information and Data fields indicate the system was unable to allocate a socket.	Contact your next level of support.
LOG_SWERR	Log Facility, 05: No Memory Resources	The log facility could not allocate the required memory resources.	There is a memory failure or a memory allocation problem.	The Information and Data fields indicate the system failed to allocate memory resources.	Contact your next level of support.
LOG_SWERR	Log Facility, 06: Log Facility User Error	The system generates this log when a log facility user causes unexpected conditions or messages.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.

LOG_SWERR	M2PA, 00: M2PA Software Errors	This log is generated when software errors are detected in M2PA.	An internal error has occurred.	The Information and Data fields report the error. If a data dump is generated by the error, the Information and Data fields include a hexadecimal data dump.	Contact your next level of support.
LOG_SWERR	M2UA, 00: M2UA Software Errors	This log is generated when software errors are detected in M2UA.	An internal error has occurred.	The Information and Data fields report the error. If a data dump is generated by the error, the Information and Data fields include a hexadecimal data dump.	Contact your next level of support.
LOG_SWERR	Mail Subsystem, 01: Mail Error	The log is reported when any problem occurs with the internal mail messaging subsystem. Typically these problems are related to subsystem initialization, or the failure to receive, send or allocate a message buffer.	An unexpected software condition has occurred.	The information in each log is dependent on the situation in which it is generated. The Information and Data fields change to match the data required to properly debug the cause of the problem.	Contact your next level of support.
LOG_SWERR	mLink Driver, 00: No Callback Registered	The mLink driver does not know how to process the TM message.	No application has registered with the mLink driver to process the TM message of this operation code.	The Information and Data fields display the 64-byte message.	Contact your next level of support.
LOG_SWERR	mLink Driver, 01: No Transmit Memory Allocated	The mLink driver could not allocate transmit memory.	There is a memory shortage.	No additional information is provided.	Contact your next level of support.
LOG_SWERR	mLink Driver, 03: Could Not Create Transmit Pool	The mLink driver could not create the transmit pool.	Memory or data structures are corrupted.	No additional information is provided.	Contact your next level of support.
LOG_SWERR	mLink Driver, 05: Could Not Initialize Pools	The mLink driver could not initialize working transmit and receive pools.	Memory or data structures are corrupted.	No additional information is provided.	Contact your next level of support.
LOG_SWERR	mLink Driver, 06: Buffer Not Released	The mLink driver could not release a buffer.	Memory or data structures are corrupted.	No additional information is provided.	Contact your next level of support.

LOG_SWERR	mLink Driver, 07: Buffer Not Queued	The mLink driver could not queue a buffer.	Memory or data structures are corrupted.	No additional information is provided.	Contact your next level of support.
LOG_SWERR	mLink Driver, 08: Invalid Opcode	An application tried to register with an invalid operation code.	The operation code passed to mlk_register_cb greater than 255.	No additional information is provided.	Contact your next level of support.
LOG_SWERR	mLink Driver, 09: Callback Already Registered	An application tried to register to an operation code that was already registered to another application.	An application is already registered with the specified operation code.	No additional information is required.	Contact your next level of support.
LOG_SWERR	mLink Driver, 10: Driver Initialization Fail	This log indicates an mLink driver initialization failure.	There is a system resource problem.	No additional information is provided.	Contact your next level of support.
LOG_SWERR	mLink Driver, 12: Driver Configuration Fail	This log indicates that the mLink driver could not bind its audit routine.	There is an mLink driver corruption or an audit facility data corruption.	No additional information is provided.	Contact your next level of support.
LOG_SWERR	MSU Trapping, 00: Software Error	The system generates this log when the MSU Trace facility encounters an unexpected condition or message. You should report this error to Nortel Networks technical support.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	MTP Level 2, 00: Software Errors	This log is generated when software errors are detected in MTP Level 2.	An internal error has occurred.	The Information and Data fields report the error. If a data dump is generated by the error, the Information and Data fields include a hexadecimal data dump.	Contact your next level of support.
LOG_SWERR	MTP Level 3 Event, 00: Level 3 Event Software Error	There is a software error involving Level 3 event activity.	An internal error has occurred.	The Information and Data fields describe the error.	Contact your next level of support.

LOG_SWERR	MTP Level 3 OMs, 01: Callback Registration Error	This log reports a callback registration error in SS7 MTP Level 3 OM applications.	An internal error has occurred.	The Information and Data fields indicate the system was unable to bind to the OM server or was unable to register callback with the OM client. The following information is also provided: RC = nn, where: nn = the return code.	Contact your next level of support.
LOG_SWERR	MTP Level 3 OMs, 02: Null Element ID	This log reports an error if a provisioned link, linkset or network appearance has a null OM element ID.	An internal error has occurred.	The Information and Data fields indicate that the OM element ID of nn=mm is null, where: nn = network appearance, link, linkset, and mm = the associated value.	Contact your next level of support.
LOG_SWERR	MTP Level 3 OMs, 03: Null Subelement ID	This log reports an error if a provisioned Special Study OM has a null OM subelement ID.	An internal error has occurred.	The Information and Data fields indicate that the OM Subelement ID of linkset = nn and SSOM = mm is null, where: nn = the linkset id. mm = the SSOM.	Contact your next level of support.
LOG_SWERR	MTP Level 3 OMs, 04: Add Element Error	This log reports an error if an attempt to add an OM element failed.	An internal error has occurred.	The Information and Data fields indicate which attempt to add an OM element failed, and element = ss, where: ss = the element text.	Contact your next level of support.

LOG_SWERR	MTP Level 3 OMs, 05: Add Subelement Error	This log reports an error if an attempt to add an OM subelement failed.	An internal error has occurred.	The Information and Data fields indicate which add OM subelement failed, and elementID = nn, subelement = ss, where: nn = the associated element ID ss = the subelement text	Contact your next level of support.
LOG_SWERR	MTP Level 3 OMs, 06: Delete Element Error	This log reports an error if an attempt to delete an element ID failed.	An internal error has occurred.	The Information and Data fields indicate the delete OM element that failed, and elementID = nn, where: nn = the associated element ID	Contact your next level of support.
LOG_SWERR	MTP Level 3 OMs, 07: Delete Subelement Error	This log reports an error if an attempt to delete a subelement ID failed.	An internal error has occurred.	The Information and Data fields indicate which delete OM subelement failed, and element ID = nn, subelement ID = ss, where: nn = the associated element ID ss = the subelement ID	Contact your next level of support.
LOG_SWERR	MTP Level 3 OMs, 08: Linkset or ASP Not Found	This log reports an error if a provisioned linkset or ASP does not exist.	An internal error has occurred.	The Information and Data fields indicate the linkset or ASP = nn is not found, and inact_start_time not set, where: nn = the linkset ID or ASP ID	Contact your next level of support.
LOG_SWERR	MTP Level 3 OMs, 09: Data Out Of Sequence	This log reports an error when the OM server's SS7 OM callback receives an invalid sequence number.	An internal error has occurred.	The Information and Data fields indicate the invalid sequence number received (nn), where: nn = the received sequence number .	Contact your next level of support.

LOG_SWERR	MTP Level 3 OMs, 13: Index Out of Range	This log indicates an error when the index used to access a data array is out of range.	An internal error has occurred.	The Information and Data fields indicate that the index exceeds ar[] boundary, and idx = nn, where: ar[] = the array. nn = the index number.	Contact your next level of support.
LOG_SWERR	MTP Level 3 OMs, 14: 5-Min Write Failed	This log indicates the 5-minute write failed.	The five-minute OM write failed.	The text field indicates: 5Min OM write failed: Element = e (e_hex) e = OM element ID in decimal e_hex = OM element ID in hex 5Min OM write failed: Element = e (e_hex), Subelement = s (s_hex) e = OM element ID in decimal e_hex = OM element ID in hex s = OM subelement ID in decimal s_hex = OM subelement ID in hex The data field indicates: Link, Path, ASP or Linkset NA = l, ElId = e, AppID = a, RegId = r, RegVal = v, OpCode = o l = the link or path ID a = the OM application ID r = the OM register ID of element e v = the OM register value of register r o = the OM operation code.	Contact your next level of support.
LOG_SWERR	MTP Level 3 OMs, 15: OM data collection failed	This log indicates that the OM data collection has failed.	The OM data received in the collection node is invalid.	The text field indicates the problem description of the error encountered.	If problem persists, contact your next level of support.
LOG_SWERR	MTP Restart, 00:	MTP Restart could not complete or initiate a request.	An internal error has occurred.		Contact your next level support.

LOG_SWERR	MTP Restart, 01:	MTP Restart could not derive the Network Appearance object from the specified Link.	An internal error has occurred.	The Link number and Network Appearance number are displayed. MTP Restart will not be applied to the Link.	Contact your next level support.
LOG_SWERR	MTP Restart, 02:	MTP Restart could not derive the Link Set object from the specified Link.	An internal error has occurred.	The Link number and Link Set number are displayed. MTP Restart will not be applied to the Link.	Contact your next level support.
LOG_SWERR	MTP Restart, 03:	MTP Restart could not derive the Network Appearance object from the specified Link Set.	An internal error has occurred.	The Link Set number and Network Appearance number are displayed. MTP Restart will not be applied to the Link.	Contact your next level support.
LOG_SWERR	MTP Restart, 04:	MTP Restart could not start a timer associated with an NA.	An internal error has occurred.	T22, T23, T24, T26 or T27 in ANSI could not be started T18 or T20 in ITU could not be started The timer will be displayed as a number. MTP Restart procedures will cease.	Contact your next level support.
LOG_SWERR	MTP Restart, 05:	MTP Restart could not start a timer associated with an NA.	An internal error has occurred.	T25, T28, T29 or T30 in ANSI could not start T19 or T21 in ITU could not start MTP Restart will cease.	Contact your next level support.
LOG_SWERR	MTP Restart, 06:	MTP Restart could not determine the Link Set object from time out message	An internal error has occurred.	The Link Set number is displayed. MTP Restart will cease.	Contact your next level support.
LOG_SWERR	MTP Restart, 07:	MTP Restart could not determine the Network Appearance object from time out message	An internal error has occurred.	The Network Appearance number is displayed. MTP Restart will cease.	Contact your next level support.

LOG_SWERR	MTP Restart, 08:	MTP Restart could not determine the timer reference for a Link Set	An internal error has occurred.	Timer reference and Link Set number are displayed. MTP Restart will cease.	Contact your next level support.
LOG_SWERR	MTP Restart, 09:	MTP Restart could not determine the timer reference for a Network Appearance	An internal error has occurred.	Timer reference and Network Appearance number are displayed. MTP Restart will cease.	Contact your next level support.
LOG_SWERR	MTP Restart, 10:	MTP Restart could not cancel a timer	An internal error has occurred.	Timer reference and Network Appearance number are displayed. MTP Restart will cease.	Contact your next level support.
LOG_SWERR	MTP Restart, 11:	MTP Restart could not start a timer	An internal error has occurred.	Timer reference is displayed. No buffers available. MTP Restart will cease.	Contact your next level support.
LOG_SWERR	MTP Restart, 30:	MTP Restart has received an invalid request/state.	Programmer's error, invalid function request. Internal error.	Affected NA or LS.	None.
LOG_SWERR	MTP Restart, 39:	MTP Restart is improperly configured.	Possible corruption.	Timestamp.	Contact next level support.
LOG_SWERR	Network Clock, 00: Software Error	This log is generated when the Network Clock subsystem encounters an unexpected condition or messages. This is an internal error that should be reported to Nortel Networks technical support.	An internal error has occurred in the clock messaging path.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	Network, 02: Software Error	This log indicates that a software error has occurred withing the network audit subsystem.	An internal error has occurred.	The Information and Data fields may provide additional information	Contact your next level of support.

LOG_SWERR	OAM API, 01: OAM API Communication Error	This log reports any OAM API communication errors. The OAM command stops executing. This log is used only by Nortel Networks technical support.		Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred. Contact your next level of support.	
LOG_SWERR	OAM API, 02: OAM Data Schema Error	This log reports any Data Schema access related errors. The resulting message indicates an internal error. This log is used only by Nortel Networks technical support.		Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred. Contact your next level of support.	
LOG_SWERR	OAM API, 03: OAM Software Error	The log is reported when OAM API encounters any software errors. This log is used only by Nortel Networks technical support.		Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred. Contact your next level of support.	
LOG_SWERR	OAM API, 04: OAM Server Error	The log is reported when OAM Server encounters any software errors. This log is used only by Nortel Networks technical support.		Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred. Contact your next level of support.	

LOG_SWERR	OAM API, 05: OAM Replication Error	This log is reported when the OAM API is unable to replicate a transaction.		The system node to which replication failed is indicated as well as the reason for the failure. Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred. Reload the system node that is indicated in the log. If the problem persists, contact your next level of support.	
LOG_SWERR	Office Parameters, 00: Software Error	This log is generated when the Office Parameters subsystem encounters an unexpected condition or messages. This is an internal error.	A data corruption has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	OM RDM Utilities, 00: Software Error	This log is generated when the OM RDM Database Utilities encounter an unexpected condition.	An internal error has generated an unexpected condition.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	OMs, 00: Software Error	This log is generated when the OM subsystem encounters an unexpected condition or message.	An internal error created the unexpected condition or message.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	OMs, 03: Critical Number of OM Timer Users	This log is generated when the number of clients using the OM Timer facility is approaching the capacity threshold.	An internal error has occurred.	No additional information is provided.	Contact your next level of support.

LOG_SWERR	OMs, 04: Memory Shortage	This log is generated when the OM subsystem has failed to allocate memory for the OM Timer buffers during initialization.	An internal error has occurred.	No additional information is provided.	Contact your next level of support.
LOG_SWERR	Power, 00: Software Error	This log is generated when the Power subsystem encounters an unexpected condition or messages.	An internal error created the unexpected condition or messages.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	Processor Exception, 00: Hardware Exception Error	The system generates this log when the hardware exception handler encounters unexpected conditions or messages.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	Processor Exception, 03: Initialization Software Error	The system generates this log during system node initialization if an error occurs that will prevent the system node from performing its required functions.	An internal error has occurred during the initialization of a system node. The system will attempt to reload the RTC, CC, or application system node automatically.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Monitor the status of the system node. If it does not recover, refer to the USP Fault Management Manual.
LOG_SWERR	Processor Exception, 09: Unhandled critical fault	The system generates this log when a card has encountered a service affecting fault and is taking itself out of service, but no software is available to remove the card from service.	An internal unhandled error has occurred.	Nortel Networks uses the information available from the card itself to determine the status of the card and what fault had occurred.	Usually no corrective action is required. The card reset that follows this log should clear any faults and the card should properly return to service. Monitor the system to ensure that the proper services are being provided and that no unusual faults exist. If there continue to be problems with the system, then contact your next level of support.

LOG_SWERR	RDM Utilities, 01: API Error	This log is generated when an RDM API call resulted in an error.	An internal error has occurred.	The Information field indicates what task caused the error. A more detailed cause of the error is displayed.	Contact your next level of support.
LOG_SWERR	RDM Utilities, 02: Resource Limit	This log is generated when a system resource is exhausted because of an RDM utility call.	The error is caused by excessive use of the RDM utility or system memory resources.	The Information field indicates what task caused the error. The resource that was exceeded is also listed in the Information field.	Contact your next level of support.
LOG_SWERR	RDM Utilities, 03: Database Not Open	This log is generated when a task attempts to access an unopened database.	An internal error has occurred.	The Information field indicates what task caused the error. A more detailed cause of the error is displayed.	Contact your next level of support.
LOG_SWERR	RDM Utilities, 04: Database Error	This log is generated when an RDM error occurs.	An internal error has occurred.	The Information and Data fields display the RDM error number and return codes. A detailed cause of the error is also displayed.	Contact your next level of support.
LOG_SWERR	SCCP Connectionless control, 00: SCCP Connectionless control Error	This log reports an error in SCCP Connectionless control.	Unable to create a reassembly instance on the link card.	The Information and Data fields describe the error.	Contact your next level of support.
LOG_SWERR	SCCP Management, 00: SCCP Management Error	This log reports an error in SCCP management.	An internal error has occurred.	The Information and Data fields describe the error.	Contact your next level of support.
LOG_SWERR	SCCP OMs, 01: Callback Registration Error	This log reports a callback registration error in SS7 SCCP OM applications.	An internal error has occurred.	The Information and Data fields indicate the system was either unable to bind to the OM server, and/or unable to register a callback with the OM client, and RC = nn, where: nn = the return code.	Contact your next level of support.

LOG_SWERR	SCCP OMs, 02: Null Element ID	This log reports an error when a provisioned network appearance has a null OM element ID.	An internal error has occurred.	The Information and Data fields contain the following information: The OM element ID of NA = mm is null, where: mm = the network appearance value.	Contact your next level of support.
LOG_SWERR	SCCP OMs, 03: Null Subelement ID	This log reports an error if a provisioned GTT type has a null OM subelement ID.	An internal error has occurred.	The Information and Data fields indicate that the OM subelement ID of NA = nn, TT = mm is null, where: nn = the network appearance number mm = represents the GTT type value.	Contact your next level of support.
LOG_SWERR	SCCP OMs, 04: Add Element Error	This log reports an error when an attempt to add an OM element failed.	An internal error has occurred.	The Information and Data fields indicate which attempt to add an OM element failed, and element = ss, where: ss = the element text.	Contact your next level of support.
LOG_SWERR	SCCP OMs, 05: Add Subelement Error	This log reports an error when an attempt to add an OM subelement fails.	An internal error has occurred.	The Information and Data fields indicate which attempt to add an OM subelement failed, including elementID = nn and subelement = ss, where: nn = the associated element ID ss = the subelement text.	Contact your next level of support.

LOG_SWERR	SCCP OMs, 06: Delete Element Error	This log reports an error when an attempt to delete an element ID fails.	An internal error has occurred.	The Information and Data fields indicate which attempt to delete an OM element failed, including elementID = nn, where : nn = the associated element ID.	Contact your next level of support.
LOG_SWERR	SCCP OMs, 07: Delete Subelement Error	This log reports an error when an attempt to delete an OM subelement ID fails.	An internal error has occurred.	The Information and Data fields indicate which attempt to delete an OM subelement failed, including elementID = nn, subelementID = mm, where: nn = the associated element ID ss = the subelement ID.	Contact your next level of support.
LOG_SWERR	SCCP OMs, 08: Linkset or ASP Not Found	This log reports an error when a provisioned linkset or ASP does not exist.	An internal error has occurred.	The Information and Data fields indicate that linkset or ASP = nn was not found, and inact_start_time is not set, where: nn = the linkset ID or ASP ID.	Contact your next level of support.

LOG_SWERR	SCCP OMs, 12: SCCP OM 5-Min Write Failed	This log indicates an error when the 5-minute write fails.	An internal error has occurred.	The Information and Data fields provide the following information: 5Min OM write request: Element = e (e_hex) e = OM element ID in decimal e_hex = OM element ID in hexadecimal 5Min OM write request: Element = e (e_hex), subelement = s (s_hex) e = OM element ID in decimal e_hex = OM element ID in hexadecimal s = OM subelement ID in decimal s_hex = OM subelement ID in hexadecimal	Contact your next level of support.
LOG_SWERR	SCCP OMs, 14: SCCP OM Software Error	The system generates this log when the SCCP Operational Measurement interface encounters an unexpected condition. You should report this error to Nortel Networks technical support.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	SCTP, 00: SCTP Software Errors	This log is generated when software errors are detected in SCTP.	An internal error has occurred.	The Information and Data fields report the error. If a data dump is generated by the error, the Information and Data fields include a hexadecimal data dump.	Contact your next level of support.
LOG_SWERR	SCTP, 06: SCTP OM	This log is generated when software errors are detected in SCTP OMs.	An internal error has occurred.	The Information and Data fields report the error. If a data dump is generated by the error, the Information and Data fields include a hexadecimal data dump.	Contact your next level of support.

LOG_SWERR	Shelf, 00: Software Error	This log is generated when the Shelf subsystem encounters an unexpected condition or messages.	The unexpected condition or messages has created an internal error.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	Signaling Network Management, 00: SNM Software Error	This log reports an SS7 signaling network management (SNM) error.	An internal error has occurred.	The text field describes the error.	Contact your next level of support.
LOG_SWERR	SIP Application Group, 00: SIP Appl Software Error	There is a software error involving the SIP protocol and application subsystem.	An internal error has occurred.	The Information and Data fields describe the error.	Contact your next level of support.
LOG_SWERR	Software Upgrade, 00: Software Error	This log is generated when the software upgrade subsystem encounters an unexpected condition or messages. This is an internal error that should be reported to Nortel Networks technical support.	An internal error has occurred during software upgrade processing.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	SS7 Data, 01: Software Error	This log is generated when the Data subsystem encounters an unexpected condition or message.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	SS7 Data, 03: System Error	This log is generated when the Data subsystem encounters an unexpected system error condition or message.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	SS7 Data, 04: File Input/Output Error	This log is generated when the Data subsystem encounters an unexpected file input/output error condition or message.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.

LOG_SWERR	SS7 TCAP Decode, 00: TCAP Decode Error	This log reports an error in TCAP decoding.	An internal error has occurred.	The Information and Data fields describe the error.	Contact your next level of support.
LOG_SWERR	SS7 TCAP Tagging, 00: TCAP Tagging Error	This log reports an error in TCAP tagging.	An internal error has occurred.	The Information and Data fields describe the error.	Contact your next level of support.
LOG_SWERR	SS7 TCAP Tagging, 02: Invalid TCAP Message Tag	This log reports an error in TCAP tagging due to an invalid tag.	An internal error has occurred.	The Information and Data fields describe the error.	Contact your next level of support.
LOG_SWERR	SS7 User Part, 01: C7UP Error	This log reports failures during C7 User Part OM processing. This log is used only by Nortel Networks technical support.	A C7UP OM processing error has occurred.	The data output by the log depends on the error scenario.	Contact your next level of support.
LOG_SWERR	SSCS Messaging Layer, 00: Default	This log is generated when a particular SSCS log does not map to an existing SSCS log type.	An SSCS log does not map to an existing SSCS log type.	The Information and Data fields describe the nature of the error.	Contact your next level of support.
LOG_SWERR	SSCS Messaging Layer, 01: Mapped from SSCS SME_LOG_USRERR	This log is generated when the SSCS facility experiences a user error.	The SSCS facility received an unknown, incorrectly formatted, or out-of-sequence primitive.	The Information field describes the error.	Contact your next level of support.
LOG_SWERR	SSCS Messaging Layer, 03: Mapped from SSCS SME_LOG_ERR	This log is generated when the SSCS facility experiences a software error.	An internal error has occurred.	The Information field describes the error.	Contact your next level of support.
LOG_SWERR	SSCS Messaging Layer, 04: Mapped from SSCS SME_LOG_FATAL	This log is generated when the SSCS facility experiences an unrecoverable error.	An internal error has occurred.	The Information field describes the error.	Contact your next level of support.

LOG_SWERR	SSCS Messaging Layer, 05: Function Called By SSCS Returned Error	This log is generated when an SSCS function call fails.	The called SSCS function failed.	The Information field indicates the calling and called functions that returned a failure indication. The Information field will also contain, in parentheses, some additional information that distinguishes between multiple logs of the same type, when necessary. The Data field indicates the return code received from the called function, when a return code is present.	Contact your next level of support.
LOG_SWERR	Summary Log, 00: Log Summary system error	The system generates this log when log summary encounters an unexpected condition. You should report this error to Nortel Networks technical support.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	Summary Log, 01: Summary log	The system generates this log to report the number of logs not displayed during the summary period. You should investigate and fix the problem reported in the log that is being summarized.	None.	None.	Investigate and fix the original problem if necessary.
LOG_SWERR	SUNI Event Manager, 01: Callback Registration Failed	This log indicates that an application was unable to register a callback with the SUNI Event Manager.	NULL callback function pointer passed in to bind routine.	The Information field indicates that invalid callback registration for SUNI Events occurred.	Contact your next level of support.
LOG_SWERR	SUNI Event Manager, 02: Callback Cancellation Failed	This log indicates that an application was unable to cancel a callback with the SUNI Event Manager.	Invalid (out of range) callback ID passed into cancel routine or NULL callback function found (at location specified by callback ID).	The Information field indicates that invalid callback cancellation for SUNI Events occurred.	Contact your next level of support.

LOG_SWERR	SUNI Event Manager, 04: Callback Failed	This log indicates that an application callback was unable to process the event.	There is a logic error in the callback.	The Information field indicates that the callback was unable to completely process the event.	Contact your next level of support.
LOG_SWERR	System Administration, 02: No User Accounts	This log is generated by the HMI server task when there are no system administration user accounts in the system. This is an error condition because there should always be at least one default system administration user account in the system.	An internal error has occurred.	The Information field indicates that there are no system administration user accounts in the system.	Contact your next level of support.
LOG_SWERR	System Administration, 07: Get User Data Failed	This log is generated by the HMI server task when the user account data in the database cannot be accessed.	An internal error has occurred.	The Information field indicates that the attempt to access the user account data in the database has failed.	Contact your next level of support.
LOG_SWERR	System Administration, 08: Set User Data Failed	This log is generated by the HMI server task when the user account data in the database cannot be set.	An internal error has occurred.	The Information field indicates that the attempt to store the user account data in the system database has failed.	Contact your next level of support.
LOG_SWERR	System Administration, 09: Find User Data Failed	This log is generated by the HMI server task when specific user account data cannot be found in the database.	An internal error has occurred.	The Information field indicates that the system cannot locate the user account data in the system database.	Contact your next level of support.
LOG_SWERR	System Administration, 10: Add User Account Failed	This log is generated by the HMI server task when a user account cannot be added to the database.	An internal error has occurred or an identical user ID may already exist.	The Information field indicates that the attempt to add a new user account to the system database has failed.	Try to add the user account using a different user ID. Refer to the User Accounts section of the USP User Guide for more for more information. If this does not correct the problem, contact your next level of support.
LOG_SWERR	System Administration, 11: Delete User Account Failed	This log is generated by the HMI server task when user account data cannot be deleted from the database.	An internal system error has occurred.	The Information field indicates that the attempt to remove a user account from the system database has failed.	Contact your next level of support.

LOG_SWERR	System Administration, 12: Set Time Failed	This log is generated by the HMI server task when the system time cannot be set.	An internal system error has occurred.	The Information field indicates that the attempt to set the system time has failed.	Contact your next level of support.
LOG_SWERR	System Administration, 13: Login Resource	This log is generated by the HMI server task when a user tries to log into the system and the system is unable to process the user ID and the associated HMI task ID properly.	An internal error has occurred.	The Information field indicates that the attempt to log a user into the system has failed.	Contact your next level of support.
LOG_SWERR	System Administration, 14: Logout Resource	This log is generated by the HMI server task when a logged-in user tries to log out of the system and the system cannot process the user ID and the associated HMI task ID properly.	An internal error has occurred.	The Information field indicates that the attempt to log a user ID out of the system has failed.	Contact your next level of support.
LOG_SWERR	System Administration, 15: Find Resource Failed	This log is generated by the system administration subsystem when the system cannot find the current task ID in the Task ID to User list.	An internal error has occurred.	The Information field indicates the attempt to find the user ID associated with the current running task has failed.	Contact your next level of support.
LOG_SWERR	System Administration, 17: Find Load Image File Failed	This log is generated when the System Administration subsystem tries to find and list the available load image files on the system and none are found.	An internal error has occurred.	The Information field indicates that no load image files were found on the SCSI disk associated with an RTC system node.	Contact your next level of support.
LOG_SWERR	System Administration, 19: Load Image File Deletion Failed	This log is generated by the System Administration subsystem when the user tries to delete a load image file from the system and the operation fails.	An internal error has occurred.	The Information field indicates that the attempt to delete a load image file from the system failed.	Contact your next level of support.
LOG_SWERR	System Administration, 20: Get Software Data Failed	This log is generated by the HMI server task when it is not possible to get detailed software load information.	An internal error has occurred.	The Information field indicates that the attempt to get software load information has failed.	Contact your next level of support.
LOG_SWERR	System Administration, 22: Get Data Snapshot Information Failed	This log is generated by the HMI server task when information about the current data snapshot cannot be retrieved.	An internal error has occurred.	The Information field indicates that information about the current data snapshot cannot be retrieved.	Contact your next level of support.

LOG_SWERR	System Administration, 24: Data Snapshot Deletion Failed	This log is generated by the system when it is not able to delete the specified data snapshot.	If the snapshot is stored on the Alternate Boot Server, this log may indicate that the system does not have adequate file permissions (someone may have changed the permissions manually on the file)	The Information field indicates that the attempt to delete a data snapshot has failed.	Verify file permissions on the Alternate Boot Server. If the problem persists, contact your next level of support.
LOG_SWERR	System Administration, 26: Create Data Snapshot Failed	This log is generated by the System Administration subsystem when an error occurs while a data snapshot is being generated.	An internal error has occurred.	The Information field indicates that the attempt to generate a data snapshot has failed.	Contact your next level of support.
LOG_SWERR	System Administration, 28: Open Device Failed	This log is generated by the System Administration subsystem when an attempt to open the SCSI disk fails.	An internal error has occurred.	The Information field indicates that the attempt to open the SCSI disk has failed.	Contact your next level of support.
LOG_SWERR	System Administration, 32: NFS Copy	This log is generated by the system administration subsystem when the system attempt to use the NFS Server to copy a data snapshot or load image file from the OAM&P workstation to the SCSI disk associated with an RTC system node has failed.	An internal system error has occurred or the network between the USP and the OAM&P workstation has gone down.	The Information field indicates that the attempt to use the NFS Server to copy a data snapshot or load image file from the OAM&P workstation to the SCSI disk associated with an RTC system node has failed.	Contact your next level of support.
LOG_SWERR	System Administration, 33: Putenv Function Failed	This log is generated by the system administration subsystem when the VxWorks function, putenv, fails to store the environment variable, TIMEZONE.	An internal error has occurred.	The Information field indicates that the attempt to set the TIMEZONE environment variable has failed.	Contact your next level of support.
LOG_SWERR	System Administration, 34: Getenv Function Failed	This log is generated by the system administration subsystem when the VxWorks function, getenv, retrieves a null string for the environment variable, TIMEZONE.	An internal error has occurred.	The Information field indicates that the attempt to get the TIMEZONE environment variable returned a null string.	Contact your next level of support.

LOG_SWERR	System Administration, 45: Administration Software Error	The system generates this log when the OAM subsystem related to administration and/or security encounters an unexpected condition. You should report this error to Nortel Networks technical support.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	System Administration, 53: Get Authentication Data Failed	This log is generated by the Authentication routine that is used to authenticate users when they login to the system. It is generated when the data that is necessary proceed with authentication can not be accessed.	An internal error has occurred.	The Information field indicates that the attempt to access the user account data or remote authentication data in the database has failed.	Contact your next level of support.
LOG_SWERR	System Administration, 54: Authentication SSL connection Failed	This log is generated by the Authentication routine that is used to authenticate users when they login to the system. It is generated when establishing a connection or communicating with the Remote Authentication server fails.	An internal error has occurred, or Remote Authentication server failed communication.	The Information field indicates that one of several stages in the SSL connection with the Remote Authentication server was not successful.	Contact your next level of support.
LOG_SWERR	System Node Maintenance, 00: Software Error	This log is generated when the system node maintenance subsystem encounters unexpected conditions or messages.	A software error has occurred in Node Maintenance code.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	Task Management, 00: Failed to Register with OMs	This log is generated when the Task Management subsystem fails to register with the OM subsystem.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	Task Management, 01: OM Data Exceeded	This log is generated when the Task Management subsystem OM data exceeds a buffer.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system at the time the problem occurred.	Contact your next level of support.

LOG_SWERR	Task Management, 02: OM Opcode Invalid	This log is generated when the Task Management subsystem OM opcode is invalid.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	Task Management, 03: Write Error	This log is generated when the Task Management subsystem has a write error.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	Task Management, 05: Idle Task Exit	This log is generated when the Task Management subsystem detects that the idle task has exited.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	Task Management, 06: Task Audit Software Error	This log is generated when the Task Audit subsystem encounters an unexpected software condition.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR	Throttle, 00: Throttle Error	This log reports an error in the event throttle mechanism.	An internal error has occurred.	The Information and Data fields describe the error.	Contact your next level of support.
LOG_SWERR	Time of Day, 00: Software Error	This log is generated when the Time of Day system encounters an unexpected condition or messages. Report this error to Nortel Networks technical support.	An internal error has occurred.	The Information and Data fields describe the context in which the error occurred.	Contact your next level of support.
LOG_SWERR	Timer Facility, 00: Bad Timer Action	This log is generated when an application has attempted to start or cancel a timer with an unknown Timer Action.	An internal error has occurred.	The Information and Data fields indicate the invalid action requested.	Contact your next level of support.
LOG_SWERR	Timer Facility, 01: No Timer Buffers	This log is generated when the system tries to start a new timer but the timer facility is out of buffers.	There is a shortage of internal timer buffers.	The Information and Data fields indicate the action requested.	Contact your next level of support.

LOG_SWERR	Timer Facility, 02: Memory Allocation Failure	This log is generated when there is a shortage of system memory resources.	There is a system resource management problem.	The Information and Data fields indicate the amount of memory requested.	Contact your next level of support.
LOG_SWERR	Timer Facility, 03: Semaphore Not Granted	This log is generated when there is a shortage of system resources. The Timer Facility semaphore was requested, but not granted.	A system resourcing internal error has occurred.	The Information and Data fields display the semaphore ID.	Contact your next level of support.
LOG_SWERR	TXMGR, 00: Transaction Manager Software Error	The system generates this log when the Transaction Management subsystem encounters an unexpected condition. You should report this error to Nortel Networks technical support.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.
LOG_SWERR, LOG_INFO	Buffer Manager, 04: Internal Problem with the buffer	This log is generated to indicate a change in the congestion level for SS7 links or to report an internal problem with a buffer.	For LOG_INFO logs, the system is experiencing congestion and messages will be discarded according to SS7 standards. For LOG_SWERR logs, an unexpected software condition has occurred.	LOG_INFO logs indicate congestion the internal LinkId, DiscardLvl and CongLvl parameters that can be used to monitor the congestion level. LOG_SWERRs contain data for debugging software problems.	For LOG_INFO logs, no action is required. For LOG_SWERR logs, contact your next level of support.
LOG_TRAP	Processor Exception, 02: Exception record	The system generates this log when a task causes a hardware exception, such as dividing by zero or trying to access invalid memory locations. The operating system suspends the task when this occurs. If possible, the system will automatically reload the faulted RTC, CC, or application system node.	An internal error has occurred.	Nortel Networks uses the information in the Information and Data fields to determine the status of your system when the problem occurred.	Contact your next level of support.

Appendix E: MG9000 Reported Alarms, Event Logs, Audit Logs

New or changed in SN09

New or changed in SN09FF

MG9000 Reported Alarms

Alarm Id	Fault Type	Severity	Description	Supported	Procedure To Generate Alarm, and Alarm Recovery
CES305	cesLossOfCell	Major	Loss of Cells	Yes	This alarm is raised when CES IWF stops receiving cells for the ATM network. To introduce this condition SVC between the local endpoint and the remote endpoint must be broken. This can be done 2 different ways: 1. At Dshell prompt, type /cesnv/disconn lflIndex. 2. From EM, this can only be done for 'half services'. Disconnect the remote endpoint to observe Loss of Cells at the local. Recovery: This condition is observed in the field when there is an issue with ATM connectivity. The alarm will be cleared when ATM connection is restored. So, any issue with the ATM connection needs to be investigated.
norCarrFault (NORTEL-UEMG-CARRIER-					
MGCA301	los	DS1 - Minor OC3 - Critical	lossOfSignal	yes	On DS1 Link, pull Rx fiber to set LOS
MGCA302	ais	DS1 - Minor OC3 - Critical	alarm indication signal	yes	On DS1 Link, use test set (TBERD) to inject line AIS
MGCA303	lof	DS1 - Minor OC3 - Critical	lossOfFrame	yes	On DS1 Link, Use test (TBERD) set to inject LOF
MGCA304	rai	DS1 - Minor	remote alarm indication	yes	
MGCA305	bersf	OC3 - Critical	bitErrorRate S F...	yes	On DS1 Link, Use test set (TBERD) to inject line B2, Bit Error Rate of 10e-3
MGCA306	bersd	OC3 - Major	bitErrorRate SigDegrade	yes	On DS1 Link, Use test set (TBERD) to inject line B2, Bit Error Rate of 10e-5
MGCA307	rdi	OC3 - Minor	remote defect indication	yes	On DS1 Link, Use test set (TBERD) to inject line RDI
MGCA308	plm	OC3 - Minor	path label mismatch	yes	On DS1 Link, Use test set (TBERD) to change C2 label from 0x13 to 0x00
MGCA309	lop	OC3 - Minor	loss of Pointer	yes	On DS1 Link, Use test set (TBERD) to inject path LOP error
MGCA310	uneq	OC3 - Minor	unequipped	yes	On DS1 Link, Use test set (TBERD) to set C2 to 0x00 (unequipped)
MGCA312	imaLinkLif	Minor	IMA link- Loss of IMA Frame	yes	At the IMA card pull the DS1 cable (Can't report Alarm if link is down)
MGCA313	imaLinkLods	Minor	IMA link- Loss of delayed synchronization	yes	This alarm 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 "fakeInkfm" command in the /hal/ima MG9K Dshell directory.
MGCA314	imaLinkRfi	Minor	IMA link- Remote failure indication	yes	At the Edgelink (or other MUX) manually send AIS to the PP15000
MGCA315	imaLinkTxMisConne	Minor	IMA link Transmit misconnect	yes	This alarm 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 "fakeInkfm" command in the /hal/ima MG9K Dshell directory.
MGCA316	imaLinkRxMisConne	Minor	IMA link receive misconnect	yes	Same as above
MGCA317	imaLinkTxFault	Minor	IMA link transmit fault	yes	Change the "transmit Clock Mode" to ITC on the IMA link at the PP15000
MGCA318	imaLinkRxFault	Minor	IMA link receive fault	yes	This alarm 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 "fakeInkfm" command in the /hal/ima MG9K Dshell directory.
MGCA319	imaLinkTxUnusableF	Minor	IMA link transmit unusable far end	yes	Change the "transmit Clock Mode" to ITC on the IMA link at the PP15000

MGCA320	maLinkRxUnusableF	Minor	IMA link receive unusable far end	yes	Same as above
MGCA321	maGroupStartupFe	Major	IMA group startup far end	yes	This alarm 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 "fakelgrpfm" command in the /hal/ima MG9K Dshell directory.
MGCA322	imaGroupCfgAbort	Critical	IMA group configuration abort	yes	Same as above
MGCA323	maGroupCfgAbortF	Major	IMA group configuration abort far end	yes	Same as above
MGCA324	maGroupInsuffLink	Critical	IMA group insufficient links	yes	At the IMA card pull the DS1 cable (Can't report Alarm if link is down)
MGCA325	aGroupInsuffLinks	Major	IMA group insufficient links far end	yes	Same as above
MGCA326	maGroupBlockedF	Minor	IMA group blocked far end	yes	Block the IMA group at the PP15000
MGCA327	maGroupTimingSyn	Major	IMA group timing synchronization	yes	Change the "transmit Clock Mode" to ITC on the IMA link at the PP15000
MGCA328	abiLossOfClock	Critical	ABI Loss of Clock on DS512 optical link	yes	On the DS512 link, Use test set (TBERD) to set LOC
MGCA329	abiLossOfFrame	Critical	ABI Loss of Frame on DS512 optical link	yes	On the DS512 link, Use test set (TBERD) to set LOF
MGCA330	abiLowLightLevel	Critical	ABI Loss of Signal (low light level) on DS512 optical link	yes	On the DS512 link, Use test set (TBERD) to set LOS
MGCA331	biChannelParityErr	Minor	ABI Channel parity error on DS512 optical link	yes	On the DS512 link, Use test set (TBERD) to set C2 to 0x00 (unequipped)
MGCA332	tim	Minor	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	yes	Recovery: 1) Ensure that the host carrier is generating the correct Trace Identifier. 2) Ensure that the correct fiber is connected to the OC3 card. 3) Update the Path Trace Identifier at the LCI. 4) Using the STM-1 EM GUI screen button check the transmitted Path Trace Identifier to ensure it is the "provisioned" Path Trace Identifier.
MGCA333	ds3Ais		DS3 - Alarm Indication Signal - Check far-end carrier faults	yes	
MGCA334	ds3Lof		DS3 - Loss Of Frame	yes	
MGCA335	ds3Rai		DS3 - Remote Indication Signal - Check far-end carrier faults	yes	
SCC2 Log Output Example: *C01 MGCA330 0746 TBL MG9K NorCarrFault Location: 1-RM9K-Frame000.Shelf1.Slot06.Port00 Notification Id: 824 State: not acknowledged Category: Communication Alarm Cause: Loss Of Signal Time: Apr 24 14:01:11 2003 Component Id: Port.frame0.shelf1.slot6.ABI.abi Specific Problem: NorCarrFault - ABI loss of signal Description: Loss Of Signal (i.e., Low Light Level) on DS512 Optical Link Site Flr RPos Bay_id FFFF FF FFF FFFF FFF				NTSTD Log Output Example: MSH10_I06BE *** MGCA330 APR24 14:01:11 0746 TBL MG9K NorCarrFault Location: 1-RM9K-Frame000.Shelf1.Slot06.Port00 Notification Id: 824 State: not acknowledged Category: Communication Alarm Cause: Loss Of Signal Time: Apr 24 14:01:11 2003 Component Id: Port.frame0.shelf1.slot6.ABI.abi Specific Problem: NorCarrFault - ABI loss of signal Description: Loss Of Signal (i.e., Low Light Level) on DS512 Optical Link Site Flr RPos Bay_id FFFF FF FFF FFFF FFF	
nnAtmFaultType (NORTEL-UEMG-ATM-					
VC301	vcITpAis	Minor	atmVcl Alarm indication signal	yes	This Alarm cannot be generated under normal condition or with a test set. The following Dshell command must be used "cd atmss/atmoam" aisalarm. Recovery: Tear down the SVC and reestablish, check DS1 card for proper operation.

VC302	vclTpRdi	Minor	atmVcl Remote Detection Indicator	yes	This Alarm cannot be generated under normal condition or with a test set. The following Dshell commacd must be used "cd atmss/atmoam" rdialarm. Recovery: Tear down the SVC and reestablish, check DS1 card for proper operation.
VC303	vclLoc	Minor	loss of continuity, vcl	yes	This Alarm cannot be generated under normal condition or with a test set. The following Dshell commacd must be used "cd atmss/atmoam" ccalarm. Recovery: Tear down the SVC and reestablish, check DS1 card for proper operation.
VC304	vccTpAis	Minor	atmVcc Alarm indication signal	yes	This Alarm cannot be generated under normal condition or with a test set. The following Dshell commacd must be used "cd atmss/atmoam" aisalarm. Recovery: Tear down the SVC and reestablish, check DS1 card for proper operation.
VC305	vccTpRdi	Minor	atmVcc Remote Detection Indicator	yes	This Alarm cannot be generated under normal condition or with a test set. The following Dshell commacd must be used "cd atmss/atmoam" rdialarm. Recovery: Tear down the SVC and reestablish, check DS1 card for proper operation.
VC306	vccLoc	Minor	loss of continuity, vcc	yes	This Alarm cannot be generated under normal condition or with a test set. The following Dshell commacd must be used "cd atmss/atmoam" ccalarm. Recovery: Tear down the SVC and reestablish, check DS1 card for proper operation.
nnShfFault (NORTEL-UEMG-SHF-MIB)					
SHLF301	shelfTalkBatteryA	Critical	SIC Talk Battery A	yes	Pull Talk Battery A Fuse (at BIP panel) Recovery: Check fuse.
SHLF302	shelfTalkBatteryB	Critical	SIC Talk Battery B	yes	Pull Talk battery B fuse (at BIP panel) Recovery: Check fuse.
SHLF303	shelfSignalBatteryA	Major	SIC Signal Battery A	yes	Pull Signal Battery A fuse (at BIP panel) Recovery: Check fuse.
SHLF304	shelfSignalBatteryB	Major	SIC Signal Battery B	yes	Pull Signal Battery B fuse (at BIP panel) Recovery: Check fuse.
SHLF305	shelfSignalBatteryAfuse	Major	SIC Signal Battery A Fuse	yes	Put Blown Signal Battery A fuse in BIP Panel Recovery: Check fuse.
SHLF306	shelfSignalBatteryBfuse	Major	SIC Signal Battery B Fuse	yes	Put Blown Signal Battery B fuse in BIP Panel Recovery: Check fuse.
SHLF307	shelfFailLED	Indeterminate	SIC Shelf Fail LED	yes	Any Shelf failure Recovery: Remove all Shelf Failures.
SHLF308	bipSignalBatteryA1	Major	BIP Signal Battery A1	yes	Pull Signal Battery A1 Fuse (at BIP panel) Recovery: Check fuse.
SHLF309	bipSignalBatteryA2	Major	BIP Signal Battery A2	yes	Pull Signal Battery A2 Fuse (at BIP panel) Recovery: Check fuse.
SHLF310	bipSignalBatteryB1	Major	BIP Signal Battery B1	yes	Pull Signal Battery B1 Fuse (at BIP panel) Recovery: Check fuse.
SHLF311	bipSignalBatteryB2	Major	BIP Signal Battery B2	yes	Pull Signal Battery B2 Fuse (at BIP panel) Recovery: Check fuse.
SHLF312	bipTalkBatteryA	Minor	BIP Talk Battery A	yes	Remove (or Offline/Lock ate EM) TB A Filter card Recovery: Re-insert (or Unlock/Online ate EM) TB A Filtercard
SHLF313	bipTalkBatteryB	Minor	BIP Talk Battery B	yes	Remove (or Offline/Lock ate EM) TB B Filter card Recovery: Re-insert (or Unlock/Online ate EM) TB B Filtercard
SHLF314	bipFilterA	Minor	BIP Filter A Fail	yes	Requires Bad card or use of Dshell to generate the alarm Recovery: Replace bad card
SHLF315	bipFilterB	Minor	BIP Filter B Fail	yes	Requires Bad card or use of Dshell to generate the alarm Recovery: Replace bad card
SHLF316	bipScanPoint1	Indeterminate	BIP Scan Point 1	yes	Requires closure of Specifid Scan Point pins on the Scan Point cable. This may require a test board. Alternitively Dshell can be used to generate this alarm. To do this Telnet into an active ITX card and enter the following command "/glan/dsend XX 03 01 b5 70 06 07 00 82 YY 01 00 b2 e9". To clear the alarm use "/glan/dsend XX 03 01 b5 70 06 07 00 82 YY 00 00 b2 e9". XX = ITP slot number and YY = 08 Recovery: Investigate Scan Point Source to determine problem.

SHLF317	bipScanPoint2	Indeterminate	BIP Scan Point 2	yes	Same as above except XX = 09 Recovery: Investigate Scan Point Source to determine problem.
SHLF318	bipScanPoint3	Indeterminate	BIP Scan Point 3	yes	Same as above except XX = 0a Recovery: Investigate Scan Point Source to determine problem.
SHLF319	bipScanPoint4	Indeterminate	BIP Scan Point 4	yes	Same as above except XX = 0b Recovery: Investigate Scan Point Source to determine problem.
SHLF320	bipScanPoint5	Indeterminate	BIP Scan Point 5	yes	Same as above except XX = 0c Recovery: Investigate Scan Point Source to determine problem.
SHLF321	bipScanPoint6	Indeterminate	BIP Scan Point 6	yes	Same as above except XX = 0d Recovery: Investigate Scan Point Source to determine problem.
SHLF322	bipScanPoint7	Indeterminate	BIP Scan Point 7	yes	Same as above except XX = 0e Recovery: Investigate Scan Point Source to determine problem.
SHLF323	bipScanPoint8	Indeterminate	BIP Scan Point 8	yes	Same as above except XX = 0f Recovery: Investigate Scan Point Source to determine problem.
SHLF324	bipScanPoint9	Indeterminate	BIP Scan Point 9	yes	Same as above except XX = 10 Recovery: Investigate Scan Point Source to determine problem.
SHLF325	bipScanPoint10	Indeterminate	BIP Scan Point 10	yes	Same as above except XX = 11 Recovery: Investigate Scan Point Source to determine problem.
SHLF326	bipScanPoint11	Indeterminate	BIP Scan Point 11	yes	Same as above except XX = 12 Recovery: Investigate Scan Point Source to determine problem.
SHLF327	bipTalkBatteryA1	Major	Talk Battery A1 Power Feed	yes	Pull PDA fuse Recovery: Check Power feed connection and PDA fuse
SHLF328	bipTalkBatteryA2	Major	Talk Battery A Power Feed	yes	Pull PDA fuse Recovery: Check Power feed connection and PDA fuse
SHLF329	bipTalkBatteryB1	Major	Talk Battery B1 Power Feed	yes	Pull PDA fuse Recovery: Check Power feed connection and PDA fuse
SHLF330	bipTalkBatteryB2	Major	Talk Battery B2 Power Feed	yes	Pull PDA fuse Recovery: Check Power feed connection and PDA fuse
SHLF332	bipEcuTemp0	Minor	BIP Environmental Control Unit 0 Temperature	yes	Through Dshell reset the the threshold to value that will trigger this alarm. To do this Telnet into an active ITX card and enter the following command "/glan/dsend XX 03 01 b5 70 06 07 00 82 YY 01 00 b2 e9". To clear the alarm use "/glan/dsend XX 03 01 b5 70 06 07 00 82 YY 00 00 b2 e9". XX = ITP slot number and YY = 18
SHLF333	bipEcuTemp1	Minor	BIP Environmental Control Unit 1 Temperature	yes	Through Dshell reset the the threshold to value that will trigger this alarm. To do this Telnet into an active ITX card and enter the following command "/glan/dsend XX 03 01 b5 70 06 07 00 82 YY 01 00 b2 e9". To clear the alarm use "/glan/dsend XX 03 01 b5 70 06 07 00 82 YY 00 00 b2 e9". XX = ITP slot number and YY = 1A
SHLF334	bipEcuFan0	Minor	BIP Environmental Control Unit 0 Fan	yes	Remove Fan Cable Recovery: Check Fan cable, fuses, or replace fan.
SHLF335	bipEcuFan1	Minor	BIP Environmental Control Unit 1 Fan	yes	Remove Fan Cable Recovery: Check Fan cable, fuses, or replace fan.
SHLF336	bipRemoteAlarmcutoff	Indeterminate	BIP Remote Alarm Cut Off	yes	Engage Remote Alarm Cut Off button on BIP panel Recovery: Disengage Alarm cut Off button on BIP panel
SHLF337	bipLocalAlarmcutoff	Indeterminate	BIP Local Alarm Cut Off	yes	Engage Alarm Cut Off button on BIP panel Recovery: Disengage Remote Alarm cut Off button on BIP panel
SHLF338	bipAbsFusefail	Major	BIP ABS Fuse Fail	yes	Remove ABS fuse Recovery: Replace ABS fuse
SHLF339	bipAbsPowerSupply	Critical	BIP ABS Battery Power Supply	yes	Remove ABS power cable Recovery: Check (replace if necessary) ABS Power supply, Check Power supply power cables and leads
SHLF340	bipShfBreakerTrip	Major	BIP Shelf Circuit Breaker Trip	yes	Turn off Breaker Recovery: Check Breaker. Turn on Breaker.
SHLF341	bipCsApresence	Major	Presence of BIP's Current-Sense Card A	yes	Remove BIP's Current-Sense Card A Recovery: Install BIP's Current-Sense Card A

SHLF342	bipCsBpresence	Major	Presence of BIP's Current-Sense Card B	yes	Remove BIP's Current-Sense Card B Recovery: Install BIP's Current-Sense Card B
SHLF343	pAlmRelayPresent	Major	Presence of BIP's Alarm Relay Card	yes	Remove BIP's Alarm Relay Card Recovery: Install BIP's Alarm Relay Card
SHLF344	pCSAshf0HighThre	Minor	Current-Sense Card A Shelf 0 High Threshold exceeded	yes	Through Dshell reset the the threshold to value that will trigger this alarm. To do this Telnet into an active ITX card and enter the following command "/glan/dsend XX 03 01 b5 70 06 07 7a 92 YY 04 c0 ff". To clear the alarm use "/glan/dsend XX 03 01 b5 70 06 07 68 92 YY 03 c0 ff". XX = ITP slot number and YY = 3E
SHLF345	pCSAshf1HighThre	Minor	Current-Sense Card A Shelf 1 High Threshold exceeded	yes	Same as above except YY = 3F
SHLF346	pCSAshf2HighThre	Minor	Current-Sense Card A Shelf 2 High Threshold exceeded	yes	Same as above except YY = 40
SHLF347	pCSAshf3HighThre	Minor	Current-Sense Card A Shelf 3 High Threshold exceeded	yes	Same as above except YY = 41
SHLF348	pCSBshf0HighThre	Minor	Current-Sense Card B Shelf 0 High Threshold exceeded	yes	Same as above except YY = 42
SHLF349	pCSBshf1HighThre	Minor	Current-Sense Card B Shelf 1 High Threshold exceeded	yes	Same as above except YY = 43
SHLF350	pCSBshf2HighThre	Minor	Current-Sense Card B Shelf 2 High Threshold exceeded	yes	Same as above except YY = 44
SHLF351	pCSBshf3HighThre	Minor	Current-Sense Card B Shelf 3 High Threshold exceeded	yes	Same as above except YY = 45
SHLF352	bipTempHighThres	Minor	Current High Temperature Threshold exceeded	yes	Through Dshell reset the the threshold to value that will trigger this alarm. To do this Telnet into an active ITX card and enter the following command "/glan/dsend XX 03 01 b5 70 06 07 50 92 3d 04 c0 ff". XX = ITP slot number.
SHLF353	pCSAshf0LowThre	Minor	Current-Sense Card A Shelf 0 Low Threshold exceeded	yes	Through Dshell reset the the threshold to value that will trigger this alarm. To do this Telnet into an active ITX card and enter the following command "/glan/dsend XX 03 01 b5 70 06 07 5f 92 YY 02 c0 ff". To clear the alarm use "/glan/dsend XX 03 01 b5 70 06 07 58 92 YY 01 c0 ff". XX = ITP slot number and YY = 3E
SHLF354	pCSAshf1LowThre	Minor	Current-Sense Card A Shelf 1 Low Threshold exceeded	yes	Same as above except YY = 3F
SHLF355	pCSAshf2LowThre	Minor	Current-Sense Card A Shelf 2 Low Threshold exceeded	yes	Same as above except YY = 40
SHLF356	pCSAshf3LowThre	Minor	Current-Sense Card A Shelf 3 Low Threshold exceeded	yes	Same as above except YY = 41
SHLF357	pCSBshf0LowThre	Minor	Current-Sense Card B Shelf 0 Low Threshold exceeded	yes	Same as above except YY = 42
SHLF358	pCSBshf1LowThre	Minor	Current-Sense Card B Shelf 1 Low Threshold exceeded	yes	Same as above except YY = 43
SHLF359	pCSBshf2LowThre	Minor	Current-Sense Card B Shelf 2 Low Threshold exceeded	yes	Same as above except YY = 44
SHLF360	pCSBshf3LowThre	Minor	Current-Sense Card B Shelf 3 Low Threshold exceeded	yes	Same as above except YY = 45
SHLF361	bipTempLowThres	Minor	Current Low Temperature Threshold exceeded	yes	Through Dshell reset the the threshold to value that will trigger this alarm. To do this Telnet into an active ITX card and enter the following command "/glan/dsend XX 03 01 b5 70 06 07 00 92 3d 01 c0 ff". XX = ITP slot number.
SHLF362	ipSignalBatteryFus	Major	Status of the Signal Battery Fuse	yes	Pull Signal Battery Fuse at the BIP panel Recovery: Check fuse and replace if necessary
SHLF363	ipTalkBatteryAFus	Major	Status of Talk Battery A Fuse	yes	Pull Talk Battery A Fuse at the BIP panel Recovery: Check fuse and replace if necessary
SHLF364	ipTalkBatteryBFus	Major	Status of Talk Battery B Fuse	yes	Pull Talk Battery B Fuse at the BIP panel Recovery: Check fuse and replace if necessary
SHLF365	bipEcuFuse0	Minor	Status of Cooling Unit 0 Fuse	yes	Pull Cooling Unit 0 Fuse at the BIP panel Recovery: Check fuse and replace if necessary
SHLF366	bipEcuFuse1	Minor	Status of Cooling Unit 1 Fuse	yes	Pull Cooling Unit 1 Fuse at the BIP panel Recovery: Check fuse and replace if necessary
SHLF367	bipEndAisleFuse	Minor	Status of the End-Aisle Fuse	yes	Pull End-Aisle Fuse at the BIP panel Recovery: Check fuse and replace if necessary
SHLF368	bipSignalDistributi	Indeterminat	BIP Signal Distribution	yes	At the MG9000 EM enable this SDP
SHLF369	bipSignalDistributi	Indeterminat	BIP Signal Distribution	yes	At the MG9000 EM enable this SDP
SHLF370	bipSignalDistributi	Indeterminat	BIP Signal Distribution	yes	At the MG9000 EM enable this SDP
SHLF371	bipSignalDistributi	Indeterminat	BIP Signal Distribution	yes	At the MG9000 EM enable this SDP
SHLF372	bipVisualCritical	Indeterminat	BIP Visual Critical	yes	Generate any Critical Alarm on an MG9000 within the Frame Recovery: Clear all Critical Alarm on an MG9000 within the Frame
SHLF373	bipVisualMajor	Indeterminat	BIP Visual Major	yes	Generate any Major Alarm on an MG9000 within the Frame Recovery: Clear all any Major Alarm on an MG9000 within the Frame
SHLF374	bipVisualMinor	Indeterminat	BIP Visual Minor	yes	Generate any Minor Alarm on an MG9000 within the Frame Recovery: Clear all any Minor Alarm on an MG9000 within the Frame
SHLF375	bipAudibleCritical	Indeterminat	BIP Audible Critical	yes	Generate any Critical Alarm on an MG9000 within the Frame Recovery: Clear all Critical Alarm on an MG9000 within the Frame

SHLF376	bipAudibleMajor	Indeterminate	BIP Audible Major	yes	Generate any Major Alarm on an MG9000 within the Frame Recovery: Clear all any Major Alarm on an MG9000 within the Frame
SHLF377	bipAudibleMinor	Indeterminate	BIP Audible Minor	yes	Generate any Minor Alarm on an MG9000 within the Frame Recovery: Clear all any Minor Alarm on an MG9000 within the Frame
SHLF378	bipAlarmCutOffLED	Indeterminate	BIP Alarm CutOff LED	yes	Engage Alarm Cut Off button on BIP panel Recovery: Dis
SHLF379	bipTalkBatteryFailALED	Indeterminate	BIP Talk Battery A Fail LED	yes	Remove (or Offline/Lock ate EM) TB A Filter card Recovery: Re-insert (or Unlock/Online ate EM) TB A Filtercard
SHLF380	bipTalkBatteryFailBLED	Indeterminate	BIP Talk Battery B Fail LED	yes	Remove (or Offline/Lock ate EM) TB B Filter card Recovery: Re-insert (or Unlock/Online ate EM) TB B Filtercard
SHLF381	bipCriticalLEDbank	Indeterminate	BIP Critical LED Bank	yes	Generate any Critical Alarm on an MG9000 within the Frame Recovery: Clear all Critical Alarm on an MG9000 within the Frame
SHLF382	bipMajorLEDbank	Indeterminate	BIP Major LED Bank	yes	Generate any Major Alarm on an MG9000 within the Frame Recovery: Clear all any Major Alarm on an MG9000 within the Frame
SHLF383	bipMinorLEDbank	Indeterminate	BIP Minor LED Bank	yes	Generate any Minor Alarm on an MG9000 within the Frame Recovery: Clear all any Minor Alarm on an MG9000 within the Frame
SHLF384	bipEcu1LED	Indeterminate	BIP Environmental Control Unit 0 LED	yes	Remove Fan Cable Recovery: Check Fan cable, fuses, or replace fan
SHLF385	bipEcu2LED	Indeterminate	BIP Environmental Control Unit 1 LED	yes	Remove Fan Cable Recovery: Check Fan cable, fuses, or replace fan
SHLF386	bipAlarmFailLED	Indeterminate	BIP Alarm Processor Card Fail LED	yes	At EM Offline/Lock the BIP Alarm Processor Card Recovery: At EM Online/Unlock the BIP Alarm Processor Card
SHLF387	bipAisleAlarm	Indeterminate	BIP Aisle Alarm	yes	Generate any SHLF alarm Recovery: Clear all SHLF alarms
SHLF388	bipFrameFail	Indeterminate	BIP Frame Fail	yes	Generate any Frame alarm Recovery: Clear all Frame alarms
SHLF389	bipAlmRelayLed	Indeterminate	Presence of BIP's Alarm Relay Card LED	yes	Remove BIP's Alarm Relay Card Recovery: Install BIP's Alarm Relay Card
SHLF390	bipCsAled	Indeterminate	Status of Current-Sense Card A LED	yes	At EM Offline/Lock the BIP Current-Sense Card A Recovery: At EM Online/Unlock the BIP Current-Sense Card A
SHLF391	bipCsBled	Indeterminate	Status of Current-Sense Card B LED	yes	At EM Offline/Lock the BIP Current-Sense Card B Recovery: At EM Online/Unlock the BIP Current-Sense Card B
SHLF392	shelfCompatibility		This log is generated when a shelfCompatibility fault is received	yes	
	cardDiscovery		This log is generated when a cardDiscovery fault is received	yes	
	cardDiscPow/o		This log is generated when a cardDiscPow/o fault is received	yes	
	cardDiscPowSic		This log is generated when a cardDiscPowSic fault is received	yes	
	cardDiscSlot02		This log is generated when a cardDiscSlot2 fault is received	yes	
	cardDiscSlot03		This log is generated when a cardDiscSlot3 fault is received	yes	
	cardDiscSlot04		This log is generated when a cardDiscSlot4 fault is received	yes	
	cardDiscSlot05		This log is generated when a cardDiscSlot5 fault is received	yes	

SHLF393	cardDiscSlot06		This log is generated when a cardDiscSlot6 fault is received	yes	
	cardDiscSlot07		This log is generated when a cardDiscSlot7 fault is received	yes	
	cardDiscSlot08		This log is generated when a cardDiscSlot8 fault is received	yes	
	cardDiscSlot09		This log is generated when a cardDiscSlot9 fault is received	yes	
	cardDiscSlot10		This log is generated when a cardDiscSlot10 fault is received	yes	
	cardDiscSlot11		This log is generated when a cardDiscSlot11 fault is received	yes	
	cardDiscSlot12		This log is generated when a cardDiscSlot12 fault is received	yes	
	cardDiscSlot13		This log is generated when a cardDiscSlot13 fault is received	yes	
	cardDiscSlot14		This log is generated when a cardDiscSlot14 fault is received	yes	
	cardDiscSlot15		This log is generated when a cardDiscSlot15 fault is received	yes	
	cardDiscSlot16		This log is generated when a cardDiscSlot16 fault is received	yes	
	cardDiscSlot17		This log is generated when a cardDiscSlot17 fault is received	yes	
	cardDiscSlot18		This log is generated when a cardDiscSlot18 fault is received	yes	
	cardDiscSlot19		This log is generated when a cardDiscSlot19 fault is received	yes	
	cardDiscSlot20		This log is generated when a cardDiscSlot20 fault is received	yes	
	cardDiscSlot21		This log is generated when a cardDiscSlot21 fault is received	yes	
norLineFault (NORTEL-UEMG-LINE-MIB)					
SWLN301	lineFault	Minor	Line in Fault	yes	Requires bad hardware. Recovery: Perform Line Card diag and replace card if faulty.
SWLN302	lineProtectionFault	Minor	Hazardous Voltage	yes	Apply higher voltage across the loop. An alternative if to do the following: You can force a line to be in fault (HazardVoltage) via the sethazard command on the active itp. (/linemtc/circuit/setbabble). Do this on a WLC based linecard circuit. ITP [3 2 12] dSH> setbabble 2 31 Slot: 2 Circuit: 31 Recovery: Remove voltage. Perform Line Card Diag and Replace card if faulty.

SWLN303	lineBabbleState	Minor	Line in Babbling state	yes	Requires test gear to generate this alarm condition. An alternative if to do the following: You can force a line to be in fault (HazardVoltage) via the sethazard command on the active itp. (/linemtc/circuit/sethazard). Do this on a WLC based linecard circuit. ITP [3 2 12] dSH> sethazard 2 31 Slot: 2 Circuit: 31 Recovery: Perform Line Card diag and replace card if faulty.
nnDsIfFault (NORTEL-UEMG-DSL-MIB)					
XDSL301	losATUC	Minor	Loss of signal - Local modem	yes	At the DSL line card pull the cable connector Recovery: See lolATUC
XDSL302	lofATUC	Minor	Loss of frame - Local modem	yes	Utilize the UASHOST PC program to generate faults. A notebook PC is connected directly to the line card via a serial cable and RS232-TTL converter. Recovery: See lolATUC
XDSL303	lprATUC	Critical	Loss of Power - Local modem	yes	Utilize the UASHOST PC program to generate faults. A notebook PC is connected directly to the line card via a serial cable and RS232-TTL converter. Recovery: Reset and/or reseat line card. Investigate shelf/linecard power supplies.
XDSL304	lolATUC	Minor	Loss of link - Local modem	yes	At the DSL line card pull the cable connector Recovery: Generally indicates the CPE has been powered off. If customer complains, it may indicate loop impairment or faulty modem. Check subscriber connection to line card.
XDSL305	losATUR	Minor	Loss of signal - Remote modem	yes	Using an ADSL Modem test set inject this type of fault. Recovery: See lolATUC
XDSL306	lofATUR	Minor	Loss of frame - Remote modem	yes	Using an ADSL Modem test set inject this type of fault. Recovery: See lolATUC
XDSL307	lprATUR	Minor	Loss of power - Remote modem	yes	Using an ADSL Modem test set inject this type of fault. Recovery: None. This signifies a Dying Gasp from the remote modem (normal power-off condition).
XDSL308	lolATUR	Minor	Loss of link - Remote modem	yes	Using an ADSL Modem test set inject this type of fault. Recovery: See lolATUC
XDSL309	aturNotPresent	Minor	No remote modem present	yes	At the DSL line card pull the cable connector (wait a minute or two) Recovery: If persistent, changing provisioning parameters of the circuit may improve immunity to loop impairments. Replacing the remote modem or linecard may also correct the problem.
XDSL310	noClock	Critical	Local modem clock failure	yes	Using an ADSL Modem test set inject this type of fault. Recovery: same as above
XDSL311	handshakeFail	Critical	Protocol error	yes	At the ADSL Modem set it to G.lite Recovery: same as above
XDSL312	linkMismatch	Critical	Configuration error	yes	Using an ADSL Modem test set inject this type of fault. Recovery: same as above
XDSL313	vpiNonzero	Critical	ATM traffic dropped at WAC - upstream	yes	Using an ATM test set (ADTECH) inject this type of fault Recovery: If persistent, reset and/or reseat the linecard. If still not clear, replace linecard.
XDSL314	lcdlATUC	Critical	Loss of sync of ATM cells - upstream	yes	Using an ATM test set (ADTECH) inject this type of fault Recovery: If persistent, reset and/or reseat the linecard. If still not clear, replace remote modem and/or linecard.
XDSL315	lcdlATUR	Critical	Loss of sync of ATM cells - downstream	yes	Using an ATM test set (ADTECH) inject this type of fault Recovery: same as above
XDSL316	failATUC	Critical	Local modem critical failure - not responding, in Kernel mode, download failure or message corrupted	yes	Using an ADSL Modem test set inject this type of fault. Recovery: See vpiNonzero
XDSL317	circuitHardwareFault	Critical	General H/W fault indication - circuit	yes	Utilize the UASHOST PC program to generate faults. A notebook PC is connected directly to the line card via a serial cable and RS232-TTL converter. Recovery: Replace linecard.
BWSelfFault (NORTEL-UEMG-					

BW300	bwResBandwShelfFault	Warning	Reserved bandwidth used on the indicated shelf has exceeded the Bandwidth Congestion Threshold	yes	At EM (Bandwidth Management view) set this threshold to a very low value. Generate enough traffic on the shelf (including PLoA) to exceed the threshold. Recovery: Alarm is cleared when reserved bandwidth on the shelf is 10% below the Bandwidth Congestion Threshold. Increase threshold, try to decrease the number of active calls on the shelf, or take no action.
BandwidthFault (NORTEL-UEMG-					
BW301	bwResBandwTotalFault	Warning	This alarm is generated when 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.	yes	At EM (Bandwidth Management view) set this threshold to a very low value. Generate enough traffic on the MG9000 (including PLoA) to exceed the threshold. Recovery: The alarm is cleared when reserved bandwidth on the network interface is 10% less than the threshold.
BW302	bwResBandwSLoaFault	Warning	This alarm is generated when reserved bandwidth dedicated to switched lines connections on the network interface has	yes	At EM (Bandwidth Management view) set this threshold to a very low value. Generate enough SLoA traffic on the MG9000 to exceed the threshold. Recovery: The alarm is cleared when reserved Switched lines bandwidth on the network interface is 10% less than the threshold.
BW304	bwSwitchFabricTotalFault	Warning	Overall Cell Queue Congestion Alarm. Overall atm cell queue is at least 90% full.	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 "bwevents" command with the "swfabric" option. Recovery: Alarm is cleared when the overall cell queue fill is less than 80% full.
BW305	bwSwitchFabricCbrFault	Warning	CBR Cell Queue Congestion Alarm. Atm cell queue for this service type is at least 90% full.	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 "bwevents" command with the "swfabric" option. Recovery: Alarm is cleared when this service type cell queue is less than 80% full.
BW306	bwSwitchFabricRtVbrFault	Warning	RT-VBR Cell Queue Congestion Alarm. Atm cell queue for this service type is at least 90% full.	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 "bwevents" command with the "swfabric" option. Recovery: Alarm is cleared when this service type cell queue is less than 80% full.
BW307	bwSwitchFabricNrtVbrFault	Warning	NRT-VBR Cell Queue Congestion Alarm. Atm cell queue for this service type is at least 90% full.	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 "bwevents" command with the "swfabric" option. Recovery: Alarm is cleared when this service type cell queue is less than 80% full.
BW308	bwSwitchFabricUbrFault	Warning	UBR Cell Queue Congestion Alarm. Atm cell queue for this service type is at least 90% full.	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 "bwevents" command with the "swfabric" option. Recovery: Alarm is cleared when this service type cell queue is less than 80% full.
BW309	bwSwitchFabricUbrPlusFault	Warning	UBR-PLUS Cell Queue Congestion Alarm. Atm cell queue for this service type is at least 90% full.	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 "bwevents" command with the "swfabric" option. Recovery: Alarm is cleared when this service type cell queue is less than 80% full.

BW310	bwSwitchFabricControlFault	Warning	CONTROL Channel Cell Queue Congestion Alarm. Atm cell queue for this service type is at least 90% full.	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 "bwevents" command with the "swfabric" option. Recovery: Alarm is cleared when this service type cell queue is less than 80% full.
BW311	wResBandwAbiFault	Warning	This alarm is generated when 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.	yes	At EM (Bandwidth Management view) set this threshold to a very low value. Generate enough ABI traffic on MG9000 to exceed the threshold. Recovery: The alarm is cleared when reserved ABI lines bandwidth on the network interface is 10% less than the threshold.
nnClkSyncFault (NORTEL-UEMG-					
CLK301	lossOfPhaseLock	Minor	Phase PLD [altera 7064b] detected a minimum phase difference greater than eight nano seconds. (FRAME PULSES BETWEEN ITPs DO NOT MATCH)	yes	This alarm cannot be generated by a test set or manual action. These are HW or SW faults. The easist way to produce them is to use the MG9000 FITS Dshell commands. To set it ---> 1. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a092 0x0020 2. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a090 0x0020 To clear it --> 1. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a092 0x0000 2. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a090 0x0020
CLK302	lossOfFramePulseLock	Major	Frame pulse alignment did not get established with the active card -- it	yes	Pull the Mate ITP card
CLK303	lossOfMyClock	Major	The high and low levels of the SYNC PLL clock are not toggling. (OUTPUT OF FREQUENCY PLL HAS BEEN LOST)	yes	This alarm cannot be generated by a test set or manual action. These are HW or SW faults. The easist way to produce them is to use the MG9000 FITS Dshell commands. To set it ---> 1. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a092 0x0080 2. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a090 0x0080 To clear it --> 1. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a092 0x0000 2. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a090 0x0080
CLK304	lossOfMateClock	Minor	The high and Low levels	yes	Pull the Mate ITP card
CLK305	lossOfClockOutput	Major	Phase PLD reference clock oscillator not toggling. (OUTPUT OF PHASE PLL HAS BEEN LOST)	yes	This alarm cannot be generated by a test set or manual action. These are HW or SW faults. The easist way to produce them is to use the MG9000 FITS Dshell commands. To set it ---> 1. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a092 0x0100 2. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a090 0x0100 To clear it --> 1. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a092 0x0000 2. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a090 0x0100
CLK306	singleReferenceFailure	Minor	Single monitored reference source has been lost	yes	With the MG9000 using BITS but with network clocking available, pull the BITS cable

CLK307	allReferenceFailure	Major	Absolute and Delta reference source signals have been lost	yes	Remove the receive side of the active DCC cards fiber
CLK308	singleSyncUnitFailure	Major	Stratum 3 unit on ITP failed	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 Dshell FITS commands
CLK312	signalLos	Minor	Single/All source	yes	Remove both Clock sources (BITS and Network Interface)
CLK313	signalLof	Minor	Single/All source(s) reference occurred due to out of frame	yes	?
norNodeFault (NORTEL-UEMG-NODE-					
	FlashRsrc	Major	Flash Memory	yes	GW software may not detect all alarm conditions listed. However, GW provides capability to generate these alarms using the debug commands in DSHELL. In DSHELL enter the following commands: > cd /nmtc/resources > injectfault When this command is entered, values for additional parameters are listed. Recovery: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	ProcessorRsrc	Major	Processor	yes	GW software may not detect all alarm conditions listed. However, GW provides capability to generate these alarms using the debug commands in DSHELL. In DSHELL enter the following commands: > cd /nmtc/resources > injectfault When this command is entered, values for additional parameters are listed. Recovery: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	idpromRsrc	Major	idprom	yes	Same as Processor fault Recovery: same as above
	Atm50PortRsrc	Minor	ATM200 Port [0-19]: Not	yes	Same as Processor fault
	RamRsrc	Major	RAM	yes	Same as Processor fault Recovery: same as above
	CardTypeMismatchRsrc	Critical	Incorrect Card In Slot	yes	Same as Processor fault Recovery: same as above
	RedundancyLostRsrc	Warning	Simplex Mode - No Redundancy	yes	Same as Processor fault Recovery: same as above
	CardPairOOSRsrc	Warning	Active/Master Card Out Of Service	yes	Same as Processor fault Recovery: same as above
	CardRsrc	Major	DS1 Card	yes	Same as Processor fault Recovery: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	DS1Aal1SarRsrc	Major	AAL1 SAR - DS1 Card TDM to ATM converter	yes	Same as Processor fault Recovery: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	DS1LinkRsrc	Minor	DS1 Link [0 to 15]	yes	Same as Processor fault Recovery: same as above
	DS1FramerRsrc	Major	DS1 Framer for DS1 links [0-7, or 8-15]	yes	Same as Processor fault Recovery: same as above
	DS1LIURsrc	Major	DS1 Line IF Unit for DS1 links [0-7, or 8-15]	yes	Same as Processor fault Recovery: same as above
	CardRsrc	Major	ITP card	yes	Same as Processor fault Recovery: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	ITPTimeswitchRsrc	Major	Timeswitch - call processing engine	yes	Same as Processor fault Recovery: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.

NE301	DspServiceCircuits	Major	DSP [0-3]	yes	Same as Processor fault Recovery: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	EchoCancellationF	Minor	ECAN	yes	Same as Processor fault Recovery: same as above
	ITPAal1SarRsrc	Major	AAL1 SAR - Call Traffic TDM to ATM converter	yes	Same as Processor fault Recovery: same as above
	AtmBusControllerF	Major	Serial Link Control - controls communication with ITX cards	yes	Same as Processor fault Recovery: 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.
	ITPDdcIdpromRsrc	Minor	DDC Idprom - DSP Daughter Card Idprom	yes	Same as Processor fault Recovery: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	ITPDdcCalistoRsrc	Major	DDC Calisto - DSP Daughter Card Calisto	yes	Same as Processor fault Recovery: same as above
	ITPVoicePathRsrc	Critical	Voice Path	yes	Same as Processor fault Recovery: same as above
	CardRsrc	Major	ITX Card	yes	Same as Processor fault Recovery: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	CardRsrc	Major	SCO/SCI card	yes	Same as Processor fault Recovery: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	SCTerminalIfRsrc	Warning	RS-232 Port	yes	Same as Processor fault Recovery: same as above
	CBootFlashMemRs	Warning	Flash Memory containing software load	yes	Same as Processor fault Recovery: same as above
	CLocalBusRamRs	Major	Local Memory	yes	Same as Processor fault Recovery: same as above
	SCEthernetIfRsrc	Warning	Ethernet port	yes	Same as Processor fault Recovery: same as above
	SCSWRsrc	Minor	ATM Switch - MMC Chipset	yes	Same as Processor fault Recovery: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	SCNetworkIfRsrc	Major	Network Interface (SCO) [0-7] (SCI)	yes	Same as Processor fault Recovery: same as above
	SCAtmFwdRsrc	Critical	ATM Cell Forwarder	yes	Same as Processor fault Recovery: same as above
	CardRsrc	Major	ABI card	yes	Same as Processor fault Recovery: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	TimeswitchNetSide	Major	Timeswitch - call p engine (network side)	yes	Same as Processor fault Recovery: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	TimeswitchLineSide	Major	Timeswitch - call p engine (Line side)	yes	Same as Processor fault Recovery: same as above
	ABITimeswitchRsrc	Major	Timeswitch - call processing engine	yes	Same as Processor fault Recovery: same as above
	EchoCancellationF	minor	ECAN - unit 0 ECAN - unit 1	yes	Same as Processor fault Recovery: same as above
	ABIAal1SarRsrc	Major	AAL1 SAR - Call Traffic TDM to ATM converter	yes	Same as Processor fault Recovery: same as above
	ABIAal1NetSideRsrc	Major	Aal1 Network side - unit 0 Aal1 Network side - unit 1	yes	Same as Processor fault Recovery: same as above
	ABIAal1LineSideRsrc	Major	Aal1 Line side - unit 0 Aal1 Line side - unit 1	yes	Same as Processor fault Recovery: same as above

	AtmBusControllerF	Major	Serial Link Control - controls communication with ITX cards	yes	Same as Processor fault Recovery: 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.
	ABIVoicePathRsrc	Critical	Voice Path	yes	Same as Processor fault Recovery: same as above
	CardRsrc	Major	8X8 ADSL Card	yes	Same as Processor fault Recovery: Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
NE302	AtmDataSyncRsrc	Critical	ATM Data Sync	yes	Same as Processor fault Recovery: 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.
	BalDataSyncRsrc	Critical	BAL Data Sync	yes	Same as Processor fault Recovery: same as above
	MegacoDataSyncRsrc	Critical	Megaco Data Sync	yes	Same as Processor fault Recovery: same as above
	BaseSubsystemRsrc	Critical	Startup failure: Base Platform	yes	Same as Processor fault Recovery: same as above
	CarrierSubsystemRsrc	Critical	Startup failure: Carrier Maintenance	yes	Same as Processor fault Recovery: same as above
	NodeSubsystemRsrc	Critical	Startup failure: Node Maintenance	yes	Same as Processor fault Recovery: same as above
	MegacoSubsystemRsrc	Critical	Startup failure: Megaco	yes	Same as Processor fault Recovery: same as above
	DLMSSubsystemRsrc	Critical	Startup failure: Data Line Maintenance	yes	Same as Processor fault Recovery: same as above
	TestSubsystemRsrc	Critical	Startup failure: Test Mib	yes	Same as Processor fault Recovery: same as above
	MTASubsystemRsrc	Critical	Startup failure: MTA Mib	yes	Same as Processor fault Recovery: same as above
	ShfSubsystemRsrc	Critical	Startup failure: Shelf Maintenance	yes	Same as Processor fault Recovery: same as above
	LineSubsystemRsrc	Critical	Startup failure: Line Maintenance	yes	Same as Processor fault Recovery: same as above
	ClockSyncSubsystemRsrc	Critical	Startup failure: Clock Sync Mib	yes	Same as Processor fault Recovery: same as above
	PatchingSubsystemRsrc	Critical	Startup failure: Patching	yes	Same as Processor fault Recovery: same as above
	DTASubsystemRsrc	Critical	Startup failure: DTA	yes	Same as Processor fault Recovery: same as above
	MegacoOMSSubsystemRsrc	Critical	Startup failure: Megaco OMs	yes	Same as Processor fault Recovery: same as above
	SoftwareUpgradeSubsystemRsrc	Critical	Startup failure: Software Upgrade	yes	Same as Processor fault Recovery: same as above
	SNMPMasterAgentSubsystemRsrc	Critical	Startup failure: SNMP Master Agent	yes	Same as Processor fault Recovery: same as above
	TimeOfDaySubsystemRsrc	Critical	Startup failure: Time of Day	yes	Same as Processor fault Recovery: same as above
	ESASubsystemRsrc	Critical	Startup failure: ESA	yes	Same as Processor fault Recovery: same as above
	LinkMaintenanceSubsystemRsrc	Critical	Startup failure: Link Maintenance	yes	Same as Processor fault Recovery: same as above
	MarketFitSubsystemRsrc	Critical	Startup failure: Market Fit	yes	Same as Processor fault Recovery: same as above
	TestRsrc	variable	Test Resource	yes	Same as Processor fault Recovery: same as above
	HeapRsrc	Critical/Major	Low Memory	yes	Same as Processor fault Recovery: same as above
	MateCardCommunicationFailureRsrc	Critical	Mate Card Communication Failure	yes	Same as Processor fault Recovery: same as above
	CPCSUNI signallingRsrc	Major	CPCS UNI Signalling	yes	Same as Processor fault Recovery: same as above

	TPWBCallConnRsrc	Major	Call Control Connection	yes	Same as Processor fault Recovery: 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.
	NEDataSyncRsrc	Critical	NE Data Sync	yes	Same as Processor fault Recovery: 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.
	BIWBCallConnRsrc	Major	Call Control Connection	yes	Same as Processor fault Recovery: 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.
NE303	Crit/Maj/Minor		Card Restored (SWACT and now inactive)		
	S1NetworkLinkRsrc	Minor	Link to DCC Card in slot [10 or 11] - Isolation In Progress	yes	Same as Processor fault Recovery: This alarm means two cards cannot communicate with each other. The diagnostics will determine (isolate) where the fault is and this alarm will change into an NE305 within 3 minutes.
	LineSideExternalR	Minor	Line Card 0, or link to Line Card	yes	Same as Processor fault Recovery: same as above
	TPNetworkLinkRsrc	Minor	Link to ITX, port [0 to 1] - Isolation in progress Link to Mate ITP	yes	Same as Processor fault Recovery: same as above
	ITXLinkRsrc	Minor	Link to DCC in slot [10 or 11] - Isolation in progress Link 4 to ITP card - Isolation in progress Link 5 to ITP card - Isolation in progress Link 6 to ITP card - Isolation in progress Link 7 to ITP card - Isolation in progress Link 8 to ITP card - Isolation in progress Link 9 to ITP card - Isolation in progress Link 10 to ITP card - Isolation in progress Link 11 to ITP card -	yes	Pull cable on ITP card (to ITX card) Recovery: same as above

NE304	SCLineLinkRsrc	Minor	Link to Master Shf ITP 13 - Isolation in progress Link to Master Shf ITP 12 - Isolation in progress Link to Mate DCC - Isolation in progress Link to card in slot 2 - Isolation in progress Link to card in slot 6 - Isolation in progress Link to card in slot 14 - Isolation in progress Link to card in slot 18 - Isolation in progress Link to card in slot 3 - Isolation in progress Link to card in slot 7 - Isolation in progress Link to card in slot 15 - Isolation in progress Link to card in slot 19 - Isolation in progress Link to card in slot 4 - Isolation in progress Link to card in slot 8 - Isolation in progress Link to card in slot 16 - Isolation in progress Link to card in slot 20 - Isolation in progress Link to card in slot 5 - Isolation in progress Link to card in slot 9 - Isolation in progress	yes	Pull an ITX card Recovery: same as above
	ABINetworkLinkRsrc	minor	Link to DCC Card in slot 10 - Isolation in progress Link to DCC Card in slot	yes	Same as Processor fault Recovery: same as above
	Aal5SarRsrc	Major	AAL5-SAR, Messaging	yes	Same as Processor fault Recovery: 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.
	1NetworkExternalF	minor	EXTERNAL: DCC Slot 10 EXTERNAL: DCC Slot 11	yes	Same as Processor fault Recovery: 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 DS1 and DCC. Reseat DS1 card, see if problem clears. Reseat DCC card, see if problem clears.
	S1NetworkPortRsrc	Minor	Serial Device 0 - to DCC Card in slot 10 Serial Device 1 - to DCC Card in slot	yes	Same as Processor fault Recovery: 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.
	S1UtopiaBridgeRsrc	Major	Utopia Bus Master - AAL1, AAL5 to ATM PHYs	yes	Same as Processor fault Recovery: same as above
	PNetworkExternalR	Minor	EXTERNAL: Mate ITP EXTERNAL: ITX attached to port [0,1]	yes	Same as Processor fault Recovery: Check the ITX to see if it has alarms. If so, handle them first. If no alarms on ITX, or only EXTERNAL alarms on the ITX, replace the cable between ITX and ITP.
	TPNetworkPortRsrc	Minor	Serial Device [0 to 1] - to ITX cards HDLC Device - Connects to mate ITP	yes	Same as Processor fault Recovery: 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.
	ITPLineSidelfRsrc	Major	Serial device 0 - to Line Card	yes	Same as Processor fault Recovery: 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.
	PDDCAAL5SARRsrc	Major	DDC AAL5 SAR - Call		

NE305	ITXExternalRsrc	Minor	EXTERNAL: DCC Slot 10 serial device EXTERNAL: DCC Slot 11 serial device EXTERNAL: ITP attached to port [0-7]	yes	Same as Processor fault Recovery: 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 ITX, replace the cable between ITX and ITP. If the alarm is to a DCC card, fix any DCC alarms first. Reseat ITX card, see if problem clears. Reseat DCC card, see if problem clears.
	ITXPortRsrc	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	yes	Same as Processor fault Recovery: same as above
	TXLineSideGrpRsrc	Major	Link [0 to 7] to ITP pair	yes	Same as Processor fault Recovery: same as above
	TXNetForwarderRsrc	Major	Net side cell forwarder	yes	Same as Processor fault Recovery: 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.
	TXLineForwarderRsrc	Major	Line side cell forwarder	yes	Same as Processor fault Recovery: 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.
	SCLineExternalRsrc	Minor	EXTERNAL: Master Shelf ITP slot 13 EXTERNAL: Master Shelf ITP slot 12 EXTERNAL: Mate DCC EXTERNAL: Card in slot [2-9, 14-21]	yes	Same as Processor fault Recovery: 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. Reseat other card in question, see if problem clears. Reseat DCC card, see if problem clears.

	SCLinePortRsrc	Minor	Serial Device 0 - to Master Shelf ITP Slot 13 Serial Device 1 - to Master Shelf ITP Slot 12 Serial Device 3 - Link to Mate 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 19 Serial Device 12 - 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	yes	Same as Processor fault Recovery: 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.
	QuadSerContGrpR	Major	Group of Serial Ports	yes	Same as Processor fault Recovery: same as above
	INetworkExternalR	Minor	EXTERNAL: DCC slot [10 or 11]	yes	Same as Processor fault Recovery: 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 ABI and DCC. Reseat ABI card, see if problem clears. Reseat DCC card, see if problem clears.
	ABINetworkPortRsrc	minor	Serial Device 0 - to DCC Card in slot 10 Serial Device 1 - to DCC Card in slot 11	yes	Same as Processor fault Recovery: 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.
	INetworkSideGrpR	Critical	Both links to DCC Card	yes	Same as Processor fault Recovery: same as above
NE306	GlanRsrc	minor	GLAN Link to hub on Active ITP card	yes	Same as Processor fault Recovery: The GLAN hub is located on the active ITP in the shelf where the fault appears. First try swacting ITPs and re-run diags on the afflicted card. If that fixes the problem, replace the newly inactive ITP, otherwise treat the fault as a card fault.
	ITPGlanHubRsrc	Critical	GLAN Hub, communicates with other cards on shelf	yes	Same as Processor fault Recovery: The GLAN hub is located on the active ITP in the shelf where the fault appears. First try swacting ITPs and re-run diags on the afflicted card. If that fixes the problem, replace the newly inactive ITP, otherwise treat the fault as a card fault.
NE307	ABILineSidelfRsrc	Major	DS512 port	yes	Same as Processor fault Recovery: - Verify UEMG is in service - Verify this ABI card is unlocked - Verify this ABI card is not disabled, if so, solve other issues causing this card to be disabled. - Check DS512 fibers. (light check, clean fibers, verify fibers are present)
	ILineSideExternalR	minor	XPM unit, or DS512 connection	yes	Same as Processor fault Recovery: same as above

	ABILkmAllChnlsRsrc	Major	All DS512 channels closed	yes	Pull cable to XPM Recovery: - Verify UEMG is in service - Verify this ABI card is unlocked - Verify this ABI card is not disabled, if so, solve other issues causing this card to be disabled. - Check DS512 fibers. (light check, clean fibers, verify fibers are present)
NE308	OWanBlDrOAMPResrc	Major	Inband Messaging OAMP Link [0,1]	yes	Same as Processor fault Recovery: - Check for alarms on shelf controller - Use LCI to verify that AESA provisioning information is correct. - if the problem persists, call your next level of support.
	SCWanBlDrCCResrc	Major	Inband Messaging CC Link [0,1]	yes	Same as Processor fault Recovery: same as above
	SCWanBlDrHBRsrc	Major	Heartbeat to Element Manager	yes	Same as Processor fault Recovery: same as above
	OWanBlDrDS512Resrc	Major	Inband Messaging DS512 Link [0,1]	yes	Same as Processor fault Recovery: same as above
NE309	ITPClockSyncRsrc	Critical	Clock Sync	yes	Same as Processor fault Recovery: - 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.
	PClockPhaseLockRsrc	Major	Clock Sync: Loss of Phase Lock	yes	Same as Processor fault Recovery: same as Clock Sync above
	ClockFramePulseRsrc	Major	Clock Sync: Loss of Frame Pulse Lock	yes	Same as Processor fault Recovery: same as Clock Sync above
	PClockMyClockRsrc	Major	Clock Sync: Loss of My Clock	yes	Same as Processor fault Recovery: same as Clock Sync above
	PClockMateClockRsrc	Minor	Clock Sync: Loss of Mate Clock	yes	Same as Processor fault Recovery: same as Clock Sync above
	ITPClockOutputRsrc	Major	Clock Sync: Loss of Clock Output	yes	Same as Processor fault Recovery: same as Clock Sync above
	PSyncSingleRefRsrc	Minor	Clock Sync: Single Reference Failure	yes	Same as Processor fault Recovery: same as Clock Sync above
	ITPSyncAllRefRsrc	Major	Clock Sync: All Reference Failure	yes	Same as Processor fault Recovery: same as Clock Sync above
	PSyncSingleSyncRsrc	Major	Clock Sync: Single Sync Unit Failure	yes	Same as Processor fault Recovery: same as Clock Sync above
	ITPSyncLOSRsrc	Minor	Clock Sync: Loss of Signal	yes	Same as Processor fault Recovery: same as Clock Sync above
	ITPSyncOOFRsrc	Minor	Clock Sync: Out of Frame	yes	Same as Processor fault Recovery: same as Clock Sync above
	ITPClockRsrc	variable	Clock Sync: Clock	yes	Same as Processor fault Recovery: same as Clock Sync above
	ITPSyncRsrc	variable	Clock Sync: Sync	yes	Same as Processor fault Recovery: same as Clock Sync above
	ITPSyncHORsrc	Minor	Clock Sync: Holdover Mode	yes	Same as Processor fault Recovery: same as Clock Sync above
	SCBitsFwdRsrc	Major	BITS Forwarder	yes	Same as Processor fault Recovery: same as Clock Sync above
	SCBitsRefRsrc	Minor	BITS clock reference [A or B]	yes	Same as Processor fault Recovery: same as Clock Sync above

	ITXFramerRsrc	Major	Framer - timing synchronization device	yes	Same as Processor fault Recovery: - 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.
	ITXBITSrefRsrc	Minor	BITS clock reference A		
	ITXBITSrefRsrc	Minor	BITS clock reference B		
NE310	NetworkSideifPortF	Minor	Port 2 on serial device -		
	QuadsercontPortR	Minor	Serial Port 1 - UNUSED link to ITP slot 12		
	QuadsercontPortR	Minor	Serial Port 0 - UNUSED link to ITP slot 13		
	SCSerLinkRsrc	Minor	Unused [was serial link #]	yes	Same as Processor fault Recovery: N/A
	COctalPhyContRsrc	Warning	Octal PHY [Unused] Device for ports [0-5] or [8-13]	yes	Same as Processor fault Recovery: No action required.
	OctalPhyContPortF	Warning	Octal PHY [Unused] Port [0-13]	yes	Same as Processor fault Recovery: No action required.
NE311	SCTimeOfDayRsrc	minor	Time of Day: Access to time server [ip] failed	yes	Same as Processor fault Recovery: 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 LCI to re-submit the Time of day parameters, this forces immediate time server access.
NE312	ITPCableRsrc	minor	Cable configuration conflict	yes	Same as Processor fault Recovery: One of the cables to the ITXs has been connected in an unsupported way. Check to see if the cable on the two ITXes match, and that the ITP ends of the cable are in the right ports.
	ITXCableRsrc	Minor	Cable configuration conflict, port [0 to 7]	yes	Same as Processor fault Recovery: One of the cables to the ITPs has been connected in an unsupported way. Check to see if the cable on this ITX matches the mate ITX, and that the ITP ends of the cable are in the right ports
NE313	BIActivityCableRsrc	minor	Activity control cable between ABI cards	yes	Pull activity cable between ABI card pair Recovery: The activity control cable is a small cable on the front of the ABI cards that is used for activity determination. - Verify the cable is attached to both cards. - Replace cable. - If the fault persists, replace the inactive card. - If the problem still persists, swact, replace newly inactive card

NE314	SCXcRsrc	Minor	Backplane Cross Connect	yes	Same as Processor fault Recovery: The carriers between the two DCC cards cannot communicate. - Verify and fix any CARRIER alarms - If seen on Active DCC 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, swact DCC cards. This will cause carriers to go down momentarily. Be sure to call next level to verify it is permissible to swact. 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.
NE315	SCLinksRsrc	Major	Resource Bandwidth	yes	Same as Processor fault Recovery: Some of the carriers are not providing bandwidth. - Verify and fix any CARRIER alarms. - If problem persists, restart the card.
NE316	downstreamFIFO	Major	ADSL: Downstream FIFO	yes	Recovery: Throttle back the downstream data from the SCO
	downstreamHEC	Major	ADSL: Downstream HEC error	yes	
	atm50Fault	Critical	ADSL: ATM50 fault	yes	Recovery: Restart linecard
	stream buffer overf	Critical	ADSL: Upstream buffer overflow	yes	Recovery: Throttle back the upstream data rate on the linecard
	nstream buffer ove	Critical	ADSL: Downstream buffer overflow	yes	Recovery: Throttle back the downstream data to the linecard
	atm device timeout	Critical	ADSL: ATM Device timeout	yes	Recovery: Reset linecard
	clock accuracy	Critical	ADSL: Loss of clock accuracy	yes	Recovery: Reset linecard
	dsp lockup	Critical	ADSL: DSP Lockup	yes	Recovery: Reload DSPs
NE317		Crit/Maj/Minor	Shelf SIC Card Alarm		
		Crit/Maj/Minor	Shelf PIO Card Alarm		
		Crit/Maj/Minor	Shelf BIP card Alarm		
NE318		Major	SCI Card NE Proxy		
NE320	AudRecoveryRsrc	Major	quire Audit Recovery Exec	yes	Clear Flash on an ITP pair, Pull both cards and replace Recovery: No action required.
SCC2 Log Output Example: **59 NE 318 1513 TBL MG9K NorNodeFault Location: 1-RM9K-Frame000.Shelf2.Slot12 Notification Id: 850 State: not acknowledged Category: Equipment Alarm Cause: Equipment Malfunction Time: Apr 24 14:59:40 2003 Component Id: Card.frame0.shelf2.slot12.ITP Specific Problem: Node Fault - Proxy fault Description: Card communication failure - Proxy mode activated Site Flr RPos Bay_id FFFF FF FFF FFFF FFF				NTSTD Log Output Example: MSH10_i06BE ** NE318 APR24 14:59:40 1513 TBL MG9K NorNodeFault Location: 1-RM9K-Frame000.Shelf2.Slot12 Notification Id: 850 State: not acknowledged Category: Equipment Alarm Cause: Equipment Malfunction Time: Apr 24 14:59:40 2003 Component Id: Card.frame0.shelf2.slot12.ITP Specific Problem: Node Fault - Proxy fault Description: Card communication failure - Proxy mode activated Site Flr RPos Bay_id FFFF FF FFF FFFF FFF	

MG9000 Manager Reported Faults					
MGEM300	EmDbUnavailable	Major	Generated when MG9000 EM is not able to make connection to the Element Manager Database	Yes	1. Make sure that persistence is turned on. 2. Make the database unavailable. 3. Perform some action (add/delete/change) on a VMG or termination. 4. Check the alarm browser for the alarm being SET. Recovery: 1. Re-establish the database connection. 2. Perform some action (add/delete/change) on a VMG or termination. 3. Check the alarm browser for the alarm being CLEARED.
MGEM301	CommsLostToNE	Critical	Generated when the MG9000 EM loses SNMP communication with MG9000	Yes	Break connection between the GW and the MG9K EM server. This can be done by taking the GWs OC3 OOS at the PP15000, or disabling the Ethernet connect to the MG9K EM Server (disconnect the cable). Recovery: 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 OC3 CIPOA port to validate IP connectivity. 3. Check connectivity between EM and MG. 4. Check for status of the OC3 card and Node Maintenance task
MGEM302	InvalidEMIPAddress	Major	Generated when the MG9000 Manager has added an new MG9000 and tries to discover the NE. It will check the	Yes	At the MG9000 LCI set the IP address of the MG9000 Manager to an incorrect value. At the MG9000 Manager do a manual discovery of that MG9000. Recovery: At the MG9000 LCI check the IP address of the MG9000 Manager and correct if necessary.
MGEM303	AlarmsBeingThrottled	Critical	MG9000 sends too many alarms within a 5 second window. When this happens the MG9000 Manager will request this particular MG9000 stop	yes	At the MG9000 using DSHELL use the alarm generation utility and generate at least 15 alarms a second for at least 10 seconds. Recovery: At the MG9000 LCI check the IP address of the MG9000 Manager and correct if necessary.
MGEM304	MG9K AlarmAuditFailed	Critical	Alarm Audit Failed - The alarm audit on the GW failed	yes	
SCC2 Log Output Example: *C57 MGEM301 9232 TBL MG9K CommsLostToNE Location: 2-HS9K Notification Id: 817 State: not acknowledged Category: Communication Alarm Cause: Communications Subsystem Failure Time: Apr 24 10:57:05 2003 Component Id: MG9k EM Comm Network Specific Problem: Comm Channel Down - Communication Lost to the NE Description: Loss of Heartbeat to NE Site Flr RPos Bay_id FFFF FF FFF FFFF FFF				NTSTD Log Output Example: MSH10_i06BE *** MGEM301 APR24 10:57:05 9232 TBL MG9K CommsLostToNE Location: 2-HS9K Notification Id: 817 State: not acknowledged Category: Communication Alarm Cause: Communications Subsystem Failure Time: Apr 24 10:57:05 2003 Component Id: MG9k EM Comm Network Specific Problem: Comm Channel Down - Communication Lost to the NE Description: Loss of Heartbeat to NE Site Flr RPos Bay_id FFFF FF FFF FFFF FFF	
(MEDIA_GATEWAY_MIB)					
MGC300	medGwyInvalidControllerAddress		Indicates that a message was received from a controller that did not	no	N/A
MGC301	medGwyInvalidTerminationId		Indicates a mismatch of Termination ID	no	N/A
MGC302	medGwyInvalidPackageElement		Indicates that a message was received from a controller that contained an event signal or	no	N/A
nMtaFault (NORTEL_MG_MTA_mib)					
TEST302	icSysHardwareFault			no	N/A
TEST303	taSysHardwareFault			no	N/A

TEST 304		sysConfigAmbiguity		no	N/A
nnEsaFault (NORTEL-UEMG-ESA-MIB)					
ESA300	esaStatusChange	Critical	Communication between GWC and GW is lost. Entered ESA mode	yes	Break connection between the GW and the GWC when ESA is enabled. This can be done by taking the GWs OC3 OOS at the PP15000, or disabling the Ethernet connect to the GWC (disconnect the cable). Recovery: Using the Traceroute or Ping MG9000 Manager tool test the network communications path between the EM the the MG9K, and the EM and the GWC. Check OC3 connection at the MG900, PP15000, and the SAM21 Shelf Controller, Check the Ethernet connection at the GWC, PP8600, and SAM21 Shelf Controller, Check the state of the DCC cards at the MG9000. Correct any problems found
ESA301	esaDataFileFailure	Critical	Data download of ESA data from the CS2K Core has failed	yes	
ESA303	esaEnterFailure	Critical	Failed to enter ESA	yes	
nnEsaColFault (NORTEL-UEMG-ESA-					
ESA304	esaCommOfInterest	Major	This log is generated by the EM in response to a trap from the MG9000 (nnEsaColFault). The MG9000 sends this trap when it detects communication problems to other nodes in the same community of interest.	yes	
MG9000 Manager Reported Faults					
ESA302		Critical	Failed to set up FTP connection: login failure - EM failed to push ESA to VMG	yes	
ESA311		Minor	Core Download Failed - This log is generated by the EM in when a problem is detected when trying to download the datafile from the core	yes	
ESA312		Major	This log is generated by the EM when a failure occurs whilst trying to provision internodal community of interest data for a given NE.	yes	
nnMegacoFault (NORTEL-UEMG-					
VMG300	VMG OOS	Critical	Generated when Root Termination goes out of service (Communication between Gateway and GWC is lost and ESA is not enabled)	yes	Break connection between the GW and the GWC when ESA is disabled. This can be done by taking the GWs OC3 OOS at the PP15000, or disabling the Ethernet connect to the GWC (disconnect the cable). Recovery: Using the Traceroute or Ping MG9000 Manager tool test the network communications path between the EM the the MG9K. Check OC3 connection at the MG900, Check the state of the DCC cards at the MG9000. Correct any problems found.
SCC2 Log Output Example:				NTSTD Log Output Example:	
nnMegacoQosFault (NORTEL-UEMG-					

VMG301	BadCalls	Minor	QoS Alarm that is generated when the number of bad call reaches a certain threshold	SLoIP only	In the MG9000 EM set the QoS thresholds to a low level. Using a "Packet Storm" or "Shunra" test set, inject errors on the OC3/STM1 network interface on a particular active calls SVC. Recovery: 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.
VMG302	PacketLoss	Minor	QoS Alarm that is generated when the number of Packet Loss reaches a certain threshold	SLoIP only	Same as above
VMG303	Jitter	Minor	QoS Alarm that is generated when IP message Jitter reaches a certain threshold	SLoIP only	Same as above
VMG304	Latency	Minor	QoS Alarm that is generated when IP message Latency reaches a certain threshold	SLoIP only	Same as above
nnMegacoFault (NORTEL-UEMG-					
VMG311	megacoTaskInput	Major	Application layer framing (ALF) alarm occurs when the MG 9000 is experiencing Megaco		Recovery: Verify the MG 9000 is in service from the GWC perspective. Check the network connection between the GWC and the MG 9000.
VMG312	megacoALF	Major	Megaco task alarm indicates one or more of the Megaco Task's input buffers are over 90 % full for a period of 5 minutes or more.		Recovery: Check the following based on the inputsource: • line card - indicates the MG 9000 has a babbling line card. All line cards should be checked. • DSP - indicates the MG 9000 has a babbling DSP. If the alarm is not raised on the inactive ITP card, perform a SWACT of the ITP card. • GWC - indicates the GWC is flooding the MG 9000 with messages. Check the GWC for faults. • datasync - indicates the active ITP card is flooding the inactive ITP card with messages.
VMG313	megacoDspRes			Yes	
VMG322	vmgAdminStatusOutOfService	Critical	Admin State Out Of Service - Call Processing	Yes	
VMG323	cardInitializing	Critical	VMG Initializing - Call Processing Out of	Yes	
VMG324	cardLocked	Critical	Card Locked - Call Processing Out of	Yes	
VMG325	cardDisabled	Critical	Card Disabled - Call Processing Out of	Yes	
VMG328	lineMtcNotReady	Critical	Line Maintenance Not Ready - Call Processing	Yes	
VMG329	megacoMtcNotReady	Critical	Megaco Maintenance Not Ready - Call Processing	Yes	
VMG373	gwcUnreachable	Critical	GWC Unreachable - Call Processing Out of	Yes	
VMG374	noGwcReply	Critical	GWC Reachable But No Reply To Service Change	Yes	
VMG376	aalBearerSubsysNotReady	Critical	AAL1 Bearer Not Ready - Call Processing Out of	Yes	
VMG377	ipBearerSubsysNotReady	Critical	IP Bearer Not Ready - Call Processing Out of	Yes	
Performance (NORTEL-UEMG-PERFMON-					

OVLD304	Performance Degraded	Minor/Major	Overload Detection Alarm that is generated whenever the MG9000 actually enters an overload condition.	Yes	
SCTP (NORTEL-UEMG-REMSGING-					
OVLD808	relMsgLinkFail	Critical	An external messaging link has closed and cannot send/receive	Yes	
OVLD809	MsgLinkSevDegrade	Major	Message loss is high enough such that the message link is in a degraded service state.	Yes	
OVLD810	relMsgLinkDegrade	Minor	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.	Yes	
GIGE (NORTEL-UEMG-GIGE-MIB)					
GIGE301	LOS	Critical	Loss of Signal	Yes	
GIGE302	RFI	Critical	Remote Failure Indication	Yes	
GIGE303	TxF	Critical	Transmit Failure	Yes	
GIGE304	TEM	Critical	threshold exceeded	Yes	
GIGE305	POW	Critical	Low Power Indicated	Yes	
GIGE306	RxSD	Critical	Transmit Signal	Yes	
GIGE307	RxEER	Critical	Transmit Excessive Error	Yes	
GIGE308	TBC	Critical	Transmit Bias Current	Yes	
GIGE309	LINT	Critical	Link Initialization	Yes	
GIGE310	OPT	Critical	Transmit Optical Power	Yes	
GIGE311	OPR	Critical	Receive Optical Power	Yes	
GIGE312	GARP	Critical	GARP failure	Yes	
GIGE313	LKINT	Critical	Link Integrity Failure	Yes	
GIGE314	Auto negotiation	Critical	Auto negotiation Failure	Yes	
GIGE315	non preferred link	Critical	Non Preferred Link is	Yes	
GIGE316	Link Invalid Status	Critical	Link Invalid Status	Yes	
GIGE317	No Protection Group	Critical	No Protection Group	Yes	
OMC300		Critical	Indicates that OM Collector failed to collect OM file from MG9K during a particular collection interval.	Yes	
IPSec (NORTEL-UEMG-IPSEC-MIB)					
IPSC300	ipsecMismatchSharedKey	Critical	During negotiation, the key received did not match the one locally set	Yes	
IPSC301	ipsecIkePeerLink	Critical	Phase 1 security	Yes	
IPSC302	ipsecSecurePeer	Critical	Phase 2 security	Yes	
IPSC303	ipsecDoSCallp	Critical	Packets are being replayed to the call	Yes	
IPSC304	ipsecDoSMgmt	Critical	Packets are being replayed to the call	Yes	
IPSC305	ipsecMaxDiscardedPktRate	Minor	An inordinate percentage of the received/transmitted packets are being	Yes	
IPSC306	ipsecRadiusTime	Major	MG9K's requests sent to	Yes	
IPSC307	nnIpsecCertifFault	Major	EXPIRED_LOCAL_CER	Yes	

IPSC308	nnlpsecCertifFault	Major	CERTIF_EXPIRES_IN_4	Yes	
IPSC309	nnlpsecCertifFault	Major	INVALID_FROM_DATE	Yes	
IPSC310	nnlpsecCertifFault	Major	NO_CERTIF_INSTALL	Yes	
IPSC311	nnlpsecCertifFault	Major	REMOTE_CERTIF_VERI	Yes	
IPSC312	nnlpsecCertifFault	Major	MISSING_SUBJ_ALT_N	Yes	
IPSC313	nnlpsecCertifFault	Major	Certificate Processing	Yes	
IPSC314	PKI Certificate Download Fault	Major	PKI Certificate failed to Download	Yes	

REX-related logs

REX600	REX log notification	Info	Indicates the start or completion of REX on a card/card-pair. The cards under consideration are ITP, ITX and DCC.		
REX601	REX log notification	Info	Indicates the success or failure of REX on a card/card-pair. The cards under consideration are ITP, ITX and DCC.		
REX602	REX log notification	Info	Indicates that the REX for the card/card-pair under consideration has been skipped. The card types considered are ITP, ITX and DCC		

Appendix F: CICM Logs and Alarms

The following table is the list of events that can be generated by the SAM21 blade-based CICM product in SN09. Some notes on the table's contents at the time of writing:

- All logs with a CICM Log Output Path of "Alarm_Trail_to_IEMS" or "/var/log/customerlog" are visible to a fault OSS at the IEMS northbound log interface. "Alarm_Trail_to_IEMS" logs are reporting the raising and clearing of alarms and are part of a set/clear pair of logs. (See exception below.) "/var/log/customerlog" logs are autonomous INFO logs with no severity and are not part of a set/clear pair. Output paths of "/var/log/auditlog" and "/var/log/securitylog" are not available at IEMS's northbound log interface.
- 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.
- The CICM353 log events are unique to the SAM16-based CICM product and are not contained in the table below.
- Items highlighted in bold are changes one can expect from the previous release. At the time of writing, in SN09 only 1 new instance (SubtractConnectionAckFailed) of the CICM363 log is known. This is an autonomous INFO log which has no severity and is not part of a set/clear pair.

Log	CICM Log Output Path	Alarm	Log Severity	Component Id	Category	Description	Specific Problem
CICM300	/var/log/customerlog	LegacyError	None	Unknown ./var/log/customerlog,Platform	environmental	Legacy Error Log.	Log details: XXX
CICM300	/var/log/customerlog	LegacyWarning	None	Unknown ./var/log/customerlog,Platform	environmental	Legacy Warning Log.	Log details: XXX
CICM301	Alarm_Trail_to_IEMS	softwareMismatch	Minor	CICM=<nodename>;NodeT ype=Platform	environmental	Software Version Mismatch.	Version Mismatch. Local Version XXX. Mate Version XXX.
CICM301	Alarm_Trail_to_IEMS	softwareMismatch Clear	None	CICM=<nodename>;NodeT ype=Platform	environmental	Software Version Mismatch.	Version Mismatch. Local Version XXX. Mate Version XXX.
CICM302	/var/log/customerlog	RouteOrElementSt ateMismatch	None	Unknown ./var/log/customerlog,Platform	communications	Route/element state mismatch	Resetting adapter, state= XXX mate=XXX
CICM303	/var/log/customerlog	CorruptVLCM	None	Unknown ./var/log/customerlog,Platform	equipment	Corrupt VLCM.	VLCM name XXX is corrupt - in memory gateway already has id of XXX.
CICM304	/var/log/customerlog	UnableBindIP	None	Unknown ./var/log/customerlog,Platform	communications	Unable to bind IP.	Unable to bind IP address XXX to interface XXX.
CICM305	/var/log/customerlog	NoAdapterMib	None	Unknown ./var/log/customerlog,Platform	processingError	Unable To Bind Adapter.	Unable to obtain dynamic adapter config from Mib - cannot bind adapter.
CICM306	/var/log/customerlog	NoAdminIPNodeA	None	Unknown ./var/log/customerlog,Platform	processingError	No admin Ip for node A.	No admin address datafilled for node A
CICM306	/var/log/customerlog	NoAdminIPNodeB	None	Unknown ./var/log/customerlog,Platform	processingError	No admin Ip for node B.	No admin address datafilled for node B
CICM306	/var/log/customerlog	NoAdminNetMask	None	Unknown ./var/log/customerlog,Platform	processingError	No admin net mask.	No admin net mask datafilled
CICM306	/var/log/customerlog	InvalidAdminAddr	None	Unknown ./var/log/customerlog,Platform	processingError	Invalid admin address.	Invalid admin ip address specified XXX
CICM306	/var/log/customerlog	InvalidAdminMask	None	Unknown ./var/log/customerlog,Platform	processingError	Invalid admin mask.	Invalid admin mask specified XXX

CICM307	/var/log/customerlog	SkippingDisabledAdapter	None	Unknown ./var/log/customerlog,Platform	communications	Skipping disabled adapter	Skipping disabled XXX adapter.
CICM308	/var/log/customerlog	UFTPSessionTimeout1	None	Unknown ./var/log/customerlog,Cicm	communications	UFTPSessionTimeout.	Timed out after XXX secs - No request details received from client
CICM308	/var/log/customerlog	UFTPSessionTimeout2	None	Unknown ./var/log/customerlog,Cicm	communications	UFTPSessionTimeout.	Timed out after XXX secs - No response from client
CICM308	/var/log/customerlog	UFTPSessionTimeout3	None	Unknown ./var/log/customerlog,Cicm	communications	UFTPSessionTimeout.	Timed out after XXX secs - Terminated after error occurred
CICM309	/var/log/customerlog	NoStreamsAvailable	None	Unknown ./var/log/customerlog,Cicm	communications	NoStreamsAvailable.	No streams available for CreateConnection, XXX streams already allocated
CICM310	/var/log/customerlog	H248SendPortNotFoundInMIB	None	Unknown ./var/log/customerlog,Cicm	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	Unknown ./var/log/customerlog,Cicm	communications	H248 Listen Port Not Found in MIB.	XXX : H248 listen port not found in MIB.Defaulting to XXX
CICM311	/var/log/customerlog	CouldNotOpenRegistryKey	None	Unknown ./var/log/customerlog,Platform	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	Unknown ./var/log/customerlog,Platform	processingError	Mib failed to open key.	Mib node error: failed to open key XXX.
CICM312	/var/log/customerlog	MIBCompatFailure	None	Unknown ./var/log/customerlog,Platform	processingError	MIB compatibility failure.	MIB compatibility failure. Could not find the MIB entries for release XXX
CICM312	/var/log/customerlog	MIBCompatRemoteFailure	None	Unknown ./var/log/customerlog,Platform	processingError	MIB compatibility remote failure.	MIB compatibility failure. Could not find the MIB entries for release XXX on remote node
CICM313	Alarm_Trap_to_IEMS	GWCCConnectionLoss	Critical	CICM=<nodename>;Node Type=Cicm	communications	GWC Connection Loss	CICM has lost connection with the GWC
CICM313	Alarm_Trap_to_IEMS	GWCCConnectionLossClear	None	CICM=<nodename>;Node Type=Cicm	communications	GWC Connection Loss	CICM has regained connection with GWC
CICM314	/var/log/customerlog	MibReadFailure	None	Unknown ./var/log/customerlog,Platform	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	Unknown ./var/log/customerlog,Platform	communications	Unable to create a socket.	Unable to create a socket. Error = XXX
CICM316	/var/log/customerlog	UnableBindSocketAddr	None	Unknown ./var/log/customerlog,Platform	communications	Unable to Bind Socket to IP.	Unable to Bind Socket to IP address.

CICM316	/var/log/customerlog	AddrNotAvailable	None	Unknown ./var/log/customerlog,Platform	communications	Addr not available.	Specified address is not available on the local host.
CICM316	/var/log/customerlog	AddrInUse	None	Unknown ./var/log/customerlog,Platform	communications	Addr already in use.	Specified address is already in use.
CICM316	/var/log/customerlog	NoAsyncReadMode	None	Unknown ./var/log/customerlog,Platform	communications	No async read mode	Unable to select asynchronous read mode. Error = XXX
CICM316	/var/log/customerlog	ErrorSetSocketTMO	None	Unknown ./var/log/customerlog,Platform	communications	Error setting socket tmo	Error setting socket timeout.Error = XXX
CICM322	Alarm_Trail_to_IEMS	SystemShutdown	Critical	CICM=<nodename>;NodeType=Platform	processingError	System Shutdown	System is shutting down due to user command.
CICM322	Alarm_Trail_to_IEMS	SystemStartUp	None	CICM=<nodename>;NodeT ype=Platform	processingError	System Shutdown	System is starting up.
CICM323	/var/log/customerlog	SlaveAdapterReceivedNoPackets	None	Unknown ./var/log/customerlog,Platform	communications	Slave adapter received no packets	Slave adapter XXX received no packets
CICM324	/var/log/customerlog	FatalStateError	None	Unknown ./var/log/customerlog,Cicm	equipment	Fatal Error in state	Fatal error in state XXX.
CICM325	/var/log/customerlog	ElementNotConfigured	None	Unknown ./var/log/customerlog,Cicm	processingError	Element Not Configured.	Element XXX is not configured.
CICM325	/var/log/customerlog	ElementNotConfigured2	None	Unknown ./var/log/customerlog,Cicm	processingError	Config data missing.	Configuration data missing, service cannot start.
CICM326	/var/log/customerlog	UnableToGetPhysicalLinkStatusForDevice	None	Unknown ./var/log/customerlog,Platform	communications	Unable to get physical link status	Unable to get physical link status for device XXX
CICM327	/var/log/customerlog	FailedStartNetObj	None	Unknown ./var/log/customerlog,Cicm	equipment	Failed to start network status	Failed to start network status object, hr=0x XXX
CICM328	Alarm_Trail_to_IEMS	WindowsRestart	Critical	CICM=<nodename>;NodeT ype=Cicm	equipment	Windows restart	Auto reboot on failure is set. Initiating windows restart.
CICM329	/var/log/customerlog	AuditMateDown	None	Unknown ./var/log/customerlog,Cicm	equipment	Audit Mate Node Down	Node initialisation: mate node is down
CICM329	/var/log/customerlog	AuditMateActive	None	Unknown ./var/log/customerlog,Cicm	equipment	Audit Mate Node Down	Node initialisation: mate node is active in state XXX
CICM330	/var/log/customerlog	CantDoPhysicalCheckOnLink	None	Unknown ./var/log/customerlog,Platform	communications	Can't do physical check on link	Can't do physical check on link XXX
CICM331	/var/log/customerlog	CompFailureShutdown	None	Unknown ./var/log/customerlog,Cicm	equipment	Component failure : shutdown	Component XXX has failed. Initiating shutdown. XXX
CICM332	/var/log/customerlog	BadTransition	None	Unknown ./var/log/customerlog,Cicm	equipment	Bad transition on mate node	Bad transition on mate node from XXX to XXX
CICM333	/var/log/customerlog	NoAccessRemoteName	None	Unknown ./var/log/customerlog,CicmE M	communications	No access to remote name	No access to the remote name in the MIB.
CICM334	Alarm_Trail_to_IEMS	MateFailure	None	CICM=<nodename>;NodeT ype=Cicm	equipment	Audit: Mate Node Failed	Mate node failed - Broadcast failure and ask components to promote to Master.
CICM334	Alarm_Trail_to_IEMS	MateRecovered	None	CICM=<nodename>;NodeT ype=Cicm	equipment	Audit: Mate Node Failed	Mate node recovered.

CICM335	/var/log/customerlog	RouteElementInvalid	None	Unknown ./var/log/customerlog,Platform	communications	Route Element Invalid	Local route element XXX or remote route element XXX is invalid
CICM336	/var/log/customerlog	NetworkRecovery	None	Unknown ./var/log/customerlog,Cicm	communications	Network loss and recovery	Network has been lost and then recovered, mate (slave) must reboot.
CICM337	Alarm_Train_to_IEMS	NoMessageToA	Major	CICM=<nodename>;NodeT ype=Cicm;Component=Chassis	equipment	Message To Node A Failed	Failed to send message to Node A.
CICM337	Alarm_Train_to_IEMS	NoMessageToAClear	None	CICM=<nodename>;NodeT ype=Cicm;Component=Chassis	equipment	Message To Node A Failed	Clear Failed to send message to Node A.
CICM338	/var/log/customerlog	NetworkElementHasFailed	None	Unknown ./var/log/customerlog,Platform	communications	Network Element Failed	Network Element XXX Failed
CICM339	Alarm_Train_to_IEMS	NoMessageFromB	Major	CICM=<nodename>;NodeT ype=Cicm	equipment	No Message Received From B	Have not received a message from Node B for 1.5*ALARM_POLL_PERIOD Seconds. XXX
CICM339	Alarm_Train_to_IEMS	NoMessageFromB Clear	None	CICM=<nodename>;NodeT ype=Cicm	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	Unknown ./var/log/customerlog,Platform	communications	Can't set local adapter	Can't set local adapter, invalid adapter specified
CICM341	Alarm_Train_to_IEMS	BackupFail	Minor	CICM=<nodename>;NodeT ype=Platform	processingError	Backup Fail.	Scheduled/on-demand backup failed during last iteration.
CICM341	Alarm_Train_to_IEMS	BackupFailClear	None	CICM=<nodename>;NodeT ype=Platform	processingError	Backup Fail.	Scheduled/on-demand backup failed during last iteration.
CICM342	/var/log/customerlog	UnableToBindAdminIPaddressToInterface	None	Unknown ./var/log/customerlog,Platform	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	Unknown ./var/log/customerlog,Platform	communications	Can't set slave adapter	Can't set slave adapter, invalid adapter specified XXX
CICM345	/var/log/customerlog	EMMateDown	None	Unknown ./var/log/customerlog,CicmEM	communications	EM Mate Down	Mate node down. Name: XXX. XXX
CICM346	/var/log/customerlog	EMMibWriteFail	None	Unknown ./var/log/customerlog,CicmEM	communications	EM Mate Down	Couldn't write EM remote node status to Mib
CICM348	/var/log/customerlog	ChangingSlaveAdapter	None	Unknown ./var/log/customerlog,Platform	communications	Changing slave adapter	Changing slave adapter from XXX to XXX
CICM350	/var/log/customerlog	GetInterfaceDeviceMapping	None	Unknown ./var/log/customerlog,Platform	communications	Get Interface Device Mapping Failed	Get Interface Device Mapping Failed
CICM352	/var/log/customerlog	CantMapAdapter	None	Unknown ./var/log/customerlog,Platform	communications	Can't map adapter	Can't map XXX to an NT device, link state won't be checked

CICM354	/var/log/customerlog	maxRudpSessionsNotPresent	None	Unknown ./var/log/customerlog,Cicm	communications	maxRudpSessionsNotPresent.	Maximum sessions configuration not present
CICM354	/var/log/customerlog	UnableToSetMaxRUDPSessions	None	Unknown ./var/log/customerlog,Cicm	communications	UnableToSetMaxRUDP Sessions.	unable to set max RUDP sessions [may already be started]
CICM355	/var/log/customerlog	VmgIpAddressBindFailed	None	Unknown ./var/log/customerlog,Cicm	communications	Bind UDP socket for vmg failed.	Failed to start UDP socket. hr XXX
CICM355	/var/log/customerlog	VmgTerminationInvalid	None	Unknown ./var/log/customerlog,Cicm	communications	VMG termination invalid.	VMG XXX termination XXX invalid
CICM356	/var/log/customerlog	AdapterDown	None	Unknown ./var/log/customerlog,Platform	communications	Adapter down	Adapter XXX is down - aborting start until all adapters are up
CICM357	/var/log/customerlog	EchoServerPortNotPresent	None	Unknown ./var/log/customerlog,Cicm	communications	EchoServerPortNotPresent.	Echo server port configuration not present
CICM358	/var/log/customerlog	UnableToMapNEToInterfaceNumber	None	Unknown ./var/log/customerlog,Platform	communications	Unable to map ne to an interface number	Unable to map ne XXX to an interface number
CICM359	Alarm_Trap_to_IEMS	MateNodeComFailure	Major	CICM=<nodename>;Node Type=Platform	communications	Mate Node COM Failure.	COM method failed to mate node (XXX).
CICM359	Alarm_Trap_to_IEMS	MateNodeComFailureClear	None	CICM=<nodename>;Node Type=Platform	communications	Mate Node COM Failure.	COM method succeeded to mate node.
CICM360	/var/log/customerlog	AutoBindAdapter	None	Unknown ./var/log/customerlog,Platform	communications	Auto-bind adapter problem	Auto-bind adapter XXX XXX
CICM361	/var/log/customerlog	HostPortNotPresent	None	Unknown ./var/log/customerlog,Cicm	communications	HostPortNotPresent.	Host port configuration not present
CICM362	/var/log/customerlog	SwactRequestRejected	None	Unknown ./var/log/customerlog,Platform	communications	Swact request rejected	Swact request rejected XXX
CICM363	/var/log/customerlog	CreateConnectionAckFailed	None	Unknown ./var/log/customerlog,Cicm	communications	Create ConnectionAck Failed.	CreateConnectionAck::can't determine destination for message
CICM363	/var/log/customerlog	ModifyConnectionAckFailed	None	Unknown ./var/log/customerlog,Cicm	communications	Modify ConnectionAck Failed.	ModifyConnectionAck::can't determine destination for message
CICM363	/var/log/customerlog	noPtimeCanBeNegotiated	None	Unknown ./var/log/customerlog,Cicm	communications	no ptime can be negotiated.	Ensure a common ptime exists between the GWC and the CICM terminal audio profile
CICM363	/var/log/customerlog	SystemShutdown	None	Unknown ./var/log/customerlog,Cicm	communications	Subtract ConnectionAck Failed.	SubtractConnectionAck::can't determine destination for message
CICM363	/var/log/customerlog	noPtimeCanBeNegotiated	None	Unknown ./var/log/customerlog,Cicm	communications	no ptime can be negotiated.	Ensure a common ptime exists between the GWC and the CICM terminal audio profile
CICM363	/var/log/customerlog	noCodecCanBeNegotiated	None	Unknown ./var/log/customerlog,Cicm	communications	no codec can be negotiated.	Ensure a common codec exists between the GWC and the CICM terminal audio profile

CICM364	/var/log/customerlog	RegisterGatewayFailed	None	Unknown ./var/log/customerlog,Cicm	communications	Register Gateway Failed	Register Gateway XXX Failed
CICM364	/var/log/customerlog	UnRegisterGatewayFailed	None	Unknown ./var/log/customerlog,Cicm	communications	UnRegister Gateway Failed	UnRegister Gateway XXX Failed
CICM365	/var/log/customerlog	MibSyncMateFail	None	Unknown ./var/log/customerlog,Cicm	equipment	Mib Sync Mate Failure	Mate node failed during MIB synchronisation. This node will start partially Synchronised.
CICM366	/var/log/customerlog	MibSyncSCMPollFail	None	Unknown ./var/log/customerlog,Cicm	equipment	Mib Sync SCM Poll Failure	Opening Service Control Manager FAILURE.
CICM367	/var/log/customerlog	ErrorDatafillTones	None	Unknown ./var/log/customerlog,Cicm	equipment	Error Datafilling Tones	Error encountered datafilling tones!.
CICM368	/var/log/customerlog	NoMaxSessions	None	Unknown ./var/log/customerlog,Cicm	equipment	Max Sessions Not Present	Invalid config. Max Sessions not present.
CICM368	/var/log/customerlog	MaxSessionsNotPresent	None	Unknown ./var/log/customerlog,Cicm	communications	MaxSessionsNotPresent.	Maximum sessions configuration not specified
CICM369	/var/log/customerlog	NoDomainLicense	None	Unknown ./var/log/customerlog,Cicm	equipment	No Domain License	No network domain license for terminal at XXX
CICM370	Alarm_Train_to_IEMS	MateFailure	Major	CICM=<nodename>;NodeType=Platform	communications	Mate Failure.	Admin reports mate node failure.
CICM370	Alarm_Train_to_IEMS	MateStarting	Major	CICM=<nodename>;NodeType=Platform	communications	Mate Failure.	Admin reports Mate Node start.
CICM371	/var/log/customerlog	TerminalError	None	Unknown ./var/log/customerlog,Cicm	equipment	An Error Occured on the Terminal	Terminal Error XXX
CICM372	/var/log/customerlog	UnableToMapAdapter	None	Unknown ./var/log/customerlog,Platform	communications	Unable to map adapter	Unable to map XXX adapter XXX to an ip address.
CICM373	/var/log/customerlog	UFTPFWareFileOpenFailed	None	Unknown ./var/log/customerlog,Cicm	communications	UFTPFWareFileOpenFailed.	Failed to open file XXX.
CICM373	/var/log/customerlog	UFTPFWareFileOpenFailedFatal	None	Unknown ./var/log/customerlog,Cicm	communications	UFTPFWareFileOpenFailed.	Invalid directory or file XXX not found
CICM373	/var/log/customerlog	UFTPFWareFileReadError	None	Unknown ./var/log/customerlog,Cicm	communications	UFTPFWareFileReadError.	Firmware file XXX read error
CICM373	/var/log/customerlog	UFTPCommandFileReadError	None	Unknown ./var/log/customerlog,Cicm	communications	UFTPCommandFileReadError.	UFTPCommandFileReadError
CICM373	/var/log/customerlog	UFTPCommandFileCreationError	None	Unknown ./var/log/customerlog,Cicm	communications	UFTPCommandFileCreationError.	Command = XXX
CICM373	/var/log/customerlog	UFTPBaseDirectoryMissing	None	Unknown ./var/log/customerlog,Cicm	communications	UFTPBaseDirectoryMissing.	UFTP base directory missing from registry
CICM374	/var/log/customerlog	ReadPollPeriodFail	None	Unknown ./var/log/customerlog,CicmEM	communications	Poll Period Read Fail	Couldn't read gwPollPeriod from mib. Defaulting to 30 seconds.
CICM375	Alarm_Train_to_IEMS	SAM21VersionMismatch	Minor	CICM=<nodename>;NodeType=Platform	processingError	SAM21 Version Mismatch.	SAM21 Version Mismatch. Version XXX

CICM375	Alarm_Trap_to_IEMS	SAM21VersionMismatchClear	None	CICM=<nodename>;NodeType=Platform	processingError	SAM21 Version Mismatch.	SAM21 Version Mismatch. Version XXX
CICM376	/var/log/customerlog	ShuttingDownTerminals	None	Unknown ./var/log/customerlog,Cicm	communications	ShuttingDownTerminal s.	Shutdown counter set to zero minutes, shutting down terminals immediately
CICM376	/var/log/customerlog	TerminalShutDownAborted	None	Unknown ./var/log/customerlog,Cicm	communications	TerminalShutDownAborted.	Terminal shutdown aborted
CICM377	Alarm_Trap_to_IEMS	SyslogFailure	Major	CICM=<nodename>;NodeType=Platform	communications	Syslog Failure.	Syslog failure. Last stream in failure XXX.
CICM377	Alarm_Trap_to_IEMS	SyslogFailureClear	None	CICM=<nodename>;NodeType=Platform	communications	Syslog Failure.	Syslog failure clear.
CICM378	/var/log/customerlog	ExcessNodes	None	Unknown ./var/log/customerlog,CicmEM	communications	Excessive Nodes on EM	More than 100 nodes present, unrecommended configuration
CICM379	/var/log/customerlog	RegisterSessionFailed	None	Unknown ./var/log/customerlog,Cicm	communications	Register Session Failed	Register Session Failed on Gateway XXX
CICM379	/var/log/customerlog	RegisterSessionFailedRange	None	Unknown ./var/log/customerlog,Cicm	communications	Register Gateway Failed	Register Gateway XXX Failed termination XXX is out of range
CICM379	/var/log/customerlog	RegisterSessionFailedInvalid	None	Unknown ./var/log/customerlog,Cicm	communications	Register Gateway Failed	Register Gateway XXX Failed termination XXX is invalid
CICM379	/var/log/customerlog	CouldntStartAuditTimer	None	Unknown ./var/log/customerlog,Cicm	communications	Couldn't start audit timer	Couldn't start audit timer
CICM380	Alarm_Trap_to_IEMS	FailedPollIMG	None	CICM=<nodename>;NodeType=Platform	communications	Fail Poll MG	Failed to Poll Media Gateway XXX.
CICM380	Alarm_Trap_to_IEMS	FailedPollIMGClear	None	CICM=<nodename>;NodeType=Platform	communications	Fail Poll MG	Failed to Poll Media Gateway XXX.
CICM381	Alarm_Trap_to_IEMS	NetworkLoss	Critical	CICM=<nodename>;NodeType=Platform	communications	Network Loss.	Critical network connection loss on adapter XXX
CICM381	Alarm_Trap_to_IEMS	ClearNetworkLoss	None	CICM=<nodename>;NodeType=Platform	communications	Network Loss.	Critical network connection loss cleared on adapter XXX
CICM381	Alarm_Trap_to_IEMS	NetworkLossMajor	Major	CICM=<nodename>;NodeType=Platform	communications	Network Loss.	Major network connection loss on adapter XXX
CICM381	Alarm_Trap_to_IEMS	ClearNetworkLossMajor	None	CICM=<nodename>;NodeType=Platform	communications	Network Loss.	Major network connection loss cleared on adapter XXX
CICM381	Alarm_Trap_to_IEMS	NetworkRedundancyLoss	Major	CICM=<nodename>;NodeType=Platform	communications	Network Redundancy Loss.	Network redundancy lost to the mate node
CICM381	Alarm_Trap_to_IEMS	ClearNetworkRedundancyLoss	None	CICM=<nodename>;NodeType=Platform	communications	Network Redundancy Loss.	Network redundancy restored to the mate node
CICM382	Alarm_Trap_to_IEMS	RemoteHostFail	Minor	CICM=<nodename>;NodeType=Platform	communications	Remote Host Fail.	Disabling client XXX with interface XXX.
CICM382	Alarm_Trap_to_IEMS	RemoteHostFailClear	None	CICM=<nodename>;NodeType=Platform	communications	Remote Host Fail.	Enabling client XXX with interface XXX.
CICM383	/var/log/customerlog	FirmwareUpgradeNotSupportedUFTPOverUnistim	None	Unknown ./var/log/customerlog,Cicm	communications	FirmwareUpgradeNotSupportedUFTPOverUnistim.	Firmware upgrade is not supported via UFTP over Unistim. File XXX

CICM383	Alarm_Train_to_IEMS	FirmwareUpgrade Fail	None	CICM=<nodename>;NodeT ype=Cicm;Component=Ter minals	communications	Firmware upgrade failure.	Firmware upgrade failure.
CICM383	Alarm_Train_to_IEMS	FirmwareUpgrade FailClear	None	CICM=<nodename>;NodeT ype=Cicm;Component=Ter minals	communications	Firmware upgrade failure.	Firmware upgrade failure.
CICM384	/var/log/customerlog	NodeIsolatedForci ngTransitionFrom MasterToSlave	None	Unknown ./var/log/customerlog,Platfor m	communications	Node Isolated - Forcing transition from master to slave	Node Isolated - Forcing transition from master to slave
CICM385	/var/log/customerlog	SlaveNodeIsolated	None	Unknown ./var/log/customerlog,Platfor m	communications	Slave Node isolated	Slave Node isolated
CICM386	/var/log/customerlog	UFTPmaxSession sMIBDataFatal	None	Unknown ./var/log/customerlog,Cicm	communications	UFTPmaxSessions value in the mib is incorrect	UFTPmaxSessions must be at least one. Value XXX is invalid
CICM386	/var/log/customerlog	UFTPmaxSession sMIBDataNonFatal	None	Unknown ./var/log/customerlog,Cicm	communications	UFTPmaxSessions value is missing from the mib	UFTPmaxSessions missing using default value XXX
CICM387	Alarm_Train_to_IEMS	CommsFailedCic m	Major	CICM=<nodename>;NodeT ype=CICMEM;Cicm=<node IP address>	communications	CICM Poll Failed	Failed to Poll CICM Node XXX.
CICM387	Alarm_Train_to_IEMS	CommsFailedCic mClear	None	CICM=<nodename>;NodeT ype=CICMEM;Cicm=<node IP address>	communications	CICM Poll Failed	Failed to Poll CICM Node XXX.
CICM388	/var/log/customerlog	UFTPtimerTimeou tMIBDataNonFatal	None	Unknown ./var/log/customerlog,Cicm	communications	UFTPtimerTimeout value is missing from the mib	UFTPtimerTimeout missing using default value XXX
CICM389	/var/log/customerlog	UFTPInvalidClient Message	None	Unknown ./var/log/customerlog,Cicm	communications	UFTP_INVALID_CLIE NT_MESSAGE	UFTP_INVALID_CLIE NT_MESSAGE XXX value XXX is invalid
CICM390	Alarm_Train_to_IEMS	FailedPAMConn	Major	CICM=<nodename>;NodeT ype=CicmEM	communications	Failed To Connect PAM server	PAM server XXX is not responding to authentication requests
CICM390	Alarm_Train_to_IEMS	FailedPAMConnCl ear	None	CICM=<nodename>;NodeT ype=CicmEM	communications	Failed To Connect PAM server	PAM server XXX is now responding to authentication requests
CICM391	/var/log/customerlog	ProcessNetworkSt ateTransitionState Error	None	Unknown ./var/log/customerlog,Platfor m	communications	Invalid transition	ProcessNetworkState Transition() called with invalid transition XXX
CICM392	/var/log/customerlog	PAMServerTMO	None	Unknown ./var/log/customerlog,CicmE M	communications	PAM Server TMO	Timeout occurred whilst awaiting response from PAM server XXX
CICM393	/var/log/customerlog	TakeoverManualA bortedIsNotImple mented	None	Unknown ./var/log/customerlog,Platfor m	communications	Takeover manual aborted, is not implemented	Takeover manual aborted, is not implemented
CICM394	/var/log/customerlog	FailedToUnbindAd apter	None	Unknown ./var/log/customerlog,Platfor m	communications	Fatal error: Unable to unbind adapter	Fatal error: Unable to unbind adapter.
CICM395	/var/log/customerlog	MateNodeFailedT emporarily	None	Unknown ./var/log/customerlog,Platfor m	communications	Mate node failed temporarily	Mate node failed temporarily for XXX iterations
CICM396	/var/log/customerlog	TakeoverAbort	None	Unknown ./var/log/customerlog,Platfor m	communications	Takeover aborted, reverting to Master	Takeover aborted, reverting to Master
CICM397	/var/log/customerlog	MateNodeLostFor cingTransitionFro mSlaveToMaster	None	Unknown ./var/log/customerlog,Platfor m	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	Unknown ./var/log/customerlog,Platfor m	communications	Mate node lost	Mate node lost

CICM399	/var/log/customerlog	RouteMapError	None	Unknown ./var/log/customerlog,Platform	communications	Route map error	Resetting adapter, state= XXX mate=XXX
CICM500	/var/log/customerlog	StateChange	None	Unknown ./var/log/customerlog,Platform	processingError	State Change.	Admin reports a state change to XXX for component XXX.
CICM503	/var/log/customerlog	NetAccessStateChange	None	Unknown ./var/log/customerlog,CicEM	communications	Network Access State Change	Netork access state change to XXX
CICM504	/var/log/customerlog	EMNetworkChange	None	Unknown ./var/log/customerlog,CicEM	communications	EM Network State Change	Network connectivity XXX. hr=XXX
CICM505	/var/log/customerlog	StopMonitoring	None	Unknown ./var/log/customerlog,CicEM	communications	Stop Monitoring	Stopped monitoring node XXX
CICM506	/var/log/auditlog	MonitorStart	None	Unknown ./var/log/auditlog,CicEM	communications	Start Monitoring	Started to monitor node XXX.
CICM507	/var/log/auditlog	ConnectToPAMServer	None	Unknown ./var/log/auditlog,CicEM	environmental	Connect to PAM.	Connect to PAM.
CICM508	/var/log/customerlog	SlaveInstructedToChangeToInvalidAdapter	None	Unknown ./var/log/customerlog,Platform	communications	Slave instructed to change to invalid adapter, selecting default	Slave instructed to change to invalid adapter, selecting default
CICM509	Alarm_Train_to_IEMS	ProcessStateChange	Critical	CICM=<nodename>;NodeT ype=Platform;SoftwareCom ponent=<component id>	processingError	Critical Process State Change.	Critical Process XXX is not running.
CICM509	Alarm_Train_to_IEMS	ProcessStateChangeClear	None	CICM=<nodename>;NodeT ype=Platform;SoftwareCom ponent=<component id>	processingError	Critical Process State Change.	Critical Process XXX is running.
CICM509	Alarm_Train_to_IEMS	ServiceStateChange	Major	CICM=<nodename>;NodeT ype=Platform;SoftwareCom ponent=<component id>	processingError	Service State Change.	Service XXX is not running.
CICM509	Alarm_Train_to_IEMS	ServiceStateChangeClear	None	CICM=<nodename>;NodeT ype=Platform;SoftwareCom ponent=<component id>	processingError	Service State Change.	Service XXX is running.
CICM510	/var/log/auditlog	EMMateUp	None	Unknown ./var/log/auditlog,CicEM	environmental	EM Mate Up.	EM Mate Up. Name: XXX.
CICM512	/var/log/customerlog	StartSWACT	None	Unknown ./var/log/customerlog,Platform	processingError	Start SWACT.	Admin reports a request to start SWACT.
CICM512	/var/log/customerlog	PromoteToMaster	None	Unknown ./var/log/customerlog,Platform	processingError	Promote to Master.	Admin reports a request to promote to Master.
CICM512	/var/log/customerlog	DemoteToSlave	None	Unknown ./var/log/customerlog,Platform	processingError	Demote to Slave.	Admin reports a request to demote to slave.
CICM513	/var/log/auditlog	ChangingLocalAdapter	None	Unknown ./var/log/auditlog,Platform	communications	Changing local adapter	Changing local adapter from XXX to XXX
CICM603	/var/log/customerlog	InvalidEventReport	None	Unknown ./var/log/customerlog,Platform	processingError	Invalid Event Report.	Invalid report received from Admin.
CICM604	/var/log/customerlog	MateSyncErrState	None	Unknown ./var/log/customerlog,Platform	processingError	Mate sync error state.	request for mate synchronisation received in state XXX.
CICM605	/var/log/customerlog	GWRegBadState	None	Unknown ./var/log/customerlog,Platform	equipment	GW Reg in Bad State.	Gateway registration received in state XXX.

CICM606	/var/log/customerlog	PremSlaveGWReg	None	Unknown ./var/log/customerlog,Platform	equipment	Premature reg slave gw.	Premature registration of the slave gateway.
CICM607	/var/log/customerlog	SwactReqRemoteMGM	None	Unknown ./var/log/customerlog,Platform	equipment	Swact Request from Remote MGM.	Swact request received from the remote MGM.
CICM608	/var/log/customerlog	RetransRUDPMessagesThrottled	None	Unknown ./var/log/customerlog,Platform	communications	Retransmitted RUDP messages.	Retransmitted XXX RUDP messages, XXX retransmissions were throttled.
CICM609	/var/log/customerlog	RetransRUDPMessages	None	Unknown ./var/log/customerlog,Platform	communications	Retransmitted RUDP messages.	Retransmitted XXX RUDP messages.
CICM610	/var/log/customerlog	LossOfLogs	None	Unknown ./var/log/customerlog,Platform	communications	Loss of logs.	XXX logs have been lost due to buffering.
CICM610	/var/log/customerlog	LossOfTraps	None	Unknown ./var/log/customerlog,Platform	communications	Loss of traps.	XXX traps have been lost due to buffering.
CICM611	Alarm_Trap_to_IEMS	ThresholdReached	Major	CICM=<nodename>;NodeType=Platform	qualityOfService	Resource Threshold Crossed	Resource XXX is near or above its threshold of XXX
CICM611	Alarm_Trap_to_IEMS	ThresholdReachedClear	None	CICM=<nodename>;NodeType=Platform	qualityOfService	Threshold Crossed	Resource XXX is near or above its threshold value of XXX
CICM612	/var/log/customerlog	AuditStart	None	Unknown ./var/log/customerlog,Cicm	environmental	Start Audit.	Starting the daily audit.
CICM612	/var/log/customerlog	AuditEnd	None	Unknown ./var/log/customerlog,Cicm	environmental	Audit Complete	Daily audit completed.
CICM614	/var/log/customerlog	MsgFromInvalidComp	None	Unknown ./var/log/customerlog,Cicm	equipment	Message from invalid component	Message received from invalid component type = 0x XXX
CICM615	/var/log/customerlog	NodeForcedMaster	None	Unknown ./var/log/customerlog,Cicm	equipment	Node forced to master	Node is being forced to become master.
CICM615	/var/log/customerlog	NodeForcedSlave	None	Unknown ./var/log/customerlog,Cicm	equipment	Node forced to slave	Node is being forced to become slave.
CICM617	/var/log/customerlog	MibSyncPollFail	None	Unknown ./var/log/customerlog,Cicm	equipment	Mib Sync Poll Failure	Network status remote state query returned hr=0x XXX.
CICM618	/var/log/customerlog	NoLineID	None	Unknown ./var/log/customerlog,Cicm	equipment	No Line ID	User XXX has no LineId attribute in the mib.
CICM619	/var/log/customerlog	NoToneset	None	Unknown ./var/log/customerlog,Cicm	equipment	No Toneset Found	Toneset XXX not found A standard tone will be used in place of all toneIds
CICM620	/var/log/customerlog	InvalidToneIndex	None	Unknown ./var/log/customerlog,Cicm	equipment	Invalid Tone Component Index	Invalid tone component index toneset XXX toneid XXX
CICM621	/var/log/customerlog	NoVolume	None	Unknown ./var/log/customerlog,Cicm	equipment	Invalid Volume Datafilled	No volume datafilled for toneset XXX toneid XXX
CICM622	/var/log/customerlog	Invalidtone	None	Unknown ./var/log/customerlog,Cicm	equipment	Invalid Tone Frequency	Invalid tone frequency count toneset XXX toneid XXX

CICM623	/var/log/customerlog	NoFrequency	None	Unknown ./var/log/customerlog,Cicm	equipment	Invalid Frequency Datafilled	No frequency datafilled for toneset XXX toneid XXX
CICM624	/var/log/customerlog	InvalidCadenceCo unt	None	Unknown ./var/log/customerlog,Cicm	equipment	Invalid Cadence Count	Invalid tone cadence count toneset XXX toneid XXX
CICM625	/var/log/customerlog	NoCadenceOff	None	Unknown ./var/log/customerlog,Cicm	equipment	No Cadence Off	No Cadence off datafilled for toneset XXX toneid XXX
CICM625	/var/log/customerlog	NoCadenceOn	None	Unknown ./var/log/customerlog,Cicm	equipment	No Cadence On	No Cadence on datafilled for toneset XXX toneid XXX
CICM627	/var/log/customerlog	InvalidConnMap	None	Unknown ./var/log/customerlog,Cicm	equipment	Connection mapped to invalid line	Connection XXX is mapped to line XXX which isn't valid.
CICM628	/var/log/customerlog	ConnNonE1	None	Unknown ./var/log/customerlog,Cicm	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/customerlog	ResetNoConn	None	Unknown ./var/log/customerlog,Cicm	equipment	Reset Connection isn't in NO_CONNECTION state	Resetting connection for line XXX which isn't in NO_CONNECTION state.
CICM630	/var/log/customerlog	CreateConFail	None	Unknown ./var/log/customerlog,Cicm	equipment	Create Connection Fail	Create connection failed. Call type = XXX, result = XXX
CICM631	/var/log/customerlog	DelConFail	None	Unknown ./var/log/customerlog,Cicm	equipment	Delete Connection Fail	Delete connection failed.
CICM632	/var/log/customerlog	NoLineObject	None	Unknown ./var/log/customerlog,Cicm	equipment	No line object	Create Connection: Could not find line object for conflicting connection XXX with lineid = XXX
CICM633	/var/log/customerlog	CorruptConnMap	None	Unknown ./var/log/customerlog,Cicm	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/customerlog	NoConIDMap	None	Unknown ./var/log/customerlog,Cicm	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/customerlog	UnableChangeLos s	None	Unknown ./var/log/customerlog,Cicm	equipment	Unable Change Rx Loss	Unable to change rx loss for connection XXX
CICM636	/var/log/customerlog	TooManyFeatures	None	Unknown ./var/log/customerlog,Cicm	equipment	Too Many Features	Terminal type has too many features on the main set (max is XXX).
CICM637	/var/log/customerlog	TooManyFeatures Ext	None	Unknown ./var/log/customerlog,Cicm	equipment	Too Many Features	Terminal type has too many features on the extension set (max is XXX).
CICM638	/var/log/securitylog	AuthUserProblem	None	Unknown ./var/log/securitylog,Cicm	equipment	Auth User Failed	User XXX
CICM639	/var/log/securitylog	LogoutSuccess	None	Unknown ./var/log/securitylog,Cicm	equipment	Logout Success	User XXX

CICM639	/var/log/securitylog	LoginSuccess	None	Unknown ./var/log/securitylog,Cicm	equipment	Login Success	User XXX
CICM641	/var/log/securitylog	ChangePassword	None	Unknown ./var/log/securitylog,Cicm	equipment	Change Password Attempt	User XXX
CICM642	/var/log/securitylog	ReleaseAuth	None	Unknown ./var/log/securitylog,Cicm	equipment	Release Authentication	
CICM643	/var/log/customerlog	InvalidFirmwareProt	None	Unknown ./var/log/customerlog,Cicm	equipment	Invalid Firmware Protocol	Invalid FirmwareProtocol for TerminalType= XXX
CICM644	/var/log/customerlog	InvalidFWLevel	None	Unknown ./var/log/customerlog,Cicm	equipment	Invalid Firmware Level	Invalid Firmware level for TerminalType= XXX
CICM645	/var/log/customerlog	NoFWLevel	None	Unknown ./var/log/customerlog,Cicm	equipment	No Firmware Level	Terminal has no firmware level recorded in the MIB
CICM646	/var/log/customerlog	InvalidUFTPHost	None	Unknown ./var/log/customerlog,Cicm	equipment	Invalid UFTP Host	Invalid UFTP host port
CICM647	/var/log/customerlog	InvalidUnistimHost	None	Unknown ./var/log/customerlog,Cicm	equipment	Invalid Unistim Host	Invalid Unistim host address
CICM648	/var/log/customerlog	InvalidFWTFPTAdr	None	Unknown ./var/log/customerlog,Cicm	equipment	Invalid Firmware TFPT Address	Invalid Firmware TFTP Address for TerminalType=XXX
CICM649	/var/log/auditlog	ConfigDataChange	None	Unknown ./var/log/auditlog,Platform	processingError	Config Data Change.	Admin reports a configuration data change.
CICM650	/var/log/auditlog	InitialisingAsMaster	None	Unknown ./var/log/auditlog,Platform	communications	Initialising as master	Initialising as master
CICM650	/var/log/auditlog	InitialisingAsMasterNoSlave	None	Unknown ./var/log/auditlog,Platform	communications	Initialising as master (no slave)	Initialising as master (no slave)
CICM650	/var/log/auditlog	InitialisingAsSlave	None	Unknown ./var/log/auditlog,Platform	communications	Initialising as slave	Initialising as slave
CICM650	/var/log/auditlog	StartingTakeover	None	Unknown ./var/log/auditlog,Platform	communications	Starting takeover	Starting takeover
CICM650	/var/log/auditlog	TakeoverSucceededNowSlave	None	Unknown ./var/log/auditlog,Platform	communications	Takeover succeeded, now slave	Takeover succeeded, now slave
CICM650	/var/log/auditlog	TakeoverSucceededNowMaster	None	Unknown ./var/log/auditlog,Platform	communications	Takeover succeeded, now Master	Takeover succeeded, now Master
CICM650	/var/log/auditlog	ForcingTransitionFromSlaveToMaster	None	Unknown ./var/log/auditlog,Platform	communications	Forcing transition from slave to master	Forcing transition from slave to master
CICM650	/var/log/auditlog	ForcingTransitionFromMasterToSlave	None	Unknown ./var/log/auditlog,Platform	communications	Forcing transition from master to slave	Forcing transition from master to slave
CICM650	/var/log/auditlog	MateNodeRecoveredForcingtransitionFromSlaveToMaster	None	Unknown ./var/log/auditlog,Platform	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	Unknown ./var/log/auditlog,Platform	communications	Processing Swact	Processing Swact request
CICM652	/var/log/auditlog	addGateway	None	Unknown ./var/log/auditlog,CicmEM	communications	Adding a gateway	Gateway XXX has been added.
CICM653	/var/log/auditlog	deleteGateway	None	Unknown ./var/log/auditlog,CicmEM	communications	Deleting a gateway	Deleting gateway XXX
CICM654	/var/log/auditlog	addProfile	None	Unknown ./var/log/auditlog,CicmEM	communications	Adding a profile	Adding a XXX profile for gateway XXX
CICM655	/var/log/auditlog	delProfile	None	Unknown ./var/log/auditlog,CicmEM	communications	Deleting a profile	Deleting XXX profile for gateway XXX
CICM656	Alarm_Trap_to_IEMS	maxRxRateExceeded	Minor	CICM=<nodename>;NodeType=Platform	processingError	Max Rx Rate Exceeded.	Max rx rate of XXX has been exceeded by rate XXX.

CICM656	Alarm_Trap_to_IEMS	maxRxRateExceededClear	None	CICM=<nodename>;NodeType=Platform	processingError	Max Rx Rate Exceeded.	Clear max rx rate of XXX has been exceeded.
CICM657	Alarm_Trap_to_IEMS	maxCreateAttempts	Minor	CICM=<nodename>;NodeType=Platform	communications	Max Creation Attempts.	Reached the max creation attempts for the session.
CICM657	Alarm_Trap_to_IEMS	maxCreateAttemptsClear	None	CICM=<nodename>;NodeType=Platform	communications	Max Creation Attempts.	Reached the max creation attempts for the session.
CICM658	/var/log/auditlog	MateNodeRecovered	None	Unknown ./var/log/auditlog,Platform	communications	Mate node recovered	Mate node recovered
CICM659	/var/log/auditlog	SlaveAdapterRecovered	None	Unknown ./var/log/auditlog,Platform	communications	Slave adapter recovered	Slave adapter XXX recovered
CICM660	/var/log/securitylog	SuccessfulPAMAuthentication	None	Unknown ./var/log/securitylog,CicmEM	environmental	Successful PAM Authentication.	User XXX has started a session on the CICM-EM
CICM661	/var/log/securitylog	PAMAuthenticationFailure	None	Unknown ./var/log/securitylog,CicmEM	processingError	PAM Authentication Failure.	User XXX authentication failure
CICM662	/var/log/securitylog	UserRevoked	None	Unknown ./var/log/securitylog,CicmEM	environmental	User Privileges Revoked.	Privileges revoked
CICM663	/var/log/securitylog	UserUpgraded	None	Unknown ./var/log/securitylog,CicmEM	environmental	User Privileges upgraded.	Privileges upgraded
CICM664	/var/log/securitylog	InactiveUserTMO	None	Unknown ./var/log/securitylog,CicmEM	environmental	Inactive User Timeout.	User XXX is no longer active on the CICM-EM
CICM665	/var/log/auditlog	NetworkElementHasRecovered	None	Unknown ./var/log/auditlog,Platform	communications	Network Element recovered	Network Element XXX recovered
CICM668	Alarm_Trap_to_IEMS	MaxNoSessions	None	CICM=<nodename>;NodeType=Cicm	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	CICM=<nodename>;NodeType=Cicm	processingError	Reached the maximum number of sessions.	Current number of active sessions is below the maximum of XXX.
CICM680	/var/log/auditlog	RegisterGatewaySucceeded	None	Unknown ./var/log/auditlog,Cicm	communications	Register Gateway Succeeded	Register Gateway XXX Succeeded
CICM681	/var/log/auditlog	ConfigurationChange	None	Unknown ./var/log/auditlog,CicmEM	communications	Configuration change	XXX
CICM682	/var/log/auditlog	ProvisioningChange	None	Unknown ./var/log/auditlog,CicmEM	communications	Provisioning change	XXX
CICM749	/var/log/securitylog	AccountDisabled	None	Unknown ./var/log/securitylog,Cicm	equipment	Account Disabled	User XXX
CICM750	/var/log/securitylog	ChangePasswordFail	None	Unknown ./var/log/securitylog,Cicm	equipment	Change Password Attempt	User XXX
CICM801	Alarm_Trap_to_IEMS	bhhcaMinorAlarm	Minor	CICM=<nodename>;NodeType=Cicm	qualityOfService	BHHCA Minor Alarm	BHHCA is close to maximum value.
CICM801	Alarm_Trap_to_IEMS	bhhcaMinorAlarmClear	None	CICM=<nodename>;NodeType=Cicm	qualityOfService	BHHCA Minor Alarm	BHHCA is close to maximum value.
CICM802	Alarm_Trap_to_IEMS	bhhcaMajorAlarm	Major	CICM=<nodename>;NodeType=Cicm	qualityOfService	BHHCA Major Alarm	BHHCA is at Maximum Limit. Calls may not succeed.
CICM802	Alarm_Trap_to_IEMS	bhhcaMajorAlarmClear	None	CICM=<nodename>;NodeType=Cicm	qualityOfService	BHHCA Major Alarm	BHHCA is at Maximum Limit. Calls may not succeed.
CICM803	Alarm_Trap_to_IEMS	bhhcaCriticalAlarm	Critical	CICM=<nodename>;NodeType=Cicm	qualityOfService	BHHCA Critical Alarm	BHHCA is well above Maximum Limit. Calls will be Throttled.

CICM803	Alarm_Trap_to_IEMS	bhhcaCriticalAlarm Clear	None	CICM=<nodename>;NodeT ype=Cicm	qualityOfService	BHHCA Critical Alarm	BHHCA is well above Maximum Limit. Calls will be Throttled.
CICM804	Alarm_Trap_to_IEMS	registryFlushAlarm	Minor	CICM=<nodename>;NodeT ype=Platform	equipment	Registry Flush Minor Alarm	Registry has not been flushed for 1 hour. Registry data could be lost if power outage occurs.
CICM804	Alarm_Trap_to_IEMS	registryFlushAlarm Clear	None	CICM=<nodename>;NodeT ype=Platform	equipment	Registry Flush Minor Alarm	Registry has not been flushed for 1 hour. Registry data could be lost if power outage occurs.

Appendix G: Ethernet Routing Switch 8600 Trap List

```

<?xml version="1.0" encoding="ISO-8859-1" ?>
_ <!--
    severity = 6|5|4|3|2|1
    Critical = 1
    Major = 2
    Minor = 3
    Warning = 4
    Clear = 5
    Info = 6
-->
_ <TRAPS>
_ <TRAP oid=".1.3.6.1.2.1.16.0.1" name="risingAlarm">
_ <PROPERTIES>
<eventprop name="severity" value="3" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="310" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="qualityOfService" />
<eventprop name="entity" value="$ip_alarmStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; alarmIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Threshold crossed." />
<eventprop name="description" value="Threshold Crossed: alarmIndex= $1( Threshold=
$2 alarmValue= $3)" />
<eventprop name="specificProblem" value="Rising threshold crossed" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.2.1.16.3.1.1.1" property="$1" />
<varbind name=".1.3.6.1.2.1.16.3.1.1.7" property="$2" />
<varbind name=".1.3.6.1.2.1.16.3.1.1.5" property="$3" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.2.1.16.0.2" name="fallingAlarm">
_ <PROPERTIES>
<eventprop name="severity" value="5" />

```

```
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="311" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="qualityOfService" />
<eventprop name="entity" value="$ip_alarmStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; alarmIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Threshold crossed" />
<eventprop name="description" value="Threshold Crossed: alarmIndex = $1( Threshold =
$2 alarmValue = $3)" />
<eventprop name="specificProblem" value="Falling threshold crossed" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.2.1.16.3.1.1.1" property="$1" />
<varbind name=".1.3.6.1.2.1.16.3.1.1.8" property="$2" />
<varbind name=".1.3.6.1.2.1.16.3.1.1.5" property="$3" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.6.3.1.1.5.1.0" name="coldStart">
_ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="313" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="operator" />
<eventprop name="entity" value="$ip_coldStart" />
<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Agent reinitialized itself with default settings"
/>
<eventprop name="description" value="A coldStart trap signifies that the snmp agent is
reinitializing itself with default settings." />
<eventprop name="specificProblem" value="Agent reinitialized itself with default settings"
/>
</PROPERTIES>
```



```
</TRAP>
_ <TRAP oid=".1.3.6.1.6.3.1.1.5.2.0" name="warmStart">
_ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="315" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="operator" />
<eventprop name="entity" value="$ip_warmstart" />
<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Agent reinitialized itself with its configuration
unaltered." />
<eventprop name="description" value="A warmStart trap signifies that the SNMPv2 agent
is reinitializing itself such that its configuration is unaltered." />
<eventprop name="specificProblem" value="Agent reinitialized itself with its configuration
unaltered." />
</PROPERTIES>
</TRAP>
_ <TRAP oid=".1.3.6.1.6.3.1.1.5.3.0" name="linkDown">
_ <PROPERTIES>
<eventprop name="severity" value="2" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="317" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_linkStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; ifIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="loss of communication" />
<eventprop name="description" value="Link Down: ifIndex = $1( AdminStatus = $2
OperationStatus = $3 $X)" />
<eventprop name="specificProblem" value="Generic Link Status" />
</PROPERTIES>
_ <VARBINDS>
```

```
<varbind name=".1.3.6.1.2.1.2.2.1.1" property="$1" />
<varbind name=".1.3.6.1.2.1.2.2.1.7" property="$2" />
<varbind name=".1.3.6.1.2.1.2.2.1.8" property="$3" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.6.3.1.1.5.4.0" name="linkUp">
_ <PROPERTIES>
<eventprop name="severity" value="5" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="318" />
<eventprop name="event'Type" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_linkStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; ifIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="communication regained" />
<eventprop name="description" value="Link Up: ifIndex = $1( AdminStatus = $2
OperationStatus = $3 $X)" />
<eventprop name="specificProblem" value="Generic Link Status" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.2.1.2.2.1.1" property="$1" />
<varbind name=".1.3.6.1.2.1.2.2.1.7" property="$2" />
<varbind name=".1.3.6.1.2.1.2.2.1.8" property="$3" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.6.3.1.1.5.5.0" name="authenticationFailure">
_ <PROPERTIES>
<eventprop name="severity" value="4" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="319" />
<eventprop name="event'Type" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="security" />
<eventprop name="entity" value="$ip_authenticationFailure" />
```

```

<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="6" />
<eventprop name="probableCause" value="Authentication failure" />
<eventprop name="description" value="Authentication failure occurred" />
<eventprop name="specificProblem" value="Authentication failure" />
</PROPERTIES>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.6" name="rcnChasPowerSupplyDown">
_ <PROPERTIES>
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="322" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_rcnSupplyStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; SupplyId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Power Supply down" />
<eventprop name="description" value="Power Supply Status: SupplyId = $1(
OperationStatus = $2 )" />
<eventprop name="specificProblem" value="Power Supply Status" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.4.8.1.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.4.8.1.1.2" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.6" name="rcChasPowerSupplyDown">
_ <PROPERTIES>
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="322" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />

```

```
<eventprop name="entity" value="$ip_rcSupplyStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; SupplyId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Power supply down" />
<eventprop name="description" value="Power Supply Status: SupplyId = $1(
OperationStatus = $2 )" />
<eventprop name="specificProblem" value="Power Supply Status" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.4.8.1.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.4.8.1.1.2" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.14" name="rcChasPowerSupplyUp">
_ <PROPERTIES>
<eventprop name="severity" value="5" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="323" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_rcSupplyStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; SupplyId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Power supply up" />
<eventprop name="description" value="Power Supply Status: SupplyId = $1(
OperationStatus = $2 )" />
<eventprop name="specificProblem" value="Power Supply Status" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.4.8.1.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.4.8.1.1.2" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.14" name="rcnChasPowerSupplyUp">
_ <PROPERTIES>
```

```
<eventprop name="severity" value="5" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="323" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_rcnSupplyStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; SupplyId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Power supply up" />
<eventprop name="description" value="Power Supply Status: SupplyId = $1(
OperationStatus = $2 )" />
<eventprop name="specificProblem" value="Power Supply Status" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.4.8.1.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.4.8.1.1.2" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.7" name="rcnChasFanDown">
_ <PROPERTIES>
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="324" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_rcnFanStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; fanId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Fan status down" />
<eventprop name="description" value="Fan Down: fanId= $1( OperationStatus = $2 )" />
<eventprop name="specificProblem" value="Fan down" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.4.7.1.1.1" property="$1" />
```

```
<varbind name=".1.3.6.1.4.1.2272.1.4.7.1.1.2" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.7" name="rcChasFanDown">
_ <PROPERTIES>
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="324" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_rcFanStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; fanId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Fan Status Down" />
<eventprop name="description" value="Fan Down: fanId= $1( OperationStatus = $2 )" />
<eventprop name="specificProblem" value="Fan down" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.4.7.1.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.4.7.1.1.2" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.21" name="rcnChasFanUp">
_ <PROPERTIES>
<eventprop name="severity" value="5" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="325" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_rcnFanStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; fanId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Fan Status Up" />
<eventprop name="description" value="Fan Up: fanId= $1( OperationStatus = $2 )" />
```

```
<eventprop name="specificProblem" value="Fan Up" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.4.7.1.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.4.7.1.1.2" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.21" name="rcChasFanUp">
_ <PROPERTIES>
<eventprop name="severity" value="5" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="325" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_rcFanStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; fanId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Fan Status Up" />
<eventprop name="description" value="Fan Up: fanId= $1( OperationStatus = $2 )" />
<eventprop name="specificProblem" value="Fan Up" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.4.7.1.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.4.7.1.1.2" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.11" name="rcn2kCardDown">
_ <PROPERTIES>
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="326" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_rcn2KCardStatus_$1" />
```

```
<eventprop name="componentID" value="ERS8600=$ip; cardIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Rc 2k Card Down" />
<eventprop name="description" value="Card Down: cardIndex = $1( AdminStatus = $2
OperationStatus = $3)" />
<eventprop name="specificProblem" value="RC 2k Card Status" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.100.6.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.100.6.1.4" property="$2" />
<varbind name=".1.3.6.1.4.1.2272.1.100.6.1.5" property="$3" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.11" name="rc2kCardDown">
_ <PROPERTIES>
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="326" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_rc2KCardStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; cardIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Rc 2k Card Down" />
<eventprop name="description" value="Card Down: cardIndex = $1( AdminStatus = $2
OperationStatus = $3)" />
<eventprop name="specificProblem" value="RC 2k Card Status" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.100.6.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.100.6.1.4" property="$2" />
<varbind name=".1.3.6.1.4.1.2272.1.100.6.1.5" property="$3" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.12" name="rcn2kCardUp">
```



```

_ <PROPERTIES>
<eventprop name="severity" value="5" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="327" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_rcn2KCardStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; cardIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Card status Up" />
<eventprop name="description" value="Card Up: cardIndex = $1( AdminStatus = $2
OperationStatus = $3)" />
<eventprop name="specificProblem" value="RC 2k Card Status" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.100.6.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.100.6.1.4" property="$2" />
<varbind name=".1.3.6.1.4.1.2272.1.100.6.1.5" property="$3" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.12" name="rc2kCardUp">
_ <PROPERTIES>
<eventprop name="severity" value="5" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="327" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_rc2KCardStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; cardIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Card Up" />
<eventprop name="description" value="Card Up: cardIndex = $1( AdminStatus = $2
OperationStatus = $3)" />
<eventprop name="specificProblem" value="RC 2K Card Status" />

```

```
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.100.6.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.100.6.1.4" property="$2" />
<varbind name=".1.3.6.1.4.1.2272.1.100.6.1.5" property="$3" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.13" name="rcn2kTemperature">
_ <PROPERTIES>
<eventprop name="severity" value="$1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="328" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_rcn2kTemperature" />
<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Over-heating of the chassis detected" />
<eventprop name="description" value="Chassis over-heating: rc2kChassisTemperature =
$1" />
<eventprop name="specificProblem" value="RC 2K Chassis Temperature" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.100.1.2" property="$1" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.3" name="rcnErrorNotification">
_ <PROPERTIES>
<eventprop name="severity" value="$1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="329" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="other" />
<eventprop name="entity" value="$ip_ErrorNotification" />
```

```
<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Error condition occurred" />
<eventprop name="description" value="Error occured: Error Level = $1( Error Code = $2
Error Text = $3) />
<eventprop name="specificProblem" value="RC 2K Error" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.20.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.20.2" property="$2" />
<varbind name=".1.3.6.1.4.1.2272.1.20.3" property="$3" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.8" name="rcnLinkOscillation">
_ <PROPERTIES>
<eventprop name="severity" value="2" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="330" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_linkOscillation_$1" />
<eventprop name="componentID" value="ERS8600=$ip; portIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Link Oscillation detected" />
<eventprop name="description" value="LinkOscillation: portIndex = $1" />
<eventprop name="specificProblem" value="RC Link Oscillation" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.4.10.1.1.1" property="$1" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.9" name="rcnMacViolation">
_ <PROPERTIES>
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />
```

```
<eventprop name="logNumber" value="331" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="other" />
<eventprop name="entity" value="$ip_MacViolation_$1" />
<eventprop name="componentID" value="ERS8600=$ip; portIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="RC Mac Violation" />
<eventprop name="description" value="RC Mac Violation: portIndex= $1( rcErrorText =
$2)" />
<eventprop name="specificProblem" value="RC Mac violation" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.4.10.1.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.20.3" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.10" name="rcnSonetTrap">
_ <PROPERTIES>
<eventprop name="severity" value="4" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="332" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="other" />
<eventprop name="entity" value="$ip_SonetTrap_$1" />
<eventprop name="componentID" value="ERS8600=$ip; portIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Sonet port status change" />
<eventprop name="description" value="Sonet Trap: portIndex = $1( TrapType = $2
TrapIndication = $3)" />
<eventprop name="specificProblem" value="Sonet port status change" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.4.10.1.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.26.5.1" property="$2" />
```

```
<varbind name=".1.3.6.1.4.1.2272.1.26.5.2" property="$3" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.4" name="rcnStpNewRoot">
_ <PROPERTIES>
<eventprop name="severity" value="4" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="333" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="other" />
<eventprop name="entity" value="$ip_StpNewRoot_$1" />
<eventprop name="componentID" value="ERS8600=$ip; stgId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Stp New Root" />
<eventprop name="description" value="Stp New Root: stgId = $1" />
<eventprop name="specificProblem" value="Stp New Root" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.13.4.1.1" property="$1" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.5" name="rcnStpTopologyChange">
_ <PROPERTIES>
<eventprop name="severity" value="4" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="334" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="other" />
<eventprop name="entity" value="$ip_StpTopoChange_$1" />
<eventprop name="componentID" value="ERS8600=$ip; stgId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Stp Topology change" />
<eventprop name="description" value="Stp Topology change: stgId= $1( portIndex = $2)" />
/>
```

```
<eventprop name="specificProblem" value="Stp Topology change" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.13.4.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.4.10.1.1" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.16" name="rcnStpTCN">
_ <PROPERTIES>
<eventprop name="severity" value="4" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="335" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="other" />
<eventprop name="entity" value="$ip_StpTCN_$1" />
<eventprop name="componentID" value="ERS8600=$ip; portIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Stp TCN" />
<eventprop name="description" value="Stp TCN: portIndex= $1( stgId= $2
BridgeAddress= $3)" />
<eventprop name="specificProblem" value="Stp TCN" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.4.10.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.13.4.1.1" property="$2" />
<varbind name=".1.3.6.1.4.1.2272.1.13.4.1.4" property="$3" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.15" name="rcn2kAtmPvcLinkStateChange">
_ <PROPERTIES>
<eventprop name="severity" value="$4" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="336" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
```

```
<eventprop name="category" value="environmental" />
<eventprop name="entity" value="$ip_LinkState_$1" />
<eventprop name="componentID" value="ERS8600=$ip; rc2kAtmPvcIfIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="PVC link status change" />
<eventprop name="description" value="Atm Pvc Link State Change: AtmPvcIfIndex = $1(
AtmPvcVpi = $2 AtmPvcVci = $3 AtmPvcOamVcStatus = $4)" />
<eventprop name="specificProblem" value="PVC link status change" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.100.9.3.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.100.9.3.1.2" property="$2" />
<varbind name=".1.3.6.1.4.1.2272.1.100.9.3.1.3" property="$3" />
<varbind name=".1.3.6.1.4.1.2272.1.100.9.3.1.18" property="$4" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.17" name="rcnSmltIstLinkUp">
_ <PROPERTIES>
<eventprop name="severity" value="5" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="337" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="other" />
<eventprop name="entity" value="$ip_SplitLinkStatus" />
<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Split MLT link status up" />
<eventprop name="description" value="Split MLT link status up" />
<eventprop name="specificProblem" value="Split MLT link status up" />
</PROPERTIES>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.18" name="rcnSmltIstLinkDown">
_ <PROPERTIES>
<eventprop name="severity" value="2" />
<eventprop name="logName" value="PP" />
```

```
<eventprop name="logNumber" value="338" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="other" />
<eventprop name="entity" value="$ip_SplitLinkStatus" />
<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Split MLT Link Status Down" />
<eventprop name="description" value="Split MLT Link Status Down" />
<eventprop name="specificProblem" value="Split MLT Link Status Down" />
</PROPERTIES>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.19" name="rcnSmltLinkUp">
_ <PROPERTIES>
<eventprop name="severity" value="5" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="339" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="other" />
<eventprop name="entity" value="$ip_rcnSmltLinkStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; rcMltSmltId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Split SMLT link up" />
<eventprop name="description" value="Split SMLT link up: rcMltSmltId = $1" />
<eventprop name="specificProblem" value="Split SMLT Link status" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.17.10.1.13" property="$1" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.19" name="rcSmltLinkUp">
_ <PROPERTIES>
<eventprop name="severity" value="5" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="339" />
```



```
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="other" />
<eventprop name="entity" value="$ip_rcSmltLinkStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; rcMltSmltId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Split SMLT link up" />
<eventprop name="description" value="Split SMLT link up: rcMltSmltId = $1" />
<eventprop name="specificProblem" value="Split SMLT Link status" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.17.10.1.13" property="$1" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.20" name="rcnSmltLinkDown">
_ <PROPERTIES>
<eventprop name="severity" value="2" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="340" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="other" />
<eventprop name="entity" value="$ip_rcnSmltLinkStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; rcMltSmltId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Split SMLT Link down" />
<eventprop name="description" value="Split SMLT link down: rcMltSmltId = $1" />
<eventprop name="specificProblem" value="Split SMLT link status" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.17.10.1.13" property="$1" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.20" name="rcSmltLinkDown">
_ <PROPERTIES>
<eventprop name="severity" value="2" />
```

```
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="340" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="other" />
<eventprop name="entity" value="$ip_rcSmltLinkStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; rcMltSmltId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Split SMLT link down" />
<eventprop name="description" value="Split SMLT link down: rcMltSmltId = $1" />
<eventprop name="specificProblem" value="Split SMLT Link status" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.17.10.1.13" property="$1" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.22" name="rcnPasswordChange">
_ <PROPERTIES>
<eventprop name="severity" value="4" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="341" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="security" />
<eventprop name="entity" value="$ip_CLIPasswordChanged" />
<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="CLI password changed" />
<eventprop name="description" value="CLI password changed ( PasswordChange = $1
PassChangeResult = $2)" />
<eventprop name="specificProblem" value="CLI password has been changed" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.19.17" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.19.18" property="$2" />
</VARBINDS>
```

```
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.25" name="rcnPcmciaCardRemoved">
_ <PROPERTIES>
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="342" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_PCMCIARemoved" />
<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="PCMCIA card is being removed." />
<eventprop name="description" value="PCMCIA card is being removed." />
<eventprop name="specificProblem" value="PCMCIA card removed." />
</PROPERTIES>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.26" name="rcnSmartCpldTimerFired">
_ <PROPERTIES>
<eventprop name="severity" value="2" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="343" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_cpldTimerFired_$1" />
<eventprop name="componentID" value="ERS8600=$ip; CardIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="cpld timer fired" />
<eventprop name="description" value="cpld timer fired: CardIndex = $1" />
<eventprop name="specificProblem" value="cpld timer fired" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.100.6.1.1" property="$1" />
</VARBINDS>
</TRAP>
```

```
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.27" name="rcnCardCpldNotUpDate">
_ <PROPERTIES>
<eventprop name="severity" value="2" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="344" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_cpldNotUpDate_$1" />
<eventprop name="componentID" value="ERS8600=$ip; CardIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="cpld is not up to date" />
<eventprop name="description" value="cpld is not up to date: CardIndex = $1" />
<eventprop name="specificProblem" value="cpld not up to date" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.100.6.1.1" property="$1" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.28" name="rcnIgapLogFileFull">
_ <PROPERTIES>
<eventprop name="severity" value="2" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="345" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="processingError" />
<eventprop name="entity" value="$ip_IgapLogFileFull" />
<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Igap Log file full" />
<eventprop name="description" value="Igap accounting time-out Log File reach the
maximum." />
<eventprop name="specificProblem" value="Igap Log file full" />
</PROPERTIES>
</TRAP>
```

```
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.29" name="rcnCpLimitShutDown">
_ <PROPERTIES>
<eventprop name="severity" value="2" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="346" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_CPLimitShutDown_$1" />
<eventprop name="componentID" value="ERS8600=$ip; PortIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="cp limit for the port is shutting down" />
<eventprop name="description" value="Cp limit for port is shutting down: PortIndex= $1(
AdminStatus = $2 OperStatus = $3 CpLimitShutDown = $4)" />
<eventprop name="specificProblem" value="cp limit for the port is shutting down" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.4.10.1.1" property="$1" />
<varbind name=".1.3.6.1.2.1.2.2.1.7" property="$2" />
<varbind name=".1.3.6.1.2.1.2.2.1.8" property="$3" />
<varbind name=".1.3.6.1.4.1.2272.1.4.10.1.1.50" property="$4" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.30" name="rcnSshServerEnabled">
_ <PROPERTIES>
<eventprop name="severity" value="5" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="347" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_SshServerStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; SshGlobalPort=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="SSH server is enabled" />
<eventprop name="description" value="SSH server is enabled: SshGlobalPort = $1" />
```

```
<eventprop name="specificProblem" value="SSH server enabled" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.34.1.2" property="$1" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.31" name="rcnSshServerDisabled">
_ <PROPERTIES>
<eventprop name="severity" value="2" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="348" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_SshServerStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; SshGlobalPort=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="SSH server is disabled" />
<eventprop name="description" value="SSH server is disabled: SshGlobalPort = $1" />
<eventprop name="specificProblem" value="SSH server disabled" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.34.1.2" property="$1" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.32" name="rcnSshSessionLogin">
_ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="349" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_SshSessionStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; SshGlobalHostIpAddr=$1" />
<eventprop name="alarmClear" value="3" />
```

```
<eventprop name="probableCause" value="SSH Session login" />
<eventprop name="description" value="SSH session login occurred: SshGlobalHostIpAddr
= $1" />
<eventprop name="specificProblem" value="SSH Session login" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.34.1.12" property="$1" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.33" name="rcnSshSessionLogout">
_ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="350" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_SshSessionStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; SshGlobalHostIpAddr=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="SSH session logout" />
<eventprop name="description" value="SSH session logout occurred: SshGlobalHostIpAddr
= $1" />
<eventprop name="specificProblem" value="SSH session logout" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.34.1.12" property="$1" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.34" name="rcnSshUnauthorizedAccess">
_ <PROPERTIES>
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="351" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
```

```
<eventprop name="category" value="security" />
<eventprop name="entity" value="$ip_SshUnauthorizedAccess_$1" />
<eventprop name="componentID" value="ERS8600=$ip; SshGlobalHostIpAddr=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Unauthorized access" />
<eventprop name="description" value="Unauthorized access occurred:
SshGlobalHostIpAddr = $1" />
<eventprop name="specificProblem" value="Unauthorized access" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.34.1.12" property="$1" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.35" name="rcnHaCpuState">
_ <PROPERTIES>
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="352" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_HaCpuState_$1" />
<eventprop name="componentID" value="ERS8600=$ip; CardIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="State of the HA-CPU" />
<eventprop name="description" value="State of the HA-CPU: CardIndex = $1 (HaCpuState
= $2)" />
<eventprop name="specificProblem" value="State of the HA-CPU" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.100.6.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.32.1" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.36" name="rcnInsufficientMemory">
_ <PROPERTIES>
```



```
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="353" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="environmental" />
<eventprop name="entity" value="$ip_InsufficientMemory_$1" />
<eventprop name="componentID" value="ERS8600=$ip; CardIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Insufficient memory on CPU blade for proper
operation" />
<eventprop name="description" value="Insufficient memory: CardIndex = $1" />
<eventprop name="specificProblem" value="Insufficient memory on CPU" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.100.6.1.1" property="$1" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.37" name="rcnSaveConfigAction">
_ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="354" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="processingError" />
<eventprop name="entity" value="$ip_SaveConfig" />
<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Switch run time or boot configuration is saved"
/>
<eventprop name="description" value="Switch configuration saved: SysAction = $1" />
<eventprop name="specificProblem" value="Switch configuration saved" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.1.8" property="$1" />
```

```
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.38" name="rcnLoopDetectOnPort">
_ <PROPERTIES>
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="355" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_LoopOnPort_$1" />
<eventprop name="componentID" value="ERS8600=$ip; PortIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Loop detected on port. The vlan on that port
will be disabled" />
<eventprop name="description" value="Loop detected on port: PortIndex = $1 (rcVlanId =
$2)" />
<eventprop name="specificProblem" value="Loop detected on port." />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.4.10.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.3.2.1.1" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.2.1.46.1.3.0.3.0" name="vrrpTrapStateTransition">
_ <PROPERTIES>
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="356" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_TrapStateTransition_$1" />
<eventprop name="componentID" value="ERS8600=$ip; ifIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="State transition has occurred on vrrp interface"
/>
```

```
<eventprop name="description" value="State Transition: ifIndex = $1 (TransitionType = $2
TransitionCause = $3 $X)" />
<eventprop name="specificProblem" value="Trap state transition" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.2.1.2.2.1.1" property="$1" />
<varbind name=".1.3.6.1.2.1.46.1.1.14" property="$2" />
<varbind name=".1.3.6.1.2.1.46.1.1.15" property="$3" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.23" name="rcnEmError">
_ <PROPERTIES>
<eventprop name="severity" value="4" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="357" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_EmError_$1" />
<eventprop name="componentID" value="ERS8600=$ip; CardIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Em error detected" />
<eventprop name="description" value="Em error: CardIndex = $1 (Em Error = $2)" />
<eventprop name="specificProblem" value="Em error detected" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.100.6.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.4.23" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.2.1.14.16.2.1" name="ospfVirtIfStateChange">
_ <PROPERTIES>
<eventprop name="severity" value="$4" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="358" />
<eventprop name="eventType" value="TBL" />
```

```
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="environmental" />
<eventprop name="entity" value="$ip_IfStateChange_$1" />
<eventprop name="componentID" value="ERS8600=$ip; ospfRouterId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="OSPF virtual interface state change" />
<eventprop name="description" value="OSPF virtual interface state change: ospfRouterId
= $1 (AreaId = $2 Neighbor = $3 State = $4)" />
<eventprop name="specificProblem" value="OSPF virtual interface state change" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.2.1.14.1.1" property="$1" />
<varbind name=".1.3.6.1.2.1.14.9.1.1" property="$2" />
<varbind name=".1.3.6.1.2.1.14.9.1.2" property="$3" />
<varbind name=".1.3.6.1.2.1.14.9.1.7" property="$4" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.2.1.14.16.2.2" name="ospfNbrStateChange">
_ <PROPERTIES>
<eventprop name="severity" value="$4" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="359" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_NbrStateChange_$1_$3" />
<eventprop name="componentID" value="ERS8600=$ip; ospfRouterId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Non-virtual neighbor state change" />
<eventprop name="description" value="Non-virtual neighbor state change: RouterId = $1
(NbrIpAddr = $2 NbrRouter = $3 State = $4)" />
<eventprop name="specificProblem" value="Non-virtual OSPF neighbor state change" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.2.1.14.1.1" property="$1" />
<varbind name=".1.3.6.1.2.1.14.10.1.1" property="$2" />
```

```
<varbind name=".1.3.6.1.2.1.14.10.1.3" property="$3" />
<varbind name=".1.3.6.1.2.1.14.10.1.6" property="$4" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.2.1.14.16.2.3" name="ospfVirtNbrStateChange">
_ <PROPERTIES>
<eventprop name="severity" value="$4" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="360" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="environmental" />
<eventprop name="entity" value="$ip_VirtNbrStateChange_$1_$3" />
<eventprop name="componentID" value="ERS8600=$ip; ospfRouterId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Virtual OSPF neighbor state change" />
<eventprop name="description" value="Virtual neighbor state change: RouterId = $1
(NbrArea = $2 NbrRouter = $3 State = $4)" />
<eventprop name="specificProblem" value="Virtual OSPF neighbor state change" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.2.1.14.1.1" property="$1" />
<varbind name=".1.3.6.1.2.1.14.11.1.1" property="$2" />
<varbind name=".1.3.6.1.2.1.14.11.1.2" property="$3" />
<varbind name=".1.3.6.1.2.1.14.11.1.5" property="$4" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.2.1.14.16.2.4" name="ospfIfConfigError">
_ <PROPERTIES>
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="361" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_IfConfigError" />
```

```
<eventprop name="componentID" value="ERS8600=$ip; ospfRouterId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Configuration error" />
<eventprop name="description" value="IfConfig Error: ospfRouterId = $1 (IpAddress =
$2)" />
<eventprop name="specificProblem" value="configuration error" />
</PROPERTIES>
┌ <VARBINDS>
<varbind name=".1.3.6.1.2.1.14.1.1" property="$1" />
<varbind name=".1.3.6.1.2.1.14.7.1.1" property="$2" />
</VARBINDS>
</TRAP>
┌ <TRAP oid=".1.3.6.1.2.1.14.16.2.5" name="ospfVirtIfConfigError">
┌ <PROPERTIES>
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="362" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_VirtIfConfigError_$1" />
<eventprop name="componentID" value="ERS8600=$ip; ospfRouterId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Virtual interface configuration error" />
<eventprop name="description" value="VirtIfConfigError: ospfRouterId = $1 (AreaId = $2
Neighbor = $3 ErrorType =$4 )" />
<eventprop name="specificProblem" value="Virtual interface configuration error" />
</PROPERTIES>
┌ <VARBINDS>
<varbind name=".1.3.6.1.2.1.14.1.1" property="$1" />
<varbind name=".1.3.6.1.2.1.14.9.1.1" property="$2" />
<varbind name=".1.3.6.1.2.1.14.9.1.2" property="$3" />
<varbind name=".1.3.6.1.2.1.14.16.1.2" property="$4" />
</VARBINDS>
</TRAP>
┌ <TRAP oid=".1.3.6.1.2.1.14.16.2.6" name="ospfIfAuthFailure">
```

```
_ <PROPERTIES>
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="363" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="security" />
<eventprop name="entity" value="$ip_IfAuthFailure_$1" />
<eventprop name="componentID" value="ERS8600=$ip; ospfRouterId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="ospf If authentication failure" />
<eventprop name="description" value="ospf If authentication failure: ospfRouterId = $1
(ConfigErrorType =$2)" />
<eventprop name="specificProblem" value="ospf If authentication failure" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.2.1.14.1.1" property="$1" />
<varbind name=".1.3.6.1.2.1.14.16.1.2" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.2.1.14.16.2.7" name="ospfVirtIfAuthFailure">
_ <PROPERTIES>
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="364" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="security" />
<eventprop name="entity" value="$ip_VirtIfAuthFailure_$1" />
<eventprop name="componentID" value="ERS8600=$ip; ospfRouterId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="ospf virtual interface authentication failure" />
<eventprop name="description" value="ospfVirtIfAuthFailure: ospfRouterId = $1 (AreaId
= $2 Neighbor = $3 ErrorType =$4 )" />
<eventprop name="specificProblem" value="" />
</PROPERTIES>
```

```
_ <VARBINDS>
<varbind name=".1.3.6.1.2.1.14.1.1" property="$1" />
<varbind name=".1.3.6.1.2.1.14.9.1.1" property="$2" />
<varbind name=".1.3.6.1.2.1.14.9.1.2" property="$3" />
<varbind name=".1.3.6.1.2.1.14.16.1.2" property="$4" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.2.1.14.16.2.16" name="ospfIfStateChange">
_ <PROPERTIES>
<eventprop name="severity" value="$3" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="365" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_ifStateChange_$1_$2" />
<eventprop name="componentID" value="ERS8600=$ip; ospfRouterId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Non-virtual OSPF interface state change" />
<eventprop name="description" value="Non-virtual OSPF interface state change:
ospfRouterId = $1 (IpAddress = $2 State =$3)" />
<eventprop name="specificProblem" value="Non-virtual OSPF interface state change" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.2.1.14.1.1" property="$1" />
<varbind name=".1.3.6.1.2.1.14.7.1.1" property="$2" />
<varbind name=".1.3.6.1.2.1.14.7.1.12" property="$3" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.1" name="rcnCardDown">
_ <PROPERTIES>
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="366" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
```



```
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_rcnCardStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; rcCardIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="RC Card status down" />
<eventprop name="description" value="RC card status down: CardIndex = $1
(AdminStatus = $2 OperStatus = $3)" />
<eventprop name="specificProblem" value="RC Card status" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.4.9.1.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.4.9.1.1.5" property="$2" />
<varbind name=".1.3.6.1.4.1.2272.1.4.9.1.1.6" property="$3" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.1" name="rcCardDown">
_ <PROPERTIES>
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="366" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_rcCardStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; rcCardIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="RC Card Status down." />
<eventprop name="description" value="RC card status down: CardIndex = $1
(AdminStatus = $2 OperStatus = $3)" />
<eventprop name="specificProblem" value="RC Card Status" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.4.9.1.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.4.9.1.1.5" property="$2" />
<varbind name=".1.3.6.1.4.1.2272.1.4.9.1.1.6" property="$3" />
</VARBINDS>
```

```
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.2" name="rcnCardUp">
_ <PROPERTIES>
<eventprop name="severity" value="5" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="367" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_rcnCardStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; rcCardIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="RC card status up" />
<eventprop name="description" value="RC card status up: CardIndex = $1 (AdminStatus
= $2 OperStatus = $3)" />
<eventprop name="specificProblem" value="RC Card Status" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.4.9.1.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.4.9.1.1.5" property="$2" />
<varbind name=".1.3.6.1.4.1.2272.1.4.9.1.1.6" property="$3" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.2" name="rcCardUp">
_ <PROPERTIES>
<eventprop name="severity" value="5" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="367" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_rcCardStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; rcCardIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="RC card status up" />
<eventprop name="description" value="RC card status up: CardIndex = $1 (AdminStatus
```

```

= $2 OperStatus = $3)" />
<eventprop name="specificProblem" value="RC Card Status" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.4.9.1.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.4.9.1.1.5" property="$2" />
<varbind name=".1.3.6.1.4.1.2272.1.4.9.1.1.6" property="$3" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.39" name="rcnbgpEstablished">
_ <PROPERTIES>
<eventprop name="severity" value="5" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="368" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_bgpLinkStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; rcIpBgpPeerIpAddress=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="BGP FSM entered the ESTABLISHED state"
/>
<eventprop name="description" value="BGP FSM entered ESTABLISHED state:
PeerIpAddress = $1 (PeerLastError = $2 PeerState = $3)" />
<eventprop name="specificProblem" value="BGP FSM entered the ESTABLISHED state"
/>
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.8.101.9.1.2" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.8.101.9.1.26" property="$2" />
<varbind name=".1.3.6.1.4.1.2272.1.8.101.9.1.25" property="$3" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.40" name="rcnbgpBackwardTransition">
_ <PROPERTIES>
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />

```

```
<eventprop name="logNumber" value="369" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_bgpLinkStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; rcIpBgpPeerIpAddress=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="BGP FSM backward transition" />
<eventprop name="description" value="BGP FSM backward transition: PeerIpAddress =
$1 (PeerLastError = $2 PeerState = $3)" />
<eventprop name="specificProblem" value="BGP FSM backward transition" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.8.101.9.1.2" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.8.101.9.1.26" property="$2" />
<varbind name=".1.3.6.1.4.1.2272.1.8.101.9.1.25" property="$3" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.41" name="rcnAggLinkUp">
_ <PROPERTIES>
<eventprop name="severity" value="5" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="370" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_AggLinkStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; rcMltId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Aggregator up" />
<eventprop name="description" value="Aggregator up: rcMltId = $1" />
<eventprop name="specificProblem" value="Aggregator status" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.17.10.1.1" property="$1" />
</VARBINDS>
```

```
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.42" name="rcnAggLinkDown">
_ <PROPERTIES>
<eventprop name="severity" value="2" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="371" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_AggLinkStatus_$1" />
<eventprop name="componentID" value="ERS8600=$ip; rcMltId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Aggregator Down" />
<eventprop name="description" value="Aggregator Down: rcMltId = $1" />
<eventprop name="specificProblem" value="Aggregator status" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.17.10.1.1" property="$1" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.43" name="rcnIgmpNewGroupMember">
_ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="372" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_GroupMember_$1" />
<eventprop name="componentID" value="ERS8600=$ip; rcIgmpGroupIfIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="New Group member in interface" />
<eventprop name="description" value="New Group member in interface:
rcIgmpGroupIfIndex = $1 (GroupIpAddress = $2 Port = $3 Members $4)" />
<eventprop name="specificProblem" value="New Group member in interface" />
</PROPERTIES>
```

```
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.8.6.1.5" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.8.6.1.1" property="$2" />
<varbind name=".1.3.6.1.4.1.2272.1.8.6.1.3" property="$3" />
<varbind name=".1.3.6.1.4.1.2272.1.8.6.1.2" property="$4" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.44" name="rcnIgmpLossGroupMember">
_ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="373" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_GroupMember_$1" />
<eventprop name="componentID" value="ERS8600=$ip; rcIgmpGroupIfIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Group member lost on interface" />
<eventprop name="description" value="Group member lost on interface:
rcIgmpGroupIfIndex = $1 (GroupIpAddress = $2 Port = $3 Members $4)" />
<eventprop name="specificProblem" value="Group member lost on interface" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.8.6.1.5" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.8.6.1.1" property="$2" />
<varbind name=".1.3.6.1.4.1.2272.1.8.6.1.3" property="$3" />
<varbind name=".1.3.6.1.4.1.2272.1.8.6.1.2" property="$4" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.45" name="rcnIgmpNewQuerier">
_ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="374" />
<eventprop name="eventType" value="INFO" />
```

```
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_Querier_$1" />
<eventprop name="componentID" value="ERS8600=$ip; igmpInterfaceIfIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="New Querier in interface" />
<eventprop name="description" value="New Querier in interface: igmpInterfaceIfIndex =
$1 (igmpInterfaceQuerier = $2 )" />
<eventprop name="specificProblem" value="New Querier in interface" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.3.59.1.1.1.1.1" property="$1" />
<varbind name=".1.3.6.1.3.59.1.1.1.1.5" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.46" name="rcnIgmpQuerierChange">
_ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="375" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_QuerierChange_$1" />
<eventprop name="componentID" value="ERS8600=$ip; igmpInterfaceIfIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Querier changed" />
<eventprop name="description" value="Querier changed: igmpInterfaceIfIndex = $1 (
NewQuerier = $2 igmpInterfaceQuerier = $3 )" />
<eventprop name="specificProblem" value="Querier changed" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.3.59.1.1.1.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.30.1.1.25" property="$2" />
<varbind name=".1.3.6.1.3.59.1.1.1.1.5" property="$3" />
</VARBINDS>
```



```
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.47" name="rcnDvmrpIfStateChange">
_ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="376" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_DvmrpStateChange_$1" />
<eventprop name="componentID" value="ERS8600=$ip; dvmrpInterfaceIfIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="DVMRP interface state change" />
<eventprop name="description" value="DVMRP interface state change:
dvmrpInterfaceIfIndex = $1 (OperState = $2 )" />
<eventprop name="specificProblem" value="DVMRP interface state change" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.3.62.1.1.3.1.1" property="$1" />
<varbind name=".1.3.6.1.3.62.1.1.3.1.3" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.48" name="rcnDvmrpNewNbrChange">
_ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="377" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_NbrChange_$1" />
<eventprop name="componentID" value="ERS8600=$ip; dvmrpNeighborIfIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="New neighbor is up on DVMRP interface" />
<eventprop name="description" value="New neighbor is up on DVMRP interface:
dvmrpNeighborIfIndex = $1 (NeighborAddress = $2 )" />
```



```
<eventprop name="specificProblem" value="New neighbor is up on DVMRP interface" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.3.62.1.1.4.1.1" property="$1" />
<varbind name=".1.3.6.1.3.62.1.1.4.1.2" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.49" name="rcnDvmrpNbrLossChange">
_ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="378" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_NbrChange_$1" />
<eventprop name="componentID" value="ERS8600=$ip; dvmrpNeighborIfIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Neighbor gone down on DVMRP interface" />
<eventprop name="description" value="Neighbor gone down on DVMRP interface:
dvmrpNeighborIfIndex = $1 (NeighborAddress = $2 )" />
<eventprop name="specificProblem" value="Neighbor gone down on DVMRP interface" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.3.62.1.1.4.1.1" property="$1" />
<varbind name=".1.3.6.1.3.62.1.1.4.1.2" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.59" name="rcnFdbProtectViolation">
_ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="379" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
```

```
<eventprop name="entity" value="$ip_FdbProtect_$1_$2" />
<eventprop name="componentID" value="ERS8600=$ip; PortIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="fdb-entries limit violation" />
<eventprop name="description" value="fdb-entries limit violation: PortIndex = $1 (VlanId
= $2 )" />
<eventprop name="specificProblem" value="fdb-entries limit violation" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.4.10.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.3.2.1.1" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.60" name="rcnLogMsgControl">
_ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="380" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_Log" />
<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Log Message control trap" />
<eventprop name="description" value="rcnLogMsgControl: SysMsgLogFrequency = $1
(SysMsgLogText = $2 )" />
<eventprop name="specificProblem" value="Log Message control trap" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.1.66" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.1.67" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.61" name="rcnSaveConfigFile">
_ <PROPERTIES>
```

```
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="381" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_SaveConfig" />
<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Run time / boot config saved on switch" />
<eventprop name="description" value="Config saved on switch: SysAction = $1
(SysConfigFileName = $2 )" />
<eventprop name="specificProblem" value="Run time / boot config saved on switch" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.1.8" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.1.34" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.62" name="rcnDNSRequestResponse">
_ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="382" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_DNSResponse" />
<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Request/Response from DNS server" />
<eventprop name="description" value="Request sent to or response got from DNS server:
DnsServerListIpAddr = $1 (DnsRequestType = $2 )" />
<eventprop name="specificProblem" value="Request/Response from DNS server" />
</PROPERTIES>
_ <VARBINDS>
```

```
<varbind name=".1.3.6.1.4.1.2272.1.1.71" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.1.72" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.2.1.80.0.1.0" name="pingProbeFailed">
_ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="383" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_ProbeFailed" />
<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Probe failure is detected" />
<eventprop name="description" value="Probe failure is detected: (ping TargetAddress =
$1)" />
<eventprop name="specificProblem" value="Probe failure is detected" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.2.1.80.1.2.1.4" property="$1" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.2.1.80.0.2.0" name="pingTestFailed">
_ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="384" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_pingTestFail" />
<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Ping test failed" />
```

```
<eventprop name="description" value="Ping test failed: (ping TargetAddress = $1)" />
<eventprop name="specificProblem" value="Ping test failed" />
</PROPERTIES>
┌ <VARBINDS>
<varbind name=".1.3.6.1.2.1.80.1.2.1.4" property="$1" />
</VARBINDS>
</TRAP>
┌ <TRAP oid=".1.3.6.1.2.1.80.0.3.0" name="pingTestCompleted">
┌ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="385" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_pingTestComp" />
<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Ping test completed" />
<eventprop name="description" value="Ping test completed: (ping TargetAddress = $1)" />
<eventprop name="specificProblem" value="Ping test completed." />
</PROPERTIES>
┌ <VARBINDS>
<varbind name=".1.3.6.1.2.1.80.1.2.1.4" property="$1" />
</VARBINDS>
</TRAP>
┌ <TRAP oid=".1.3.6.1.2.1.81.0.1.0" name="traceRoutePathChange">
┌ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="386" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_traceRouteChange" />
<eventprop name="componentID" value="ERS8600=$ip" />
```

```
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="The path to a target has changed" />
<eventprop name="description" value="The path to a target has changed: (TargetAddress
= $1)" />
<eventprop name="specificProblem" value="The path to a target has changed" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.2.1.81.1.2.1.4" property="$1" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.2.1.81.0.2.0" name="traceRouteTestFailed">
_ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="387" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_RouteTestFail" />
<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Could not determine the path to a target" />
<eventprop name="description" value="Could not determine the path to a target:
(TargetAddress = $1)" />
<eventprop name="specificProblem" value="Could not determine the path to a target" />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.2.1.81.1.2.1.4" property="$1" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.2.1.81.0.3.0" name="traceRouteTestCompleted">
_ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="388" />
<eventprop name="eventType" value="INFO" />
```

```
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_RouteTestComplete" />
<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="The path to a target has just been determined." />
<eventprop name="description" value="The path to a target has just been determined: (TargetAddress = $1)" />
<eventprop name="specificProblem" value="The path to a target has just been determined." />
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.2.1.81.1.2.1.4" property="$1" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.562.42.5.1.3.2.2" name="UDPEapSessionEndTrap">
_ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="389" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="other" />
<eventprop name="entity" value="$ip_UDPEapSessionEnd" />
<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Session end trap" />
<eventprop name="description" value="UDPEapSession end trap" />
<eventprop name="specificProblem" value="Session end trap" />
</PROPERTIES>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.562.42.5.1.3.2.1" name="UDPEapSessionStartTrap">
_ <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="390" />
```

```
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="other" />
<eventprop name="entity" value="$ip_UDPEapSessionSart" />
<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Session start trap" />
<eventprop name="description" value="UDPEapSession start trap" />
<eventprop name="specificProblem" value="Session start trap" />
</PROPERTIES>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.63" name="rcnDuplicateIpAddress">
_ <PROPERTIES>
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="391" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_DuplicateIp" />
<eventprop name="componentID" value="ERS8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="More than one host with the same IP address
have been detected on a subnet." />
<eventprop name="description" value="Duplicate IP address detected on subnet:
NetAddress=$1 (PhysicalAddress=$2)" />
<eventprop name="specificProblem" value="Duplicate IP address detected on the subnet."
/>
</PROPERTIES>
_ <VARBINDS>
<varbind name=".1.3.6.1.2.1.4.22.1.3" property="$1" />
<varbind name=".1.3.6.1.2.1.4.22.1.2" property="$2" />
</VARBINDS>
</TRAP>
_ <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.64" name="rcnLoopDetectPortDown">
_ <PROPERTIES>
<eventprop name="severity" value="1" />
```

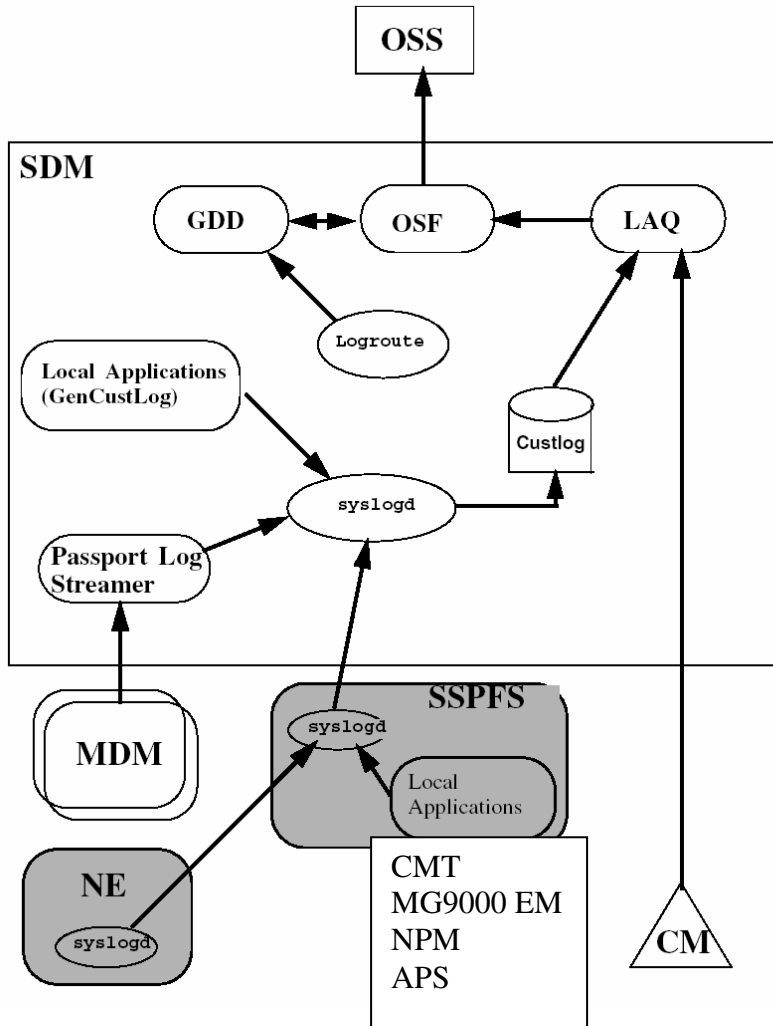


```
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="392" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_LoopDetect_$1" />
<eventprop name="componentID" value="ERS8600=$ip; portIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="A network configuration error is creating a
loop between ports in a vlan" />
<eventprop name="description" value="Loop detected on port: PortIndex=$1
(AdminStatus=$2 OperStatus=$3)" />
<eventprop name="specificProblem" value="Loop detected on a port and port is going to
shut down" />
</PROPERTIES>
<VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.4.10.1.1.1" property="$1" />
<varbind name=".1.3.6.1.2.1.2.2.1.7" property="$2" />
<varbind name=".1.3.6.1.2.1.2.2.1.8" property="$3" />
</VARBINDS>
</TRAP>

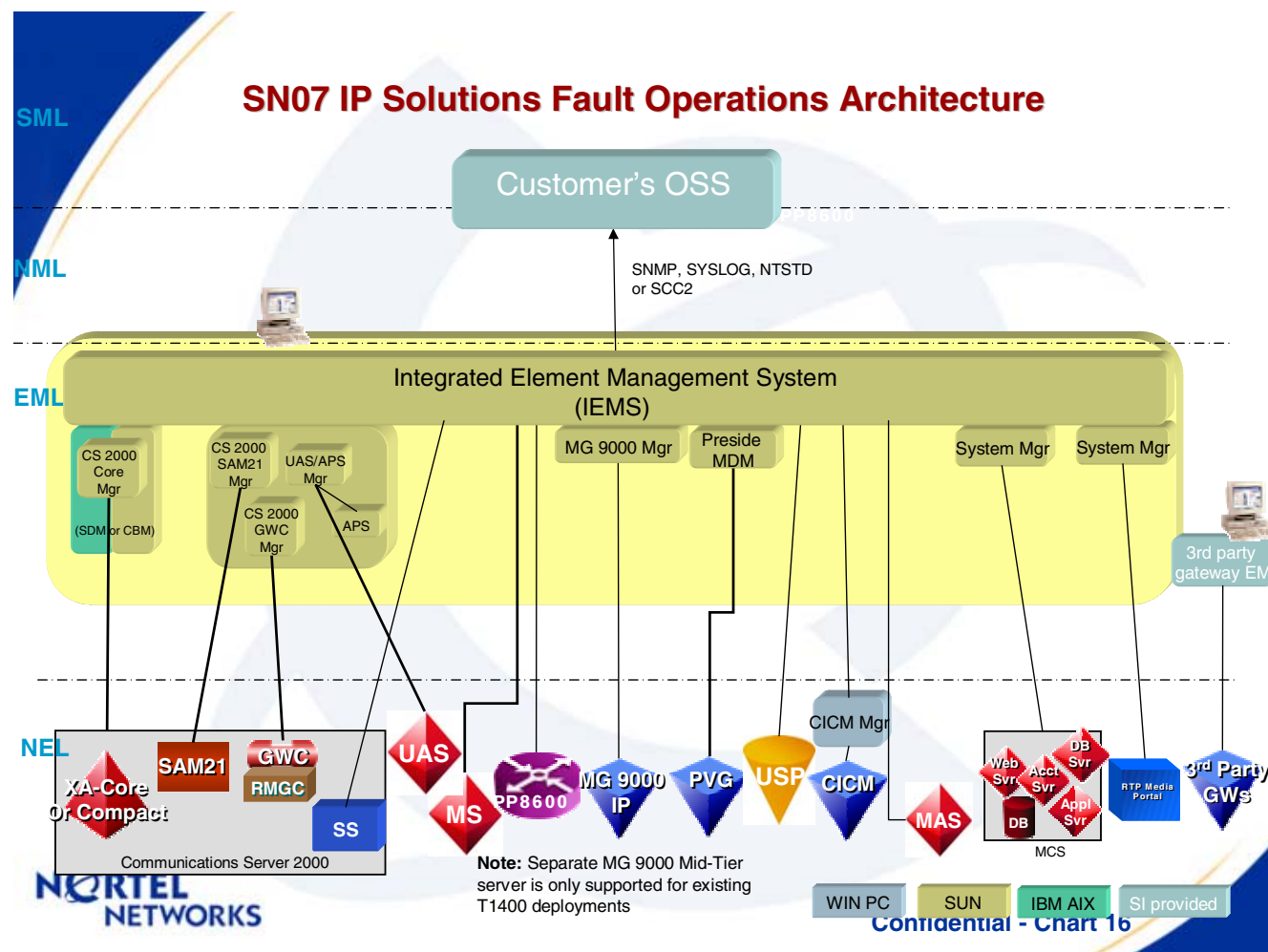
</TRAPS>
```

Appendix H: IEMS Fault Transparency with SDM/CBM

Prior to IEMS, which had its first Generally Available release in SN07, Succession supported sending faults and events from network elements via Syslog to the SDM/CBM. This feature, SYSLOG Consolidation for Succession, then allows the SDM/CBM to convert these logs to SCC2 or NTSTD to forward to the OSS. See the Figure below.



The fault feeds, delivered via IEMS supports SCC2 & NTSTD to the OSS, as did SDM/CBM. The implementation with IEMS used a more robust interfaces between the NE/EMS to IEMS and thus on a NE by NE basis there may be changes in the SCC2 log feed versus the SDM/CBM implementation. To understand fault diagram with IEMS see the diagram below.



This document is updated as new or changed information with respect to SDM/CBM and IEMS log transparency is learned. To understand the differences between the IEMS implementation and the SDM implementation see the tables below.

On NT STD and SCC2 Log Format Delimiters (SDM/CBM or IEMS to Fault OSS)

Table 1- ASCII Character Legend

ASCII Character Legend			
Character Name	Hexidecimal	Decimal	Control Character
Line Feed:	0A	10	^J
Carriage Return:	0D	13	^M
End of Message:	19	25	^Y
Null:	00	00	^@
Space:	20	32	space

Table 2 - STD and SCC2 Log Delimiter Comparison between SDM/CBM and IEMS

STD and SCC2 Log Delimiter Comparison Between SDM/CBM and IEMS					
Last Updated:		Sept. 8, 2005			
SDM/CBM Load:		SN07/SN08: final compile & patch current; SN09: pre final compile 22.18.1.0			
IEMS Load:		SN07/SN08: final compile & patch current; SN09: IEMS_090_0531_1			
Platform/Product:		SDM/CBM	IEMS	SDM/CBM	IEMS
Log Format:		STD/STD_OLD	STD	SCC2/SCC2_OLD	SCC2
Start of Log String:		0A 0D	0D (pre-SN09);	0A 0D	0A 0D
End of Line String:		0A 0D	0A 0D (SN09+)	0A 0D	0A 0D
End of Log String:		20 0A 0D 0A 0D 00	0A 0D 00 0A	0A 19 0A 0D	0A 0D 0A 19 0A

Comments on Table 2:

- The Log Delimiter String data applies to releases SN07 through to SN09 for the loads indicated as of the Last Updated date.
- **Last known change: IEMS NT STD Start of Log String has been changed from just 0D to 0A0D in SN09.**
- Previous change: IEMS SCC2 Start of Log String was changed to 0D to 0A0D to in SN09 and it was patched back to SN08 and SN07.
- Future changes: None planned. Through currently the End of Log String does differ between SDM/CBM and IEMS.
- The spaces between the hexadecimal numbers in Table 2 are there just to enhance readability. ie. 0D immediately follows 0A in the Start of Log String for SDM/CBM.
- In the SDM/CBM, the logroute interface allows customers to modify, if desired (but not recommended), the:
 - Start of Log String (default value: 0A 0D in hex)
 - End of Line String (default value: 0A 0D in hex) and the provisionable portions of the:

- End of Log String (default value: 20 0A 0D 0A 0D 00 where the first 0A 0D is the currently provisioned value in logroute for the End of Line string and the second 0A 0D sequence is the currently provisioned value logroute for the End of Log string.")
- The log delimiters of IEMS are not provisionable in any release as of the Last Updated date.
- IEMS was first generally available to customers (GA) in SN07. There was an SN06.2 beta where the delimiters for IEMS may have been different.
- SDM log stream delimiters have been the same since at least SN05. An OSS should consider the potential requirement of having to support multiple Nortel software releases concurrently. As well as SDM/CBM and IEMS concurrently.

Table 3 - NE/EM Comparision

NE/EM & SCC2 Transparency	Difference or Notes	OSS Impacting				
CS2000, & Peripherals, IW-SPM, MG4000, SDM, CBM, cCS2000 – Transparent with the following Notes	Differences:	a) No Impact				
	a) IEMS mandatory indent rule - IEMS has a mandatory indent rule where if it comes across a log from the CS2K/SDM that is not indented appropriately in its view, it will add 8 spaces to the beginning of the line. Very few logs (such as BOOT201 below) are believed to be affected by this issue. With well written OSS templates and the fix in place, the affected logs should not be adversely affected when it comes to OSS parsing.					
	<table><tr><th>SDM SCC2 Samples:</th><th>IEMS SCC2 Sample:</th></tr><tr><td>* 08 BOOT201 INFO Bootp log report Mac Address : 0001af0bc772 MAC addr to node_id lookup failure : 11 INM permission to boot failure : 0 Core IP address lookup failure : 0 SEND_UDP_MSG failure : 0</td><td>* 08 BOOT201 INFO Bootp log report Mac Address : 0001af0bc772 MAC addr to node_id lookup failure : 11 INM permission to boot failure : 0 Core IP address lookup failure : 0 SEND_UDP_MSG failure : 0</td></tr></table>		SDM SCC2 Samples:	IEMS SCC2 Sample:	* 08 BOOT201 INFO Bootp log report Mac Address : 0001af0bc772 MAC addr to node_id lookup failure : 11 INM permission to boot failure : 0 Core IP address lookup failure : 0 SEND_UDP_MSG failure : 0	* 08 BOOT201 INFO Bootp log report Mac Address : 0001af0bc772 MAC addr to node_id lookup failure : 11 INM permission to boot failure : 0 Core IP address lookup failure : 0 SEND_UDP_MSG failure : 0
	SDM SCC2 Samples:		IEMS SCC2 Sample:			
	* 08 BOOT201 INFO Bootp log report Mac Address : 0001af0bc772 MAC addr to node_id lookup failure : 11 INM permission to boot failure : 0 Core IP address lookup failure : 0 SEND_UDP_MSG failure : 0		* 08 BOOT201 INFO Bootp log report Mac Address : 0001af0bc772 MAC addr to node_id lookup failure : 11 INM permission to boot failure : 0 Core IP address lookup failure : 0 SEND_UDP_MSG failure : 0			
Notes:						
a) Certain logs generated by the CS2K such as OMAU, OMGA, and the protologs (SWER, TRAP, INIT and so on) have no log number, just blank spaces. This is how they look on the CS2K and SDM/CBM. In an SN07 office where the SDM is feeding CS2K logs to IEMS, IEMS adds 000 for a log number. Eg. SWER000. In SN08, a resolution was implemented in IEMS whereby the 000 log number was no longer added to these SDM/CBM logs and the 3 spaces are maintained as it is received. Resolved in SN08 via CR Q00980472.						
	b) When IEMS receives logs from managed components, it implements an 80 character per line rule for log bodies. If 80 characters is exceeded, an End of Line String is inserted at the 80 th character and the remainder of the line is put onto the next line. In the case of logs from the SDM/CBM, where rows often exceed 80 characters, this wrap rule could result in visual or transparency differences between what the log looks like on SDM/CBM and IEMS. In some cases, trailing whitespace in a row could potentially be wrapped resulting in a blank line being created. In order to maintain transparency and avoid parsing issues with blank lines and so on, the 80 character wrap rule has been removed from the incoming feed to IEMS from SDM/CBM. Resolved in SN07 via patch IEM0507D					
	c) Certain CS2K logs such as CARR and PM support an optional field called Equipment Identifier that shows up at the end					

	of the log header after the Event Label. The CS2K has a "newline" rule (which the SDM/CBM implements as well) where the Equipment Identifier is removed from the header line in that it has its own line immediately following the header. The SDM/CBM's Log Delivery Service at SN07 final compile in its implementation of the 65 character newline rule incorrectly took into consideration the 9 characters for the optional ECORE_FORMAT field. (Even when ECORE is set to OFF in the SDM/CBM log device in logroute). This results in the Equipment Identifier field being "newlined" when the CS2K normally would not. (A transparency difference between what the log looks like on the CS2K and on the SDM/CBM). The end result of all this is that templates parsing CARR and PM logs (and any other Equipment Identifier-supporting logs) may no longer be able to parse these logs properly prior to implementation of the patch for this CR. Resolved in SN07 via patches SDM_BASE.logs-20.82.7.10.tape, SDM_BASE.gdd-20.82.7.3.tape for SDM and NTLOGS208208-15.patch, NTGDD208208-03.patch for CBM. d) SDM / CBM transparency issue. In the SN07 CBM product, some applications had started to communicate their failure events via an alarmd process. The resultant log looks different than the original (as seen on SDM). For failure events common to both SDM and CBM platforms, this created 2 versions of the log. 1 for SDM and 1 for CBM. Known logs affected were SDM327/SDM627. This second CBM version was undone in that . Resolved in SN07 CBM patch CR Q01001000-01			
STORM Partially Transparent	Differences: a) Log name/numbers are retained but log formats are different. Believed to affect approx. 8 logs. See example below.	a) No Impact if no existing OSS support for STM logs. Otherwise, the template would have to change.		
	<table><tr><td>SDM SCC2 Samples:</td><td>IEMS SCC2 Sample:</td></tr><tr><td>* 59 STM 803 5090 THR Threshold exceeded Status: Alarm raised. Number of zombie(s) is 1. Minor alarm threshold value is 1.</td><td>* 40 STM 803 0088 FLT STM Fault Location: 172.18.17.6 Notification Id: 56 State: Raised Category: qualityOfService Cause: thresholdCrossed Time: Sep 07 09:40:17 2004 Component Id: STORMIA=storm0 Specific Problem: Description: Status: Alarm raised. Number of zombie(s) is 1. Minor alarm threshold value is 1.</td></tr></table>		SDM SCC2 Samples:	IEMS SCC2 Sample:
SDM SCC2 Samples:	IEMS SCC2 Sample:			
* 59 STM 803 5090 THR Threshold exceeded Status: Alarm raised. Number of zombie(s) is 1. Minor alarm threshold value is 1.	* 40 STM 803 0088 FLT STM Fault Location: 172.18.17.6 Notification Id: 56 State: Raised Category: qualityOfService Cause: thresholdCrossed Time: Sep 07 09:40:17 2004 Component Id: STORMIA=storm0 Specific Problem: Description: Status: Alarm raised. Number of zombie(s) is 1. Minor alarm threshold value is 1.			

NE/EM & SCC2 Transparency	Difference or Notes	OSS Impacting
GWC and GWC EM Partial Transparency	Differences: a) GWC3XX set logs. (Approx. 17 logs). The syntax of the Category and Cause fields in the log body are different (spaces and Upper case characters). b) GWC399 (the clear log for the GWC3XX set logs) is not transparent. IEMS version of the log has 2 extra lines. (mainly for human interpretation). Note: The Component Id structure difference in the example below is tracked by CR Q00976754 and resolved in SN07 patch ZOD41O7D. It is not an SDM / IEMS transparency issue.	a) No Impact. b) No Impact. A single OSS template should be able to handle both versions these GWC logs.

	SDM SCC2 Samples: **16 GWC 301 5129 TBL GWC Fault Location: GWC-1-UNIT-1 NotificationID: 1 State: Raise Category: Quality of Service Cause: Underlying resource unavailable Time: Sep 01 13:16:11 2004 Component Id: GWC-1-UNIT-1 Specific Problem: Unit Out of Service: Unit is system disabled; Service is not available Description: Standby unit disabled.	IEMS SCC2 Sample: **28 GWC 301 0036 TBL GWC Fault Location: GWC-0-UNIT-1 NotificationID: 1 State: Raise Category: qualityOfService Cause: underlyingResourceUnavailable Time: Aug 27 13:28:43 2004 Component Id: GWC=GWC-?-UNIT-? Version=GN070CB;Unit=unit_1;Software=NODE MTC Specific Problem: Unit Out of Service: Unit is system disabled; Service is not available Description: Standby unit disabled.	
	16 GWC 399 5155 INFO GWC Fault Location: GWC-1-UNIT-1 NotificationID: 1 State: Clear Time: Sep 01 13:16:21 2004	30 GWC 399 0050 INFO GWC Fault Location: GWC-0-UNIT-1 NotificationID: 1 State: Clear Time: Aug 27 13:30:45 2004 Component Id: GWC=GWC-?-UNIT-? Version=GN070CB;Unit=unit_1;Software=NODE MTC Description: Standby unit disabled.	
MG9K ATM/IP & MG9000 EM Partial Transparency	Differences: a) For all MG9000 logs having a format which includes the Category and State fields (generally alarm logs - approx. 200 in SN07, and 40 more in SN08), you will find that the syntax of the field value between SDM and IEMS can be slightly different. This is due to the MG9K EM outputting syslog to SDM and Corba to IEMS. Example for SDM: State: cleared Category: Equipment Alarm Example for IEMS: State: Cleared Category: equipment Notes: a) In SN07, the MG9000 Element Manager in an IEMS implementation was duplicating alarm logs sent to IEMS by including them in the syslog feed in addition to the Corba feed to IEMS. Application of the MG9000 EM patch will de-activate sending alarm logs to syslog remove the duplication. Resolved in SN07 via patch IEM0807D for IEMS and 9K EM patch ZOD50		a) No Impact
SAM21 Transparent	Differences: a) Some SAM21 logs (worst case 19 SCU logs) indent the event label 1 character (space). When IEMS processes this, the leading space in the Event Label is removed. SDM maintains the leading space.		a) No Impact
NE/EM & SCC2	Difference or Notes		OSS Impacting

Transparency			
Passport 8600 Not transparent	Differences: (SN07) a) The logs reporting Passport 8600 SNMP trap events are completely different between SDM/CBM and IEMS. In SN07, the SDM uses the PPES300-307 log name/number set and obtains the data for these logs from MDM. IEMS listens to SNMP traps directly from the Passport 8600 and implements the PP398 log for the sets and PP399 for the clears.		SN07: a) No impact – OSS coding support challenges may be present with extracting data from the Specific Problem and Description fields and being able to correlate the sets with the clears. b) Impact Major - A customer is either other going to ignore all IEMS602s or mark all critical – either way, it is going to be problem in SN07. c) Impact Major - There is insufficient information (only an IP address) to determine what is causing the fault and what needs to be corrected. SN08: a) No impact – The above SN07 issues are resolved in SN08 and as with any new logs in a release, new templates will have to be written to support them. With the current flexibility of the IEMS aging policy and that of an OSS, a working fault management system should be possible between the two of them.
	SN07 SDM SCC2 Samples:	SN07 IEMS SCC2 Sample:	
	**20 PPES300 1486 TBL time: 2003 11 14 12 17 03 event: set compId: PP8600 BATMAN IF 72 severity: major faultCode: C0000002 alarmType: communications commentData: Link down trap interface: 72	** PP398 SEP08 21:37:57 9992 TBL PP Fault Location: 10.102.15.130 State: Raise Specific Problem: Generic Link Status Description: Link Down: ifIndex = 167 (AdminStatus = up OpeationStatus = down)	
	20 PPES307 1487 TBL time: 2003 11 14 12 17 06 event: clear compId: PP8600 BATMAN IF 72 severity: cleared faultCode: C0000002 alarmType: commentData: Explicated CLEAR Alarm generated by GMDR.	38 PP399 SEP08 21:38:00 9994 INFO PP Fault Location: 10.102.15.130 State: Clear Specific Problem: Generic Link Status Description: Link Up: ifIndex = 167 (AdminStatus = up OpeationStatus = up)	
	20 PPES300 1488 TBL time: 2003 11 14 12 17 06 event: clear compId: PP8600 BATMAN IF 72 severity: cleared faultCode: C0000002 alarmType: communications commentData: Link up trap interface: 72		
	b) IEMS only supported a limited set of Passport 8600 traps in SN07. (The ones listed below). The unsupported Passport 8600 SNMP traps are treated by IEMS as unknown and reported northbound to the OSS as IEMS602 (Unknown Trap from Known Device).		
	Alarm Name	Trap OID (v2c)	Log
	coldStart	1.3.6.1.6.3.1.1.5.1.0	PP399
	coldStart	1.3.6.1.4.1.2272.0.99001	PP398
	warmStart	1.3.6.1.6.3.1.1.5.2.0	PP399

	<table><tr><td>warmStart</td><td>1.3.6.1.4.1.2272.0.99002</td><td>PP398</td></tr><tr><td>linkDown</td><td>1.3.6.1.6.3.1.1.5.3.0</td><td>PP398</td></tr><tr><td>linkUp</td><td>1.3.6.1.6.3.1.1.5.4.0</td><td>PP399</td></tr><tr><td>rcChasPowerSupplyDown</td><td>1.3.6.1.4.1.2272.1.21.6.0</td><td>PP398</td></tr><tr><td>rcChasPowerSupplyUp</td><td>1.3.6.1.4.1.2272.1.21.14.0</td><td>PP399</td></tr><tr><td>rcChasFanDown</td><td>1.3.6.1.4.1.2272.1.21.7.0</td><td>PP398</td></tr><tr><td>rcChasFanUp</td><td>1.3.6.1.4.1.2272.1.21.21.0</td><td>PP399</td></tr><tr><td>rc2kCardDown</td><td>1.3.6.1.4.1.2272.1.21.11.0</td><td>PP398</td></tr><tr><td>rc2kCardUp</td><td>1.3.6.1.4.1.2272.1.21.12.0</td><td>PP399</td></tr><tr><td>rcSmltLinkUp</td><td>1.3.6.1.4.1.2272.1.21.19.0</td><td>PP399</td></tr><tr><td>rcSmltLinkDown</td><td>1.3.6.1.4.1.2272.1.21.20.0</td><td>PP398</td></tr></table> • Exception: PP368 and PP369 are the SN08 logs which have been patched back to SN07. (Only these 2 logs to date have been patched back).	warmStart	1.3.6.1.4.1.2272.0.99002	PP398	linkDown	1.3.6.1.6.3.1.1.5.3.0	PP398	linkUp	1.3.6.1.6.3.1.1.5.4.0	PP399	rcChasPowerSupplyDown	1.3.6.1.4.1.2272.1.21.6.0	PP398	rcChasPowerSupplyUp	1.3.6.1.4.1.2272.1.21.14.0	PP399	rcChasFanDown	1.3.6.1.4.1.2272.1.21.7.0	PP398	rcChasFanUp	1.3.6.1.4.1.2272.1.21.21.0	PP399	rc2kCardDown	1.3.6.1.4.1.2272.1.21.11.0	PP398	rc2kCardUp	1.3.6.1.4.1.2272.1.21.12.0	PP399	rcSmltLinkUp	1.3.6.1.4.1.2272.1.21.19.0	PP399	rcSmltLinkDown	1.3.6.1.4.1.2272.1.21.20.0	PP398	
warmStart	1.3.6.1.4.1.2272.0.99002	PP398																																	
linkDown	1.3.6.1.6.3.1.1.5.3.0	PP398																																	
linkUp	1.3.6.1.6.3.1.1.5.4.0	PP399																																	
rcChasPowerSupplyDown	1.3.6.1.4.1.2272.1.21.6.0	PP398																																	
rcChasPowerSupplyUp	1.3.6.1.4.1.2272.1.21.14.0	PP399																																	
rcChasFanDown	1.3.6.1.4.1.2272.1.21.7.0	PP398																																	
rcChasFanUp	1.3.6.1.4.1.2272.1.21.21.0	PP399																																	
rc2kCardDown	1.3.6.1.4.1.2272.1.21.11.0	PP398																																	
rc2kCardUp	1.3.6.1.4.1.2272.1.21.12.0	PP399																																	
rcSmltLinkUp	1.3.6.1.4.1.2272.1.21.19.0	PP399																																	
rcSmltLinkDown	1.3.6.1.4.1.2272.1.21.20.0	PP398																																	
	59 IEMS602 7505 INFO Location: 10.102.15.131 Event: .1.3.6.1.4.1.2272.1.21.8.0 Varbind0: .1.3.6.1.2.1.1.3.0: 203 days, 23 hours, 11 minutes, 22 seconds . Varbind1: .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.8.0 Varbind2: .1.3.6.1.4.1.2272.1.4.10.1.1.0: 267																																		
	c) IEMS Location Field has only an IP address. Notes: (SN08) a) SN08 feature A00007343 was created to help address the above issues in 8600 fault management via IEMS. With the feature, a new set of logs (PP310 -> PP392) was created to addresses log format/content issues [a) and c)] and PP398/399 is no longer used. Full SNMP trap support as of SN08 was implemented as well [b)] and hence no IEMS602 logs would be seen for unsupported 8600 SNMP traps. This feature does not result in transparency between SDM and IEMS but it does clean up the IEMS log situation. See the SN08 IEMS log samples below for Passport 8600. PP317 is cleared by PP318 when the Component ID matches. At the time of writing, two SN08 IEMS logs for Passport 8600 (PP368 and PP369) have been patched back to SN07.																																		
	IEMS PP317 SN08 SCC2 Sample:																																		

	Specific Problem: Generic Link Status Description: Link Down: ifIndex = 72(AdminStatus = up OperationStatus = down) .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.3.0 .1.3.6.1.2.1.1.3.0: 73 days, 5 hours, 35 minutes, 4 seconds. IEMS PP318 SN08 SCC2 Sample: 01 PP 318 0120 INFO PP Fault Location: PP8600A;10.102.15.130 State: Cleared Category: communications Cause: communication regained Time: Feb 10 16:01:48 2005 Component ID: PP8600=10.102.15.130; ifIndex=72 Specific Problem: Generic Link Status Description: Link Up: ifIndex = 72(AdminStatus = up OperationStatus = up) .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.4.0 .1.3.6.1.2.1.1.3.0: 73 days, 5 hours, 35 minutes, 6 seconds. Differences: (SN08) a) One noted difference between SN08 IEMS 8600 trap/log fault management and that of SDM/CBM via MDM is that MDM has implemented a per alarm aging mechanism where a trap is not part of a set/clear pair. (There are a lot of 8600 SNMP traps like this.) After a certain period of time, one of these autonomous logs (that has severity) will be cleared automatically. IEMS as of SN08 does not have a per alarm aging mechanism. In order to prevent a situation in IEMS where these autonomous logs are being raised but never cleared, an 8600 device alarm clearing policy has been implemented by default in the SN08 load. If any 8600 alarm has been present in IEMS for 7 days, it will automatically be cleared by this policy. The clear notification will be an IEMS608 log which will contain information required in order to clear the previous set log for the alarm. While clearing 8600 alarms related to hardware such as fan or link down after 7 days is undesirable it was felt better than having no clear for the multitude of 8600 autonomous traps. Note: An OSS does not have to take action on aging clears if it does not want to. Or it can take action on only a subset of them. The 8600 aging policy in IEMS can also be disabled or modified to be something other than 7 days.	

NE/EM & SCC2 Transparency	Difference or Notes	OSS Impacting				
MSS15000, MG15000, MDM Partial Transparency	Notes: Between IEMS and SDM/CBM, MSS15000/MG15000/MDM log names are the same and appears to use the same mapping scheme. (Where the log prefix is determined by what the first 4 digits of the fault code is). Names are PPEM, MDM and CA. Log Body tags all the same.	a) Minor impact - Log numbers of 000 are usually invalid. Customers who have written templates for CA/MDM/PPEM3XX would have to add an additional line for PPEM000. The template logic would read something like; if you get an alarm raised with a PPEM3xx look for a PPEM3xx or PPEM307 or PPEM000 with the same compID and faultCode. b) No Impact c) No Impact d) Minor impact – Fault OSS log parsing code for these logs would have to be coded to accommodate the capitalization differences. e) Minor impact – Only if fault OSS parses out the values of the alarmType field. In such a case, the log parsing code would need to accommodate “processing” or “processingError”. Having a 307 number instead of 302 should be no impact given the same format structure of all the logs.				
	Differences: (SN07 and SN08) a) Log numbers are maintained except that it would appear IEMS doesn't use PPEM/CA/MDM307 for explicit clears and instead uses a 000 number. OSS templates for PPEM000/CA000/MDM000 should be identical to PPEM307/CA307/MDM307 (explicit clear varieties). Inappropriate use of the 000 log number for explicit clears from MDM was discontinued in SN08. Resolved in SN08 via CR Q00980484.					
	<table><tr><th>SN07 SDM/CBM Explicit Clear Sample:</th><th>SN07 IEMS Explicit Clear Sample:</th></tr><tr><td>08 PPEM307 9380 TBL time: 2004 09 09 12 09 11 event: clear compId: EM P15KE LP 12 SONET 1 STS 0 severity: cleared faultCode: 70115261 alarmType: commentData: Explicated CLEAR Alarm generated by GMDR.</td><td>46 PPEM000 8088 TBL time: 2004 09 09 12 46 42 event: clear compId: EM P15KE LP 12 SONET 1 STS 0 severity: cleared faultcode: 70115261 alarmType: other commentData: Explicated CLEAR Alarm generated by GMDR.</td></tr></table>		SN07 SDM/CBM Explicit Clear Sample:	SN07 IEMS Explicit Clear Sample:	08 PPEM307 9380 TBL time: 2004 09 09 12 09 11 event: clear compId: EM P15KE LP 12 SONET 1 STS 0 severity: cleared faultCode: 70115261 alarmType: commentData: Explicated CLEAR Alarm generated by GMDR.	46 PPEM000 8088 TBL time: 2004 09 09 12 46 42 event: clear compId: EM P15KE LP 12 SONET 1 STS 0 severity: cleared faultcode: 70115261 alarmType: other commentData: Explicated CLEAR Alarm generated by GMDR.
	SN07 SDM/CBM Explicit Clear Sample:		SN07 IEMS Explicit Clear Sample:			
	08 PPEM307 9380 TBL time: 2004 09 09 12 09 11 event: clear compId: EM P15KE LP 12 SONET 1 STS 0 severity: cleared faultCode: 70115261 alarmType: commentData: Explicated CLEAR Alarm generated by GMDR.		46 PPEM000 8088 TBL time: 2004 09 09 12 46 42 event: clear compId: EM P15KE LP 12 SONET 1 STS 0 severity: cleared faultcode: 70115261 alarmType: other commentData: Explicated CLEAR Alarm generated by GMDR.			
b) IEMS has changed the field values of alarmType in some cases so that it aligns with a standard list of X.733 alarm categories. Where there was no equivalent alarm type in X.733, IEMS uses "other". (See table below). When logs come out of SDM/CBM, the original alarmtype as provided by MDM is maintained.						
<table><tr><th>SN07/08 SDM/CBM alarmtype SCC2 Sample:</th><th>SN07/SN08 IEMS alarmtype SCC2 Sample:</th></tr><tr><td>**13 PPEM305 7877 TBL time: 2005 03 08 16 13 14 event: message compId: EM P15KL NMIS \$ FMIP \$ SESSION 9 severity: major faultCode: 70060006 alarmType: security commentData: 9 contiguous FMIP login attempts failed,</td><td>**41 PPEM305 8756 TBL time: 2005 03 08 14 40 41 event: message compId: EM P15KL NMIS \$ FMIP \$ SESSION 9 severity: major faultcode: 70060006 alarmType: other commentData: 9 contiguous FMIP login attempts failed,</td></tr></table>	SN07/08 SDM/CBM alarmtype SCC2 Sample:	SN07/SN08 IEMS alarmtype SCC2 Sample:	**13 PPEM305 7877 TBL time: 2005 03 08 16 13 14 event: message compId: EM P15KL NMIS \$ FMIP \$ SESSION 9 severity: major faultCode: 70060006 alarmType: security commentData: 9 contiguous FMIP login attempts failed,	**41 PPEM305 8756 TBL time: 2005 03 08 14 40 41 event: message compId: EM P15KL NMIS \$ FMIP \$ SESSION 9 severity: major faultcode: 70060006 alarmType: other commentData: 9 contiguous FMIP login attempts failed,		
SN07/08 SDM/CBM alarmtype SCC2 Sample:	SN07/SN08 IEMS alarmtype SCC2 Sample:					
**13 PPEM305 7877 TBL time: 2005 03 08 16 13 14 event: message compId: EM P15KL NMIS \$ FMIP \$ SESSION 9 severity: major faultCode: 70060006 alarmType: security commentData: 9 contiguous FMIP login attempts failed,	**41 PPEM305 8756 TBL time: 2005 03 08 14 40 41 event: message compId: EM P15KL NMIS \$ FMIP \$ SESSION 9 severity: major faultcode: 70060006 alarmType: other commentData: 9 contiguous FMIP login attempts failed,					

last failure from 10.102.4.4 to userid: DEBUG		last failure from 10.102.13.16 to userid: DEBUG	
c) In SN07, when the alarmType value is qualityOfService, SDM reports the log number as 301 whereas IEMS reports it as 307. (Log format of 300-307 are all the same). In SN08, this is no longer the case. Resolved in SN08 via unknown CR.			
SN07 SDM/CBM SCC2 Sample:		SN07 IEMS SCC2 Sample:	
04 PPEM301 5272 TBL time: 2004 08 23 11 04 25 event: clear compId: EM P15KL COL DEBUG AG 1 severity: cleared faultCode: 70030001 alarmType: qualityOfService commentData: currentQueueSize fell back to 500f maximum. 48 records discarded since the Set alarm.		**36 PPEM307 3736 TBL time: 2004 09 23 10 36 17 event: set compId: EM P15KH COL DEBUG AG 0 severity: major faultcode: 70030001 alarmType: qualityOfService commentData: currentQueueSize exceeded 75% of maximum.	
SN08 SDM/CBM SCC2 Sample:		SN08 IEMS SCC2 Sample:	
**12 PPEM301 8786 TBL time: 2005 02 23 14 47 02 event: set compId: EM P15KE LP 2 ENG \$ AALIST \$ severity: major faultCode: 70030007 alarmType: qualityOfService commentData: current list size exceeded 750f maximum		**49 PPEM301 5863 TBL time: 2005 02 11 13 49 03 event: set compId: EM P15KL COL DEBUG AG 15 severity: major faultcode: 70030001 alarmType: qualityOfService commentData: currentQueueSize exceeded 75% of maximum.	
d) In SN07 and SN08, IEMS had a tag of “faultcode” whereas in SDM, it was “faultCode”. Resolved in SN09 via CR Q01176407.			
e) In SN07 and SN08, IEMS was mapping the alarmType value of “processing” to “other” whereas in SDM, it “processing”. In SN09, IEMS started mapping “processing” to “processingError” in order to comply with X.733 values. Also, the IEMS log number was improperly coming out as 307 instead of 302 like SDM. In SN09, IEMS started to properly report processing errors as 302 log numbers. Each Implemented/Resolved in SN09 via CR Q01176412.			
Summary of Transparency Differences Between SDM & IEMS (in bold text) for c), d) & e):			
SDM alarmTpe	SDM log number	IEMS alarmType	IEMS log number
communications	300	communications	300

	qualityOfService	301	qualityOfService	307 (SN07) / 301 (SN08)	
	processing	302	other (SN07/08)/processingError (SN09)	307 (SN07/SN08) / 302 (SN09)	
	equipment	303	equipment	303	
	environmental	304	environmental	304	
	security	305	other (SN07/08)	305	
	debug	600	(unknown)	(unknown)	
	operator	306	other (SN07/08)	306	
	unknown	307 (set log)	other (SN07/08)	307	
	(blank)	307 (explicit clear)	other (SN07/08)	000 (SN07) / 307 (SN08)	

NE/EM & SCC2 Transparency	Difference or Notes	OSS Impacting						
CMT- SESM Partial Transparency	Differences: a) CMT399 is not transparent. IEMS version of this log has 2 extra lines. b) Partial transparency amongst all CMT3XX set logs (approx. 4 logs): Syntax of Category, and Cause fields are different. (See samples below). c) In CMT302 failure scenarios, it appears that IEMS uses an inconsistent Location field value between the set and clear. In SDM, SNMP_NE_Poller is consistently used. Resolution involves making the IEMS clear have SNMP_NE_Poller. Resolved in SN08 via CR Q01078502 and CR Q01078502-02. Plans to patch back to SN07. <table><tr><th>SDM SCC2 Samples:</th><th>IEMS SCC2 Sample:</th></tr><tr><td> **14 CMT 302 9000 TBL CMT Fault Location: SNMP_NE_Poller NotificationID: 1 State: Raise Category: Communications Cause: Communications subsystem failure Time: Aug 31 13:34:14 2004 Component Id: SESM=SNMP Device Poller;Device=GWC-6-UNIT-1;DeviceID=0x00000063000000a10a660f43 Specific Problem: SNMP Timeout Description: CMT Unable to communicate with managed device </td><td> **29 CMT 302 5875 TBL GWC Fault Location: SNMP_NE_Poller NotificationID: 4 State: Raise Category: communications Cause: communicationsSubsystemFailure Time: Sep 27 13:29:37 2004 Component Id: SESM=SNMP Device Poller;Device=GWC-5-UNIT-0;DeviceID=0x00000063000000a10a660f3e Specific Problem: SNMP Timeout Description: CMT Unable to communicate with managed device </td></tr><tr><td> 15 CMT 399 9946 INFO CMT Fault Location: SNMP_NE_Poller NotificationID: 1 State: Clear Time: Aug 31 13:28:15 2004 </td><td> 38 CMT 399 6002 INFO GWC Fault Location: GWC-5-UNIT-0 NotificationID: 4 State: Clear Time: Sep 27 13:38:22 2004 Component Id: SESM=SNMP Device Poller;Device=GWC-5-UNIT-0;DeviceID=0x00000063000000a10a660f3e Description: CMT Reestablished communications with managed device </td></tr></table>	SDM SCC2 Samples:	IEMS SCC2 Sample:	**14 CMT 302 9000 TBL CMT Fault Location: SNMP_NE_Poller NotificationID: 1 State: Raise Category: Communications Cause: Communications subsystem failure Time: Aug 31 13:34:14 2004 Component Id: SESM=SNMP Device Poller;Device=GWC-6-UNIT-1;DeviceID=0x00000063000000a10a660f43 Specific Problem: SNMP Timeout Description: CMT Unable to communicate with managed device	**29 CMT 302 5875 TBL GWC Fault Location: SNMP_NE_Poller NotificationID: 4 State: Raise Category: communications Cause: communicationsSubsystemFailure Time: Sep 27 13:29:37 2004 Component Id: SESM=SNMP Device Poller;Device=GWC-5-UNIT-0;DeviceID=0x00000063000000a10a660f3e Specific Problem: SNMP Timeout Description: CMT Unable to communicate with managed device	15 CMT 399 9946 INFO CMT Fault Location: SNMP_NE_Poller NotificationID: 1 State: Clear Time: Aug 31 13:28:15 2004	38 CMT 399 6002 INFO GWC Fault Location: GWC-5-UNIT-0 NotificationID: 4 State: Clear Time: Sep 27 13:38:22 2004 Component Id: SESM=SNMP Device Poller;Device=GWC-5-UNIT-0;DeviceID=0x00000063000000a10a660f3e Description: CMT Reestablished communications with managed device	a) No Impact. b) No Impact. c) Impact Major – Customer may be unable to clear the alarm until the CR issue is resolved.
SDM SCC2 Samples:	IEMS SCC2 Sample:							
**14 CMT 302 9000 TBL CMT Fault Location: SNMP_NE_Poller NotificationID: 1 State: Raise Category: Communications Cause: Communications subsystem failure Time: Aug 31 13:34:14 2004 Component Id: SESM=SNMP Device Poller;Device=GWC-6-UNIT-1;DeviceID=0x00000063000000a10a660f43 Specific Problem: SNMP Timeout Description: CMT Unable to communicate with managed device	**29 CMT 302 5875 TBL GWC Fault Location: SNMP_NE_Poller NotificationID: 4 State: Raise Category: communications Cause: communicationsSubsystemFailure Time: Sep 27 13:29:37 2004 Component Id: SESM=SNMP Device Poller;Device=GWC-5-UNIT-0;DeviceID=0x00000063000000a10a660f3e Specific Problem: SNMP Timeout Description: CMT Unable to communicate with managed device							
15 CMT 399 9946 INFO CMT Fault Location: SNMP_NE_Poller NotificationID: 1 State: Clear Time: Aug 31 13:28:15 2004	38 CMT 399 6002 INFO GWC Fault Location: GWC-5-UNIT-0 NotificationID: 4 State: Clear Time: Sep 27 13:38:22 2004 Component Id: SESM=SNMP Device Poller;Device=GWC-5-UNIT-0;DeviceID=0x00000063000000a10a660f3e Description: CMT Reestablished communications with managed device							
CMT-QCA Partial Transparency	Differences: a) IEMS implements an 80 character log body line length for all managed components except the logs from SDM/CBM. Some of the QCA logs as output to /var/log/customerlog on the CMT have a Description field value that exceeds 80 characters. IEMS puts the excess onto a new line whereas SDM/CBM does not when it receives it from syslog.	a) No Impact						

	Notes: SN08 introduced feature A00008338 to address certain general log supportability concerns for the OSS. This corrective content feature will be patched back to SN07.	
CMT-NPM Transparent	Differences: a) Some NPM logs (11 logs worst case) indent the event label 1 character (space). When IEMS processes this, the leading space in the Event Label is removed. SDM/CBM maintains the leading space.	a) No Impact
CMT-IEMS (general northbound feed comparison with SDM)	Differences: a) For NT STD and SCC2 log formats, the characters contained within the “Start of Log” and “End of Log” string delimiters are different. See Table 1 at the beginning of this Appendix. b) When IEMS re-syncs its alarm list with devices that support re-sync, IEMS creates clear logs for when discrepancies are found. ie Alarms it thought were there but went away. These clear logs used the original log name/number for the alarm in the database and the content of the “re-sync clear” was not necessarily the same. Resolution of this CR has resulted in the creation of a new IEMS log for re-sync raises/clears. (IEMS607). SDM/CBM has no such re-sync capability. Resolved in SN07 via IEM1007D patch Notes: SN07 CR Q01001051 tracked the fact that the “end of log string” for SDM differs depending on whether ECORE_FORMAT is on or off in the device. This is not an SDM/IEMS transparency but an SDM/SDM one. (ECORE_FORMAT is not supported in Succession.) This issue has been resolved through the SN07 SDM/CBM patches. The End of Log string is now the same whether ECORE format is ON or OFF. (ECORE format is not supported in Succession and should be turned off for the SDM/CBM log device for IEMS fault communication).	a) No Impact. b) No Impact. A new template would have to be created for the IEMS607 log as is the case for any new log.

NE/EM & SCC2 Transparency	Difference or Notes	OSS Impacting				
CMT-UAS Partial Transparency	Differences: a) Minor difference in the syntax of the Cause field values. Eg. "outOfMemory" in IEMS vs "Out of memory" in SDM as per the example below. b) Minor difference in the syntax of the Category field values. Eg. "processingError" in IEMS vs "Processing Error" in SDM as per the example below. c) UAS399 not transparent. (Similar in fashion to GWC399 and CMT399). UAS399 is the clear log for all UAS3xx and 8xx raises. The IEMS version has 2 extra rows of information in the clear. See example below.	a) No Impact b) No Impact c) No Impact				
	<table><tr><th>SDM SCC2 Samples:</th><th>IEMS SCC2 Sample:</th></tr><tr><td>**19 UAS 353 1227 TBL UAS Fault Location: msh10uas-a NotificationID: 81924 State: Raise Category: Processing Error Cause: Out of memory Time: May 22 11:19:13 2003 Component Id: UAS;UASUnit=msh10uas-a;Software=LocalResourceManager_0 Specific Problem: 81924 Description: [mem_usage_high_major] Memory usage high. (803554284552sed)</td><td>**10 UAS 353 9836 TBL UAS Fault Location: cablabuas NotificationID: 81924 State: Raise Category: processingError Cause: outOfMemory Time: Aug 30 15:10:48 2004 Component Id: UAS;UASUnit=cablabuas;Software=LocalResourceManager_0 Specific Problem: 81924 Description: [mem_usage_high_major] Memory usage high. (91% used)"</td></tr></table>		SDM SCC2 Samples:	IEMS SCC2 Sample:	**19 UAS 353 1227 TBL UAS Fault Location: msh10uas-a NotificationID: 81924 State: Raise Category: Processing Error Cause: Out of memory Time: May 22 11:19:13 2003 Component Id: UAS;UASUnit=msh10uas-a;Software=LocalResourceManager_0 Specific Problem: 81924 Description: [mem_usage_high_major] Memory usage high. (803554284552sed)	**10 UAS 353 9836 TBL UAS Fault Location: cablabuas NotificationID: 81924 State: Raise Category: processingError Cause: outOfMemory Time: Aug 30 15:10:48 2004 Component Id: UAS;UASUnit=cablabuas;Software=LocalResourceManager_0 Specific Problem: 81924 Description: [mem_usage_high_major] Memory usage high. (91% used)"
	SDM SCC2 Samples:		IEMS SCC2 Sample:			
**19 UAS 353 1227 TBL UAS Fault Location: msh10uas-a NotificationID: 81924 State: Raise Category: Processing Error Cause: Out of memory Time: May 22 11:19:13 2003 Component Id: UAS;UASUnit=msh10uas-a;Software=LocalResourceManager_0 Specific Problem: 81924 Description: [mem_usage_high_major] Memory usage high. (803554284552sed)	**10 UAS 353 9836 TBL UAS Fault Location: cablabuas NotificationID: 81924 State: Raise Category: processingError Cause: outOfMemory Time: Aug 30 15:10:48 2004 Component Id: UAS;UASUnit=cablabuas;Software=LocalResourceManager_0 Specific Problem: 81924 Description: [mem_usage_high_major] Memory usage high. (91% used)"					
19 UAS 399 1228 INFO UAS Fault Location: msh10uas-a NotificationID: 81924 State: Clear Time: May 22 11:19:14 2003	53 UAS 399 0642 INFO UAS Fault Location: UAS_RTPU_TST NotificationID: 49154 State: Clear Time: May 11 10:53:37 2004 Component Id: Description:					
CMT-APS	At this time there are no known methods for an APS set log to be transmitted northbound to the OSS.	No Impact				
CICM, MCS5200, USP, USPc, RTP Portal, Session Server, MS20x0, SPC Not supported via SDM	N/A	No Impact				

Appendix I: MCS Alarms and Logs

1 Fault Management Overview

1.1 Introduction

This document shall be considered an “amendment” for MCS9.1 to the previous complete/consolidated view captured in *MCS 4.0 Logs and Alarms Description* document, which was Appendix I in the SN09 OSS Advance Feature Guide. In other words, the MCS 4.0 document will act as the “base” document with all adds/changes/deletes captured in this amendment.

Also refer to the MCS9.0 “delta” Logs and Alarms document for the changes in that release.

The MCS 4.0 Logs and Alarms Description document can be found in Livelink at <http://livelink.us.nortel.com/livelink/livelink.exe?func=ll&objId=7698565&objAction=browse&sort=name>.

2 MCS Alarms

2.1 SM Service Address (SVCA) Alarm

2.1.1 SVCA 801 <EXAMPLE FORMAT>

Add/Modify/Delete

This alarm is being <added, updated, deleted> for MCS09.1.

Explanation

This alarm is raised when the service address of System Manager is changed from the Management Console.

Format

Table 1: SVCA801 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	SVCA/SMSVCADR
Alarm Name	SM Service Address Changes
Event Type	ADMIN
Severity:	Critical
Problem Text	System Manager service address changed.
Corrective Action:	Redeploy System Manager
Clear Condition:	System Manager is redeployed.

Action

If SM service address is changed, SM needs to be redeployed to take the IP Address change. If the administrator cannot login to SM from the Management Console after SM is redeployed, contact next level of support.

Associated Operational Measurements or Performance Measurements

Not applicable

2.2 Network Interface (NIF) Alarms

No changes

2.3 Threshold (THLD) Alarms

No changes

2.4 Database Communications (DBCM) Alarms

No changes

2.5 License Key (LKEY) Alarms

No changes

2.6 Recording System (RTA) Alarms

No changes

2.7 System (SYS) Alarms

No changes

2.8 SM Proxy (SMCM) Alarms

No changes

2.9 Security (SEC) Alarms

No changes

2.10 FTP (FTP) Alarms

No changes

2.11 Audiocode Gateway (AC) Alarms

No changes

2.12 Resource Management (RESM) Alarms

No changes

2.13 NED (NED) Alarms

No changes

2.14 NE Proxy (NECM, SYNC) Alarms

No changes

2.15 Loads Directory (LOADS) Alarms

No changes

2.16 Server (SRVR) Alarms

No changes

2.17 Database Monitor (DBMN) Alarms

No changes

2.18 Keycode Resource (KCRE) Alarms

No changes

2.19 Media Application Server Provisioning (MAS) Alarms

No changes

2.20 Media Application Server Platform (MAS) Alarms

No changes

2.21 RTP Media Portal (RTP) Alarms

No changes

2.22 I/O (TCF) Alarms

No Changes

2.23 Terminal Server (TSVR) Alarms

No changes

2.24 IMDB (IMDB) Alarms

No changes

2.25 Overload Control (OLC) Alarms

No changes

2.26 NCAS Alarms

No changes

2.27 R6 Application Server

No changes

3 MCS Logs

3.1 Software Error (SWER) Logs

3.1.1 SWER 801 <EXAMPLE FORMAT>

Add/Modify/Delete

This log is being <added, updated, deleted> for MCS09.1

Explanation

This log indicates that a software error has occurred and that an alarm has been raised.

Format

Table 2: SWER 801 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	SWER/SWERR
Event Type	ABNORMAL
Severity	MINOR
Report Text	One or more Software Errors have occurred. The first one is captured below. Please collect the SWERs and the surrounding logs from the log file. SWER Reported:<swer_text>

Table 3: SWER 799 Field descriptions

Field	Value	Description
Swerr_text	String	Description of software error provided by application along with an exception stack trace.

Action

Contact next level of support.

Associated Operational Measurements or Performance Measurements

Not applicable

3.2 Address (ADDR) Logs

No changes

3.3 Session Manager Accounting (ACAT) Logs

No changes

3.4 Network Interface (NIF) Logs

No changes

3.5 OM Collection (OM) Logs

No changes

3.6 Scheduler (SCHED) Logs

No changes

3.7 Database Communications (DBCM) Logs

No changes

3.8 Alarm Agent (ALM) Logs

No changes

3.9 Log Agent (LGAT) Logs

No changes

3.10 License Key (LKEY) Logs

No changes

3.11 Network Element Communication (NEC) Logs

No changes

3.12 Recording System (RECS, RTA) Logs

No changes

3.13 Sync System (CHKP) Logs

No changes

3.14 System (SYS) Logs

No changes

3.15 Security (SEC) Logs

No changes

3.16 FPM (ALRM) Logs

No changes

3.17 SNMP (SNMP) Logs

3.17.1 SNMP 713

Delete

This log is being deleted for MCS 9.1

Explanation

This log indicates that there is an exception caught in clearing an alarm in the SNMP MIB table of active alarm because the alarm attempted to be cleared does not present in the active alarm MIB table.

Format

Table 4: SNMP 713 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	SNMP/SNMP
Event Type	ABNORMAL
Severity	ALERT
Report Text	Failed to find a matching active alarm for clearing: < alarm-data>. Exception: <error-text>

Table 5: SNMP 713 Field descriptions

Field	Value	Description
alarm-data	Varies	Data about the cleared alarm that fail to be cleared in the active alarm MIB table. The data includes its family name, alarm number, description, timestamp, source, etc
error-text	Varies	Error message of the exception caught.

Action

Restart the FPM and contact the next level of support

Associated Operational Measurements or Performance Measurements

Not applicable

3.17.2 SNMP 721

Delete

This log is being deleted for MCS 9.1

Explanation

This log indicates that there is an exception caught in updating the active alarm MIB table when an alarm has been changed.

Format

Table 6: SNMP 721 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	SNMP/SNMP
Event Type	ABNORMAL
Severity	ALERT
Report Text	Failed to update an active alarm entry into the MIB table: <alarm-data>. Exception: <error-text>

Table 7: SNMP 721 Field descriptions

Field	Value	Description
alarm-data	Varies	Data about the alarm that failed to be added to the active alarm MIB table. The data includes family name, alarm number, description, timestamp, source, etc
error-text	Varies	Error message of the exception caught.

Action

Restart the FPM and contact the next level of support

Associated Operational Measurements or Performance Measurements

Not applicable

3.17.3 SNMP 722

Delete

This log is being deleted for MCS 9.1

Explanation

This log indicates that there is an error occurred in clearing all the alarms in the active alarm MIB table for a network element instance when its OSI status becomes unknown.

Format

Table 8: SNMP 722 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	SNMP/SNMP
Event Type	ABNORMAL
Severity	ALERT
Report Text	Failed to clear alarm entry for an NE in the active alarm table

Action

Restart the FPM and contact the next level of support

Associated Operational Measurements or Performance Measurements

Not applicable

3.18 RTA Collector (RTAC) Logs

No changes

3.19 File Transport (FTP) Logs

No changes

3.20 ORV (ORV) Logs

No changes

3.21 NMI SNMP (NMI) Logs

No changes

3.22 Audiocode Gateway (AC) Logs

No changes

3.23 System Manager (SMAL) Logs

No changes

3.24 NED (NED) Logs

No changes

3.25 OMI (OMIS) Logs

No changes

3.26 Transaction State Machine (XACT) Logs

No changes

3.27 NE Proxy (NEI) Logs

No changes

3.28 OM Query (OM) Logs

No changes

3.29 LOM (LOM) Logs

No changes

3.30 MAS Platform (MAS) Logs

No changes

3.31 Base Provisioning (PROV) Logs

No changes

3.32 IP Client Manager (ESM) Logs

No changes

3.33 MAS Provisioning Manager (MAS) Logs

No changes

3.34 Media Portal (RTP) Logs

No changes

3.35 Conference (CLS) Logs

No changes

3.36 RAS SIP Gateway (RAS) Logs

No changes

3.37 Voicemail (VM) Logs

No changes

3.38 Media Portal Service (MP) Logs

No changes

3.39 Emergency Service (EMRG) Logs

No changes

3.40 Message Validator Service (MSGV) Logs

No changes

3.41 Presence Service (PRS) Logs

No changes

3.42 NCL Service (NCL) Logs

No changes

3.43 Treatment Service (TRMT) Logs

No changes

3.44 Service Package (SVP) Logs

No changes

3.45 IP Device (IDEV) Logs

No changes

3.46 TCP Framework (TCP) Logs

No changes

3.47 NCAS Logs

No changes

3.48 Static Client Audit Logs

No changes

3.49 SIP Protocol (SIP) Logs

No changes

3.50 Tones Service (TONE) Logs

No changes

3.51 Resource Management (RESM) Logs

No changes

Appendix J: MCS Operational Measurements

1 Operational Measurements Overview

1.1 Introduction

This document shall be considered an “amendment” to the previous release’s (MCS 4.0) Operational Measurements Description document. In other words, the MCS 4.0 document will act as the “base” document with all adds/changes/deletes captured in this amendment.

The MCS 4.0 OMs Description document can be found in Livelink at <http://livelink.us.nortel.com/livelink/livelink.exe?func=ll&objId=7698565&objAction=browse&sort=name>

2 OM Groups Added

The OM Groups in this section have been added to this release.

2.1 OM Group Name: NCASLINK

2.1.1 Affected NE

This OM group is for the System Manager.

2.1.2 Explanation

The NCAS OM group provides data regarding the state and usage of the NCAS link. Applications use this link for non-call-associated signaling with the CS2K Core, such as QSIP queries.

2.1.3 Register Descriptions

Table 1: NCAS Register Descriptions

Register Name	Type	Description
<i>linkUp</i>	Counter	The number of times the logical link is transitioned into a

		connected state due to administrative action, network repair, etc.
<i>linkDown</i>	Counter	The number of times the logical link is transitioned into a disconnected state due to administrative action, network failure, etc.
<i>msgSent</i>	Counter	The number of messages successfully sent over the link.
<i>msgRcvd</i>	Counter	The number of messages successfully received over the link.
<i>msgSendFail</i>	Counter	The number of messages that failed to be sent.
<i>msgRcvFail</i>	Counter	The number of messages that failed to be received.

2.1.4 Thresholding and Alarms

Not Applicable.

2.2 OM Group Name: SIP_Delay_Report

2.2.1 Affected NE

This OM group is common to all network elements.

2.2.2 Explanation

The SIP_Delay_Report OM group provides information about processing time for SIP transactions on a network element. Unless otherwise noted in the SIP_Delay_Report Row Descriptions below, transaction processing time is the time that elapses between the receipt of a SIP request message and the sending of the response to that request message. The SIP_Delay_Report OM group is a set of rows and columns, where each row is a transaction type and the columns are registers that form a histogram of discrete time values.

2.2.3 Row Descriptions

Table 2: SIP_Delay_Report Row Descriptions

Row Name	Type	Description
<i>ACK</i>	Set of Peg Registers	This row provides a set of delay peg-registers for processing delay for ACKs in transactions. The delay values for ACKs are measured as the time taken between sending a 200 response back to the originator of a request message and the originator's responding with an ACK. If the final response to an INVITE is non-200, no delay statistics for the ACK are captured in the report (the ACK is effectively ignored for purposes of delay).

<i>INFO</i>	Set of Peg Registers	This row provides a set of delay peg registers for processing delay For INFO transactions.
<i>INVITE</i>	Set of Peg Registers	This row provides a set of delay peg-registers for processing delay for INVITE transactions. Delay values for INVITE transactions are measured as the time taken until a 18x or final response is sent back to the originator to the INVITE transaction (whichever comes first).
<i>MESSAGE</i>	Set of Peg Registers	This row provides a set of delay peg-registers for processing delay for MESSAGE transactions.
<i>NOTIFY</i>	Set of Peg Registers	This row provides a set of delay peg-registers for processing delay for NOTIFY transactions.
<i>OPTIONS</i>	Set of Peg Registers	This row provides a set of delay peg-registers for processing delay for OPTIONS transactions.
<i>PUBLISH</i>	Set of Peg Registers	This row provides a set of delay peg-registers for processing delay for PUBLISH transactions.
<i>REFER</i>	Set of Peg Registers	This row provides a set of delay peg-registers for processing delay for REFER transactions.
<i>REGISTER</i>	Set of Peg Registers	This row provides a set of delay peg-registers for processing delay for REGISTER transactions.
<i>SUBSCRIBE</i>	Set of Peg Registers	This row provides a set of delay peg-registers for processing delay for SUBSCRIBE transactions.
<i>UPDATE</i>	Set of Peg Registers	This row provides a set of delay peg-registerspeg-register for processing delay for UPDATE transactions.
<i>[Totals]</i>	Set of Peg Registers	This row is the totals of the columns of all of the above rows.

2.2.4 Register Descriptions

The registers in each of the rows in SIP_Delay_Report represent discrete time values. Each register is a count of the number of transactions whose processing time took at least that amount of time but less than the amount of time represented by the next register in ascending order.

Table 2: SIP_Delay_Report Register Descriptions

Register Name	Type	Description
_25ms	Peg Register	The number of transactions of the specified type which have completed in 25 milliseconds or less.
_50ms	Peg Register	The number of transactions of the specified type which have completed in more than 25 milliseconds but less than or equal to 50 milliseconds.

_100ms	Peg Register	The number of transactions of the specified type which have completed in more than 50 milliseconds but less than or equal to 100 milliseconds.
_125ms	Peg Register	The number of transactions of the specified type which have completed in more than 100 milliseconds but less than or equal to 125 milliseconds.
_150ms	Peg Register	The number of transactions of the specified type which have completed in more than 125 milliseconds but less than or equal to 150 milliseconds.
_175ms	Peg Register	The number of transactions of the specified type which have completed in more than 150 milliseconds but less than or equal to 175 milliseconds.
_200ms	Peg Register	The number of transactions of the specified type which have completed in more than 175 milliseconds but less than or equal to 200 milliseconds.
_250ms	Peg Register	The number of transactions of the specified type which have completed in more than 200 milliseconds but less than or equal to 250 milliseconds.
_300ms	Peg Register	The number of transactions of the specified type which have completed in more than 250 milliseconds but less than or equal to 300 milliseconds.
_350ms	Peg Register	The number of transactions of the specified type which have completed in more than 300 milliseconds but less than or equal to 350 milliseconds.
_400ms	Peg Register	The number of transactions of the specified type which have completed in more than 350 milliseconds but less than or equal to 400 milliseconds.
_450ms	Peg Register	The number of transactions of the specified type which have completed in more than 400 milliseconds but less than or equal to 450 milliseconds.
_500ms	Peg Register	The number of transactions of the specified type which have completed in more than 450 milliseconds but less than or equal to 500 milliseconds.
_550ms	Peg Register	The number of transactions of the specified type which have completed in more than 500 milliseconds but less than or equal to 550 milliseconds.
_600ms	Peg Register	The number of transactions of the specified type which have completed in more than 550 milliseconds but less than or equal to 600 milliseconds.
_650ms	Peg Register	The number of transactions of the specified type which have completed in more than 600 milliseconds but less than or equal to 650 milliseconds.
_700ms	Peg Register	The number of transactions of the specified type which have completed in more than 650 milliseconds but less than or equal to 700 milliseconds.
_750ms	Peg Register	The number of transactions of the specified type which have completed in more than 700 milliseconds

		but less than or equal to 750 milliseconds.
_800ms	Peg Register	The number of transactions of the specified type which have completed in more than 750 milliseconds but less than or equal to 800 milliseconds.
_850ms	Peg Register	The number of transactions of the specified type which have completed in more than 800 milliseconds but less than or equal to 850 milliseconds.
_900ms	Peg Register	The number of transactions of the specified type which have completed in more than 850 milliseconds but less than or equal to 900 milliseconds.
_950ms	Peg Register	The number of transactions of the specified type which have completed in more than 900 milliseconds but less than or equal to 950 milliseconds.
_1000ms	Peg Register	The number of transactions of the specified type which have completed in more than 950 milliseconds but less than or equal to 1000 milliseconds.
_1250ms	Peg Register	The number of transactions of the specified type which have completed in more than 1000 milliseconds but less than or equal to 1250 milliseconds.
_1500ms	Peg Register	The number of transactions of the specified type which have completed in more than 1250 milliseconds but less than or equal to 1500 milliseconds.
_1750ms	Peg Register	The number of transactions of the specified type which have completed in more than 1500 milliseconds but less than or equal to 1750 milliseconds.
_2000ms	Peg Register	The number of transactions of the specified type which have completed in more than 1750 milliseconds but less than or equal to 2000 milliseconds.
_3000ms	Peg Register	The number of transactions of the specified type which have completed in more than 2000 milliseconds but less than or equal to 3000 milliseconds.
_4000ms	Peg Register	The number of transactions of the specified type which have completed in more than 3000 milliseconds but less than or equal to 4000 milliseconds.
_8000ms	Peg Register	The number of transactions of the specified type which have completed in more than 4000 milliseconds but less than or equal to 8000 milliseconds.
_16000ms	Peg Register	The number of transactions of the specified type which have completed in more than 8000 milliseconds but less than or equal to 16000 milliseconds.

_32000ms	Peg Register	The number of transactions of the specified type which have completed in more than 16000.

2.2.5 Thresholding and Alarms

Not Applicable.

2.3 OM Group Name: SIP_Inbound_Response_Report

2.3.1 Affected NE

This OM group is common to all network elements.

2.3.2 Explanation

The purpose of the SIP_Inbound_Response_Report OM group is to provide counts of various responses messages received by a network element in response to outgoing SIP request messages. The SIP_Inbound_Response_Report OM group consists of a set of rows with each row containing an identical set of peg-registers. Each row corresponds to an outgoing SIP request message and each register (column) corresponds to a SIP response type of an incoming response. Additional SIP Response message details can be found in RFC-3261.

2.3.3 Row Descriptions

Table 3: SIP_Inbound_Response_Report Row Descriptions

Row Name	Type	Description
<i>INFO</i>	Set of Peg Registers	This row provides a set of peg-registers for the different response types for INFO transactions. Each peg-register counts the number of responses of the specified type that have been received in response to outgoing INFO transactions.
<i>INVITE</i>	Set of Peg Registers	This row provides a set of peg-registers for the different response types for INVITE transactions. Each peg-register counts the number of responses of the specified type that have been received in response to outgoing INVITE transactions.
<i>MESSAGE</i>	Set of Peg Registers	This row provides a set of peg-registers for the different response types for MESSAGE transactions. Each peg-register counts the number of responses of the specified type that have been received in response to outgoing MESSAGE transactions.
<i>NOTIFY</i>	Set of Peg Registers	This row provides a set of peg-registers for the different response types for NOTIFY transactions. Each peg-register counts the number of responses of the specified

		type that have been received in response to outgoing NOTIFY transactions.
<i>OPTIONS</i>	Set of Peg Registers	This row provides a set of peg-registers for the different response types for OPTIONS transactions. Each peg-register counts the number of responses of the specified type that have been received in response to outgoing OPTIONS transactions.
<i>PUBLISH</i>	Set of Peg Registers	This row provides a set of peg-registers for the different response types for PUBLISH transactions. Each peg-register counts the number of responses of the specified type that have been received in response to outgoing PUBLISH transactions.
<i>REFER</i>	Set of Peg Registers	This row provides a set of peg-registers for the different response types for REFER transactions. Each peg-register counts the number of responses of the specified type that have been received in response to outgoing REFER transactions.
<i>REGISTER</i>	Set of Peg Registers	This row provides a set of peg-registers for the different response types for REGISTER transactions. Each peg-register counts the number of responses of the specified type that have been received in response to outgoing REGISTER transactions.
<i>SUBSCRIBE</i>	Set of Peg Registers	This row provides a set of peg-registers for the different response types for SUBSCRIBE transactions. Each peg-register counts the number of responses of the specified type that have been received in response to outgoing SUBSCRIBE transactions.
<i>UPDATE</i>	Set of Peg Registers	This row provides a set of peg-registers for the different response types for UPDATE transactions. Each peg-register counts the number of responses of the specified type that have been received in response to outgoing UPDATE transactions.
<i>[Totals]</i>	Set of Peg Registers	This row is a set of totals of the other rows.

2.3.4 Register Descriptions

Each of the registers in a SIP_Inbound_Response_Report row counts the SIP response messages of the indicated type which have been received in response to outgoing SIP messages corresponding to the row type. For example, the _302 register in the INVITE row is a count of the number of 302 response messages received in response to outgoing INVITE messages in the current Office Transfer Period.

Table 2: SIP_Inbound_Response_Report Register Descriptions

Register	Type	Description

Name		
_200	Peg Register	This register provides a count of the number of “200 OK” responses received in the current Office Transfer Period.
_202	Peg Register	This register provides a count of the number of “202 Accepted” responses received in the current Office Transfer Period.
_300	Peg Register	This register provides a count of the number of “300 Multiple Choices” responses received in the current Office Transfer Period.
_301	Peg Register	This register provides a count of the number of “301 Moved Permanently” responses received in the current Office Transfer Period.
_302	Peg Register	This register provides a count of the number of “302 Moved Temporarily” responses received in the current Office Transfer Period.
_303	Peg Register	This register provides a count of the number of “303 See Other” responses received in the current Office Transfer Period.
_304	Peg Register	This register provides a count of the number of “304 Warning” responses received in the current Office Transfer Period.
_305	Peg Register	This register provides a count of the number of “305 Use Proxy” responses received in the current Office Transfer Period.
_400	Peg Register	This register provides a count of the number of “400 Bad Request” responses received in the current Office Transfer Period.
_401	Peg Register	This register provides a count of the number of “401 Unauthorized” responses received in the current Office Transfer Period.
_402	Peg Register	This register provides a count of the number of “402 Payment Required” responses received in the current Office Transfer Period.
_403	Peg Register	This register provides a count of the number of “403 Forbidden” responses received in the current Office Transfer Period.
_404	Peg Register	This register provides a count of the number of “404 Not Found” responses received in the current Office Transfer Period.
_405	Peg Register	This register provides a count of the number of “405 Method Not Allowed” responses received in the current Office Transfer Period.
_406	Peg Register	This register provides a count of the number of “406 Not Acceptable” responses received in the current Office Transfer Period.
_407	Peg Register	This register provides a count of the number of “407 Proxy

		Authentication Required” responses received in the current Office Transfer Period.
_408	Peg Register	This register provides a count of the number of “408 Request Timeout” responses received in the current Office Transfer Period.
_409	Peg Register	This register provides a count of the number of “409 Conflict” responses received in the current Office Transfer Period.
_410	Peg Register	This register provides a count of the number of “410 Gone” responses received in the current Office Transfer Period.
_411	Peg Register	This register provides a count of the number of “411 Length Required” responses received in the current Office Transfer Period.
_412	Peg Register	This register provides a count of the number of “412 Conditional Request Failed” responses received in the current Office Transfer Period.
_413	Peg Register	This register provides a count of the number of “413 Request Entity Too Large” responses received in the current Office Transfer Period.
_414	Peg Register	This register provides a count of the number of “414 Request-URI Too Long” responses received in the current Office Transfer Period.
_415	Peg Register	This register provides a count of the number of “415 Unsupported Media Type” responses received in the current Office Transfer Period.
_420	Peg Register	This register provides a count of the number of “420 Bad Extension” responses received in the current Office Transfer Period.
_423	Peg Register	This register provides a count of the number of “423 Interval Too Brief” responses received in the current Office Transfer Period.
_480	Peg Register	This register provides a count of the number of “480 Temporarily Unavailable” responses received in the current Office Transfer Period.
_481	Peg Register	This register provides a count of the number of “481 Call Or Transaction Does Not Exist” responses received in the current Office Transfer Period.
_482	Peg Register	This register provides a count of the number of “482 Loop Detected” responses received in the current Office Transfer Period.
_483	Peg Register	This register provides a count of the number of “483 Too Many Hops” responses received in the current Office Transfer Period.
_484	Peg Register	This register provides a count of the number of “484 Address Incomplete” responses received in the current Office Transfer Period.

_485	Peg Register	This register provides a count of the number of “485 Ambiguous” responses received in the current Office Transfer Period.
_486	Peg Register	This register provides a count of the number of “486 Busy Here” responses received in the current Office Transfer Period.
_487	Peg Register	This register provides a count of the number of “487 Request Terminated” responses received in the current Office Transfer Period.
_488	Peg Register	This register provides a count of the number of “488 Not Acceptable Here” responses received in the current Office Transfer Period.
_489	Peg Register	This register provides a count of the number of “489 Bad Event” responses received in the current Office Transfer Period.
_491	Peg Register	This register provides a count of the number of “491 Request Pending” responses received in the current Office Transfer Period.
_500	Peg Register	This register provides a count of the number of “500 Server Internal Error” responses received in the current Office Transfer Period. Note that this register is a call failure indication, and it has configurable thresholds for minor, major, and critical alarms.
_501	Peg Register	This register provides a count of the number of “501 Not Implemented” responses received in the current Office Transfer Period.
_502	Peg Register	This register provides a count of the number of “502 Bad Gateway” responses received in the current Office Transfer Period.
_503	Peg Register	This register provides a count of the number of “503 Service Unavailable” responses received in the current Office Transfer Period.
_504	Peg Register	This register provides a count of the number of “504 Server Timeout” responses received in the current Office Transfer Period.
_505	Peg Register	This register provides a count of the number of “505 Version Not Supported” responses received in the current Office Transfer Period.
_600	Peg Register	This register provides a count of the number of “600 Busy Everywhere” responses received in the current Office Transfer Period.
_603	Peg Register	This register provides a count of the number of “603 Decline” responses received in the current Office Transfer Period.
_604	Peg Register	This register provides a count of the number of “604 Does Not Exist Anywhere” responses received in the current Office Transfer Period.

_606	Peg Register	This register provides a count of the number of “606 Not Acceptable” responses received in the current Office Transfer Period.
Unknown 2xx	Peg Register	This register provides a count of the number of unrecognized 200-series responses received in the current Office Transfer Period.
Unknown 3xx	Peg Register	This register provides a count of the number of unrecognized 300-series responses received in the current Office Transfer Period.
Unknown 4xx	Peg Register	This register provides a count of the number of unrecognized 400-series responses received in the current Office Transfer Period.
Unknown 5xx	Peg Register	This register provides a count of the number of unrecognized 500-series responses received in the current Office Transfer Period.
Unknown 6xx	Peg Register	This register provides a count of the number of unrecognized 600-series responses received in the current Office Transfer Period.
Total	Peg Register	This register provides a count of the totals of all other registers in the row.

2.3.5 Thresholding and Alarms

There is a set of configurable thresholds for “500 Server Internal Error” responses. There are 3 configurable thresholds for each SIP transaction request type (row), representing minor, major, and critical alarms. The thresholds are configured via the Configuration Parameters entry for a network element in the management GUI. Each threshold indicates a percentage of total responses which are 500 responses. Threshold checking and alarm generation or clearing is performed at the end of each Office Transfer Period. If, when the threshold check is performed, the percentage of 500 responses reaches or exceeds one of the thresholds, an alarm of the corresponding type and severity will be raised. If an alarm was previously raised and the percentage of 500 responses falls below all configured thresholds when the threshold check is performed, the alarm will be retired automatically.

2.4 OM Group Name: SIP_Outbound_Response_Report

2.4.1 Affected NE

This OM group is common to all network elements.

2.4.2 Explanation

The SIP_Outbound_Response_Report OM group consists of a set of rows with each row containing an identical set of peg-registers. Each row corresponds to an incoming SIP request message and each register (column) corresponds to a SIP response type of an outgoing response. The registers count the number of SIP responses of the corresponding type that have been sent in response to incoming SIP request messages for the corresponding row type in the current Office Transfer Period. Additional SIP Response message details can be found in RFC-3261.

2.4.3 Row Descriptions

Table 4: SIP_Outbound_Response_Report Row Descriptions

Row Name	Type	Description
<i>INFO</i>	Set of Peg Registers	This row provides a set of peg-registers for the different response types for INFO transactions. Each peg-register counts the number of responses of the specified type that have been sent in response to incoming INFO transactions.
<i>INVITE</i>	Set of Peg Registers	This row provides a set of peg-registers for the different response types for INVITE transactions. Each peg-register counts the number of responses of the specified type that have been sent in response to incoming INVITE transactions.
<i>MESSAGE</i>	Set of Peg Registers	This row provides a set of peg-registers for the different response types for MESSAGE transactions. Each peg-register counts the number of responses of the specified type that have been sent in response to incoming MESSAGE transactions.
<i>NOTIFY</i>	Set of Peg Registers	This row provides a set of peg-registers for the different response types for NOTIFY transactions. Each peg-register counts the number of responses of the specified type that have been sent in response to incoming NOTIFY transactions.
<i>OPTIONS</i>	Set of Peg Registers	This row provides a set of peg-registers for the different response types for OPTIONS transactions. Each peg-register counts the number of responses of the specified type that have been sent in response to incoming OPTIONS transactions.
<i>PUBLISH</i>	Set of Peg Registers	This row provides a set of peg-registers for the different response types for PUBLISH transactions. Each peg-register counts the number of responses of the specified type that have been sent in response to incoming PUBLISH transactions.
<i>REFER</i>	Set of Peg Registers	This row provides a set of peg-registers for the different response types for REFER transactions. Each peg-register counts the number of responses of the specified type that have been sent in response to incoming

		REFER transactions.
<i>REGISTER</i>	Set of Peg Registers	This row provides a set of peg-registers for the different response types for REGISTER transactions. Each peg-register counts the number of responses of the specified type that have been sent in response to incoming REGISTER transactions.
<i>SUBSCRIBE</i>	Set of Peg Registers	This row provides a set of peg-registers for the different response types for SUBSCRIBE transactions. Each peg-register counts the number of responses of the specified type that have been sent in response to incoming SUBSCRIBE transactions.
<i>UPDATE</i>	Set of Peg Registers	This row provides a set of peg-registers for the different response types for UPDATE transactions. Each peg-register counts the number of responses of the specified type that have been sent in response to incoming UPDATE transactions.
<i>[Totals]</i>	Set of Peg Registers	This row is a set of totals of the other rows.

2.4.4 Register Descriptions

Each of the registers in a *SIP_Outbound_Response_Report* row counts the SIP response messages of the indicated type which have been sent in response to incoming SIP messages corresponding to the row type. For example, the *_302* register in the *INVITE* row is a count of the number of 302 responses messages sent in response to incoming *INVITE* messages in the current Office Transfer Period.

Table 2: SIP_Outbound_Response_Report Register Descriptions

Register Name	Type	Description
<i>_200</i>	Peg Register	This register provides a count of the number of “200 OK” responses sent in the current Office Transfer Period.
<i>_202</i>	Peg Register	This register provides a count of the number of “202 Accepted” responses sent in the current Office Transfer Period.
<i>_300</i>	Peg Register	This register provides a count of the number of “300 Multiple Choices” responses sent in the current Office Transfer Period.
<i>_301</i>	Peg Register	This register provides a count of the number of “301 Moved Permanently” responses sent in the current Office Transfer Period.
<i>_302</i>	Peg Register	This register provides a count of the number of “302 Moved Temporarily” responses sent in the current Office Transfer Period.
<i>_303</i>	Peg Register	This register provides a count of the number of “303 See Other” responses sent in the current Office Transfer Period.

_304	Peg Register	This register provides a count of the number of “304 Warning” responses sent in the current Office Transfer Period.
_305	Peg Register	This register provides a count of the number of “305 Use Proxy” responses sent in the current Office Transfer Period.
_400	Peg Register	This register provides a count of the number of “400 Bad Request” responses sent in the current Office Transfer Period.
_401	Peg Register	This register provides a count of the number of “401 Unauthorized” responses sent in the current Office Transfer Period.
_402	Peg Register	This register provides a count of the number of “402 Payment Required” responses sent in the current Office Transfer Period.
_403	Peg Register	This register provides a count of the number of “403 Forbidden” responses sent in the current Office Transfer Period.
_404	Peg Register	This register provides a count of the number of “404 Not Found” responses sent in the current Office Transfer Period.
_405	Peg Register	This register provides a count of the number of “405 Method Not Allowed” responses sent in the current Office Transfer Period.
_406	Peg Register	This register provides a count of the number of “406 Not Acceptable” responses sent in the current Office Transfer Period.
_407	Peg Register	This register provides a count of the number of “407 Proxy Authentication Required” responses sent in the current Office Transfer Period.
_408	Peg Register	This register provides a count of the number of “408 Request Timeout” responses sent in the current Office Transfer Period.
_409	Peg Register	This register provides a count of the number of “409 Conflict” responses sent in the current Office Transfer Period.
_410	Peg Register	This register provides a count of the number of “410 Gone” responses sent in the current Office Transfer Period.
_411	Peg Register	This register provides a count of the number of “411 Length Required” responses sent in the current Office Transfer Period.
_412	Peg Register	This register provides a count of the number of “412 Conditional Request Failed” responses sent in the current Office Transfer Period.
_413	Peg Register	This register provides a count of the number of “413 Request Entity Too Large” responses sent in the current Office Transfer Period.
_414	Peg Register	This register provides a count of the number of “414 Request-URI Too Long” responses sent in the current Office Transfer Period.
_415	Peg Register	This register provides a count of the number of “415 Unsupported Media Type” responses sent in the current Office Transfer Period.

_420	Peg Register	This register provides a count of the number of “420 Bad Extension” responses sent in the current Office Transfer Period.
_423	Peg Register	This register provides a count of the number of “423 Interval Too Brief” responses sent in the current Office Transfer Period.
_480	Peg Register	This register provides a count of the number of “480 Temporarily Unavailable” responses sent in the current Office Transfer Period.
_481	Peg Register	This register provides a count of the number of “481 Call Or Transaction Does Not Exist” responses sent in the current Office Transfer Period.
_482	Peg Register	This register provides a count of the number of “482 Loop Detected” responses sent in the current Office Transfer Period.
_483	Peg Register	This register provides a count of the number of “483 Too Many Hops” responses sent in the current Office Transfer Period.
_484	Peg Register	This register provides a count of the number of “484 Address Incomplete” responses sent in the current Office Transfer Period.
_485	Peg Register	This register provides a count of the number of “485 Ambiguous” responses sent in the current Office Transfer Period.
_486	Peg Register	This register provides a count of the number of “486 Busy Here” responses sent in the current Office Transfer Period.
_487	Peg Register	This register provides a count of the number of “487 Request Terminated” responses sent in the current Office Transfer Period.
_488	Peg Register	This register provides a count of the number of “488 Not Acceptable Here” responses sent in the current Office Transfer Period.
_489	Peg Register	This register provides a count of the number of “489 Bad Event” responses sent in the current Office Transfer Period.
_491	Peg Register	This register provides a count of the number of “491 Request Pending” responses sent in the current Office Transfer Period.
_500	Peg Register	This register provides a count of the number of “500 Server Internal Error” responses sent in the current Office Transfer Period. Note that this register is a call failure indication, and it has configurable thresholds for minor, major, and critical alarms.
_501	Peg Register	This register provides a count of the number of “501 Not Implemented” responses sent in the current Office Transfer Period.
_502	Peg Register	This register provides a count of the number of “502 Bad Gateway” responses sent in the current Office Transfer Period.
_503	Peg Register	This register provides a count of the number of “503 Service Unavailable” responses sent in the current Office Transfer Period.

_504	Peg Register	This register provides a count of the number of “504 Server Timeout” responses sent in the current Office Transfer Period.
_505	Peg Register	This register provides a count of the number of “505 Version Not Supported” responses sent in the current Office Transfer Period.
_600	Peg Register	This register provides a count of the number of “600 Busy Everywhere” responses sent in the current Office Transfer Period.
_603	Peg Register	This register provides a count of the number of “603 Decline” responses sent in the current Office Transfer Period.
_604	Peg Register	This register provides a count of the number of “604 Does Not Exist Anywhere” responses sent in the current Office Transfer Period.
_606	Peg Register	This register provides a count of the number of “606 Not Acceptable” responses sent in the current Office Transfer Period.
Unknown 2xx	Peg Register	This register provides a count of the number of unrecognized 200-series responses sent in the current Office Transfer Period.
Unknown 3xx	Peg Register	This register provides a count of the number of unrecognized 300-series responses sent in the current Office Transfer Period.
Unknown 4xx	Peg Register	This register provides a count of the number of unrecognized 400-series responses sent in the current Office Transfer Period.
Unknown 5xx	Peg Register	This register provides a count of the number of unrecognized 500-series responses sent in the current Office Transfer Period.
Unknown 6xx	Peg Register	This register provides a count of the number of unrecognized 600-series responses sent in the current Office Transfer Period.
Total	Peg Register	This register provides a count of the totals of all other registers in the row.

2.4.5 Thresholding and Alarms

Not Applicable.

2.5 OM Group Name: SIP_Transaction_Report

2.5.1 Affected NE

This OM group is common to all network elements.

2.5.2 Explanation

The SIP_Transaction_Report OM group consists of a set of rows with each row containing an identical set of peg-registers. Each row corresponds to an incoming or outgoing SIP transaction. There are two registers (columns) indicating the direction of transaction and a register indicating the current number of transactions which are currently active.

2.5.3 Row Descriptions

Table 5: SIP_Transaction_Report Row Descriptions

Row Name	Type	Description
<i>ACK</i>	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active ACK transactions.
<i>BYE</i>	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active BYE transactions.
<i>CANCEL</i>	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active CANCEL transactions.
<i>INFO</i>	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active INFO transactions.
<i>INVITE</i>	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active INVITE transactions.
<i>MESSAGE</i>	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active MESSAGE transactions.
<i>NOTIFY</i>	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active NOTIFY transactions.
<i>OPTIONS</i>	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active OPTIONS transactions.
<i>PRACK</i>	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active PRACK transactions.
<i>PUBLISH</i>	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active PUBLISH transactions.
<i>REFER</i>	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound,

		and currently active REFER transactions.
<i>REGISTER</i>	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active REGISTER transactions.
<i>SUBSCRIBE</i>	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active SUBSCRIBE transactions.
<i>UPDATE</i>	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active UPDATE transactions.
<i>[Totals]</i>	Two Peg Registers and one Usage Register	This row is a set of totals of the other rows.

2.5.4 Register Descriptions

Each row in SIP_Transaction_Report contains two peg registers and one usage register. The registers are described in the SIP_Transaction_Report Register Descriptions table below.

Table 2: SIP_Transaction_Report Register Descriptions

Register Name	Type	Description
Inbound	Peg Register	This register provides a count of the number of SIP transactions of the corresponding row type which have been initiated by incoming message in the current Office Transfer Period.
Outbound	Peg Register	This register provides a count of the number of SIP transactions of the corresponding row type which have been initiated by incoming message in the current Office Transfer Period.
Active	Usage Register	This register provides a count of the currently active transactions of the corresponding row type. Each time a transaction is initiated by an incoming or outgoing message, this counter is incremented. Each time the transaction is concluded by the sending or receiving of a response message, this counter is decremented.

2.5.5 Thresholding and Alarms

Not Applicable.

2.6 OM Group Name: CPCheckpoint

2.6.1 Affected NE

Session Manager.

2.6.2 Explanation

This OM group is a usage counter on the inactive session Manager. It tracks the number of calls that the inactive session manager is checkpointing. In the event of a failover these calls will survive the failover. On the active node this counter is always 0. It is only tracking checkpointed calls on the hot standby instance.

2.6.3 Register Descriptions

Table 6: DB Register Descriptions

Register Name	Type	Description
<i>CallP Checkpoint</i>	Usage	Counts the current number of checkpointed calls.

2.6.4 Thresholding and Alarms

Not Applicable.

2.7 OM Group Name: Presence_Event_Report

2.7.1 Affected NE

This OM group is associated with the SESM only.

2.7.2 Explanation

The Presence Event Report OM group tracks the behavior of the various presence events that are processed by the SESM. Each of the rows in the report represents one of the eight presence event types as well as a total row.

Here is a brief description of the various presence events:

- Activity – A client has indicated that it has detected user activity (keyboard/mouse).
- End Call – A client has ended a call (excludes collaboration sessions).
- Inactive – A client has indicated that it has not detected user activity (keyboard/mouse) for an extended period of time.

- Login – A client has logged into the SESM.
- Logout – A client has logged out from the SESM.
- Manual – A client has indicated a presence state change through manual intervention (user interaction with the client interface).
- New Call – A client has entered into a stable call (excludes collaboration sessions).

2.7.3 Register Descriptions

Table 7: Presence Event Report Register Descriptions

Register Name	Type	Description
<i>Created</i>	Counter	The number of events of that type that have been created in the system. This gives the operator an idea of the relative frequency of occurrence for that presence event type.
<i>Processed</i>	Counter	The number of events of that type that have been processed by the presence event processor. Just because a presence event is created does not mean that it is guaranteed to ever be processed. It may be eliminated from consideration because of an opposing presence event (see optimized register).
<i>Optimized</i>	Counter	The number of events of that type that have been optimized by the presence vent processor. An event is optimized when an opposing presence vent is processed that nullifies the presence vent change that would have taken place. For instance, if a new call event is processed and the presence event processor sees that there is an opposing end call event in the queue or parked, then there is no further point in processing either event. The two events cancel each other out.
<i>Queued</i>	Usage	The number of events that are currently in the presence event processor queue waiting to be processed. This OM represents a snapshot view of the current presence event queue depth.
<i>Parked</i>	Usage	The number of events that have been initially processed, but must wait for the presence guard timer to expire before being processed. These events are “parked” waiting for the guard timer to expire. When the guard timer expires, they re-enter the presence event queue (which does not cause a second pegging of the processed counter for that event).

2.7.4 Thresholding and Alarms

Not Applicable.

2.8 OM Group Name: SyncSystem

2.8.1 Affected NE

This OM group is common to all network elements.

2.8.2 Explanation

The SyncSystem OM group tracks the processing of synchronization checkpoints between two synchronization peers. One peer is the checkpoint sender containing information to be checkpointed. The other is the checkpoint receiver requesting that information in order to be able to replicate the relevant state of the sender. Each peer group is collectively known as a "Sync System". Examples of a sync system include:

- The two network element instances in a fault tolerant pair. The checkpoint sender is the active instance and the checkpoint receiver is the synchronizing/hotStandby instance. The checkpoints contain call information.
- A network element instance and the fault processing manager (SM or FPM) to which the instance's alarms are sent¹. The checkpoint sender is the network element instance, and the checkpoint receiver the fault processing manager. The checkpoints contain alarm information.

Each sync system has two rows, one corresponding to the sender and the other to the receiver, only one of which is used at a given point in time depending on the role of the network element (i.e. sender or receiver) in the sync system. The rows follow this naming convention:

- "<SyncSystemName>:send" for the sender row. For example "FaultTolerance:send".
- "<SyncSystemName>:recv" for the sender row. For example "FaultTolerance:recv".

2.8.3 Register Descriptions

Table 8: SyncSystem Register Descriptions

Register Name	Type	Description
<i>checkpointGenerators</i>	Usage	Number of entities capable of generating checkpoints.
<i>checkpointsSent</i>	Counter	Number of checkpoints sent.
<i>receiverLag</i>	Usage	Measure of how far behind the checkpoint

¹ Note that a fault processing manager reports its own alarms to itself via an internal mechanism, not via checkpoints.

		receiver is receiving checkpoints relative to how quickly the checkpoint sender is sending them.
<i>processedLag</i>	Usage	Measure of how far behind the checkpoint receiver is processing checkpoints relative to how quickly it's receiving them.

2.8.4 Thresholding and Alarms

Not Applicable.

2.9 OM Group Name: HALayer

2.9.1 Affected NE

This new OM group is only applicable to the new IBM BladeCenter-T based RTP Media Portal.

2.9.2 Explanation

The new BladeCenter-T RTP Media Portal supports all traditional RTP Media Portal functions – and introduces support for the clustering of RTP Media Portals into “N+1” fault tolerant service clusters (i.e. “N” active instances, and “1” standby). As a result, the new BladeCenter-T RTP Media Portal and the traditional CPX8216-T RTP Media Portal are identical from a functional perspective but very different conceptually:

- the CPX8216-T RTP Media Portal is comprised of software and hardware components having a static relationship.
- the BladeCenter-T “N+1” RTP Media Portal Service Cluster is comprised of a set of logical Service Instances (“N” active instances of RTP Media Portal that actively process calls) that “float” over a predefined set of underlying physical hardware (the Service Nodes). There is no fixed relationship between an active RTP Media Portal Service Instance and its hosting hardware. This allows very robust handling of failures as Service Instances can fail and be quickly re-instantiated on another available piece of hardware.

The software sub-component that provides the fault tolerance mechanisms (heartbeating, checkpointing, failure detection,...) supporting the “N+1” RTP Media Portal Service Cluster is the High Availability Layer (HAL). The new

HALayer OM Group gathers statistics on the performance of these underlying fault tolerance mechanisms.

2.9.3 Register Descriptions

Table 9: HALayer Register Descriptions

Register Name	Type	Description
<i>statusCnt</i>	Meter	Number of internal status change events generated by the Fault-tolerance mechanisms on this Service Node.
<i>updateCnt</i>	Meter	The number of Service Instances that have joined the Service Cluster (from the perspective of this service node).
<i>chkPointsRcvd</i>	Meter	Number of checkpoints received by this Service Node.
<i>chkPointsSent</i>	Meter	The number of checkpoints sent by this Service Node.
<i>activeInstances</i>	Meter	Number of active Service Instances in the Service Cluster associated with this Service Node.
<i>standbyInstances</i>	Meter	The number of standby Service Instances in the Service Cluster associated with this Service Node.

2.9.4 Thresholding and Alarms

Not Applicable.

3 OM Groups Modified

The OM Groups in this section have been modified for this release

3.1 OM Group Name: Emergency

3.1.1 Affected NE

This OM Group is applicable to SESM

3.1.2 Explanation

This OM Group was modified to add the “operatorCallbackAttempt”, “operatorCallbackConnected”, “operatorConnectFailure” counters.

3.1.3 Register Descriptions

Table 3: Emergency Register Descriptions

Register Name	Type	Description
operatorCallbackAttempt	Counter	This OM is pegged when the E911 emergency operator attempts to callback the originating (enterprise) caller. This OM is not pegged for residential operator callback attempts.
operatorCallbackConnected	Counter	This OM is pegged when the E911 emergency operator established voicepath with the originating (enterprise) caller. This OM is not generated for residential operator callbacks.
operatorConnectFailure	Counter	This OM is pegged when a PSAP connect failure is detected while attempting to establish an emergency call. Connection failure scenarios include: no answer timeout, busy trunks or gateway unavailable.

3.2 OM Group Name: PRESENCE

3.2.1 Affected NE

This OM Group is associated with the SESM only.

3.2.2 Explanation

This OM Group was modified to add two registers: `throttleNotifySelfOnly` and `throttleNotifyAll`. These registers track interactions between the presence service and overload controls on the SESM.

3.2.3 Register Descriptions

Table 10: Presence Register Descriptions

Register Name	Type	Description
<i>throttleNotifySelfOnly</i>	Counter	This OM is pegged every time the system does not send out notifications to non-self subscriptions because of a presence state change during minor overload. This is pegged once for the entire state change, and does not reflect the actual number of NOTIFY messages that were not sent out.
<i>throttleNotifyAll</i>	Counter	This OM is pegged every time the system does not send out any notifications, including self-subscriptions because of a presence state change during major or severe overload. This is pegged once for the entire state change, and does not reflect the actual number of NOTIFY messages that were not sent out.

4 OM Groups Deleted

The OM Groups in this section have been deleted in this release.

4.1 OM Group Name: <name>

4.1.1 Affected NE

This OM Group was applicable to <xxx>.

4.1.2 Explanation

This OM Group was deleted due to <xxx>.

(I)SN09FF OSS Guide

Advance Feature Guide

Copyright © 2006 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-i09FF-OSS
Product release: (I)SN09FF
Document release: Standard 01.06
Date: June 2006
United States of America