Nortel Communication Server 1000

New in this Release

Release: 6.0
Document Revision: 03.14

www.nortel.com

NN43001-115

Nortel Communication Server 1000
Release: 6.0
Publication: NN43001-115
Document release date: 19 February 2010

Contents

How to get help 11
Getting help from the Nortel Web site 11
Getting help over the telephone from a Nortel Solutions Center 11
Getting help from a specialist by using an Express Routing Code 12
Getting help through a Nortel distributor or reseller 12

Introduction 13
Subject 13
Applicable Systems 13
Conventions 13

Overview 15
Key Attributes 15
New for CS 1000 Release 6.0 15
- Packages 16
- Hardware 16
- Applications 18
- Documents 18

Task flows 19
- Referenced documents 20
- Network 21
- Linux base and UCM 21
- Network Routing Service 22
- CS 1000E 23
- Co-res 24
- CS 1000M 25
- Signaling Server 26
- Branch Office 27
- SIP Line 28
- Subscriber Manager 29

Additional updates for CS 1000 Release 6.0 30
Features and enhancements described in this document 31

Unified Communications Management services 35
Overview 35

New for CS 1000 Release 6.0 36
Product name change 36
UCM Common Services deployment 36
CP PM Co-resident Call Server and Signaling Server 37
Virtual Terminal support for Linux based elements 37
Commercial off-the-shelf hardware platform types 37
New features 37
Certificates 38
Certificate Endpoints 38
Deployment Manager 39
Base Manager 39
Patching Manager 40
Web Services 40
Intra System Signaling Security synchronization 40

Port Access Restrictions **41**
Overview 41
Benefits 41

UDT Universal Digital Trunk card **43**
Overview 43
Feature interactions 45
Installation guidelines - default mode 45
Installation guidelines - non default mode 46
UDT CC daughter board installation 47
Physical installation of the UDT card 48
UDT card configuration 50
UDT card configuration as 2.0 Mb PRI2 (E1) 50
Task summary list 50
LD 17 configure PRI loop and D-channel interface 51
LD 15 configure PRI customer 51
LD 16 configure ISDN service route 52
LD 14 configure service channels and PRI trunks 52
LD 73 configure system timers and clock controller 53
UDT card configuration as 2.0 Mb DTI (E1) 54
Task summary list 54
LD 17 configure DTI loop 54
LD 73 configure 2.0 Mb DTI ABCD signaling bit tables and system timers 54
LD 16 configure 2.0 Mb DTI trunk route 55
LD 14 configure service channels and 2.0 Mb DTI trunks 55
UDT card configuration as DPNSS/DASS (E1) 56
Task summary list 56
LD 17 configure DPNSS/DASS loop and D-channel 56
LD 74 configure DDSL block for DPNSS/DASS2 57
LD 16 configure route data block 58

LD 14 configure DPNSS/DASS2 trunks 58
Enable UDT card 59
Enable UDT card configured as PRI/PRI2 59
Enable UDT card configured as DTI/DTI2 59
Enable UDT card configured as DPNSS/DASS 60
Enable clock controller functionality 60
Maintenance and diagnostics 60
LD programs 60
UDT card startup and status Check 62
Inventory 65
Command Line Interface 66
Main menu 67
System Maintenance 68
UDT Administration 72
UDT Maintenance 74
Remote access to the UDT card 77
Firmware upgrade 77
Feature interactions 78
Firmware download duration 78
Security 78
Loadware patch 78
Firmware download guidelines 79
Loadware Configuration Procedures 79
LD 60 Check the existing firmware version of UDT cards 80
LD 22 Print the existing peripheral software download version (PSDL) 81
LD 143 Execute the UDT card upgrade for the required UDT cards 83

Subscriber Manager 2.0 85
Overview 85
Embedded directory 85
Flow through provisioning 86
Location name mapping to element and target 86
Localized name support 86
Username property 86
Bulk add accounts 86
Account reassignment to another subscriber 86
Account disassociation from the subscriber 86
Account synchronization 87
CSV subscriber synchronization 87
LDAP subscriber synchronization 87
CSV subscriber export 87
Numbering group 87
Operation, Administration and Maintenance Transaction Audit and Security Event logging 87

Subscriber Manager license 87

Zone Based Dialing **89**
Overview 89

CP PM Co-resident Call and Signaling Server **91**
Overview 91
Supported configurations 91
Supported configurations 92
CS 1000E TDM 93
CP PM Co-res CS and SS Server limitations 94
CP PM Co-res CS and SS upgrade paths 95
SIP Line support on CP PM Co-res CS and SS Server 96
CP PM Co-res CS and SS Server patch types 100
Hardware 101
Software applications 103
High Availability support 104
IP Telephony Node Manager 104

Media Gateway 1010 (MG 1010) Chassis **105**
Overview 105
Physical description 105
Front components 106
Rear components 107

Media Gateway Extended Peripheral Equipment Controller (MG XPEC) **109**
Overview 109
Physical description 109

Commercial Off The Shelf servers **111**
Overview 111
Dell R300 specifications 111
IBM x3350 specifications 111

SIP Line **113**
Overview 113
SIP Line architecture 113
Required packages 114
Hardware and software requirements 115

UNIStim Security DTLS **117**
Overview 117
DTLS and IP Phone registration 117
Supported hardware 118
Security levels 118

Secure File Transfer Protocol 119
Overview 119
SFTP for Linux platforms 120
File transfer options for Linux and VxWorks platforms 120
SSH Library upgrade 121
Limitations 121

IP Call Recording for Office Communications Server support 123
Overview 123
Supported platforms 123

IP Client enhancements 125
Overview 125
Normal Mode Indication 125
Caller ID display order 126
Languages 126

Multi Directory Number recording 127
Overview 127

Record on Demand 129
Overview 129

TLS and SRTP 131
Overview 131

Calling Line ID Enhancement 133
Overview 133
Interfaces 133
Benefits 134

Network Routing Service enhancements 135
Overview 135
Redirect Server support on Linux-based NRS 135
MySQL Database Migration 135
Same cost routing with SPS and GK 135
Source base routing for Multimedia Convergence Manager 136
Service domain name can be configured as an IP Address in NRS Manager 136
Operation, Administration and Maintenance Transaction Activity and Security Event Logging 136
Access to NRS CLI command 136

Patching Manager 139
Overview 139

Base Manager 141
Overview 141

Deployment Manager 143
Overview 143
Application installation using Deployment Manager 143
Base applications 144
Nortel applications 144

Unicode Name Directory Server 145
Overview 145

SNMP Linux 147
Overview 147
SNMP trap and Management Information Base enhancements 147
SNMP Profile Manager 148

Web Services API Administration 149
Overview 149

OAM Transaction Activity and Security Event Logging 151
Overview 151
Log configuration 152

Linux Security Hardening 155
Overview 155

Element Manager Phone Provisioning Enhancement 157
Overview 157
Phone Key Programming 157
Terminal Number enhancements 158
Publish additional phone attributes in Subscriber Manager 158
Employee reference field 158
Create a template from existing phone 158
Export and Import of Templates 158
Migrate the Element Manager Phone Provisioning database from Solid to MySQL 158

IP security for Intra System Signaling Security 161
Overview 161
ISSS/IPsec 162
Unified Communications Management IPsec ISSS management 163
ISSS synchronization and activation 164

IP Telephony nodes 165

Vacant Number Routing and MCDN Alternate Routing 167
Overview 167

Telephony Manager 4.0 169
Overview 169

Web Report Scheduling 169
CND synchronization 169
Concurrency support 170

Instant Messaging and Presence Application 171
Deployment model 171
System Component Description 172

Software Input/Output prompts, responses and commands 175
Numerical list of new packages 175
LD 02: Traffic 175
LD 10: Analog (500/2500) Telephone Administration 176
LD 11: Digital Telephone Administration 177
LD 12: Attendant Consoles 179
LD 15: Customer Data Block 179
LD 16: Route Data Block, Automatic Trunk Maintenance 181
LD 17: Configuration Record 1 183
LD 20: Print Routine 1 185
LD 21: Print Routine 2 186
LD 22: Print Routine 3 186
LD 81: Features and Station Print 186
LD 83: Terminal Number Sort and Print 187
LD 117: Ethernet and Alarm Management 187
LD 43: Equipment Datadump 226
LD 96: D-channel Diagnostic 226
LD 135: Core Common Equipment Diagnostic 227

System messages 229
AUD: Software Audit (LD 44) 230
BUG: Software Error Monitor 231
CCBR: Customer Configuration Backup and Restore 240
DCH: D-channel Diagnostic (LD 96) 240
ELAN: Ethernet Local Area Network 241
ERR: Error Monitor (Hardware) 242
ESA: Emergency Services Access 244
HWI: Hardware Infrastructure Maintenance 245
IOD: Input/Output Diagnostic (LD 37) 245
ITG: Integrated IP Telephony Gateway 245
MGMT: Management messages. 245
MSDL: Multi-purpose Serial Data Link 246
NBWM: Network Bandwidth Management 246
NPR: Network and Peripheral Equipment Diagnostic (LD 32) 247
OSM: Operating System Messaging 247
PRI: Primary Rate Interface Diagnostic (LD 60) 249
SCH: Service Change 249

SEC: Security Notification Monitor 267
SRPT: System Reports 281
SYS: System Loader 287
TEMU: Tape Emulation 290
TFC: Traffic Control (LD 2) 291
TTY: Teletype Error Reports 291

How to get help

This chapter explains how to get help for Nortel products and services.

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the telephone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also get help over the telephone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the telephone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Introduction

This document is a global document. Contact your system supplier or your Nortel representative to verify that the hardware and software described are supported in your area.

Subject

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server (CS) 1000 Release 6.0 software. For more information on legacy products and releases, click the Technical Documentation link under Support & Training on the Nortel home page:

www.nortel.com

Applicable Systems

This document applies to the following systems:

- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)
- Meridian 1 PBX 61C
- Meridian 1 PBX 81C

Conventions

Terminology

In this document, the following systems are referred to generically as "system":

- Communication Server 1000M (CS 1000M)
- Communication Server 1000E (CS 1000E)
- Meridian 1

Overview

Communication Server (CS) 1000 Release 6.0 is the latest release for the CS 1000 family of products. CS 1000 Release 6.0 is a further evolution of the traditional TDM enterprise network to a converged IP based network.

The CS 1000 Release 6.0 is a reliable and secure platform for Voice over IP (VoIP) communications and is designed to be a more open and simplified platform, which speeds deployment and improves manageability.

Key Attributes

- **Adaptable to meet current and future needs**
  - Delivers investment protection and evolution path to next-generation multimedia communications
- **Superior IP Telephony experience**
  - More open platform to take advantage of innovative applications, and feature-rich next generation clients
- **Improved reliability and security**
  - Business continuity improvement from a reliable and secure environment
- **Simplified convergence solution**
  - Product portfolio simplified for easier deployment, configuration and management

New for CS 1000 Release 6.0

The following sections provide a description of what's new in CS 1000 Release 6.0.

Packages

CS 1000 Release 6.0 introduces two new packages.

- 417—SIP Line package supports SIP Line Service, which enables users to be configured with a Universal Extension SIPN or SIP3 and provides a logical connection for Nortel or 3rd party SIP clients
- 420—Zone Based Dialing (ZDM) package supports Zone Based Dialing, which applies to CS 1000E (including CP-PM Co-Res) and MG 1000B

Hardware

CS 1000 Release 6.0 introduces two new servers.

- Dell R300
- IBM x3350

These servers provide increased reliability through the use of redundant power supplies and RAID 1 arrays. Server performance is enhanced by more powerful processors (compared to previously introduced COTS servers) and greater memory capacity.

For more information about Dell R300 and IBM x3350 servers, see "Commercial Off The Shelf servers" (page 111).

The following hardware is not supported in CS 1000 Release 6.0:

- NTDU62AA Call Server
- NTDK20 Small System Controller (SSC) Card

UDT Universal Digital Trunk card

CS 1000 Release 6.0 introduces the NTDW79AAE5 Universal Digital Trunk (UDT) card and the NTDW12AAE5 Universal Clock Controller (UDT CC) daughter board for CS 1000E systems. The UDT card and daughter board replace the NTAK79, NTAK10, NTBK50, NTRB21, NTAK20, NTAK93, and NTAK09 cards.

Initially, the UDT card and daughter board will be available in the European Union.

For more information about the UDT card and daughterboard functionality, see *Circuit Card Reference* (NN43001-311).

For more information about the UDT card and daughterboard feature interactions, installation guidelines, configuration guidelines, maintenance and diagnostics, and firmware download guidelines, see "UDT Universal Digital Trunk card" (page 43).

Media Gateway 1010 (MG 1010) Chassis

The Media Gateway 1010 (MG 1010) is a rack mount Media Gateway chassis that provides a larger amount of card slots than a MG 1000E with Media Gateway Expander. The CS 1000E Call Server can connect to and control a maximum of 50 MG 1010s. Each MG 1010 provides a dedicated MGC slot, two dedicated CP PM card slots, and ten slots for IPE cards. The MG 1010 is a single chassis that can provide more processing power and card capacity than a MG 1000E with Media Gateway Expander.

Note: At least one DSP daughterboard is required per MGC.

For more information about the new MG 1010 chassis, see "Media Gateway 1010 (MG 1010) Chassis" (page 105).

CP PM Co-resident Call Server and Signaling Server

A CS 1000 system consists of two major components: a Call Server and a Signaling Server. These two components have historically run on separate Intel Pentium processor-based hardware platforms operating under the VxWorks Operating System.

In CS 1000 Release 6.0, the CP PM Co-resident Call Server and Signaling Server (CP PM Co-res CS and SS) can run the Call Server software, the Signaling Server software, and the System Management software on the same hardware platform operating under the RedHat Linux Operating System. Only the Call Processor-Pentium Mobile (CP PM) platform supports the CP PM Co-res CS and SS.

The key objective of co-residency is to provide a cost-effective solution for CS 1000 system installations that do not require high user capacity or a redundant Call Server.

For more information about CP PM Co-resident Call Server and Signaling Server, see "CP PM Co-resident Call and Signaling Server " (page 91) and *CP PM Co-resident Call Server and Signaling Server Fundamentals* (NN43001-509).

CS 1000E Co-resident Call Server TDM

CS 1000 Release 6.0 supports a TDM-only version of the CP PM Co-res CS and SS system.

For more information about CS 1000E Co-resident Call Server TDM, see "CP PM Co-resident Call and Signaling Server " (page 91).

Applications

CS 1000 Release 6.0 introduces SIP Line Service, which fully integrates Session Initiation Protocol (SIP) endpoints in the CS 1000 system and extends the CS 1000 telephony features to the SIP clients. The SIP Line Service is embedded in each CS 1000 Release 6.0 system and directly manages a number of SIP client applications.

The CP PM Co-resident Call Server and Signaling Server requires you to enable SIP Line. For information about enabling SIP Line on a CP PM Co-res CS and SS server, see "SIP Line support on CP PM Co-res CS and SS Server" (page 96).

For more information about SIP Line Service, see "SIP Line" (page 113).

CS 1000 Release 6.0 also introduces the Instant Messaging and Presence Application. The CS 1000 IM and Presence Application provides IM capability and phone presence information for all CS 1000 users. CS 1000 users can view presence information and exchange Instant Messaging using Nortel's IP Softphone 3456 (IPSP 3456), or Web Client (browser-based IM and Presence client).

For more information about Instant Messaging and Presence Application, see "Instant Messaging and Presence Application" (page 171).

Documents

CS 1000 Release 6.0 introduces the following new documents

- *Network Routing Service Fundamentals* (NN43001-130)

  Note: This document contains information previously contained in *Network Routing Service Installation and Commissioning* (NN43001-564), now retired.

- *SIP Line Fundamentals* (NN43001-508)
- *Signaling Server IP Line Applications Fundamentals* (NN43001-125)

  Note: This document consolidates information previously in the following documents, now retired: *Signaling Server Installation and Commissioning* (NN43001-312) and *IP Line Fundamentals* (NN43100-500).

- *Patching Fundamentals* (NN43001-407)
- *Web Services API Administration* (NN43001-640)
- *Instant Messaging and Presence Application* (NN43001-141)

Task flows

This section provides high level task flows for the installation or upgrade of a CS 1000 system. The task flow indicates the recommended sequence of events to follow when configuring a system and provides the NTP number that contains the detailed procedures required for the task.

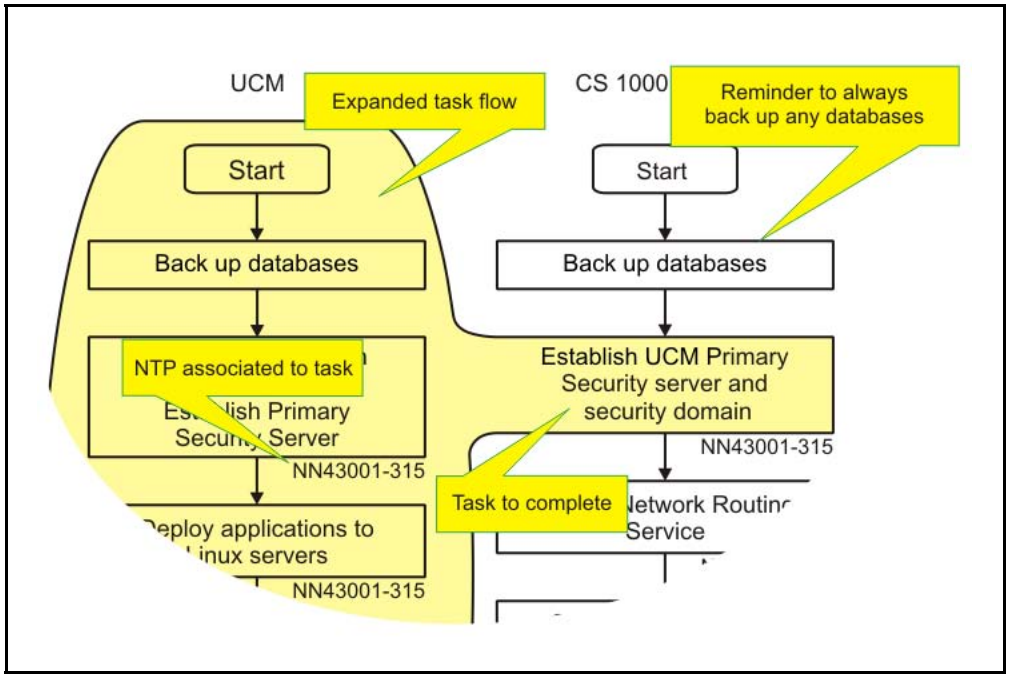
The task flows are also found in *Library Reference* (NN43001-100) are in future releases will be the home for the task flows.

This section provides information on the following topics:

- “Referenced documents” (page 20)
- “Network ” (page 21)
- “Linux base and UCM” (page 21)
- “Network Routing Service” (page 22)
- “CS 1000E” (page 23)
- “Co-res” (page 24)
- “CS 1000M” (page 25)
- “Signaling Server” (page 26)
- “Branch Office” (page 27)
- “SIP Line” (page 28)
- “Subscriber Manager” (page 29)

Figure 1 "Example task flow" (page 20) shows an example and how to interrupt the task flows.

Figure 1
Example task flow



Referenced documents

The following documents are referenced in the task flow diagrams:

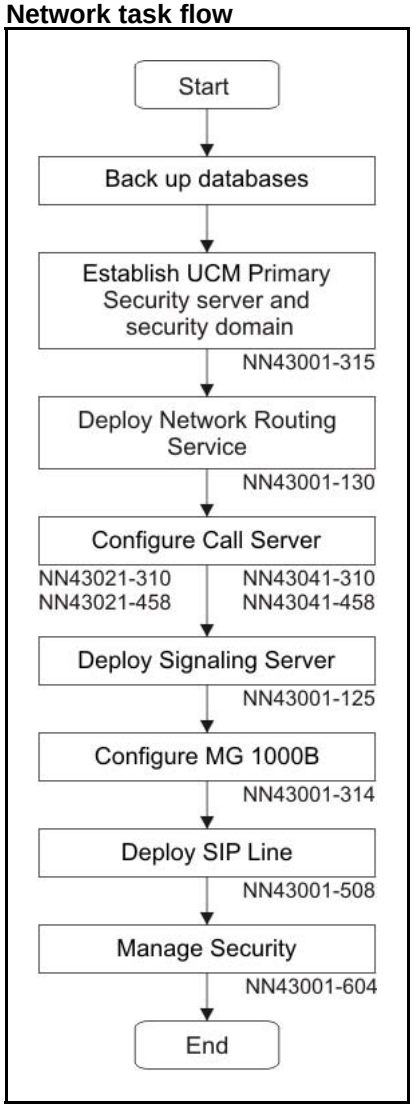
- *Planning the Network-wide Upgrade* (NN43001-406)
- *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315)
- *Unified Communications Management Fundamentals* (NN3001-116)
- *Network Routing Service Fundamentals* (NN43001-130)
- *Communication Server 1000E Installation and Commissioning* (NN43041-310)
- *Communication Server 1000E - Software Upgrades* (NN43041-458)
- *CP PM Co-resident Call Server and Signaling Server* (NN43001-509)
- *Communication Server 1000M and Meridian 1 Large System Installation and Commissioning* (NN43021-310)
- *CS 1000M and Meridian 1 Large System Upgrades Overview* (NN43021-458)
- *Signaling Server IP Line Applications Fundamentals* (NN43001-125)
- *Branch Office Installation and Commissioning* (NN43001-314)

- *SIP Line Fundamentals* (NN43001-508)
- *Subscriber Manager Fundamentals* (NN43001-120)

Network

Figure 2 "Network task flow" (page 21) appears in *Planning the Network-wide Upgrade* (NN43001-406).

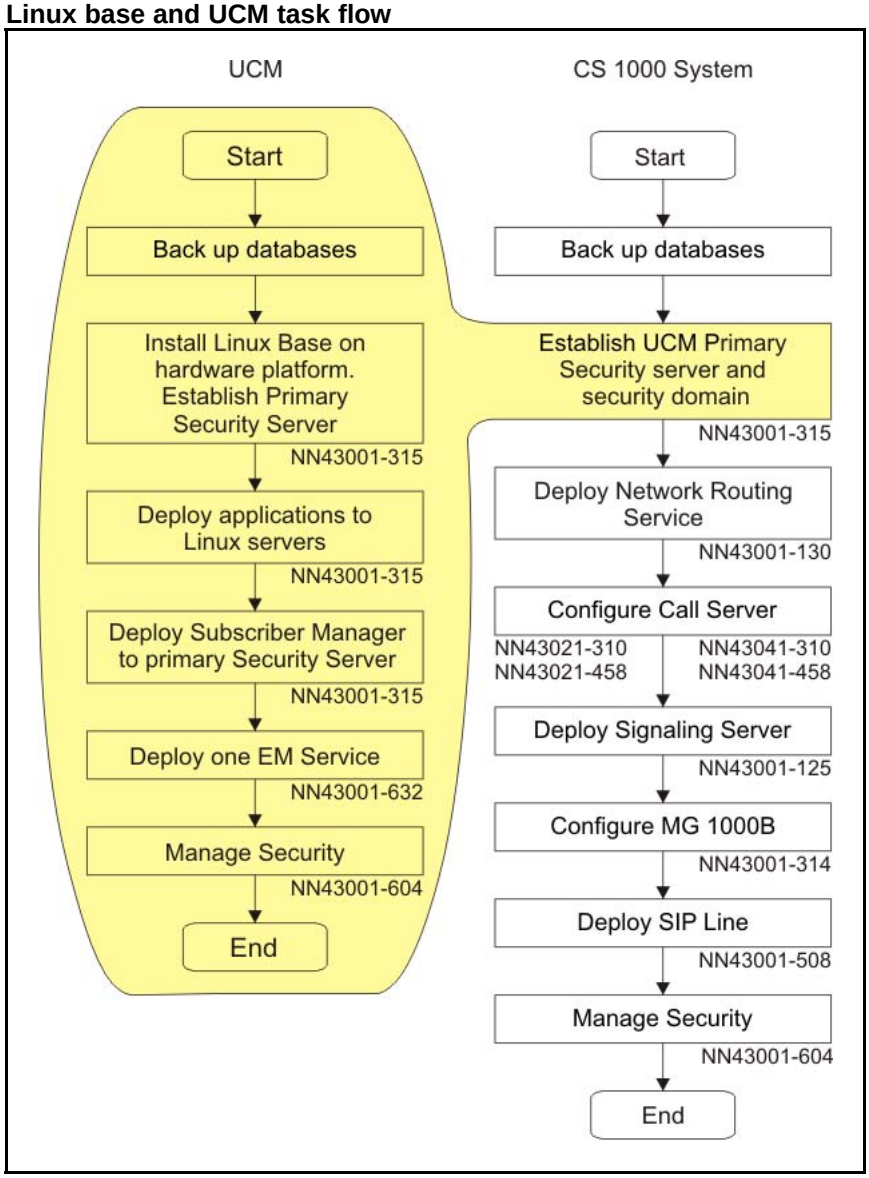
Figure 2
Network task flow



Linux base and UCM

Figure 3 "Linux base and UCM task flow" (page 22) appears in *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315) and *Unified Communications Management Fundamentals* (NN3001-116).

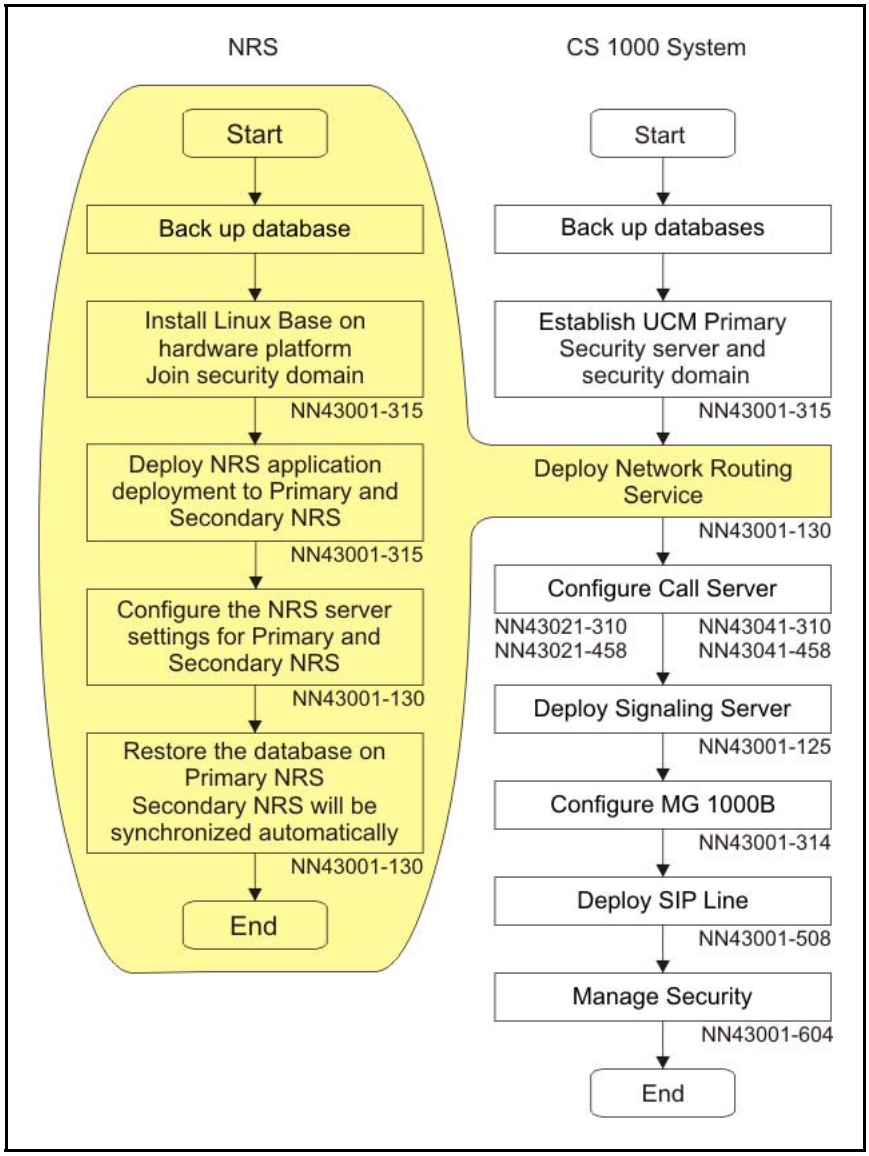
Figure 3
Linux base and UCM task flow



Network Routing Service

Figure 4 "Network Routing Service task flow " (page 23) appears in *Network Routing Service Fundamentals* (NN43001-130).

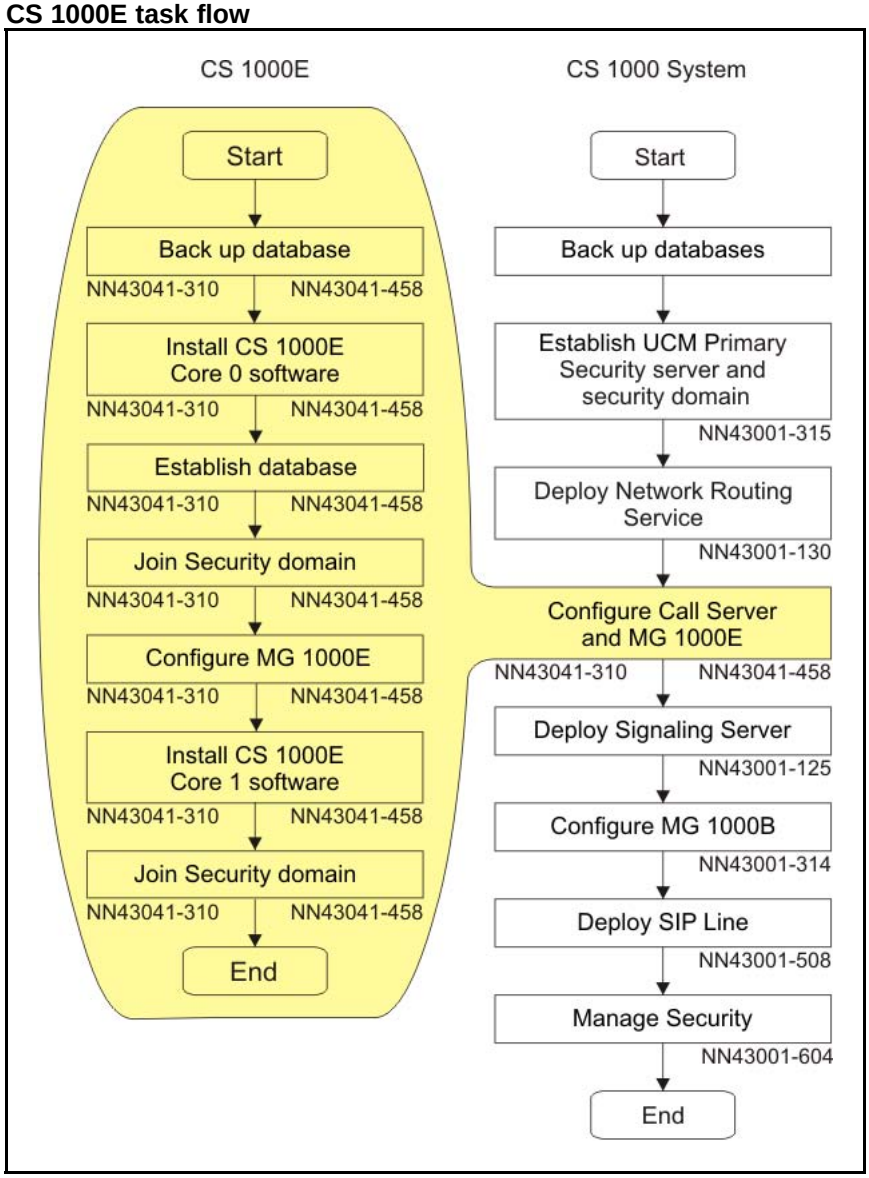
Figure 4
Network Routing Service task flow



CS 1000E

Figure 5 "CS 1000E task flow " (page 24) appears in *Communication Server 1000E Installation and Commissioning* (NN43041-310) and *Communication Server 1000E - Software Upgrades* (NN43041-458).

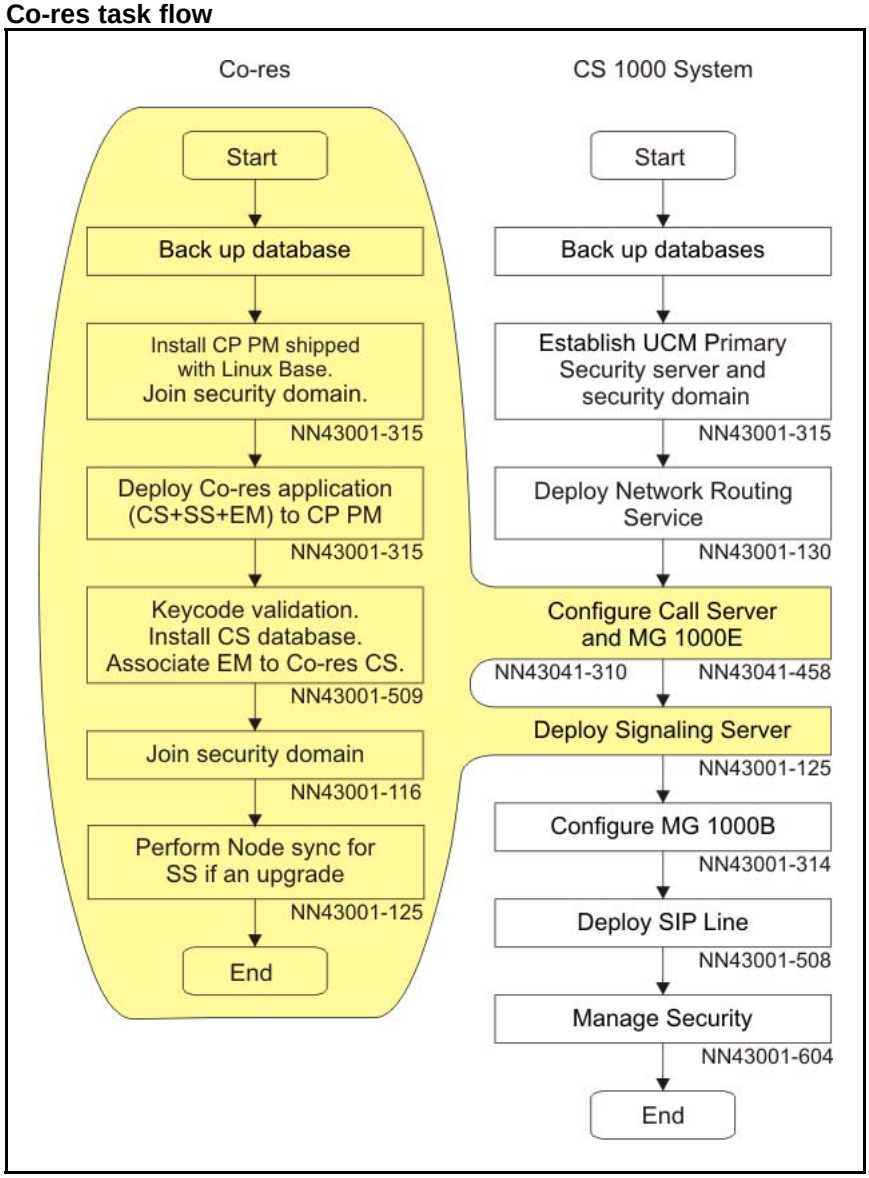
Figure 5
CS 1000E task flow



Co-res

Figure 6 "Co-res task flow " (page 25) appears in *CP PM Co-resident Call Server and Signaling Server* (NN43001-509).

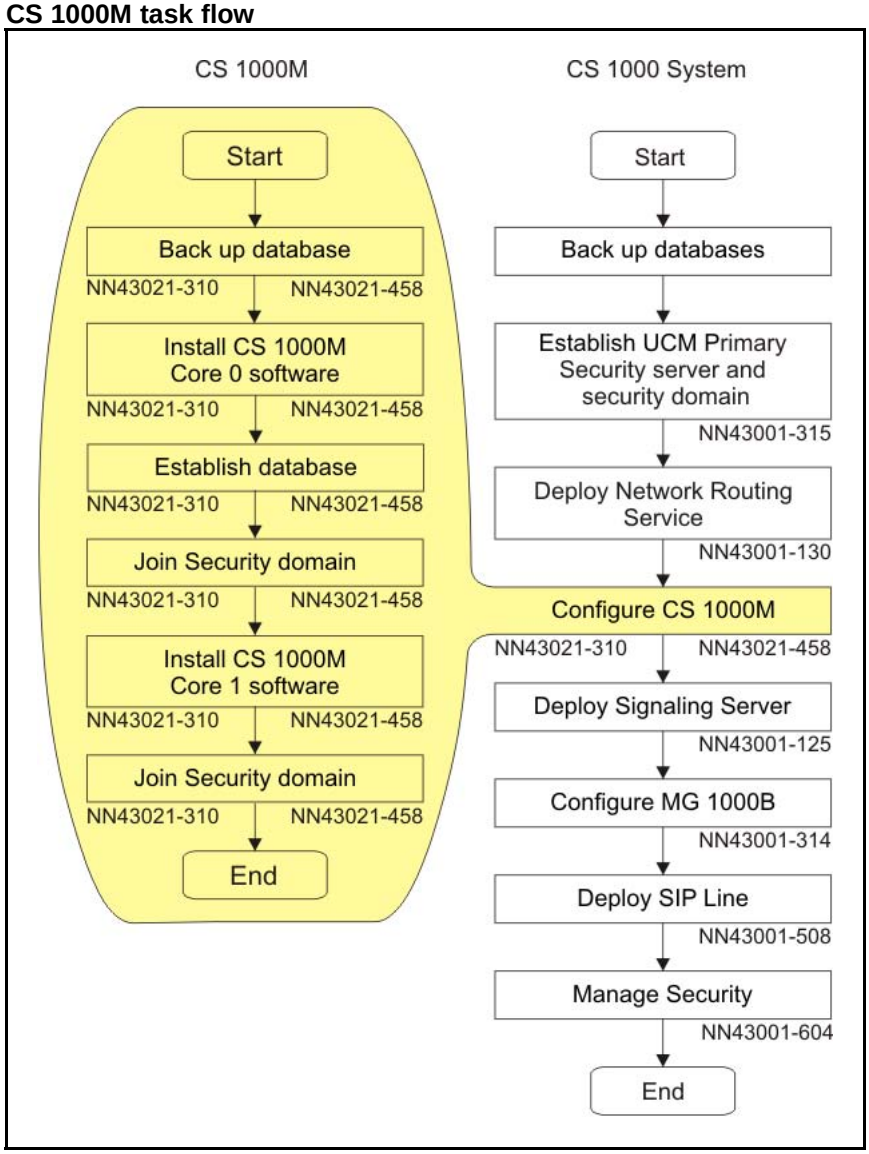
Figure 6
Co-res task flow



CS 1000M

Figure 7 "CS 1000M task flow" (page 26) appears in *Communication Server 1000M and Meridian 1 Large System Installation and Commissioning* (NN43021-310) and *CS 1000M and Meridian 1 Large System Upgrades Overview* (NN43021-458).

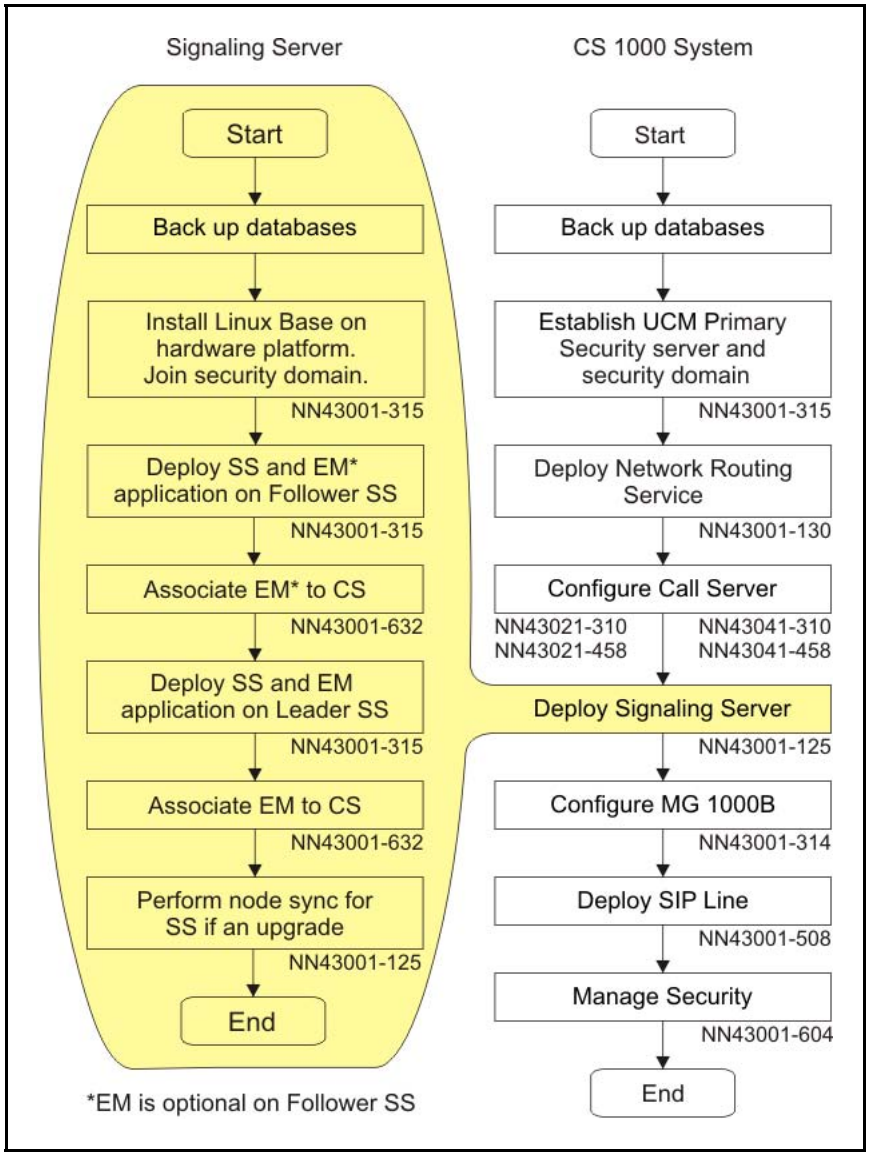
Figure 7
CS 1000M task flow



Signaling Server

Figure 8 "Signaling Server task flow" (page 27) appears in *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

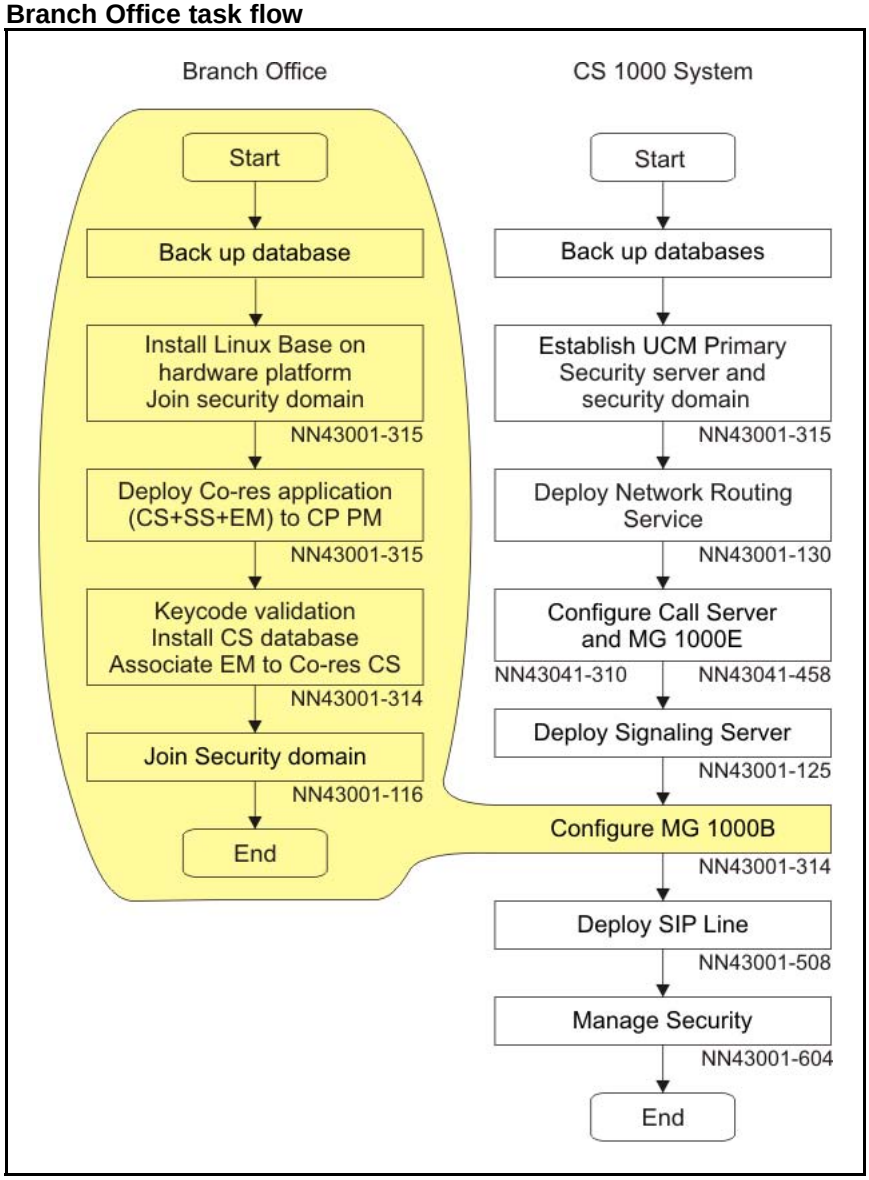
Figure 8
Signaling Server task flow



Branch Office

Figure 9 "Branch Office task flow" (page 28) appears in *Branch Office Installation and Commissioning* (NN43001-314).

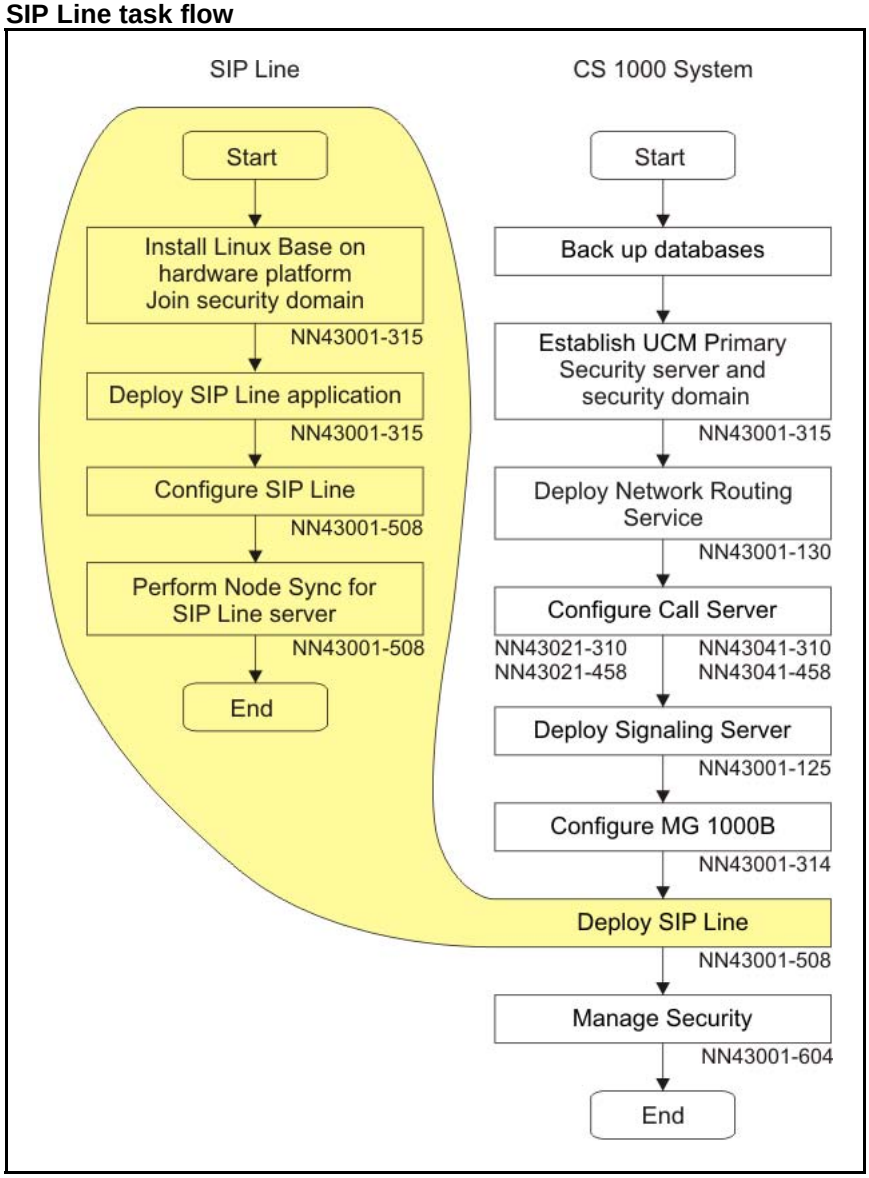
Figure 9
Branch Office task flow



SIP Line

Figure 10 "SIP Line task flow" (page 29) appears in *SIP Line Fundamentals* (NN43001-508).

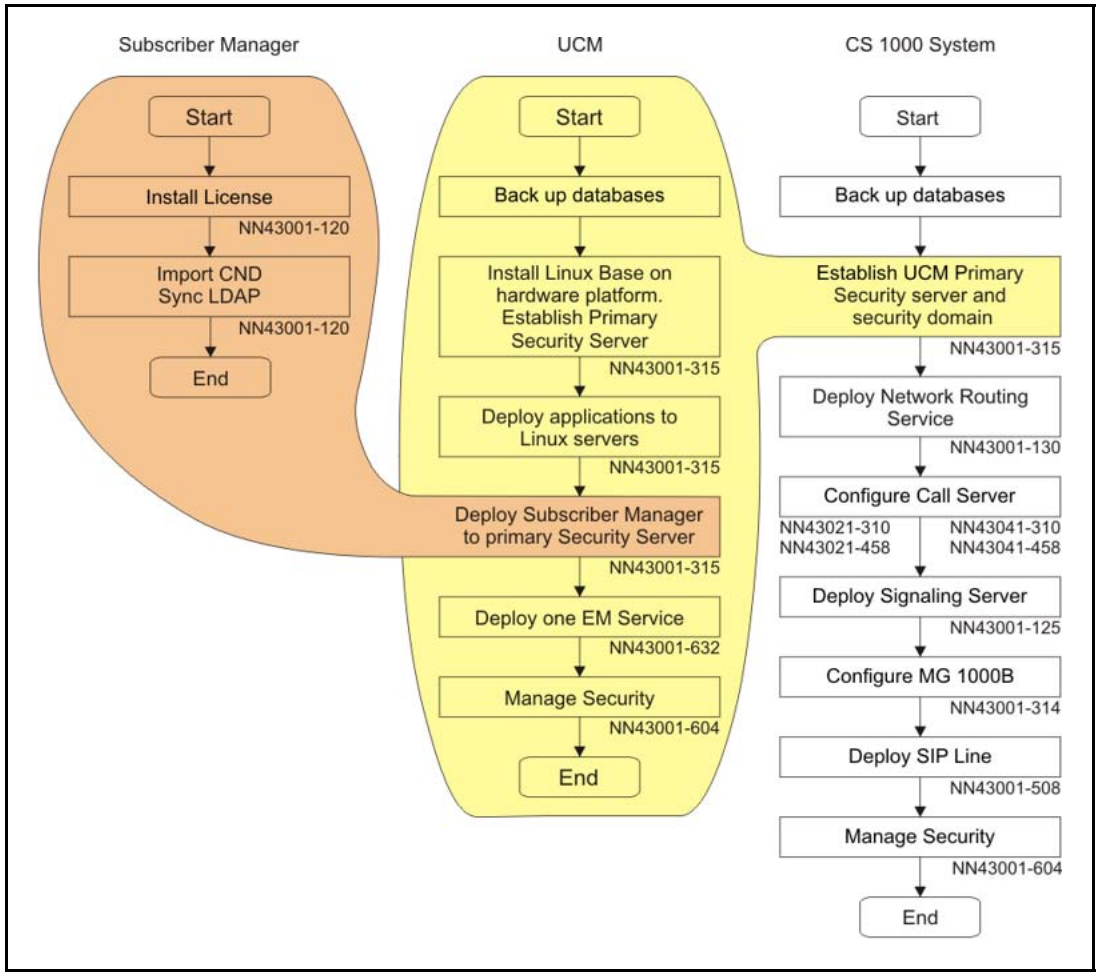
Figure 10
SIP Line task flow



Subscriber Manager

Figure 11 "Subscriber Manager task flow" (page 30) appears in *Subscriber Manager Fundamentals* (NN43001-120).

Figure 11
Subscriber Manager task flow



Additional updates for CS 1000 Release 6.0

This section describes the following additional updates for CS 1000 Release 6.0.

- Enterprise Common Manager (ECM) changes to Unified Communications Management (UCM) Common Services.
- In CS 1000 Release 5.5, ECM hosted its own version of Element Manager that served multiple Call Servers in addition to hosting an element for each Element Manager at a Call Server. In CS 1000 Release 6.0, UCM only hosts elements for each Element Manager at a Call Server. UCM does not host its own version of Element Manager.
- The following documents are retired for CS 1000 Release 6.0.

  — *Network Routing Service Fundamentals* (NN43001-154).

Information from this document is contained in a new document for CS 1000 Release 6.0: *Network Routing Service Fundamentals* (NN43001-130).

— *Signaling Server Installation and Commissioning* (NN43001-312).

Information from this document is consolidated with information from *IP Line Fundamentals* (NN43100-500) into a new document for CS 1000 Release 6.0: *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

— *IP Line Fundamentals* (NN43100-500).

Information from this document is consolidated with information from *Signaling Server Installation and Commissioning* (NN43001-312) into a new document for CS 1000 Release 6.0: *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

— *Meridian 1 Small System Overview* (NN43011-110)

— *Meridian 1 Small System Planning and Engineering* (NN43011-220)

— *Meridian 1 Small System Installation and Commissioning* (NN43011-310)

— *Meridian 1 Small System Software-only Upgrade* (NN43011-459)

— *Communication Server 1000M and Meridian 1 Small System Maintenance* (NN43011-700)

— *CS 1000M and Meridian 1 - 61C CP PII to CS1000M MG CP PII FNF Upgrade* (NN43021-464)

— *CS 1000M and Meridian 1 - 81 to CS1000M MG CP PII FNF Upgrade* (NN43021-468)

— *CS 1000M and Meridian 1 - 81C IGS to CS1000M MG CP PII FNF Upgrade* (NN43021-469)

— *CS 1000M and Meridian 1 - 81C FNF to CS1000M MG CP PII FNF Upgrade* (NN43021-470)

— *CS 1000M and Meridian 1 - CS1000M MG CP PII IGS to CS1000M MG CP PII FNF Upgrade* (NN43021-472)

Features and enhancements described in this document

The following features are described in this document:

- "Unified Communications Management services" (page 35)
- "Port Access Restrictions" (page 41)
- "UDT Universal Digital Trunk card" (page 43)
- "Subscriber Manager 2.0" (page 85)

- “Zone Based Dialing” (page 89)
- “CP PM Co-resident Call and Signaling Server ” (page 91)
- “Media Gateway 1010 (MG 1010) Chassis” (page 105)
- “Media Gateway Extended Peripheral Equipment Controller (MG XPEC)” (page 109)
- “Commercial Off The Shelf servers” (page 111)
- “SIP Line” (page 113)
- “UNIStim Security DTLS ” (page 117)
- “Secure File Transfer Protocol” (page 119)
- “IP Call Recording for Office Communications Server support” (page 123)
- “IP Client enhancements” (page 125)
- “Multi Directory Number recording” (page 127)
- “Record on Demand” (page 129)
- “TLS and SRTP” (page 131)
- “Calling Line ID Enhancement” (page 133)
- “Network Routing Service enhancements” (page 135)
- “Patching Manager” (page 139)
- “Base Manager” (page 141)
- “Deployment Manager” (page 143)
- “Unicode Name Directory Server” (page 145)
- “SNMP Linux” (page 147)
- “Web Services API Administration” (page 149)
- “OAM Transaction Activity and Security Event Logging” (page 151)
- “Linux Security Hardening” (page 155)
- “Element Manager Phone Provisioning Enhancement” (page 157)
- “IP security for Intra System Signaling Security” (page 161)
- “IP Telephony nodes” (page 165)
- “Vacant Number Routing and MCDN Alternate Routing” (page 167)
- “Telephony Manager 4.0” (page 169)
- “Instant Messaging and Presence Application” (page 171)

- “Software Input/Output prompts, responses and commands” (page 175)
- “System messages” (page 229)

Unified Communications Management services

Overview

The Nortel Unified Communications Management (UCM) solution provides you with an intuitive, common interface to manage and run managed elements. UCM is a container that stores several system management elements in a single repository. You have access to all network system management elements under the Unified Communications Management solution. You need to sign in only once to access the elements. A single sign-in eliminates the need for you to reauthenticate when a system management application starts.

UCM Security Services simplifies security control for managed elements and system management applications. UCM Security services manages secure access to Web applications and provides authentication and authorization with a single unified Common Service. UCM secures the delivery of essential identity and application information.

With UCM Common Services, administrators can control which users have access to specific managed elements. They can assign users to roles and map the permissions to those roles to control which operations a user can perform on an assigned managed element. Users can access only assigned elements and perform only the tasks specific to their assigned role and permissions for an element.

With UCM Common Services, the integration of managed elements within a single container provides users with centralized security, user access control, simplified management tasks, improved workflow efficiency, convenience, and time-saving advantages.

UCM Deployment Manager provides two functions for software deployment:

- centralized software deployment
- local software deployment

UCM Common Services runs on all commercial off-the-shelf (COTS) servers and Linux base CP PM servers. The following is a list of the supported platforms:

- IBM x306m. NTDU99AAE5
- HP DL320 G4. NTDU97AAE5
- IBM x3350. NTDW40AAE5
- Dell Power Edge R300. NTDW41AAE6
- CP PM v1

New for CS 1000 Release 6.0

This section describes updates for UCM in CS 1000 Release 6.0.

- "Product name change" (page 36)
- "UCM Common Services deployment" (page 36)
- "CP PM Co-resident Call Server and Signaling Server " (page 37)
- "Virtual Terminal support for Linux based elements" (page 37)
- "Commercial off-the-shelf hardware platform types" (page 37)

Product name change

In CS 1000 Release 6.0, Enterprise Common Manager (ECM) changed to Unified Communications Management (UCM) Common Services.

UCM Common Services deployment

The following summarizes the changes to UCM Common Services deployment:

- One primary security server is required for each secured domain and one backup security server is required on a network.
- Each security server must co-reside with an instance of the LDAP server.
- Replication is unidirectional from the LDAP primary to the backup.
- Perform all administrative changes, for example, security configuration and identity management, on the primary security server. The backup server provides only operational backup for authentication and authorization requests.
- When the primary security server is unreachable, member servers automatically select the backup.

CP PM Co-resident Call Server and Signaling Server

A CS 1000 system consists of two major components: a Call Server and a Signaling Server. These two components have historically run on separate Intel Pentium processor-based hardware platforms operating under the VxWorks Operating System.

For more information, see “CP PM Co-resident Call and Signaling Server ” (page 91) and *CP PM Co-resident Call Server and Signaling Server Fundamentals* (NN43001-509).

Virtual Terminal support for Linux based elements

Virtual Terminal (VT) is a tool that provides terminal access to various devices in the network. In Communication Server 1000 Release 6.0, VT supports a Secure Shell (SSH) connection to the end devices. TCP socket connection continues to function. The internal VT architecture for communication from the user interface to the UCM server is secured by SSLSocket and RSA/AES cryptography. RSA cryptography is a complex algorithm with a key length of 1024, therefore; AES with a VT supported key length of 128 is an improved option over previous releases for bulk data transfers.

Commercial off-the-shelf hardware platform types

The following commercial off-the-shelf (COTS) platform types are new in CS 1000 Release 6.0:

- Dell Power Edge R300
- IBM X3350

For more information about COTS servers, see “Commercial Off The Shelf servers” (page 111) and *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

New features

This section describes new features for UCM in CS 1000 Release 6.0.

- “Certificates” (page 38)
- “Certificate Endpoints” (page 38)
- “Deployment Manager” (page 39)
- “Base Manager” (page 39)
- “Patching Manager” (page 40)
- “Web Services” (page 40)
- “Intra System Signaling Security synchronization” (page 40)

Certificates

Changes to the Certificate Management page include the following:

- This release supports all certificate types. Session Initiation Protocol Transport Layer Security (SIP TLS), Web Secure Sockets Layer (SSL), and Datagram Transport Layer Security (DTLS) are built in certificate types.
- This release introduces a Certificate Revocation feature. An Administrator can revoke certificates that were previously issued, obtain a list of revoked certificates, and update the Certificate Revocation List (CRL).

  For more information about certificates, see *Unified Communications Management Common Services Fundamentals* (NN43001-116)*Security Management Fundamentals* (NN43001-604).

Table 1
Element types versus certificate types

Element type	Supported certificate types
Linux base	SIP TLS, Web SSL, DTLS, default
CS 1000	SIP TLS, DTLS
NRSM	SIP TLS
MGC	Default
SA	Default
MC32	Default

Certificate Endpoints

- A new Number of Service Profiles column in the certificate endpoints table shows the number of service profiles assigned to an endpoint. Click the option next to an endpoint to show the certificate information related to the endpoint.
- Access the service profile details for a selected endpoint by clicking the link in the Service Profile column.
- The certificate authorities table has an Update CRL button to update the Certification Revocation List (CRL) for the endpoint. The CRL is then submitted to the certificate authority.

For more information about certificates, see *Unified Communications Management Common Services Fundamentals* (NN43001-116)*Security Management Fundamentals* (NN43001-604).

Deployment Manager

The Deployment Manager is introduced in CS 1000 Release 6.0 UCM Common Services. Use Deployment Manager to deploy software applications from a central location. Every Linux server that is installed on the network is learned by UCM Common Services where the Deployment Manager is running. The Deployment Manager picks up these servers and initiates a remote software deployment from within UCM Common Services. The Service Cluster management interface adds servers to a cluster from the list of servers that UCM has learned. Before you add the servers to a Cluster, the Deployment Manager feature deploys the necessary software application to each Linux server. Centralized software deployment is the Nortel recommended solution for deployment but local deployment remains an option. Deployment Manager provides the following benefits:

- centralized application deployment and upgrades
- backup and restore capabilities
- Graphical User Interface (GUI) front end to Linux base features

For more information about Deployment Manager, see "Deployment Manager" (page 143).

For more information about certificates, see *Security Management Fundamentals* (NN43001-604).

Base Manager

The Base Manager provides access to a subset of Linux base CLI configuration commands at the UCM GUI. Click on an Element to access the base manager interface.

Linux base commands

Base Manager supports Linux base command. The following new links are supported:

Command	Link name in the navigation tree
appstart	Applications
datetimeconfig ntpconfig	Date and Time
dnsconfig.hostconfig	DNS and Hosts
ecnconfig	Explicit Congestion Notification
routeconfig	Route Table
networkconfig	Network Identity
reboot	No link
swVersionShow	No link

For more information about Base Manager, see “Base Manager” (page 141)and *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Patching Manager

The Patching Manager provides a graphical user interface (GUI) to upload and manage patches and service packs on the Linux targets in the enterprise network. The Patching Manager facilitates the centralized deployment of patches to all target Linux systems within the Unified Communications Management (UCM) security domain. For more information about Patching Manager, see “Patching Manager” (page 139).

Web Services

CS 1000 Release 6.0 introduces a new Web Services interface that is built on UCM Common Services. Web Services uses the Web browser to provide a common navigation hierarchy for installed management applications. From the Web Services interface, you can develop new applications and customize scripts. CLI and overlays remain available and supported. For more information, see “Web Services API Administration” (page 149) and *Web Services API Administration* (NN43001-640).

Intra System Signaling Security synchronization

The Intra System Signaling Security (ISSS) synchronization feature has an improved user interface. ISSS is included as part of the UCM installation and is user configurable on the Primary Security server. The ISSS feature provides a user interface to centrally manage ISSS configuration in the UCM security domain. Elements join the UCM security domain automatically or are manually added through UCM. ISSS elements are categorized as UCM targets or manual targets. UCM targets automatically belong to the UCM security domain where manual targets must be manually configured. For more information, see “IP security for Intra System Signaling Security” (page 161)and *Security Management Fundamentals* (NN43001-604).

Port Access Restrictions

Overview

The Port Access Restrictions feature limits terminal access to the exchange network, private network, and certain services and features.

Port Access Restrictions can be temporarily overridden by the use of other features, if equipped, including Forced Charge Account, Authorization Code, and System Speed Call.

During the call origination process, access checks are made by the system on the following:

- the Class of Service (CLS) of the individual terminal
- the Trunk Group Access Restriction (TGAR) code of the terminal if a direct trunk access code is dialed or as an optional feature when a Basic Alternate Route Selection (BARS) or Network Alternate Route Selection (NARS) access code is dialed
- the area and exchange codes dialed by terminals with Toll Denied or Conditionally Toll Denied Class of Service using direct trunk access codes and Code Restriction tables
- the Network Class of Service (NCOS) of the terminal if BARS/NARS or Coordinated Dialing Plan (CDP) access codes are dialed or if direct trunk access codes are dialed and New Flexible Code Restriction tables are programmed.

If any restrictions are detected when a call is placed, the call is given intercept treatment as defined in the Customer Data Block.

Benefits

On the MGC and MC32S cards, Port Access Restrictions protects the ELAN interface completely.

For more information about Port Access Restrictions, see *Features and Services Fundamentals* (NN43001-106).

UDT Universal Digital Trunk card

Overview

This section provides a description of

- "Feature interactions" (page 45)
- "Installation guidelines - default mode" (page 45)
- "Installation guidelines - non default mode" (page 46)
- "UDT CC daughter board installation" (page 47)
- "Physical installation of the UDT card" (page 48)
- "UDT card configuration" (page 50)
- "UDT card configuration as 2.0 Mb PRI2 (E1)" (page 50)
  - "Task summary list" (page 50)
  - "LD 17 configure PRI loop and D-channel interface" (page 51)
  - "LD 15 configure PRI customer" (page 51)
  - "LD 16 configure ISDN service route" (page 52)
  - "LD 14 configure service channels and PRI trunks" (page 52)
  - "LD 73 configure system timers and clock controller" (page 53)
- "UDT card configuration as 2.0 Mb DTI (E1)" (page 54)
  - "Task summary list" (page 54)
  - "LD 17 configure DTI loop" (page 54)
  - "LD 73 configure 2.0 Mb DTI ABCD signaling bit tables and system timers" (page 54)
  - "LD 16 configure 2.0 Mb DTI trunk route" (page 55)
  - "LD 14 configure service channels and 2.0 Mb DTI trunks" (page 55)
- "UDT card configuration as DPNSS/DASS (E1)" (page 56)
  - "Task summary list" (page 56)
  - "LD 17 configure DPNSS/DASS loop and D-channel" (page 56)

- — “LD 74 configure DDSL block for DPNSS/DASS2” (page 57)
- — “LD 16 configure route data block” (page 58)
- — “LD 14 configure DPNSS/DASS2 trunks” (page 58)

- “Enable UDT card” (page 59)
  - — “Enable UDT card configured as PRI/PRI2” (page 59)
  - — “Enable UDT card configured as DTI/DTI2” (page 59)
  - — “Enable UDT card configured as DPNSS/DASS” (page 60)
  - — “Enable clock controller functionality” (page 60)
- “Maintenance and diagnostics” (page 60)
  - — “LD programs” (page 60)
  - — “UDT card startup and status Check” (page 62)
  - — “Inventory” (page 65)
  - — “Command Line Interface” (page 66)
  - — “Main menu” (page 67)
  - — “System Maintenance” (page 68)
  - — “UDT Administration” (page 72)
  - — “UDT Maintenance” (page 74)
  - — “Remote access to the UDT card” (page 77)
- “Firmware upgrade” (page 77)
  - — “Feature interactions” (page 78)
  - — “Security” (page 78)
  - — “Loadware patch” (page 78)
  - — “Firmware download guidelines” (page 79)
  - — “Loadware Configuration Procedures” (page 79)
  - — “LD 60 Check the existing firmware version of UDT cards” (page 80)
  - — “LD 22 Print the existing peripheral software download version (PSDL)” (page 81)
  - — “LD 143 Execute the UDT card upgrade for the required UDT cards” (page 83)

Feature interactions

- The UDT CC daughter board can only be mounted on the UDT card.
- The NTAK20 CC daughter board can not be mounted on the UDT card.
- 75ohm impedance can be used by converting the UDT card 120ohm impedance using a proper converter.
- The RS232 port is not to be used during normal operation and is for maintenance and configuration only.
- The UDT card does not simulate the TMDI card (NTRB21). Do not configure the UDT card as a TMDI card.
- The UDT card can be used starting with software release X21 Rls 5.0 for CS 1000E systems.
- The UDT card can coexist with other digital trunk cards within the same CS 1000E cabinet.
- The UDT CC daughter board mounted on the UDT card can be used as the CC card serving other digital trunk cards within the same CS 1000E cabinet.
- The NTAK20 CC daughterboard mounted on another digital trunk card can be used as the CC card serving the UDT card within the same CS 1000E cabinet.
- The UDT card can be used as the Secondary clock reference for the NTAK20 CC daughter board.
- Other digital trunk cards can be used as the Secondary clock reference for the UDT CC daughter board.
- The UDT CC daughter board and the NTAK20 CC daughter board can be used in different cabinets within the same system.

Installation guidelines - default mode

- Mount the UDT CC daughter board on the UDT card, if required. See “UDT CC daughter board installation” (page 47).
- Set the DIP switch settings:
  - Set switch number 1
    - ON - E1
    - OFF - T1
- Default setup of E1/T1 parameters for E1 mode:

  - Usage - PRI2
  - CRC4 - NO
- Default setup E1/T1 parameters for T1 mode:
  - Usage - PRI
  - Frame Mode - ESF;
  - Line Code - B8ZS
  - Yellow Alarm - FDL
  - LBO - 0-133 FT
- Insert the UDT card and connect the carrier cable (E1/T1 link). See "Physical installation of the UDT card" (page 48).

  Note: RS232 port connectivity is not required when installing the UDT card in default mode.

- X21 configuration:
  - LD 17 (CEQU, ADAN)
  - LD 15 (NET data)
  - LD 16 (RDB)
  - LD 14 (trunks)
  - LD 73 (System timers and CC configuration)
- Enable/activate the card X21 commands:
  - LD 60
  - LD 75
  - LD 96

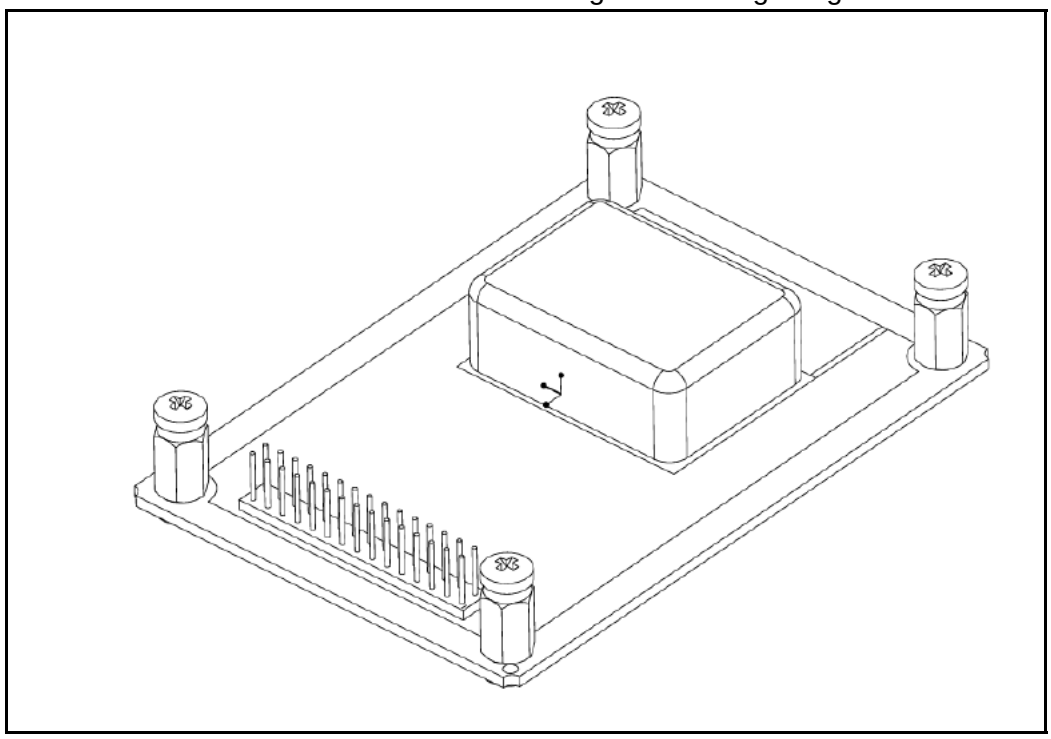
Installation guidelines - non default mode

- Mount the UDT CC daughter board on the UDT card, if required. See "UDT CC daughter board installation" (page 47).
- Set the DIP switch settings:
  - Set switch number 1
    - ON - E1
    - OFF - T1
- Insert the UDT card and connect the RS232 port and the carrier cable (E1/T1 link). See "Physical installation of the UDT card" (page 48).
- UDT card configuration is required for non default mode setup.

- X21 configuration:
  - LD 17 (CEQU, ADAN)
  - LD 15 (NET data)
  - LD 16 (RDB)
  - LD 14 (trunks)
  - LD 73 (System timers and CC configuration)
- Enable/activate the card X21 commands:
  - LD 60
  - LD 75
  - LD 96

UDT CC daughter board installation

Mount the UDT CC daughter board on the UDT card, if required. Work on a flat surface when mounting or removing daughter boards.

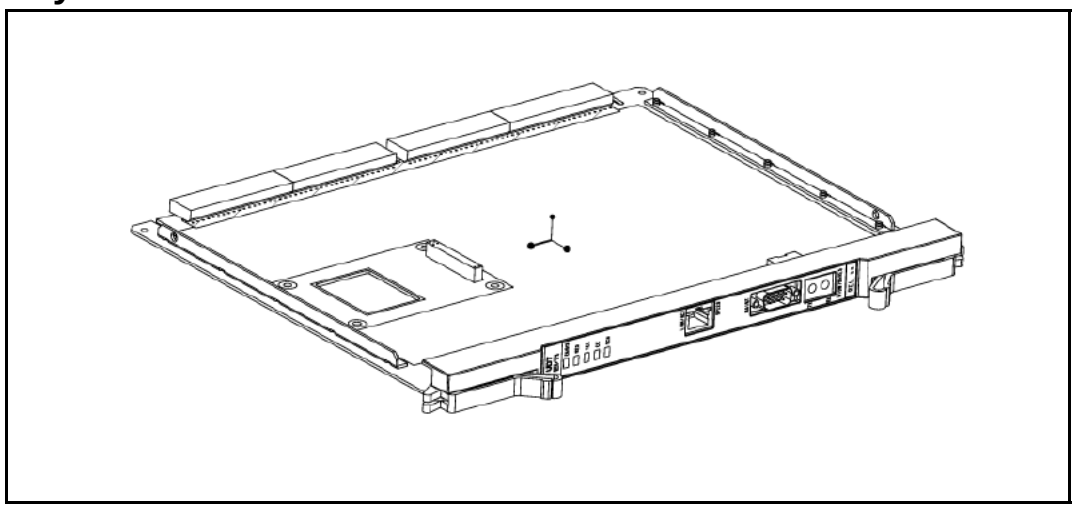


1. Visually inspect the connector pins on the underside of the daughter board. Straighten and realign any bent pins prior to mounting.
2. Place the UDT card down flat on an antistatic pad.
3. From an overhead view, with the daughter board parallel above the UDT card and the connector pins aligned over the connector sockets,

line up the mounting holes on the daughter board with the tops of the standoffs on the UDT card.

4. Slowly lower the daughter board towards the UDT card, keeping the standoffs in line with all four holes, until the holes are resting on the tops of the four standoffs. If more than a very slight amount of pressure is required at this point, the connector pins cannot be aligned with the connector socket. If so, lift the daughter board off the UDT card and return to step 2.
5. Ensure the daughter board is securely attached to UDT card (using the four supplied screws and standoffs).

Physical installation of the UDT card



1. Remove the cabinet module cover.
2. Determine the cabinet and slot location of the UDT card to be installed. The UDT card can be installed in any CE-MUX slot.
3. Unpack and inspect the card.
4. Attach the antistatic wrist strap to your wrist, or discharge static electricity on the cabinet bare metal surface
5. Set the E1/T1 mode DIP switch.
6. Flip the UDT top locking latch up and the bottom-locking latch down.
7. Insert the UDT card into the card-aligning guides in the card cage.
8. Gently push the UDT card into the slot until you feel resistance.
9. Lock the UDT card in the card cage by simultaneously pushing ends of the locking latches against the faceplate.

10. If the cabinet is turned on, the UDT card conducts a self-test. After the self-test, the EN/DIS LED remains red until the card is software-enabled in LD 60.
11. Connect the RS232 port to a terminal using a DB9 to DB25 cable. This connection is used to set the E1/T1 parameters (in case that they have values different from the default).

    Note: RS232 port connectivity is not required when installing the UDT card in default mode.

    The D-type Debug connector pin out is as follows:

Pin	Function
1	
2	TXD
3	RXD
4	
5	GND
6	
7	
8	
9	

12. Configure the terminal or terminal emulation program settings:
    - 9600 baud
    - 8 data bits
    - 1 stop bit
    - No parity
13. Connect the carrier cable to the 50-pin Amphenol connector associated with the slot in which the UDT card is installed and terminate it as required.

    Note: Nortel will not supply cables. It is the responsibility of the distributor to supply the required cables:

    - ***RS-232 serial port (D-type 9) cable***
    - ***Bantam jacks***
    - ***RJ45 Ethernet unshielded cable***

RJ45 Ethernet cable has the following pin out:

Pin	Function
1	ETHTX+/o
2	ETHTX-/o
3	ETHRX+/i
4	
5	
6	ETHRX-/i
7	
8	
9	

UDT card configuration

Configuration is performed from the CLI (Command Line Interface). The RS232 port must be connected to a terminal.

After each power up, the UDT card banner is displayed, including the following information:

- System name
- Card slot
- Protocol
- Usage
- Status
- Alarms (group I and group II)
- UDT CC
- Clock Controller track
- Current Time

For E1/T1 configuration, go to the udtadmin directory and use the E1/T1 settings command.

UDT card configuration as 2.0 Mb PRI2 (E1)

Task summary list

- “LD 17 configure PRI loop and D-channel interface” (page 51)
- “LD 15 configure PRI customer” (page 51)
- “LD 16 configure ISDN service route” (page 52)

- “LD 14 configure service channels and PRI trunks” (page 52)
- “LD 73 configure system timers and clock controller” (page 53)

LD 17 configure PRI loop and D-channel interface

Table 2
PRI Loop configuration

PROMPT	RESPONSE	DESCRIPTION
REQ	CHG	Change existing data.
TYPE	CEQU	Common Equipment
CEQU	YES	Changes to Common Equipment
. . .	. . .	
PRI2	xx	The PRI2 digital loop
MG_CARD	supl sh card	The physical card for the PRI2 loop in the associated IPMG
. . .	. . .	

Table 3
DCH configuration

PROMPT	RESPONSE	DESCRIPTION
REQ	CHG	Change existing data
TYPE	ADAN	Action Device And Number
ADAN	NEW DCH xx	Add a primary D-channel
CTYP	MSDL	D-Channel configuration on MSDL card (UDT E1/T1 includes on board DCH functionality)
MG_CARD	supl sh card	In format superloop, shelf, card
PORT	1	Port must be set to 1
USR	PRI	D-channel is used for ISDN PRI only
IFC	xx	Interface type for D-channel
DCHL	xx	PRI loop number
. . .	. . .	
SIDE	(USR) NET	The system is network/user side

LD 15 configure PRI customer

Table 4
PRI customer configuration

PROMPT	RESPONSE	DESCRIPTION
REQ	NEW CHG	Add new data Change existing data.

TYPE	NET	Networking data
CUST	xx	Customer number
. . .	. . .	
ISDN	YES	Customer is equipped with ISDN
. . .	. . .	

LD 16 configure ISDN service route

Table 5
ISDN service route configuration

PROMPT	RESPONSE	DESCRIPTION
REQ	NEW	Add new data
TYPE	RDB	Route Data Block
CUST	xx	Customer number
ROUT	xx	Route number
. . .	. . .	
TKTP	xxx	Trunk type
DTRK	YES	Digital trunk route
DGTP	PRI2	2.0 Mb PRI
IFC	xxx	Interface type
. . .	. . .	
ISDN	YES	ISDN option
MODE	PRA	Route used for PRA only
. . .	. . .	

LD 14 configure service channels and PRI trunks

Table 6
Service channels and PRI trunks configuration

PROMPT	RESPONSE	DESCRIPTION
REQ	NEW	Add new data When assigning several members at once use the multiple create command NEW XX
TYPE	xxx	Trunk type
TN	l ch	Loop and channel for digital trunks
DES	xxx	Designator field for trunk
PDCA	(1) - 16	PAD category table number

PCML	A MU	Pulse Code Modulation Law A = A-law MU = u-law
. . .	. . .	
RTMB	rt mm	Route number and Member number
. . .	. . .	
TGAR	0 – (1) - 31	Trunk Group Access Restriction
. . .	. . .	
CLS	aaaa	Class of Service
. . .	. . .	

LD 73 configure system timers and clock controller

Table 7
System timers and clock controller configuration

PROMPT	RESPONSE	DESCRIPTION
REQ	NEW CHG	Add new data Change existing data
TYPE	PRI2	2.0 Mb PRI
FEAT	SYTI	System timers
MGCLK	sl s c	Superloop, shelf and card number of the PRI2 providing the Primary Clock Reference
PREF	card	Card number of the PRI2 providing the Primary Clock Reference
SREF	card	Card number of the PRI2 providing the Secondary Clock Reference
. . .	. . .	The system can include up to 50 MG 1000E (for each MG 1000E including digital trunks, Clock Reference must be configured)
MGCLK	sl s c	Superloop, shelf and card number of the PRI2 providing the Primary Clock Reference
PREF	card	Card number of the PRI2 providing the Primary Clock Reference
SREF	card	Card number of the PRI2 providing the Secondary Clock Reference
. . .	. . .	

UDT card configuration as 2.0 Mb DTI (E1)

Task summary list

- "LD 17 configure DTI loop" (page 54)
- "LD 73 configure 2.0 Mb DTI ABCD signaling bit tables and system timers" (page 54)
- "LD 16 configure 2.0 Mb DTI trunk route" (page 55)
- "LD 14 configure service channels and 2.0 Mb DTI trunks" (page 55)

LD 17 configure DTI loop

Table 8
DTI Loop configuration

PROMPT	RESPONSE	DESCRIPTION
REQ	CHG	Change existing data.
TYPE	CEQU	Common Equipment
CEQU	YES	Changes to Common Equipment
. . .	. . .	
DTI2	xx	The DTI2 digital loop
MG_CARD	supl sh card	The physical card for the DTI2 loop in the associated IPMG
. . .	. . .	

LD 73 configure 2.0 Mb DTI ABCD signaling bit tables and system timers

Table 9
2.0 Mb DTI ABCD signaling bit tables configuration

PROMPT	RESPONSE	DESCRIPTION
REQ	NEW CHG	Add or Change Digital Trunk Interface data
TYPE	DTI2	2.0 Mb/s DTI data block
FEAT	ABCD	ABCD bit signaling category
SICA	2-16	Signaling category
. . .	. . .	

Table 10
2.0 Mb DTI system timers configuration

PROMPT	RESPONSE	DESCRIPTION
REQ	NEW CHG	Add new data Change existing data
TYPE	DTI2	2.0 Mb DTI

FEAT	SYTI	System timers
MGCLK	sl s c	Superloop, shelf and card number of the DTI2 providing the Primary Clock Reference
PREF	card	Card number of the DTI2 providing the Primary Clock Reference
SREF	card	Card number of the DTI2 providing the Secondary Clock Reference
. . .	. . .	The system can include up to 50 MG 1000E (for each MG 1000E including digital trunks, Clock Reference must be configured)
MGCLK	sl s c	Superloop, shelf and card number of the DTI2 providing the Primary Clock Reference
PREF	card	Card number of the DTI2 providing the Primary Clock Reference
SREF	card	Card number of the DTI2 providing the Secondary Clock Reference
. . .	. . .	

LD 16 configure 2.0 Mb DTI trunk route

Table 11
2.0 Mb DTI trunk route configuration

PROMPT	RESPONSE	DESCRIPTION
REQ	NEW	Add new data
TYPE	RDB	Route Data Block
CUST	xx	Customer number
ROUT	xx	Route number
. . .	. . .	
TKTP	xxx	Trunk type
DTRK	YES	Digital trunk route
DGTP	DTI2	2.0 Mb DTI
. . .	. . .	

LD 14 configure service channels and 2.0 Mb DTI trunks

Table 12
Service channels and 2.0 Mb DTI trunks configuration

PROMPT	RESPONSE	DESCRIPTION
REQ	NEW	Add new data When assigning several members at once use the multiple create command NEW XX

TYPE	xxx	Trunk type
TN	l ch	Loop and channel for digital trunks
DES	xxx	Designator field for trunk
SICA	(1) -16	Signaling Category table number
PDCA	(1) - 16	PAD category table number
PCML	 A MU	Pulse Code Modulation Law A = A-law MU = u-law
. . .	. . .	
RTMB	rt mm	Route number and Member number
. . .	. . .	
TGAR	0 – (1) - 31	Trunk Group Access Restriction
. . .	. . .	
CLS	DIP DIPF DTN MFC	Dial pulse Dial pulse digit collection Digitone Multi Frequency Compelled
. . .	. . .	

UDT card configuration as DPNSS/DASS (E1)

Task summary list

- “LD 17 configure DPNSS/DASS loop and D-channel” (page 56)
- “LD 74 configure DDSL block for DPNSS/DASS2” (page 57)
- “LD 16 configure route data block” (page 58)
- “LD 14 configure DPNSS/DASS2 trunks” (page 58)

LD 17 configure DPNSS/DASS loop and D-channel

Table 13
DPNSS/DASSI Loop configuration

PROMPT	RESPONSE	DESCRIPTION
REQ	CHG	Change existing data.
TYPE	CEQU	Common Equipment
CEQU	YES	Changes to Common Equipment
. . .	. . .	
DDCS	loop	The loop number for the new DPNSS/DASS2 link.

MG_CARD	supl sh card	The physical card for the DPNSS/DASS2 loop association to the IPMG is required.
. . .	. . .	

Table 14
DCH configuration

PROMPT	RESPONSE	DESCRIPTION
REQ	CHG	Change existing data
TYPE	ADAN	Action Device And Number
ADAN	NEW DCH xx	Add a D-channel
CTYP	DCHI	On board DCHI functionality
MG_CARD	supl sh card	The physical card for the digital loop associated with the MG 1000E.
PORT	1	Port must be set to 1
. . .	. . .	
DES	aaa…a	Designator (up to 16 alphanumeric characters)
DPNS	YES	Digital Private Network Signaling
. . .	. . .	

LD 74 configure DDSL block for DPNSS/DASS2

Table 15
DDSL block configuration for DPNSS/DASS2

PROMPT	RESPONSE	DESCRIPTION
REQ	NEW	New data
TYPE	DDSL	Digital Signaling Link
S2	0	Normal addressing mode
DDSL	xx	The D-Channel logical port number, entered in LD 17
SIGL	DA	DPNSS/DASS2 digital signaling
DDCS	xx	Loop number used for the PRI link (Reference to DDCS in LD 17)
PRIV	YES/NO	Yes - DPNSS link No - DASS2 link
SIDE	AET/BNT	The AET/BNT end of DPNSS/DASS2 link
DPNS	AET/BNT	Digital Private Network Signaling System (DPNSS) or Digital Access Signaling System (DASS2)
. . .	. . .	

LD 16 configure route data block

Table 16
Route data block configuration

PROMPT	RESPONSE	DESCRIPTION
REQ	aaa	Request (aaa = CHG, NEW)
TYPE	RDB	Route Data Block
CUST	xx	Customer number, as defined in LD 15
ROUT	xx	Route number
DES	aaa..a	Designator (up to 16 alphanumeric characters)
. . .	. . .	
TKTP	IDA	Trunk Type- Integrated digital access trunks
SIGL	DPN/DAS	Signaling interface: DPN – for DPNSS signaling DAS – for DASS signaling
. . .	. . .	
ICOG	aaa	Incoming, outgoing or both way trunks
SRCH	(LIN) RRB	Search method for outgoing trunk member
ACOD	xxx..x	One-seven-digit access code for the trunk route
TARG	0-(1)-31	Trunk Access Restriction Group Number
. . .	. . .	

LD 14 configure DPNSS/DASS2 trunks

For DPNSS, both RDC (real) and VDC (virtual) channels must be configured.

For DASS2, only RDC (real) channels configuration is required.

Table 17
Trunk data block configuration

PROMPT	RESPONSE	DESCRIPTION
REQ	NEW CHG	Request (aaa = CHG, NEW)
TYPE	RDC/VDC	Real/Virtual digital channel
TN	l ch	Terminal Number for digital trunks Where l = loop, ch = channel.Loop and channel for digital trunks
DES	aa…a	Designator field for trunk
. . .	. . .	

DDSL	xx	DASS2/DPNSS D-channel logical port number, entered in LD 74
SIGL	DPN/DAS	Signaling interface: DPN – for DPNSS signaling DAS – for DASS signaling
CUST	xx	Customer number, as defined in LD 15
NCOS	(0) - 99	Network Class of Service group
. . .	. . .	
RTMB	rt mm	Route number and Member Number
. . .	. . .	
TGAR	0 – (1) - 31	Trunk Group Access Restriction The default of 1 automatically blocks direct access.
. . .	. . .	
CLS	aaaa	Class of Service
. . .	. . .	

Enable UDT card

Enable UDT card in Call Server, as follows:

Enable UDT card configured as PRI/PRI2

1. In LD 60 enable the 2.0 Mb PRI loop:

   — ENLL L

2. In LD 96 enable the MSDL (implemented on board):

   — ENL MSDL l s c

3. In LD 96 enable the D-channel:

   — ENL DCH X

4. In LD 96 check the current status of the D-channel (the system should respond with DCH x EST meaning that the D-channel is established and operational).

   — STAT DCH X

Enable UDT card configured as DTI/DTI2

1. In LD 60 enable the 2.0 Mb DTI loop:

   — ENLL L

Enable UDT card configured as DPNSS/DASS

1. In LD 75 enable DDCS loop:

   — ENL DDCS l

2. In LD 75 enable DDSL:

   — ENL DDSL n

3. In LD 75 start the DDSL:

   — STRT n

4. In LD 75 check the current status of the DDSL (the system should respond with ENBL ACTIVE meaning that the DDSL is established and operational).

   — STAT DDSL n

Enable clock controller functionality

In LD 60 enable the clock controller, if the UDT CC daughter board is installed:

- Enable system clock controller on specified superloop and shelf:

  — ENL CC l s

- Enable clock tracking on MG 1000E specified by the superloop and shelf tracking to primary, secondary or free run:

  — TRCK aaa l s (Where aaa is: PCK = track primary clock SCLK = track secondary clock FRUN = free run mode)

- Check the status of the system clock on the specified superloop and shelf

  — SSCK l s

Maintenance and diagnostics

This section describes the maintenance and diagnostic programs used on the Call Server for the UDT card.

LD programs

LD 60 Digital trunk loop and clock controller maintenance

Table 18
LD 60 Digital trunk loop maintenance

Commands	Description
DISI loop	Disable loop when all channels are idle
DISL loop	Disable network and DTI/PRI cards of loop

DSCH l ch	Disable channel ch of loop
DSYL loop	Disable yellow alarm processing for loop
ENCH loop	Enable all channels on 2.0 Mb/s DTI/PRI
ENCH l ch	Enable channel ch of DTI/PRI loop
ENLL loop	Enable network and DTI/PRI cards of loop
ENYL loop	Enable yellow alarm processing for loop
SLFT loop	Invoke hardware self-test on loop.
SLFT l ch	Invoke partial hardware self-test on channel ch.
LCNT (loop)	List contents of alarm counters on one or all DTI/PRI loops
RLBK loop	Performs external loop back test on loop. (Card must be disabled.)
RLBK loop ch	Performs external loop back test on channel ch of loop. (Channel must be disabled.)
STAT	Get status of all loops
STAT loop	Get status of DTI/PRI loop
STAT loop ch	Get status of channel

Table 19
LD 60 Clock controller maintenance

Commands	Description
DIS CC l s	Disable system clock controller on specified superloop and shelf.
ENL CC l s	Enable system clock controller on specified superloop and shelf.
SSCK l s	Get status of system clock on specified superloop and shelf
TRCK aaa l s	Set the clock controller tracking to primary, secondary or free run Where aaa is: PCK = track primary clock SCLK = track secondary clock FRUN = free run mode

LD 96 D-Channel and MSDL maintenance

Table 20
LD 96 D-Channel and MSDL maintenance

Commands	Description
DIS DCH x	Disable DCH x.
ENL DCH x (FDL)	Enable DCH x and attempt to establish the link, and force download to MSDL.
EST DCH x	Establish multiple frame operation on D-channel x.
RLS DCH x	Release D-channel x.
RST DCH x	Reset D-channel x, inhibit signaling.
STAT DCH (x)	Get status of one or all D-channels

STAT MON (x)	Display the incoming and outgoing monitoring status of one or all D-channels.
DIS MSDL l s c (ALL)	Disable MSDL card X
ENL MSDL l s c (FDL,ALL)	Enable MSDL card X, with or without Force Download
RST MSDL l s c	Reset MSDL card X
STAT MSDL (l s c (full))	Get MSDL status X, or a “FULL STATUS”

LD 75 IDA (DPNSS/DASS2) loop and D-channel maintenance

Table 21
LD 75 IDA (DPNSS/DASS2) loop and D-channel maintenance

Commands	Description
ENL DDSL n	Enable DDSL, port n
ENL DDCS l	Enable DDCS loop l
ENL DTRC l c	Enable real channel (loop, channel)
DIS DDSL n	Disable DDSL, port n
DIS DDCS l	Disable DDCS loop n
DISI DDCS l	Disable all channels, loop l as they become idle.
DIS DTRC l c	Disable real digital channel (loop, channel}
STAT DDSL	Give status of entire DDSL
STAT DDSL n	Give status of DDSL port n
STAT DDCS	Give status of all DDCS loops
STAT DDCS l	Give status of DDCS loop l, and a count of the number of channels in each state
STAT DTRC l c	Give status of real digital channel (loop, channel)
STRT n	Start DDSL, port n. The message “OK STARTING” is displayed and further commands may be entered. Message DTM301 is displayed when the link is started successfully.

UDT card startup and status Check
UDT card PRI

Table 22
PRI startup procedure

Step	Action	Response
1	Check the status of the UDT card	The EN/DIS LED is red

2	Test the PRI loop: LD 60 DISL loop SLFT loop	SLFT OK
3	Enable the PRI loop: LD 60 ENLL loop	PRI loop is up - Remote alarm cleared
4	Enable the MSDL: ENL MSDL l s c	MSDL is enabled
5	Enable the D-channel: LD 96 ENL DCH X	DCH EST - D-channel is established (provided far-end D-channel is OK). If you do not get the DCH EST response, perform EST DCH x
6	Perform a PRI status check.	

If the PRI status is not as shown in Table 23 "PRI status check procedure" (page 63), complete the check and proceed to PRI fault clearing procedures.

Table 23
PRI status check procedure

Step	Action	Response
1	a) Check the EN/DIS status LED on UDT b) Check the associated DCH LED	The EN/DIS LED is green If the LED is Red, the MSDL is disabled.
2	Check the status of the DCH: LD 96 STAT DCH x	
3	Check the status of the PRI loop: LD 60 STAT L	
4	List PRI alarm counters: LD 60 LCNT (L) (Check the out-of-service counters)	For example: PRI LOOP L MNT NNDC NNC OOS BVP- xxx xxx xxx xxx FAP- xxx xxx xxx xxx SLP- xxx xxx xxx xxx CRC- xxx xxx xxx xxx G2 xxx xxx xxx xxx
5	Check the status of the DCH and MSDL: LD 96 STAT MSDL l s c FULL	The DCH status should be OPER (Operational) and EST (established).

UDT card DTI

Table 24
DTI startup procedure

Step	Action	Response
1	Check the status of the UDT card	The EN/DIS LED is red
2	Test the DTI loop: LD 60 DISL loop SLFT loop	 SLFT OK
3	Enable the DTI loop: LD 60 ENLL loop	 DTI loop is up - Remote alarm cleared

If the DTI status is not as shown in Table 25 "DTI status check procedure" (page 64), complete the check and proceed to DTI fault clearing procedures.

Table 25
DTI status check procedure

Step	Action	Response
1	Check the EN/DIS status LED on UDT	The EN/DIS LED is green .
2	Check the status of the DTI loop: LD 60 STAT L	
3	List DTI alarm counters: LD 60 LCNT (L) (Check the out-of-service counters)	

UDT card DPNSS/DASS2

For IDA Startup, follow the steps in Table 26 "DPNSS/DASS2 startup procedure" (page 64).

Table 26
DPNSS/DASS2 startup procedure

Step	Action	Response
1	Check the status of the DPNSS/DASS2	The EN/DIS LED is red The DCH LED is red
2	Enable DDCS: LD 75 ENL DDCS l	 DDCS l is enabled

3	Enable the DDSL: LD 75 ENL DDSL n	ENBL IDLE (DDSL enabled, but all channels are disabled)
4	Enable the LAP protocols for each real and virtual channel configured on the DPNSS1/DASS2 link: LD 75 STRT n Both ends of the link should be started within 5 minutes of each other.	ENBL STARTING (The configured LAP protocols for each real and virtual channel configured on the DPNSS1/DASS2 link are being enabled) ENBL ACTIVE (The configured LAP protocols for each real and virtual channel configured on the DPNSS1/DASS2 link are enabled)

If the IDA status is not as shown in Table 27 "IDA status check procedure" (page 65), complete the check and proceed to IDA fault clearing procedures.

Once all problems are cleared, go to IDA start-up Table 26 "DPNSS/DASS2 startup procedure" (page 64).

Table 27
IDA status check procedure

Step	Action	Response
1	Check the EN/DIS and DCH LEDs on UDT card	For normal operation, both LEDs are green.
2	Check the status of DDSL: LD 75 STAT DDSL	The DDSL status should be ENBL ACTIVE (DDSL enabled, and all configured channels are normally enabled)
3	Check the status of DDCS: LD 75 STAT DDCS (n)	

Inventory

LD 117

All UDT cards installed in the system will be included in the output of the inventory feature, when executed for UDT cards, or for all devices. (For a full description of the Inventory feature commands, see *Software Input Output Reference - Administration* (NN43001-611).)

Request the Inventory feature to generate the Inventory file for all the cards in the system. The generation produces an inventory file with all the cards configured in the system.
=>inv generate cards

The inventory command will print the UDT card as follows:
=> inv prt cards
Card inventory:
...
PRI, 1, NTDW79AAE5 01 NNTML2????????????
MSDL, 1, NTDW79AAE5 onboard UDT
PRI2, 2, NTDW79AAE5 01 NNTML2????????????
MSDL, 2, NTDW79AAE5 onboard UDT
...
DTI, 5, NTDW79AAE5 01 NNTML2????????????
DTI2, 6, NTDW79AAE5 01 NNTML2????????????
...
DPNSS1-DTCS, 8, NTDW79AAE5 01 NNTML2????????

In this example the fields of the output have the following meanings:
First filed is the Card Type;
Second field is the loop number of the UDT E1/T1;
Third and Fourth fields are the PEC code (NTDW79AAE5) and release of the card;
Fifth field is the factory code, source code, serial number and manufacturing data of the card.

Command Line Interface

The UDT card has two Command Line Interface (CLI) levels:

- basic level
- advanced level (in debug mode) which includes all the commands available at the basic level, as well as, additional commands for debug purposes only.

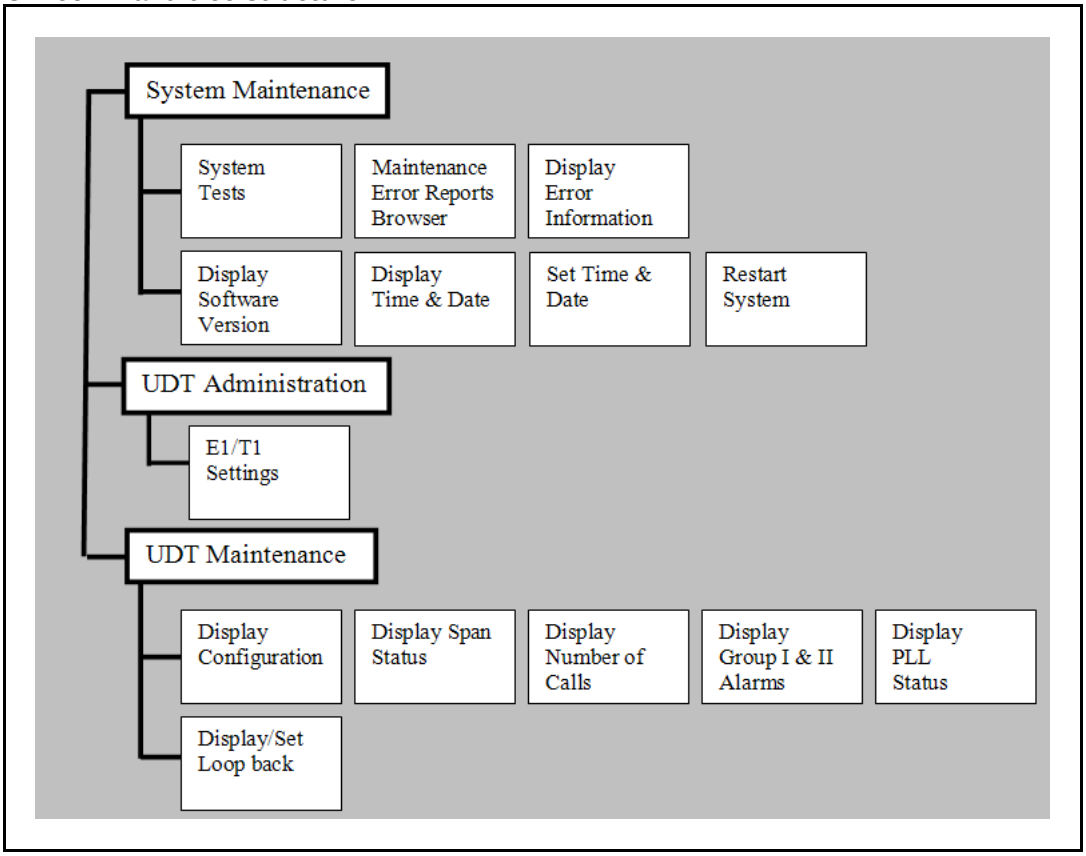
CLI commands are organized in a tree structure similar to file system folders and files. See Figure 12 "CLI command tree structure" (page 67).

To navigate the CLI tree use the following commands (similar to the Unix operating system):

- ls - lists commands and directories in current directory,
- **`cd<name>`** - moves to the specified directory,
- **`cd ..`** - returns one level up
- **`?`** – for help (displays a short description of each command or directory in the current level).

Characters input are case sensitive.

Figure 12
CLI command tree structure



Main menu

The following management activities groups are available:
smaint - System Maintenance directory;
udtadmin - UDT Administration;
udtmaint - UDT Maintenance directory.

This is the top layer, which is used for navigation purposes only.

Available commands:

- **`ls`** - lists commands and directories in current directory,
- **`cd<name>`** - moves to the specified directory,
- **`?`** – for help (displays a short description of each command or directory in the current level).

ls command

In response to the **ls** command, the following is displayed:

```
UDT [1/] ls

smaint/     udtadmin/     udtmaint/     ?
```

? command

In response to the **?** command, the following is displayed:

```
UDT [2/] ?

smaint              System Maintenance directory
udtadmin            Span Administration directory
udtmaint            Span Maintenance directory
```

System Maintenance

The following commands are available within the System Maintenance directory

- **ls** - lists commands and directories in current directory,
- **cd<name>** - moves to the specified directory,
- **cd ..** - moves to root directory
- **?** – for help (displays a short description of each command or directory in the current level).
- **stest** - System Test directory
- **crestart** - Card restart
- **mreport** - Maintenance Error Reports
- **qver** - Display software version
- **showerr** - Display Error Information
- **stad** - Set time and date
- **ttad** - Display time and date

ls command

In response to the **ls** command, the following is displayed:

```
UDT [19 /] cd smaint
UDT [20 /smaint] ls
stest/      ?         crestart    mreport     qver        showerr
stad       ttad
```

? command

In response to the **?** command, the following is displayed:

```
UDT [21 /] cd smaint
UDT [22 /smaint] ?
stest        System Test directory.
crestart     Restart System.
mreport      Browse Maintenance Error Report
             in order to analyze system problems.
qver         Display current software version.
shower       Display information for specific error code.
stad         Set current time and date.
ttad         Display current time and date.
```

System Test

The following commands are available within the System Test directory

- **ls** - lists commands and directories in current directory,
- **cd<name>** - moves to the specified directory,
- **cd ..** - moves to root directory
- **?** – for help (displays a short description of each command or directory in the current level).
- **inserv** - for in-service system test
- **outserv** - for out-of-service system test

Objective: perform system component tests.

In response to **ls** command, the following is displayed:

```
UDT [23 /] cd smaint
UDT [24 / smaint] cd stest
UDT [25 /smaint/stest] ls
?          inserv     outserv
```

In response to **?** command, the following is displayed:

```
UDT [25 /] cd smaint
UDT [26 / smaint] cd stest
UDT [27 /smaint/stest] ?
inserv      Perform in-service system test.
outserv     Perform out-of-service system test.
```

In response to **inserv** command, the following is displayed:

```
UDT [28 /] cd smaint
UDT [29 / smaint] cd stest
UDT [30 /smaint/stest] inserv
Performing in service test ... Test passed.
```

In response to **outserv** command, the following is displayed:

```
UDT [31 /] cd smaint
UDT [32 / smaint] cd stest
UDT [34 /smaint/stest] outserv
Perform service impacting test? (Yes, (No))y
```

crestart command

Objective: manual reset of the card.

In response to the **crestart** command, the following is displayed:

```
UDT [35 /] cd smaint
UDT [36 /smaint] crestart
Restart the card? (Yes, (No))y
```

mreport command

Objective: browse Maintenance Error Reports in order to analyze system problems.

All reports are time stamped (according to the time & date set by using the stad command) and contain verbal information regarding the nature of the problem. To exit before maintenance report file has been presented in full, use *<CR> (star) during printout.

The maintenance reports have the following format:

<serial number>: <severity> < error code> <timestamp> <error text>

For example:

```
UDT [37 /] cd smaint
UDT [38 /smaint] mreport
00024 INFO INIT041 06-05 06:30:48:204 POWER-UP RESET
00025 INFO PRI195 06-05 06:33:50:480 Hardware Self test succeeded
```

showerr command

In addition to the error text in the message itself, the UDT card provides on-line help for error messages. The CLI command receives as input the unique error code and prints the related information for this message:
<syntax> - definition of the message syntax.
Meaning: what does this message indicate.
Parameters: description of the message parameters (fields).
Action: steps the administrator can follow to isolate the problem and/or fix it.
Impact: possible visual/physical/higher level effects of the event.

For example:

```
UDT [39 /] cd smaint
UDT [40 /smaint] showerr  PRI025
     UDT [3 /smaint] showerr PRI025
     PRI025:        E1 alarm <alarm_name> <alarm_state> on span
     <span_number>
     Meaning:    E1 Alarm Group II condition.
     Parameters: <alarm_name> -  RAI (remote alarm indication)
                                 LOS (loss of signal)
                                 AIS (alarm indication signal)
                                 LFAS  (loss  of  frame  alignment
     signal)
                                 CLMAS    (loss    of    multi-frame
     alignment signal)
                 <alarm_state> - occurred
                                 persisted
                                 cleared
                 <span_number> - span 1.
     Action:     State "persisted" or "occurred" - Check the cabling
     and far-end
                 equipment.
                 State 'cleared' - None.
     Impact:    State "persisted" or 'occurred' - The specified span
     is not able
                 to carry calls.
                 State "cleared" - If there was no other alarms, then
     that span is
            now able to carry calls.
```

qver command

Objective: display software version.

For example:

```
UDT [41 /] cd smaint
UDT [42 /smaint] qver
Boot version:           1.11
Main Load version:      1.0.1
FPGA version:           00af
```

ttad command

Objective: display time and date on the UDT card.

For example:

```
UDT [45 /] cd smaint
UDT [46 /smaint] ttad
Card time: Feb. 10, 2008 23:45:06
```

stad command

Objective: set time and date on the UDT card.

For example:

```
UDT [47 /] cd smaint
UDT [48 /smaint] stad <month> <day> <year> <hour> <minutes> <seconds>
 Stad 2 20 2008 0 0 0
 Card time set to: Feb. 20, 2008 10:30:28
```

UDT Administration

The following commands are available within the UDT Administration directory

- **`ls`** - lists commands and directories in current directory,
- **`cd<name>`** - moves to the specified directory,
- **`cd ..`** - moves to root directory
- **`?`** – for help (displays a short description of each command or directory in the current level).
- **`E1T1Settings`** – set/modify the E1/T1 settings. The card is restarted after saving the changes.

ls command

In response to the **ls** command, the following is displayed:

```
UDT [49 /] cd udtadmin
UDT [50 /udtadmin] ls
?       E1T1Settings
```

? command

In response to the **?** command, the following is displayed:

```
UDT [51 /] cd udtadmin
UDT [52 / udtadmin] ?

E1T1Settings        Display/Modify E1/T1 Settings
                    The card is restarted after saving the changes
```

E1T1Settings command

Objective: set/modify the E1/T1 parameters.

For Protocol type E1, set the following parameters:

- **Usage** - select one of the following values: BCH, DTI2, PRI2, DDCS
- **CRC4** - select one of the following values: NO, YES
- **AIS in TS16** – select one of the following values: (NO), YES
  - available only for DTI2 Usage

For example:

```
UDT [3 /] cd udtadmin
UDT [4 /udtadmin] E1T1Settings
E1/T1 Settings:
Protocol: E1
Usage:PRI2
CRC4: No
Modify, Save, Cancel: m
Protocol E1
Usage (PRI2, 1-BCH, 2-DTI2, 4-DDCS ):2
CRC4 (No, 1-Yes ): <CR>
Ais in ts16 (No, 1-Yes ): <CR>

New E1/T1 Settings:
Protocol: E1
Usage:DTI2
CRC4: No
Ais in ts16: No

Modify, Save, cancel: s
```

UDT Maintenance

The following commands are available within the UDT Maintenance directory

- **`ls`** - lists commands and directories in current directory,
- **`cd<name>`** - moves to the specified directory,
- **`cd ..`** - moves to root directory
- **`?`** – for help (displays a short description of each command or directory in the current level).
- **`AlarmStatus`** - display group 1 and 2 alarms;
- **`ChannelStatus`** - display the number of channels which have active digital padding;
- **`Lpbck`** - display/Set loopback;
- **`PllStatus`** – display PLL status;.
- **`SpanStatus`** - display span status;
- **`UdtConfig`** – display span configuration.

ls command

In response to the **`ls`** command, the following is displayed:

```
UDT [57 /] cd udtmaint
UDT [58 /udtmaint] ls
?       AlarmStatus   ChannelStatus   Lpbck       PllStatus
        SpanStatus    UdtConfig
```

? command

In response to the ? command, the following is displayed:

```
UDT [59 /] cd udtmaint
UDT [60 / udtmaint] ?

UdtConfig      Display UDT configuration (protocol, line coding,
               Yellow alarm mode, framing, connection,
               Clock reference definitions)
SpanStatus     Display span status (Disable/Enable)
ChannelStatus  Display number of calls and details about active
               calls
AlarmStatus    Display group 1 and 2 alarms
PllStatus      Display PLL status
Lpbck          Set/Clear/Display remote/local loopback for PRI/DTI span
```

Alarm Status command

Objective: display group 1 and 2 alarms.

For example:

```
UDT [67 /] cd udtmaint
UDT [68 /udtmaint] AlarmStatus
Group I alarms  : NONE
Group II alarms : LOS
```

ChannelStatus command

Objective: display the number of channels which have active digital padding.

For example:

```
UDT [65 /] cd udtmaint
UDT [66 /udtmaint] ChannelStatus
Busy channels: 1 4 7 10 13 16 19 22
Total: 8
```

Lpbck command

Objective: Set/Clear/Display remote/local loop-back for span.

For example:

```
UDT [71 /] cd udtmaint
UDT [72 /udtmaint] Lpbck
Current settings:
No loopbacks per loop

Local loopback per channel(s): No loopbacks
Remote loopback per channel(s): No loopbacks

UDT [73  /udtmaint] Lpbck ?
Set/Clear/Display loopback for PRI/DTI span.
To Set/Clear loopback:
Syntax: Lpbck <Loop Mode><On_Off> [<chan> - optional]
Where:Loop Mode: 0 = Remote(line loopback), 1 = Local
On_Off: 0 = Clear, 1 = Set
For E1 span:chan: 1..15, 17..31
For T1 span:chan: 1..23
To Display loopback:
Syntax: Lpbck
```

PLLStatus command

Objective: display PLL status.

For example:

```
UDT [69 /] cd udtmaint
UDT [70 /udtmaint] PllStatus
 Clock Controller: Disabled
 PLL mode: FREE RUN Sync src: FREERUN
 previous: ACQUISITION           FREERUN
```

SpanStatus command

Objective: display span status. Is it enabled or disabled

For example:

```
UDT [63 /] cd udtmaint
UDT [64 /udtmaint] SpanStatus
mode: DTI
status:  Enabled
```

UdtConfig command

Objective: display span configuration.

The following information is printed: protocol, usage, line coding, yellow alarm mode, framing, LBO and clock reference definitions.

For example:

```
UDT [8 /] cd udtmaint
UDT [9 /udtmaint] UdtConfig

UDT configuration:

Universal Clock Controller: Equipped
Clock Reference Sync. Source: Primary

Protocol: E1
Usage: PRI2
Connection: RJ48 120 ohm
Framing: AFM
```

Remote access to the UDT card

The UDT card can be remotely accessed only with a modem. A modem can be connected to the UDT card serial port 9-pin connector.

The RS-232 setup is as follows:

- Speed: 9600
- Data bits: 8
- Parity: N
- Stop bit: 1

Firmware upgrade

The UDT card firmware can be upgraded by downloading a new file from the Call Server. The download for each UDT card in the system can be performed and managed through the Call Server. No additional physical connection need be made to the UDT card.

If the firmware download fails, the UDT card will always be able to come up with a working firmware, which was not affected by the downloading process.

The firmware upgrade requires a card reboot.

Feature interactions

Firmware download is implemented as a patch.

Firmware download from the Call Server is applicable only for configurations of a UDT card placed in a Media Gateway Controller shelf.

Only manual and sequential download is supported. This feature does not include any automatic upgrading.

Firmware download is not supported by Element Manager. All provisioning must be done through the TTY by running the required LD programs.

During the UDT firmware download, the Media Gateway Controller is prevented from sending any messages to the UDT other than the messages that are related with the UDT firmware download. An attempt to send messages to the Multi-purpose Serial Data Link through the UDT will be rejected. Hence, a scheduled download to the Multi-purpose Serial Data Link will fail as long as the UDT firmware download is in process.

Firmware download duration

The duration of the download process is expected to be around three minutes.

Security

The initiation of the UDT firmware download can be made only from the Call Server, so all the existing security mechanisms are applicable to the UDT firmware download process. The loadware file is located on the mass storage device of the Call Server, and it is passed to the Media Gateway Controller via the Secure IP messaging system, which includes it's own security mechanism. The Media Gateway Controller in turn, sends the loadware to the UDT via the CEMUX bus. Hence the UDT is not subject to security threats over the Ethernet network.

Loadware patch

The management of the loadware file for the UDT is the same as the loadware file of the Media Gateway Controller. The format of the UDT loadware patch name is **`UDTCAAnn.LW`**, where 'nn' is a pair of digits denoting the version number.

There is a standard file which by default is used when downloading the UDT firmware. A loadware patch can be introduced in order to use another UDT loadware file. When the UDT loadware patch is active, the UDT downloading will use the patch file rather than using the standard file. When putting the patch out of service, the standard file will be used again for the UDT downloads.

To install and activate loadware patches, see “Loadware Configuration Procedures” (page 79).

Firmware download guidelines

- Secure firmware download process from the Call Server using the existing CS 1000 Peripheral Software download (PSDL) mechanism
- Supported from X21 Release 5.5 and later.
- X21 Call Server commands are introduced or changed to support the UDT card firmware upgrade process (LD 143, 60, 22). Implemented in X21 Releases 5.5 and 6.0 by an X21 software patch
- UDT card firmware file is part of the Call server PSDL software. Implemented in X21 Releases 5.5 and 6.0 by an X21 loadware patch
- Media Gateway Controller firmware changes are introduced to support the UDT secure firmware download process
- Ensure that required X21 CS software/loadware patches (X21 Release 5.5/6.0) and Media Gateway Controller loadware patch (X21 RLS 5.5/6.0) are in service.
- Check the existing firmware version of UDT cards (LD 60).
- Print the existing peripheral software download version (PSDL) list (LD 22). Query the existing UDT card PSDL version (a desired new UDT loadware file can be loaded as a new Call Server loadware patch).
- Execute the UDT card upgrade for the required UDT cards (LD 143).

Loadware Configuration Procedures

Loadware patch for the UDT

The UDT loadware is provided to the Call Server as a loadware patch. The UDT loadware patch file should be placed in the Call Server mass storage device directory **`/u/loadware`** . Once the loadware patch file is in the **`/u/loadware`** directory, a loadware patch must be created and installed.

To create and install a loadware patch:

`pdt> lwload udtcaa15.lw`
A loadware patch handle number is provided by the Call Server.

Put the loadware patch in service:

```
pdt> lwinst 0
```

If that is the first time that a UDT loadware patch is introduced to the Call Server then the following message will be displayed:

```
UDTCAA15 was installed as the UDT permanent loadware.
```

The loadware file will be copied to the loadware permanent directory **/p/sl1/loadware** and saved as a loadware file (not a loadware patch file) with the standard file name format **UDTCaaxx.LD**.

If a UDT loadware was already introduced to the Call Server in the past, this is regarded as a request to patch the existing loadware and the following prompt is issued:

```
Loadware "UDTCAAxx" will be replaced by "UDTCAAyy+"
Do you wish to continue (y/n)?  [y].
```

If the answer is 'Y' then the following message appears:

```
UDT Loadware patch have been put into service.
```

Otherwise, the following message will appear:

```
UDT Loadware patch not installed.  Exiting.
```

To remove the loadware patch (so that the patch can be replaced with another UDT loadware patch):

```
pdt> lwout 0
Patch 0 will be removed.
Do you wish to continue (y/n)?  [y]
Loadware patch 0 has been removed successfully.
```

Loadware patch for the Media Gateway Controller

A patch to the Media Gateway Controller must be activated prior to downloading the UDT patch.

If the Media Gateway Controller is not patched, and an attempt is made to invoke UDT download, the Media Gateway Controller will fail to properly respond to the Download Start request from the Call Server, which will cause the Call Server to abort the download. No other functionality problem should occur by this situation.

LD 60 Check the existing firmware version of UDT cards

VER command

If the **VER <UDT Digital Loop Number>** command is issued, a new Special-SSD message will be sent to the MGC, asking it to query the UDT firmware version. The MGC will make an IO read to the digital loop. This specific IO read does not affect any non-UDT loop, but in case it is a UDT, this read will retrieve the UDT firmware version. The MGC will send another new Special-SSD message to the Call Server containing the retrieved version, or a zero in case the read failed. The Call Server will store the retrieved version number in the unprotected data block of the digital loop, and when LD 60 gets a timeslice it will search for this version

number. If found then it will print it out, and if not found before a certain amount of time elapses, it will print an error message stating that the loop in question failed to provide a UDT firmware version.

The format of the UDT firmware version is **UDT VER <AAnn>**.

ENLL command

When requested to enable a disabled loop, the **ENLL** command will check whether it is a UDT. If it is a UDT, it will check whether the UDT is in the middle of a download process. If the UDT is in the middle of a download process, then the enabling request will be rejected and an appropriate error message will be issued.

LD 60 new error messages

The error messages in Table 28 "LD 60 new error messages" (page 81) are assigned to X21 Release 5.5 and 6.0 patches.

Table 28
LD 60 new error messages

Error ID	Description
DTI040	A request that applies only to a UDT was made for a non UDT card
DTI4139	Failed to send Version ID query to a UDT
DTI4140	Can not enable a UDT loop while it is upgrading it's loadware

LD 22 Print the existing peripheral software download version (PSDL)

PSWV command

The existing **PRT PSWV** command is enhanced so that it also prints the version of the UDT loadware file that is present on the Call Server mass storage device.

If the UDT loadware file is present, the **PRT PSWV** command produces the following output:

```
UDT
VERSION NUMBER: AA01
```

If the loadware file was replaced by a loadware patch, the output will look like:

```
UDT
VERSION NUMBER: AAnn+
```

There is no change to the existing output of the **PRT PSWV** command if the loadware file of the UDT card is not present.

When inserting the UDT loadware patch for the first time, the loadware will be taken and treated as the permanent UDT loadware, not as a patched loadware. The output of the **PRT PSWV** command will not include the '+' sign. Also, the **ISSP** command will show no UDT loadware patch.

When it is required to change the UDT loadware, a second request to load a loadware patch will be issued. Then the UDT loadware will be regarded as patched, and the output of the **PRT PSWV** command will show the patched UDT version with the '+' sign.

When asking to take off the loadware patch, the UDT loadware that was used the first time will become active, and the UDT loadware will be treated as unpatched loadware.

To install and manage loadware patches, see "Loadware Configuration Procedures" (page 79).

ISSP command

The **ISSP** command shows the UDT active loadware patch. When the UDT loadware patch is activated for the first time, the loadware file will be used as the permanent UDT loadware, and a request to show the loadware patches in the system will show no UDT loadware patch. When activating a UDT loadware patch next time, it will be regarded as a loadware patch and will be shown by the **ISSP** command.

Following is an example of activating the UDT loadware patch for the first time while a Media Gateway Controller loadware patch exists in the system:

```
pdt> lwload udtcaa15.lw
pdt> lwinst 1
UDTCAA15 was installed as the UDT permanent loadware.
pdt> sl1input
> LD 22
REQ ISSP
INSTALLED LOADWARE PEPS : 1
PAT# PRS/CR PATCH REF # NAME DATE FILENAME
01 Q2424242 ISS1:1OF1 p222222_2 06/11/08 mgcczz99.lw
```

Following is an example of output when there is an active Media Gateway Controller loadware patch and an active UDT loadware patch:

```
pdt> lwload udtcaa16.lw
pdt> lwinst 1
Loadware "UDTCAA15" will be replaced by "UDTCAA16+"
Do you wish to continue (y/n)?  [y].
y
UDT Loadware patch have been put into service.
pdt> sl1input
```

```
> LD 22
REQ ISSP
INSTALLED LOADWARE PEPS : 2
PAT# PRS/CR PATCH REF # NAME DATE FILENAME
01 Q2424242 ISS1:1OF1 p222222_2 06/11/08 mgcczz99.lw
02 Q1234567 ISS1:1OF1 p123456_1 06/11/08 udtcaa16.lw
```

LD 143 Execute the UDT card upgrade for the required UDT cards

Start upgrade command

upgudt <supl shelf card>

If the UDT can not be reached then the following message will be printed:

UDT[LLL S CC]: Not available. Upgrade command ignored.

If an UDT upgrade is already in progress then the following message will be printed:

UDT[LLL s CC]: Doing Upgrade already. Upgrade command ignored.

upgudtabort

If the abort request was made after the UDT has erased it's old firmware then terminating the upgrade will cause the UDT to be left without any upgraded code, and it will have to come up with it's fixed factory firmware. When this is the case, to confirm the abort request the Call Server will print the following message:

UDT[LLL S CC] is undergoing an upgrade. Do you want to abort the upgrade?
ENTER Y(ES) TO CONFIRM ABORT UPGRADE, N(O) TO IGNORE COMMAND.

If confirmed, an abort message will be sent to the UDT.

UDT download status query

upgudt stat

The **upgudt stat** command reports the current UDT upgrade state and the TN of the UDT card that is currently downloaded.

If no upgrade is currently taking place, the reply will be:

Udt Upgrade is idle

If an upgrade process does exist, then the reply format will be:

UDT Upgrade is [idle / checking / starting / active / aborting]. Loop <L> [LLL S CC]

LD 143 new error messages

The error messages in "LD 143 new error messages" (page 83) are assigned to X21 Release 5.5 and 6.0 patches.

Table 29
LD 143 new error messages

Error ID	Description
CCBR030	a request that applies only to a UDT was made for a non UDT card
CCBR031	message arrived from MGC in wrong state
CCBR032	FAIL message arrived from MGC
CCBR033	REJECT message arrived from MGC
CCBR034	Response from MGC timeout
CCBR035	user asked to abort UDT download while no download is in progress.
CCBR036	UDT card is not disabled

Subscriber Manager 2.0

Overview

Communication Server (CS) 1000 Release 6.0 includes many new and enhanced features for Subscriber Manager 2.0. This section provides a description of the following features:

- "Embedded directory" (page 85)
- "Flow through provisioning" (page 86)
- "Location name mapping to element and target" (page 86)
- "Localized name support" (page 86)
- "Username property" (page 86)
- "Bulk add accounts" (page 86)
- "Account reassignment to another subscriber" (page 86)
- "Account disassociation from the subscriber" (page 86)
- "Account synchronization" (page 87)
- "CSV subscriber synchronization" (page 87)
- "LDAP subscriber synchronization" (page 87)
- "CSV subscriber export" (page 87)
- "Numbering group" (page 87)
- "Operation, Administration and Maintenance Transaction Audit and Security Event logging" (page 87)
- "Subscriber Manager license" (page 87)

For more information about Subscriber Manager, see *Subscriber Manager Fundamentals* (NN43001-120).

Embedded directory

Subscriber Manager 1.0 uses the Common Network Directory (CND) as its subscriber repository. Subscriber Manager 2.0 continues to use the CND. However, the CND is now an embedded component (that is, UCM

directory services) deployed as part of the Nortel Unified Communications Management Common Services in CS 1000 Release 6.0. The user interface to configure tasks such as Lightweight Directory Access Protocol (LDAP) synchronization, CSV Synchronization, and CSV Export are now part of the Subscriber Manager application. The repository for subscriber and account data is a fundamental feature provided by UCM directory services.

Flow through provisioning

Flow through provisioning (FTPROV) allows customers to use their LDAP data store to drive account creation in Nortel products. FTPROV replaces the Subscriber Change Notification feature in Subscriber Manager 1.0.

Location name mapping to element and target

Location name mapping simplifies the selection of elements and targets when creating an account. Users provide a list of locations that have a predefined element and target. When creating a new account, the user selects the location or a particular subscriber attribute is used to infer the location.

Localized name support

Variations on a name based on locale can be stored in Subscriber Manager. The Unicode Name Directory uses the localized name support functionality.

Username property

The username property is a new property displayed and edited in the New Subscriber Web page. The username property can be used by CS 1000 Element Manager for SIP Line phones.

Bulk add accounts

Bulk add accounts creates an account for each subscriber and a selected list of subscribers.

Account reassignment to another subscriber

Account reassignment moves an account from a subscriber to another subscriber. The main advantage of account reassignment is that the account need not be deleted and then recreated.

Account disassociation from the subscriber

Once an account is disassociated from a subscriber the user can use the anonymous account functionality to assign the account to another subscriber.

Account synchronization

While running account synchronization jobs, each Web page refresh by the user results in a real-time status update.

CSV subscriber synchronization

Comma Separated Values (CSV) subscriber synchronization imports new subscribers and updates existing subscribers using data in a CSV file.

LDAP subscriber synchronization

LDAP subscriber synchronization synchronizes subscribers in Subscriber Manager with an external LDAP directory.

CSV subscriber export

The CSV subscriber export feature exports subscribers from Subscriber Manager into a CSV file.

Numbering group

A numbering group represents common numbering planning attributes which are shared by a group of subscriber telephony accounts. Each telephony account can belong to only one numbering group. If a telephony account does not belong to a specified numbering group, it is classified as a member of the default numbering group category. A member of the default numbering group category only uses a private numbering plan (private CDP and UDP dialing).

Operation, Administration and Maintenance Transaction Audit and Security Event logging

Subscriber Manager log files are incorporated into the OAM logging system. UCM Common Services provides log viewer and file download functionality for retrieving log files. The log viewer is available from the UCM Common Services navigator. Subscriber Manager transactions and error logs are formatted in accordance with W3C extended log format by the UCM Common Services.

Subscriber Manager license

Subscriber Manager is now a separately licensed product.

Zone Based Dialing

Overview

The Zone Based Dialing (ZBD) feature enables the removal of traditional nodal PBX networks and the replacement of these with a single or a few high capacity soft switches and branch gateways for PSTN access. ZBD is also deployed by new customers who plan to setup private network in multiple locations.

The ZBD feature supports both public and private dial/numbering plans for on-net calls. For outgoing trunk calls, Calling Line Identification (CLID) is converted to E.164 format when DIALPLAN is configured as PUB, for PRV type – CLID is left as is.

For dialing configuration purposes, new numbering zones have been introduced for this feature. These numbering zones are configured on for each phone in LD 10 and LD 11. For outgoing VTRK calls, Country Code, NPA, and NXX are sent within ZBD IE of the Integrated Services Digital Network (ISDN) message. The terminating party processes this IE accordingly. The new prompt DIALPLAN is added to LD 15. If it set to PUB then the appropriate E164 CLID is displayed on a terminating set.

The Zone-Based Flexible Dialing Plan (ZFDP) simplifies the dial plan configuration. By using ZFDP it is not necessary to configure TSC blocks to cut off the site prefix before further routing inter-site calls. ZFDP normalizes a dialed public number into an E164 international number, which is configured in SPN for further routing. The 7-digit DN which is composed of two parts, the zone/site prefix (2 to 4 digits) and the extension (3 to 5 digits), must be configured. Normally, it would be 3 digits for the zone/site prefix and 4 digits for the extension. The zone or site prefix is not dialed and not displayed for same zone/site dialing. For inter-site calls, it is replaced by the corresponding E.164 prefix if the public dial plan for on-net calls has been configured.

The service package 420 (ZBD_PACKAGE) is required. This package is added to the Enhanced Service package (Tier 1) to all systems and added to the key code of all systems.

For more information about Zoned Based Dial Plan support, see *Dialing Plans Reference* (NN43001-283).

CP PM Co-resident Call and Signaling Server

Overview

A Communication Server (CS) 1000 system consists of two major functional components: a Call Server and a Signaling Server. These two components have historically run on separate Intel Pentium processor-based hardware platforms operating under the VxWorks Operating System.

CS 1000 Release 6.0 introduces the Call Processor-Pentium Mobile (CP PM) Co-resident Call Server and Signaling Server (CP PM Co-res CS and SS), which can run the Call Server software, the Signaling Server software, and System Management software on the same hardware platform operating under the RedHat Linux Operating System. For CS 1000 Release 6.0, the only supported hardware platform for the CP PM Co-res CS and SS Server is the CP PM platform.

The key objective of co-residency is to provide a cost-effective solution for CS 1000 system installations that do not require high user capacity or the need for a redundant Call Server.

For more information about CP PM Co-res CS and SS, see *CP PM Co-res CS and SS Server Fundamentals* (NN43001-509).

Supported configurations

You can deploy the CP PM Co-res CS and SS Server in the following configurations:

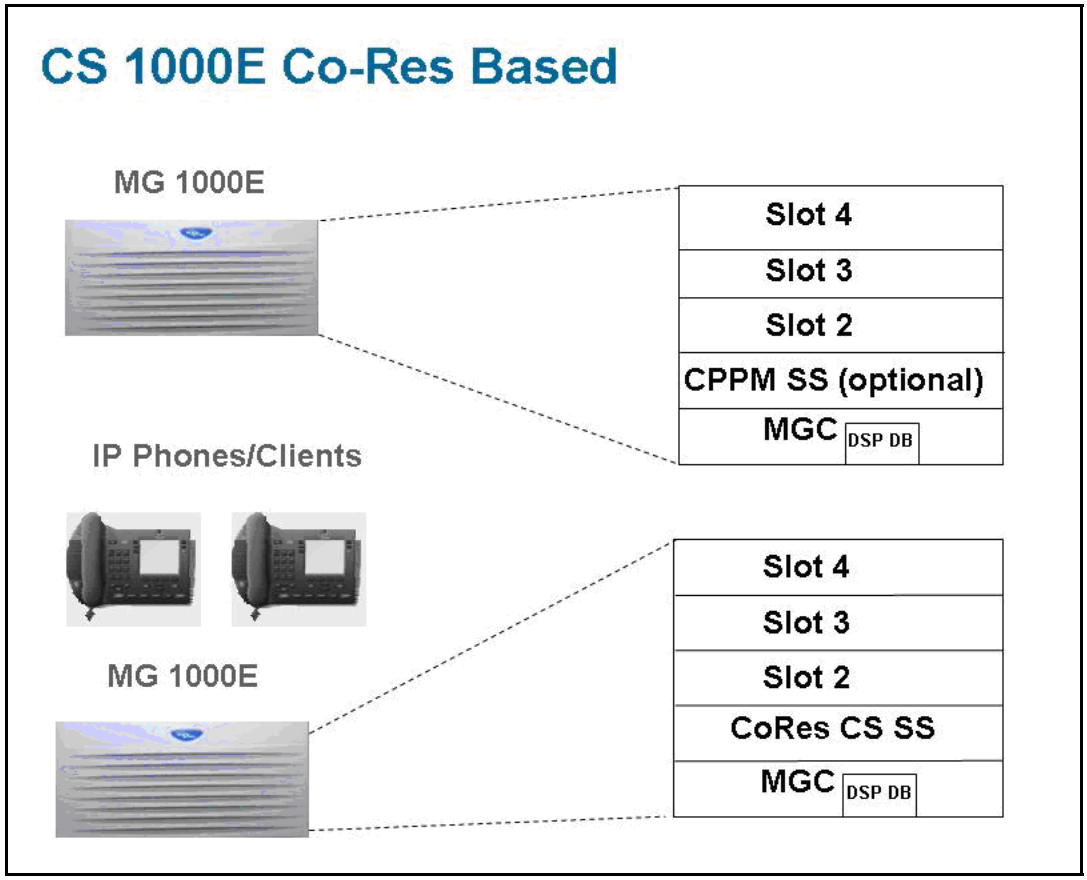
- CS 1000E
- Survivable MG 1000B branch office
- MG 1000E Survivable Media Gateway (SMG)
- CS 1000E TDM

Supported configurations

CS 1000E CP PM Co-res CS and SS based system

Figure 13 "CS 1000E CP PM Co-res CS and SS system" (page 92) provides an example of a CS 1000E CP PM Co-res CS and SS system.

Figure 13
CS 1000E CP PM Co-res CS and SS system



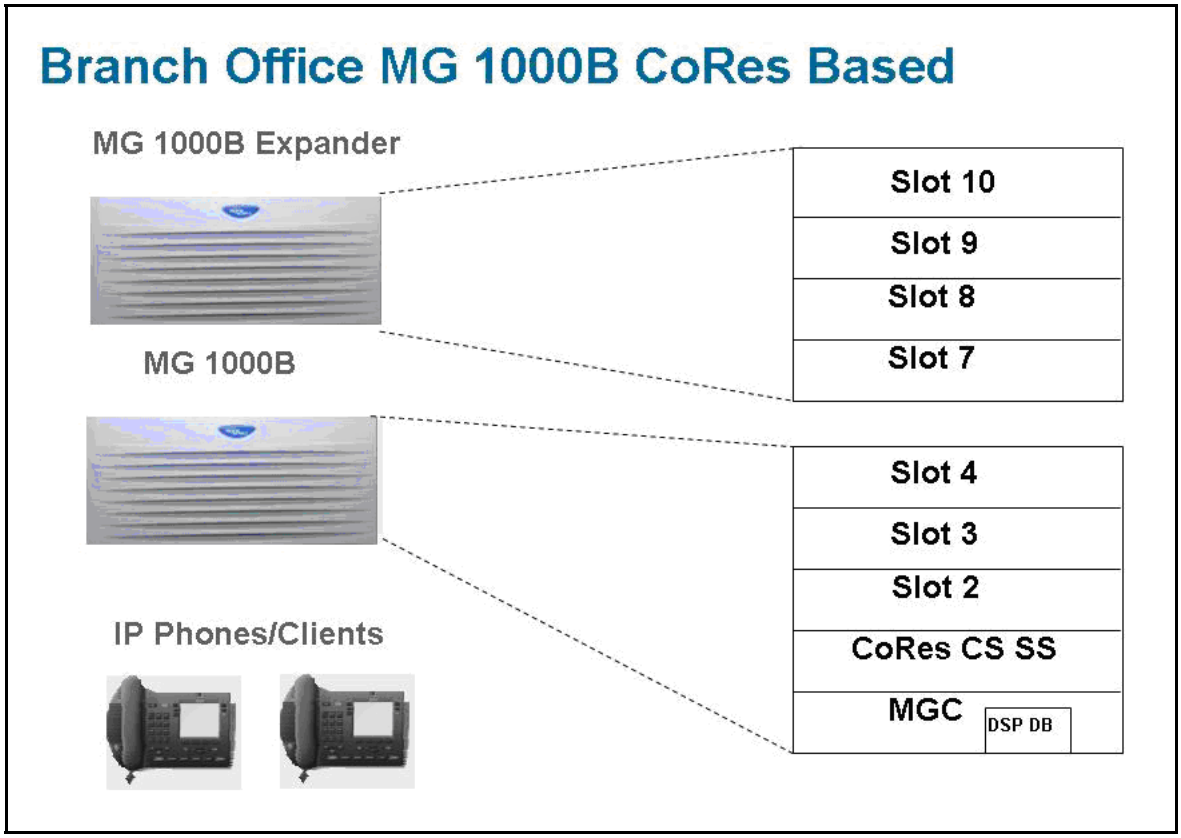
Optional second Signaling Server

For information on adding an optional second Signaling Server to a CP PM Co-res CS and SS, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

CP PM Co-res CS and SS-based MG 1000B

Figure 14 "MG 1000B CP PM Co-res CS and SS system" (page 93) provides an example of the CS 1000 Release 6.0 CP PM Co-res CS and SS based Branch Office (MG 1000B) system.

Figure 14
MG 1000B CP PM Co-res CS and SS system



CS 1000E TDM

CS 1000 Release 6.0 supports a TDM-only version of the CP PM Co-res CS and SS system. The CS 1000E TDM system has the following limitations:

- 720 combined TDM users (Analog, Digital, CLASS, DECT users, including installed plus [+] add-on)
- a maximum of five Media Gateways
- a maximum of 16 Primary Rate Interface (PRI) cards
- a maximum of 200 Automatic Call Distribution (ACD) Agents
- No (zero) IP phones (no UNIStim, no SipLine, no SipDect)
- No (zero) virtual trunks
- Network Routing Service (NRS) not supported

CP PM Co-res CS and SS Server limitations

The CP PM Co-res CS and SS Server supports the following system configurations and capacity limitations:

Table 30
CP PM Co-res CS and SS Server limitations

Maximum Capacity	CS 1000E or MG 1000E		MG 1000B		CS 1000 TDM
	With Separate SIPL Server	With Co-Res SIPL	With Separate SIPL Server	With Co-Res SIPL	Supports TMD ONLY
IP Users	UNIStim + SIPL <=1000 Where SIPL <= 400	UNIStim + SIPL <= 800 Where SIPL <= 400	UNIStim + SIPL <= 400 Where SIPL <= 400	UNIStim + SIPL <= 400 Where SIPL <= 400	n/a
PD	Same as UNIStim Users	Same as UNIStim Users	Same as UNIStim Users	Same as UNIStim Users	n/a
TDM Users	720	720	128	128	720
ACD Agents	200	200	200	200	200
Converged Desk Top	100% of Users	100% of Users	100% of Users	100% of Users	n/a
VTRK (H.323 + SIP)	400	400	400	400	n/a
PRI (T1/E1) Spans	16	16	4	4	16
IP Media Gateways (IPMG)	5	5	1	1	5
NRS Endpoints / Routing Entries	5/20	5/20	n/a	n/a	n/a
Call Rate (CS + NRS)	10,000 cph	10,000 cph	10,000 cph	10,000 cph	10,000 cph

The CP PM Co-res CS and SS Server has the following restrictions:

- The CP PM Co-res CS and SS Server does not support High Availability (HA) configuration (dual core with Active/Inactive role). Systems that require High Availability configuration should deploy the VxWorks based Call Server software.
- Network Time Protocol (NTP) configuration and management is done in Linux Base. The CP PM Co-res CS and SS Server does not support LD117 NTP management commands.
- CCBR backup and restore is supported on Media Gateway Controller (MGC) remote TTY ports. The CPPM serial port does not support CCBR backup and restore.

- Xmodem sx and rx commands are only supported on the MGC remote TTY (from the Call Server PDT shell). The sx and rx commands are supported from Linux Shell.
- Time of Day (TOD) management is done in Linux Base. LD2 TOD configuration commands are not supported. Attendant Console/Set Based Administration for TOD configuration/management is not supported; only the LD2 TOD print command is supported.
- Co-Res Call Server does not support the hardware related tier 0 and tier 1 health values.
- The Call Server, Signaling Server and System Management applications are installed as Linux Red Hat Package Manager (RPM) packages by the Deployment Manager. For the Call Server application the Deployment Manager supports:
  - Installation of the Call Server software and database
  - Installation of the Call Server software only

CP PM Co-res CS and SS upgrade paths

CP PM Co-res CS and SS Server supports the following upgrade paths:

- CS 1000 Release 5.5 or earlier CS 1000E Call Server Standard Availability (SA) to CS 1000 Release 6.0 CP PM Co-res CS and SS Server

  Note: If you upgrade from a non-CP PM based CS 1000E Call Server, you must upgrade both the software and the hardware.

- CS 1000 Release 5.5 or earlier CS 1000E Signaling Server to CS 1000 Release 6.0 CP PM Co-res CS and SS Server

  Note: If you upgrade from a non-CP PM based CS 1000E Signaling Server, you must upgrade both the software and the hardware.

- CS 1000 Release 5.5 or earlier Option 11C Call Server to CS 1000 Release 6.0 CP PM Co-res CS and SS Server
- CS 1000 Release 5.5 or earlier Option 11C Call Server to CS 1000 Release 6.0 CS 1000E TDM

- CS 1000 Release 4.5 or earlier CS 1000M Call Server (cabinet/chassis) to CS 1000 Release 6.0 CP PM Co-res CS and SS Server
- CS 1000 Release 4.5 or earlier CS 1000S Call Server to CS 1000 Release 6.0 CP PM Co-res CS and SS Server

Note: Minimum Release for Small System migration to CP PM Co-res CS and SS Server is Release 23.10.

SIP Line support on CP PM Co-res CS and SS Server

To enable SIPL on the CP PM Co-res CS and SS Server, the latest Service Pack (SP) must be loaded and put in service after deploying all the Nortel applications (such as CS, SS, EM, or NRS). The SP allows you to enable and configure the SIPL feature from the Element Manager (EM). For information about downloading and applying an SP, see *Patchng Fundamentals,* (NN43001-407)

You must configure SIP Line on the CP PM Co-res CS and SS Server to enable SIP Line service.

The workflow for a CP PM Co-res CS and SS Server with SIP Line deployed is shown in Figure 15 "SIP Line on a CP PM Co-res CS and SS Server workflow" (page 97).

The SIP Line configuration workflow is shown in Figure 16 "SIP Line configuration on a CP PM Co-res CS and SS Server workflow" (page 98).

For information about application deployment, see the Application installation using Deployment Manager section in *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

For details about configuring SIP Line on a CP PM Co-res CS and SS Server, see Procedure 1 “Configuring SIP Line on a CP PM Co-res CS and SS Server” (page 99).

Figure 15
SIP Line on a CP PM Co-res CS and SS Server workflow

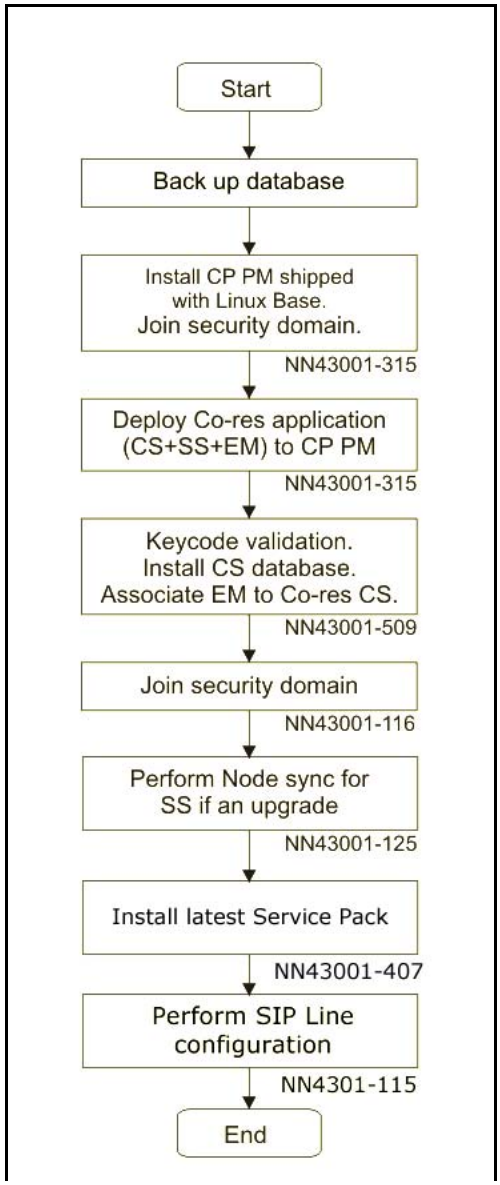
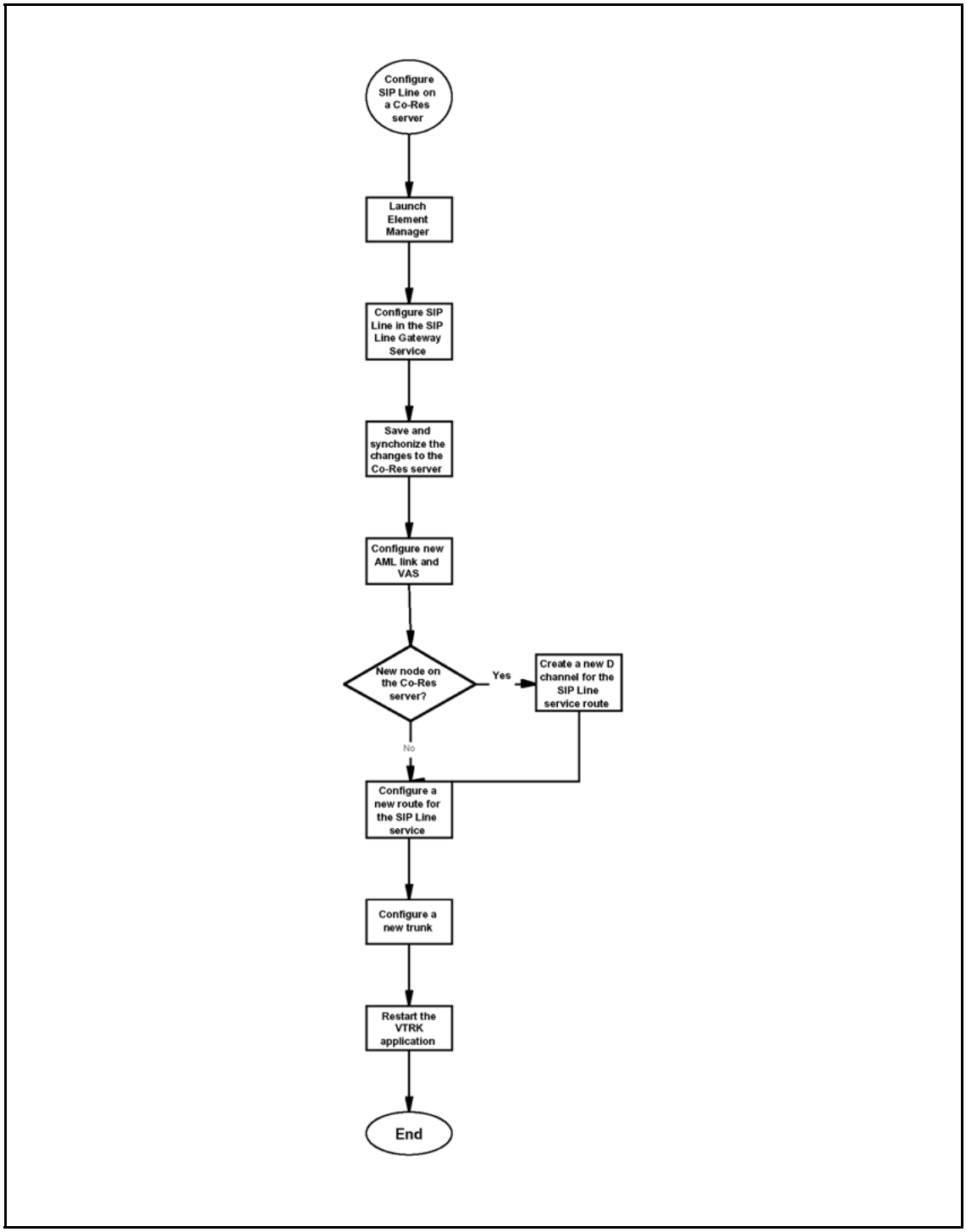


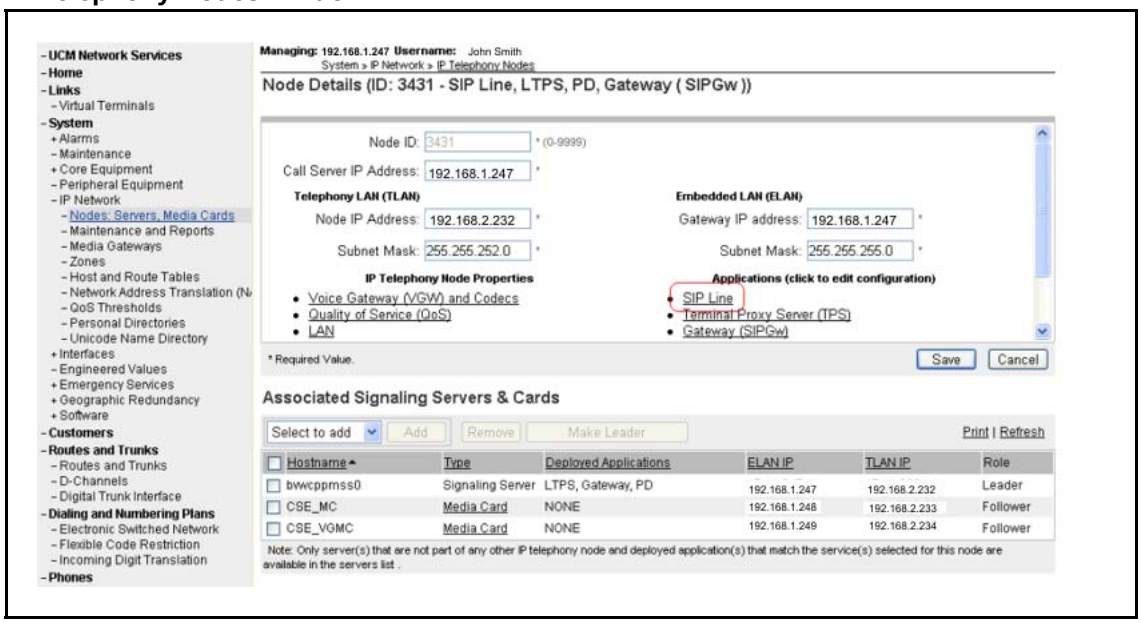
Figure 16
SIP Line configuration on a CP PM Co-res CS and SS Server workflow



Procedure 1
Configuring SIP Line on a CP PM Co-res CS and SS Server

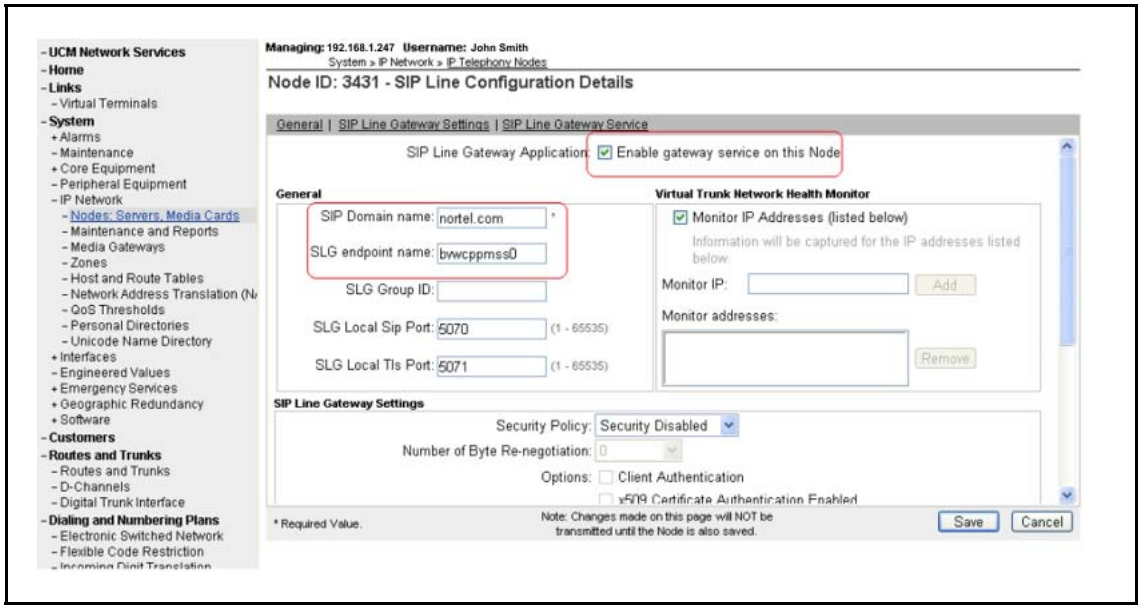
Step	Action
1	Ensure that you have installed the latest service pack.
2	Launch Element Manager.
3	In the navigation pane, click **System**, **IP Network**, **Nodes, Servers, Media Cards** The IP Telephony Nodes pages appears, as shown in Figure 17 "IP Telephony Nodes window" (page 99).

Figure 17
IP Telephony Nodes window



4	Navigate to the Node Details section.
5	In the Applications list, click **SIP Line**. The SIP Line Configuration Details screen appears, as shown in Figure 18 "SIP Line Configuration Details window" (page 100).

Figure 18
SIP Line Configuration Details window



6 Select **Enable gateway service on this node**.

7 Enter the SIP domain name.

8 Enter the SLG endpoint name.

9 Click **Save**.

10 Configure a new AML link and VAS.

11 If you are configuring a new node on the CP PM Co-res CS and SS Server, create a new D-channel for the SIP Line service route.

12 Configure a new route for the SIP Line service.

13 Configure a new trunk.

14 Restart the VTRK application.

--End--

CP PM Co-res CS and SS Server patch types

The CP PM Co-res CS and SS Server supports the following two patch types:

- Call Server Binary patches—to patch only the Co-Res Call Server. The filename for binary patches has the pxxxxx_x.cpl format.
- Linux patches—to patch Co-Res Signaling Server, Linux Base, Call Server, and other Linux-based applications.

You can execute Call Server Binary patching from either the pdt shell or the EM. Similarly, you can execute Linux patching from either the Linux shell or the Patching Manager. Patch files are transferred to the platform as a file through FTP/SFTP; USB stick; or Removable Media Device (RMD); for example, compact flash card.

Hardware

CP PM

The CP PM Co-res CS and SS server runs on the same CP PM generic Pentium-based server platform introduced in CS 1000 Release 5.0. When populated with the required 2 gigabytes (GB) of memory and 40 GB disk drive, the CP PM becomes the hardware platform for the CP PM Co-res CS and SS.

CP PM Media Storage

Fixed Media Device

The CP PM card on a new CP PM Co-res CS and SS is shipped with a 40 GB internal hard disk Fixed Media Device (FMD). For the CP PM Co-res CS and SS application to recognize that the FMD is a hard disk device (rather than a Compact Flash [CF] card), you must set switch S5 on the CP PM card to position 2.

For VxWorks-based CP PM cards that run the Call Server application, switch S5 is in position 1 to indicate a CF card is used for the FMD. This CF card FMD is accessible only when the CP PM card is removed from the system.

Removable Media Device

The CP PM Co-res CS and SS supports two Removable Media Devices (RMD):

- CF card for installing Linux Base and to back up and restore the Call Server database
- Universal Serial Bus (USB) memory stick device, used to back up and restore Linux Base and CP-PM Co-res CS and SS applications, including the Call Server database

  Note: CF cards and USB memory sticks are supported for database back up and restore.

For Linux Base and application software installation, the minimum size supported for the RMD is 1 GB. For more information on supported media for CP PM Co-res CS and SS application installation, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Ethernet Interfaces

The CP PM hardware platform has three Ethernet ports. The Co-Res Sever application uses the ELAN and TLAN ports.

Note: The CP PM Co-res CS and SS Server Release 6.0 does not support the CS High Availability feature; therefore, Co-Res Sever does not use the HSP port.

Serial Data Interface

The serial data interface (SDI) ports of the CP PM platform are routed through the backplane of the shelf to the 50-pin MDF connector on the back of the shelf. The CP PM call server is shipped with a cable that adapts the 50-pin MDF to a 25-pin DB connector (NTAK19EC). The cable provides access to serial ports Port0 and Port1. These ports are mapped to the console port for the Co-Res Call Server application. Port1 does not support root log-in or point-to-point protocol (PPP).
You must use a 25-pin null modem adapter to adapt the SDI port to a PC serial port.

Port0 has the following default TTY settings:

- Baud rate: 9600
- Data bit: 8
- Stop bit: 1
- Parity: none
- Flow control: none

LEDs

Status LED

The Status LED for the CP PM Co-res CS and SS Server indicates the following conditions.

LED color	Description
Red	Hardware/BIOS
Yellow	Loading Co-Res applications
Green	Co-Res applications loaded and started successfully (normal operation)
Off	No power

The **`reboot`** or **`reboot -l`** commands from the Call Server pdt shell change the status of the LED to yellow. When restart is completed, the LED status changes to green.

If you press the INI button on the CP PM Co-res CS and SS Server faceplate, the LED status changes to yellow followed by green.

Active CPU LED

The Active CPU LED for the CP PM Co-res CS and SS Server indicates the following conditions.

LED color	Description
Red	Single core Call Server
Off	No power

Software applications

Support is available for the following software applications on the CP PM Co-res CS and SS Server:

- Linux Call Server
- SIP Line
- Line Telephony Proxy Server
- Unicode Name Directory
- SSG including H.323 Gateway and Session Initiated Protocol (SIP) Gateway
- Failsafe SIP Proxy Service, Gatekeeper
- Personal Directory
- Network Routing Service (NRS)
  - NRS can be configured as a primary NRS, but can only be configured as a secondary NRS when the primary is also running on a CP PM Co-res CS and SS.
  - There is no support for CP PM Co-res CS and SS running a secondary or back-up NRS to a higher capacity primary NRS due to the small disk size and low call rates on the CP PM Co-res CS and SS system.
- Element Manager
- Unified Communications Management (UCM) Primary security server is supported in a very limited deployment. For detailed UCM Primary security server procedures, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

These applications are bundled into predetermined CP PM Co-res CS and SS options that you can install by using the Deployment Manager Web-based Graphical User Interface (GUI) as follows:

- Call Server, Signaling Server, and Element Manager
- Call Server, Signaling Server, Network Routing Service, and Element Manager
- Call Server, Signaling Server, Network Routing Service, Element Manager, and Subscriber Manager

High Availability support

In CS 1000 Release 6.0, the CP PM Co-res CS and SS does not support a High Availability (HA) configuration (dual core with either active or inactive role). For systems that require an HA configuration, the VxWorks-based Call Server software must be deployed.

IP Telephony Node Manager

This management interface supports configuration and enabling of Signaling Server application services such as UNIStim, LTPS, SIP Gateway, H.323 Gateway, and SIP Line.

For more information about IP Telephony Node Manager, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Media Gateway 1010 (MG 1010) Chassis

Overview

The Media Gateway 1010 (MG 1010) is a rack mount Media Gateway chassis that provides a larger amount of card slots than a MG 1000E with Media Gateway Expander. The CS 1000E Call Server can connect to and control a maximum of 50 MG 1010s. Each MG 1010 provides a dedicated MGC slot, two dedicated CP PM card slots, and ten slots for IPE cards. The MG 1010 is a single chassis that can provide more processing power and card capacity than a MG 1000E with Media Gateway Expander.

The MG 1010 media gateway does not support the Small System Controller (SSC) processor.

For more information about MG 1010, see *Communication Server 1000E Planning and Engineering* (NN43041-220).

Physical description

The Media Gateway 1010 chassis (NTC310AAE6) consists of:

- MG 1010 rack mount kit (NTC316AAE6)
- backplane assembly (NTC31002)
- Media Gateway Utility (MGU) card (NTC314AAE6)
- power supply, maximum of two with load sharing (NTC312AAE6)
- blower fans, N+1 arrangement for redundant cooling (NTC320AAE6)
- air filter (NTC315AAE6)
- front cover with EMI containment and a window to view status LEDs
- MG1010 serial cable kit (NTC325AAE6)

Nortel recommends you to use CP PM card (NTDW99) and MGC card (NTDW98) in a MG 1010. The updated cards contain metal faceplates for enhanced EMC containment.

The following sections describe the front and rear components of the MG 1010 (NTC310).

Front components

Figure 19 "Front components in the MG 1010" (page 106)shows the Media Gateway 1010 without the front cover. Note the following:

- Ten IPE card slots
- Two CP PM card slots
- One MGC card slot
- One Media Gateway Utility (MGU) card provides LED status, ringing, message waiting voltage, dual homing Ethernet cable ports, and serial cable ports
- One metal divider in chassis to separate MGU, CP PM, and MGC from the IPE cards.

Figure 19
Front components in the MG 1010

Figure 20 "MG 1010 front cover" (page 107) shows the MG 1010 with the front cover. Note the following:

- Window to view LED status of all cards
- Decorative cover provides additional EMC shielding
- Two locking latches in top corners of front cover

Figure 20
MG 1010 front cover

Rear components

Figure 21 "Rear components of the MG 1010" (page 108) shows the rear components of the MG 1010. Note the following:

- Hot swappable redundant power supplies
- Hot swappable fans in a redundant N + 1 configuration for chassis cooling
- One DECT connector
- One AUX connector
- Ten MDF connectors

Figure 21
Rear components of the MG 1010

Media Gateway Extended Peripheral Equipment Controller (MG XPEC)

Overview

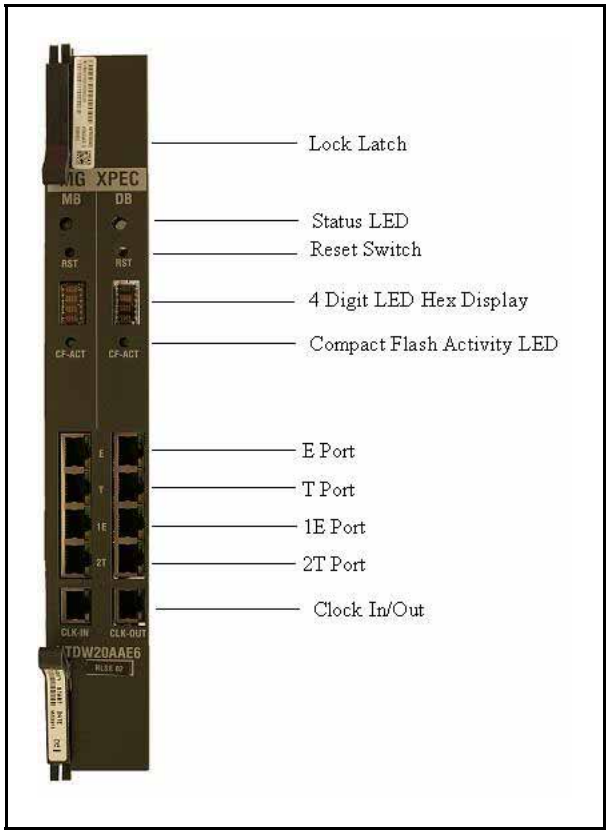
The MG XPEC provides a cost effective solution to migrate from a Meridian 1 or CS 1000M to a CS 1000E system while allowing customers to re-use most of their existing peripheral equipment. The MGXPEC is essentially equivalent to 2 MGCs, and the two halves of the MG XPEC are different IPMG loops.

For more information about MG XPEC, see *Communication Server 1000E Planning and Engineering* (NN43041-220).

Physical description

The MG XPEC is a double wide pack, dual card assembly using ported MGC hardware. It is used to control PE line cards in an IPE shelf. The MG XPEC features a motherboard and daughterboard architecture which act independently and provide the same hardware functionality as that of an MGC. Each board of the dual assembly is populated with 192 DSP resources which are recognized by the software as the equivalent of two MGC DSP daughterboards. The MG XPEC can be thought of as 2 separate MGCs bolted together with the left board (motherboard) controlling the left half of the of the IPE shelf and the right (daughterboard) controlling the right half of the IPE shelf. Figure 22 " MG XPEC faceplate" (page 110) provides a view of the MG XPEC faceplate

Figure 22
MG XPEC faceplate



Commercial Off The Shelf servers

Overview

Dell R300 and IBM x3350 servers provide increased reliability through the use of redundant power supplies and RAID 1 arrays. Server performance is enhanced by more powerful processors (compared to previously introduced Commercial Off The Shelf [COTS] servers) and greater memory capacity.

For a brief listing of server specifications, see “Dell R300 specifications” (page 111) or “IBM x3350 specifications” (page 111).

For more information about COTS servers, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Dell R300 specifications

- Intel Quad Core Xenon CPU –2.5GHz
- 250Gb RAID 1 array (2x 250GB hard drives, hot-swappable)
- 4Gb memory
- CD-RW/DVD drive
- Redundant power supply (hot-swappable)
- Dual 1 gigabit ethernet ports
- BIOS and RAID settings preconfigured for Nortel applications

IBM x3350 specifications

- Intel Core 2 Quad CPU –2.66GHz
- 250Gb RAID 1 array (2x 250GB hard drives, hot-swappable)
- 4Gb memory
- CD-RW/DVD drive
- Redundant power supply (hot-swappable)

- Dual gigabit ethernet ports
- BIOS and RAID settings preconfigured for Nortel applications

For more information about the IBM x3350 Server, go to www.ibm.com.

SIP Line

Overview

The Communication Server (CS) 1000 is a feature-rich hybrid Internet Protocol Private Branch Exchange (IP PBX) solution, which delivers Business Grade Telephony features and functionality to IP endpoints. The SIP Line Service fully integrates Session Initiation Protocol (SIP) endpoints in the CS 1000 system and extends the CS 1000 telephony features to the SIP clients.

The SIP Line Service comprises three components:

- The SIP Line Universal Extension (UEXT) called SIPL on the Call Server.

  Note: The CS 1000 Release 6.0 SIPL Universal Extension is different from the UEXT used in Release 5.5.

- The SIP Line Gateway (SLG) application.
- The system management interface (Element Manager) used to configure and manage the SIP Line Service.

The CP PM Co-resident Call Server and Signaling Server requires you to enable SIP Line. For information about enabling SIP Line on a CP PM Co-res CS and SS server, see “SIP Line support on CP PM Co-res CS and SS Server” (page 96).

SIP Line architecture

The SIP Line Service is embedded in each CS 1000 system and directly manages a number of SIP clients. The Universal Extensions (UEXT) line type provides CS 1000 Line appearance to the supported SIP clients and this extends the existing CS 1000 Networking and Line services to these SIP clients.

The inclusion of SIP endpoints in the CS 1000 system is based on the SIPL UEXT. Universal Extensions are used to represent devices and clients that are external to the CS 1000 system. Universal Extensions use virtual Terminal Numbers (TN).

ATTENTION
You must configure the SIP clients with the CS 1000 SIPL UEXT Universal Extension SIPL subtype, which provides a line appearance to the SIP clients.

The SIP Line Gateway (SLG) is the SIP Line signaling gateway, which communicates between the CS 1000 Call Server (CS) and the SIP side of the signaling. The SIP Line Gateway (SLG) serves as a SIP Registrar and a SIP Proxy server to users. The SLG uses voice signaling messages to communicate internally with the Call Server.

Required packages

The SIP Line Service depends on the following packages:

Table 31
Feature packaging

Package mnemonic	Package number	Package description
SIP_LINES	417	SIP Line Service package
FFC	139	Flexible Feature Codes
SIPL_NORTEL	415	Nortel SIP Line package
SIPL_3RDPARTY	416	Third-party SIP Line package

The FFC package is required only to enable FFC features. The Nortel SIP Line and Third-Party SIP Line packages are needed only if SIP Line supports the respective IP Phone type.

SIP Line is bound by SIP_LINES package (417). This package must be enabled to perform the following activities:

- Configure SIP Line IP Phones.
- Enable the SIP Line feature.

The following SIP IP Phones are supported in this release:

- Nortel IP Phone 1120E
- Nortel IP Phone 1140E
- Nortel IP Phone 1200 Series (IP Phone 1210, IP Phone 1220, and IP Phone 1230)
- Nortel IP Phone 1535
- Nortel IP Softphone 3456

- IpDialog SipTone V IP Phone
- Teledex 2200
- Teledex 4200

Hardware and software requirements

The SIP Line Service comprises three major software components: Call Server (CS), SIP Line Gateway (SLG), and Element Manager. Software changes on the Call Server are bundled within the SIP Line Service Package (SIP_LINES PACKAGE, 417) and reside on the supported hardware platforms with the addition of the commercial off-the-shelf (COTS) and Common Processor Pentium Mobile (CP PM) Call Processor. Both the SIP Line Gateway and Element Manager reside on the Linux COTS or CP PM servers.

Support is available for the following hardware platforms:

- HP 320 G4
- IBM x306M
- Dell R300
- IBM x3350
- Nortel Common Processor Pentium Mobile (CP PM)

For more information about SIP Line and the features offered by the SIP clients, see *SIP Line Fundamentals* (NN43001-508).

UNIStim Security DTLS

Overview

Secured Unified Networks IP Stimulus (UNIStim) signal encryption is provided by Datagram Transport Layer Security (DTLS), which encrypts the data exchanges between the Signaling Server and the IP Phones. Previously, Secure Multimedia Controllers (SMC 2450) were required for UNIStim encryption, but DTLS requires no new additional hardware and can coexist with currently installed SMCs. DTLS and non-DTLS systems can be configured on the same network.

To enable DTLS encryption, the Communication Server (CS) 1000 system must be upgraded to CS 1000 Release 6.0 and the IP Phones must have the latest firmware. Also, the system has to be configured with at least the Basic Security level.

Note: This feature does not provide signaling encryption for the Unified Networks IP Stimulus File Transfer Protocol (UFTP), which is used when transferring firmware to IP Phones. Firmware data contains no sensitive information and is protected from third-party tampering by a digital signature. Notifications from the signaling server to the phones are sent using DTLS-protected UNIStim signaling to protect the signals from intercept.

DTLS and IP Phone registration

There are two modes of IP Phone registration:

- Secure Handshake mode—the IP phone is configured to initiate a DTLS session immediately upon beginning registration.
- Switchover mode—the IP phone is configured to first establish an unencrypted Reliable User Datagram Protocol (RUDP) session to the Line Terminal Proxy Server (LTPS), then switchover to DTLS depending on the DTLS Policy.

Supported hardware

UNIStim with DTLS is supported on the following CS 1000 components:

- **Call Servers**
  - CP PIV
  - CP PM (Standalone)
  - CP PM (Co-resident)
  - MGC
- **Signaling Servers**
  - CP PM (Standalone)
  - CP PM (Co-resident)
  - HP DL320 G4
  - IBM x306m
  - IBM x3350
  - Dell R300

ATTENTION
IP Phones require UNIStim 4.0 or later to support DTLS signaling encryption.

The IP Phones support DTLS signaling encryption (after applicable firmware upgrade)

- IP Phone 1200 series (IP Phone 1210, IP Phone 1220, IP Phone 1230)
- IP Phone 1100 series (IP Phone 1110, IP Phone 1120E, IP Phone 1140E, IP Phone 1150E)
- IP Phone 2000 series (IP Phone 2001, IP Phone 2002, IP Phone 2004, IP Phone 2007)

Security levels

Various configuration options of UNIStim with DTLS can be combined to form three security levels: Basic, Advanced, and Complete. As the level of security increases, there are certain limitations on the supported hardware and software.

Note: The configuration of the security levels must be done sequentially. For example, to configure or upgrade the network to Complete security, you must first enable Basic security, then upgrade to Advanced security, and then upgrade to Complete security.

For information about configuring UNIStim DTLS, see *Security Management Fundamentals* (NN43001-604).

Secure File Transfer Protocol

Overview

Secure Shell (SSH) Secure File Transfer Protocol (SFTP) is installed and enabled on Communication Server 1000 Release 6.0 systems by default. This secure protocol replaces regular File Transfer Protocol (FTP) and other insecure data transfer protocols for several Communication Server 1000 applications.

ATTENTION
Call Pilot or Telephony Manager usually functions as a client; therefore they continue to use FTP to communicate with CS 1000 Release 6.0 Call Server that supports both SFTP and FTP.

SFTP allows data to be securely transferred between an SFTP client and server over an encrypted and authenticated secure channel. In addition, SFTP allows a client and a server to authenticate each other by using a password. Devices obtain authentication and access control permissions for CLI access from the Unified Communications Management Primary Security Server. Remote Authentication Dial In User Service (RADIUS) parameters are sent from the Unified Communications Management Primary Security Server to the Call Server using SSH protocol. SFTP uses port 22, which is the same port used by SSH.

SFTP clients do not authenticate an SFTP server by its public key. The SFTP client uses an IP address configured during installation to contact the SFTP server. Unlike the interactive use of SFTP or SSH, in which the IP addresses or Fully Qualified Domain Names (FQDN) of the servers were entered manually by users and thus subject to error, SFTP clients are configured with the correct SFTP server IP addresses.

Not all Communication Server 1000 applications are compatible with SFTP. To provide backward compatibility for those features that are not compatible with SFTP, conventional FTP is still used for file transfer sessions between CS 1000 Release 6.0 systems and systems with previous versions. For systems and applications that are not compatible with SFTP, IPsec protocols are used for security.

ATTENTION
SSH SFTP is SSHv2 and SFTPv3 compliant.

The following characteristics apply to SFTP:

- the public key of a SFTP server is always trusted by SFTP clients, so there is no requirement for verification
- a user name and password is used by a SFTP server to authenticate a SFTP client (public key-based authentication is not supported for authenticating a SFTP client)
- TFTP for transferring tone and cadence files is not changed
- not all FTP applications use SFTP; some continue using standard FTP
- configuring the system time could have an impact on the connection timeout of SFTP

SFTP for Linux platforms

SFTP for Linux is provided by the integrated openSSH and openSFTP functionality that is part of the Linux base operating system.

File transfer options for Linux and VxWorks platforms

The following table shows the file transfer options for Linux and VxWorks platforms.

Table 32
File transfer options for VxWorks and Linux platforms

	Linux			VxWorks		
Method	**FTP**	**SFTP**	**TFTP**	**FTP**	**SFTP**	**TFTP**
Default	ON	ON	ON	ON	ON	ON
Options	OFF/ON[1]	ON	OFF/ON [1]	OFF/ON [2]	OFF/ON [3]	ON
[1] with Linux harden command						
[2] with Disable/Enable Transfer Insecure command						
[3] with Disable/Enable Transfer Secure command						

SSH client

The SSH client is implemented to facilitate access to an SSH server. There is no Command Line Interface (CLI) implementation of the SSH client for VxWorks platforms; however, there is access to the SSH client on Linux hosts. The joinSecDomain/REGISTER UCMSECURITY [DEVICE/SYSTEM] command, used for joining the Unified Communications Management security domain, uses the SSH client to communicate with the Unified Communications Management primary server but does not provide any shell level access.

The Communication Server 1000 Release 6.0 system supports unsecured remote access methods, such as rlogin and telnet, but you can disable them.

For information about Secure File Transfer Protocol, see *Security Management Fundamentals* (NN43001-604).

SSH Library upgrade

The Mocana embedded security suite version 1.36 supported in CS 1000 Release 5.0 is upgraded to the latest version 1.38 for CS 1000 Release 6.0. Version 1.38 features the following improvements:

- Enhanced Security solution
- SSH server now supports both RSA and DSA key generation and authentication negotiation with an SSH client. For example, a CS 1000 SSH server uses RSA key authentication to communicate with a UCM Primary Server SSH client, since UCM only supports RSA key authentication.
- An SFTP server
- standard DTLS solution

Limitations

The following list provides the limitations of SFTP feature.

- CS 1000 VxWorks platform device accepts up to a maximum of 20 simultaneous incoming SFTP connections. After the limit is reached, the next connection is rejected and depending on the SFTP client software (for example, openSSH) a message stating the host refuses to accept connection appears.

  To prevent an incoming connection from holding up a resource for extend period of time, an SFTP session timeout (configured through LD 17) is implemented. This means that if an SFTP session is idle for more than the timeout configured then the session is automatically closed, which frees up the SFTP session. Likewise, the SFTP authentication timeout of 15 seconds is also implemented. This means that when an incoming SFTP session is about to start and if user failed to enter the authentication information with 15 seconds then the connection drops.

- Because the SFTP client is only available to applications called there is a limit of 6 outgoing SFTP sessions allowed at any time.

  If the limit is reached then the next SFTP session fails with a debug message saying the session limit is reached.

- Public key of an SFTP server is not verified by an SFTP client and is always trusted.

- User name and password are used by an SFTP server to authenticate an SFTP client. Public key based authentication is not supported for authenticating an SFTP client.
- TFTP for transferring tone and cadence files is not changed by this feature.
- Not all FTP applications are changed to use SFTP by this feature.

IP Call Recording for Office Communications Server support

Overview

The IP Call Recording for Office Communications Server (OCS) support enhanced feature complements the Nortel Converged Office solution by providing the ability to record calls simultaneously. The Application Module Link (AML) link is used to converge the Microsoft Office Communicator (OC) client and the Nortel IP phone for Remote Call Control (RCC) to monitor an IP phone for IP Call Recording functionality. The AML Front End (FE) enables both co-resident and non-co-resident applications to acquire and control the same Directory Number (DN) of a phone at the same time. The AML front end splits a single stream of AML messages from the Call Server into two or more outgoing streams of AML messages and multiplexes two or more streams of incoming AML messages into a single stream of AML messages to the Call Server.

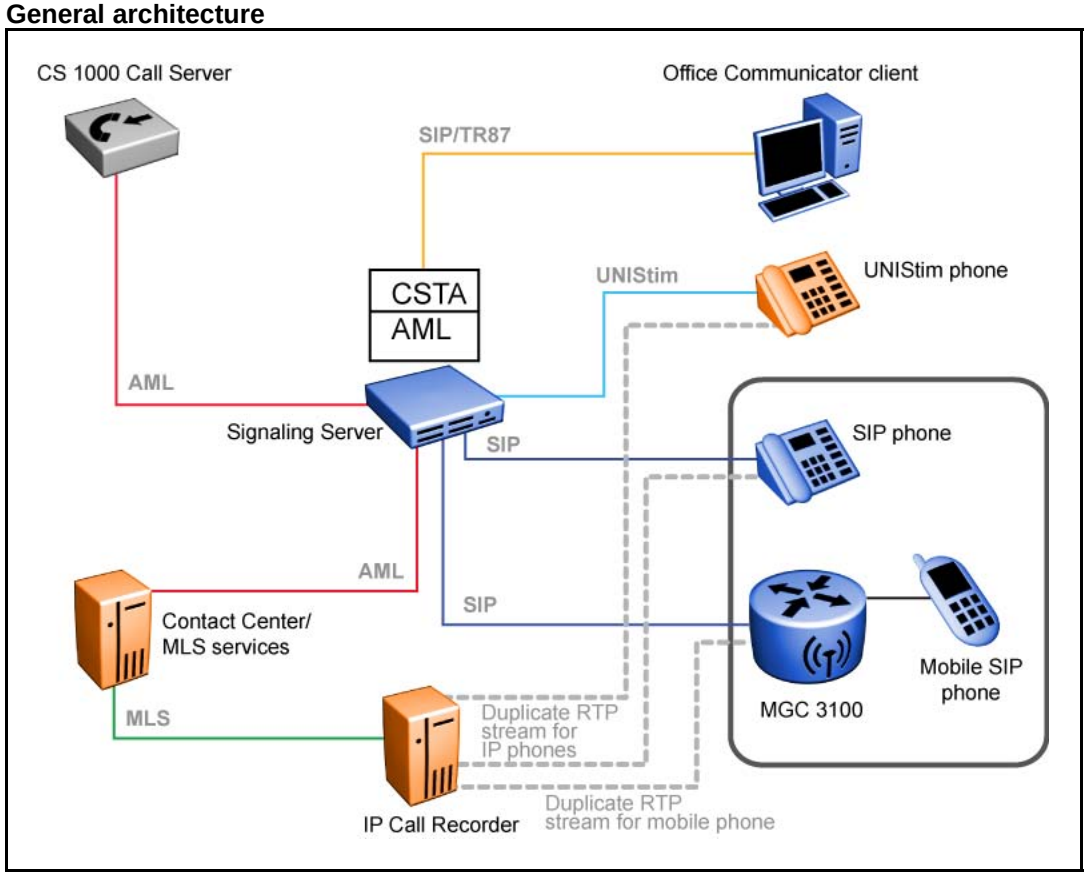
Supported platforms

IP Call Recording for OCS is supported on the following platforms

- Call Server
- CS 1000E with MG
  - CP PIV
  - CP PM (Co-resident and non Co-resident
- Signaling Server
  - CP PM
  - COTS

The general architecture of IP Call Recording is shown in the following figure.

Figure 23
General architecture



For more information about IP Call Recording for OCS, see *Automatic Call Distribution Fundamentals* (NN43001-551).

IP Client enhancements

Overview

Communication Server (CS) 1000 Release 6.0 supports the following IP Phones:

- IP Phone 2000 Series—Phone 2001, Phase II IP Phone 2002, Phase II IP Phone 2004, IP Phone 2007, IP Audio Conference Phone 2033
- IP Phone 1110 Series—IP Phone 1110, IP Phone 1120E, IP Phone 1140E, IP Phone 1150E
- IP Phone 1535
- IP Softphone 2050
- Nortel Mobile Voice Client 2050
- Nortel WLAN Handsets—WLAN Handset 2210, WLAN Handset 2210, WLAN Handset 2212, WLAN Handset 6120, WLAN Handset 6140

CS 1000 Release 6.0 introduces the following enhancements for the IP Phones.

- Normal Mode Indication
- Caller ID display order
- Languages

Normal Mode Indication

The Normal Mode Display notification can be on or off for IP Phones registered in normal mode. This feature prevents the Branch User ID (BUID) overwriting the date and time on the IP Phone 2002, IP Phone 1120E, and IP Phone 1220. This feature also stops infinite scrolling on the IP Phone 2001, IP Phone 1110, IP Phone 1210, and IP Audio Conference Phone 2033.

Caller ID display order

The Caller ID can appear in two formats:

- Number, name (Default)—Caller ID number always appears on the first line. If the number and name (Calling Party Name Display [CPND] or Preferred Name Match [PNM]) cannot fit on one line, then the name appears on the second or third line.
- Name, number—Caller ID name always appears on the first line and the number is displayed on the second line. If the name does not exist, the number appears on the first line.

Languages

The IP Phones support 25 languages. For the IP Phone 1110 and IP Phone 1210, the IP Phone display changes from three-line mode to two-line mode when the language is Greek, Hebrew, Arabic, Chinese Simplified, Chinese Traditional, Japanese, and Korean. The IP Phone displays two-line mode for these languages as the characters require more space.

For more information about CS 1000 Release 6.0 IP Clients enhancements, see *IP Phones Fundamentals* (NN43001-368).

Multi Directory Number recording

Overview

The Multi Directory Number (DN) Recording feature was developed based on the existing IP Call Recording feature. Considerable changes to voice recording activity on an IP Phone, including any expansion modules fitted irrespective of which User ID, is used.

The existing recording solution allows recording of only two keys per physical terminal. Multi DN Recording allows users to record calls on the maximum number of keys configured on a set.

Registered the keys with the IP Call Recording application only, to use the Multi DN Recording feature for recording purposes. The Associated Device (AST) registration is required for other Non IP Call Recording applications for the existing features to work.

The feature interacts with the following upcoming IP Call Recording enhancements:

- Record on Demand — provides the ability with respect to start/stop call recording and saving/deleting the recording conversation on their phone set.
- AML Multiplex — provides the call recording on Converged Office with Microsoft LCS/OCS.

A new prompt, MRCD is introduced in Overlay 11 to keep track of the user IDs, DN/POSID, registered for recording. MRCD is a dynamic prompt that displays the key numbers for the user IDs registered with Change Request (CR).

The licensing for the feature is done on the Contact Center Manager Server (CCMS).

For more information about the Multi DN Number recording feature, see *Features and Services Fundamentals* (NN43001-106).

Record on Demand

Overview

You can use the Record on Demand (ROD) feature to record and save a telephone conversation.

The ROD feature is supported on the following phones:

- IP Phone 2002
- IP Phone 2004
- IP Phone 2007
- IP Softphone 2050
- Mobile Voice Client 2050
- IP Phone 1120E
- IP Phone 1140E
- IP Phone 1150E

The ROD feature has two functions:

- Record an active telephone conversation on demand
- Save an active recording

When you press the ROD key, the Call Recording (CR) application is notified on the key press event and starts the telephone conversation recording (as for any basic IP call recording). To stop the recording, press the ROD key again. You can start or stop the recording by pressing the ROD key anytime time during an active call. The Save/Delete key saves or deletes the current recording.

Record and SaveCall are displayed on the phone for ROD and SAVE keys respectively.

For more information about the Record on Demand feature, see *Features and Services Fundamentals* (NN43001-106).

TLS and SRTP

Overview

Enhancements to TLS and SRTP are implemented to provide enhanced interoperability with third-party products such as Microsoft products.

The following subsystems on the Communication Server (CS) 1000 are affected by the SRTP enhancements:

- Call Server
- Signaling Server
- Digital Signaling Processors (DSP)
- Phase 2 UNIStim clients
- SIGMA Release 3.0 telephones
- SDesc

The following three areas of SRTP implementation changed:

- Best effort method for SRTP negotiation. The three additional attributes are tcap, pcfg, and acfg.
- Crypto keying materials used in SIP REINIVITES for call holding and resuming. SIP, SDP, and SDESC crypto attribute lines are updated to remove trailing zeroes as specified in RFC4568.
- Master Key Index (MKI).

The following are the TLS enhancements:

- increased chance of being authenticated by others by sending the full certificate chain
- improved process to validate certificates by verifying that any certificate in the certificate chain was not revoked and that the FQDN and IP of the connection are consistent

For more information about TLS and SRTP, see *Nortel Converged Office Fundamentals – Microsoft Office Communications Server 2007* (NN43001-121).

Calling Line ID Enhancement

Overview

Caller Line Identification (CLID) Enhancement extends the Calling Party Privacy Enhancement feature to all ISDN interfaces (and signaling applications using ISDN formatted signaling, such as Voice over IP). It creates a new prompt to selectively allow or reject the calling party number to Auxiliary (Aux) applications like Contact Center Manager (CCM) when the calling party number is received with presentation indicator set to restrict. This allows these applications to use the number to route (as required), without making the number or name available to all users.

This provides a route option to ignore the Calling Party Privacy Indicator on incoming calls received from the North American public ISDN network. When the Privacy Indicator Ignore (PII) prompt is set to YES, the Calling Line Identification (CLID) Presentation Indicator and the Calling Party Name Display (CPND) Indicator (if it exists) are changed from restricted/denied to “allowed”.

Interfaces

The PII prompt and functionality is supported to the following interfaces for Primary Rate Interface (PRI) and Basic Rate Interface (BRI):

- Meridian Customer Defined Network (MCDN) Enterprise networking variants (including the peer to peer variant- SL1 and the enterprise UNI variant- SL100).
- Euro ISDN (All variants)
- APAC (All variants)
- QSIG (ISO and ETSI)
- H323 and SIP (The new feature supports the H323 and SIP protocols as they use the MCDN peer to peer version SL1 between the call server and the signaling server).

Benefits

The route option Auxiliary processor applications (AUXP) allows greater granularity to honor or ignore the Privacy indicator for a Calling Party Privacy call for each incoming route. If the option is set to YES, the CLID Presentation Indicator and the CPND Indicator (in an incoming SETUP message) are changed from restricted/denied to allowed for Aux applications and if AUXP is NO, then the CLID Presentation Indicator does not change.

For more information about the CLID) Enhancement for the Calling Party Privacy Enhancement feature, see *ISDN Primary Rate Interface Features Fundamentals* (NN43001-569).

Network Routing Service enhancements

Overview

Communication Server 1000 Release 6.0 includes many new and enhanced features for Linux Network Routing Service (NRS).

For information on the features described in this chapter, see *Network Routing Service Fundamentals* (NN43001-130).

Redirect Server support on Linux-based NRS

The Linux-based NRS can act as a SIP Proxy or as a SIP Redirect Server on a per end point basis. Configuration of Gateway and User endpoints is provided through NRS Manger. Calls can be made between Proxy mode and Redirect Server mode endpoints.

The SIP Redirect Server mode offers a significant improvement in call capacity, but most advanced features (such as Post-routing SIP URI modification) are not supported in Redirect Server mode.

MySQL Database Migration

In CS 1000 Release 6.0, MySQL Enterprise 5.1 server is used to store and query the NRS routing data. Migration from the Solid database, used in previous releases to MySQL provides significant improvement in call processing capacity and system stability. There is no impact on the user interface due to MySQL migration.

Same cost routing with SPS and GK

When executing a location query during server/client session set up, a target set consisting of multiple addresses can be produced with the same cost value. Same cost routing provides load balancing by random selection among multiple gateway routes with the same cost factor.

Source base routing for Multimedia Convergence Manager

Source based routing interworks with Multimedia Convergence Manager (MCM). All calls (SIP sessions) originated by the Office Communications client go through the home CS 1000 where the originator's DN belongs. If homing can not be done on MCM by using the phone number, MCM forces the SIP Proxy or SIP Redirect Server to do the routing using the first SIP gateway endpoint instead of the phone number.

Service domain name can be configured as an IP Address in NRS Manager

In CS 1000 Release 6.0, the Service Domain name can be configured as the Primary NRS Server TLAN IP address when required for interworking with third party gateways that do not support a Service Domain name.

Operation, Administration and Maintenance Transaction Activity and Security Event Logging

The Operation, Administration and Maintenance (OAM) Transaction Activity and Security Event Logging is a secure record of all system administrator OAM activities and security related events. The OAM Transaction Activity and Security Event Logging is maintained in a centralized location on the Nortel Unified Communications Management Common Services. It can be forwarded to an external Operational Support System using the Linux syslog daemon.

The OAM log records include security, operational, configuration and maintenance events of CS 1000 management applications. The security audit logs contain sufficient information for after-the-fact investigation, or analysis, of security incidents. The audit logs provide a means for accomplishing several security-related objectives including individual accountability, reconstruction of past events, intrusion detection and problem analysis.

Access to NRS CLI command

The maintenance and administration, system administration, and database administration CLI commands have been renamed and moved to a new location under a new policy based access method.

The maintenance and administration commands are accessible only by users belonging to the UCM Common Services maintenance and administration group (maintadmin).

The system administration commands are accessible only by users belonging to the UCM Common Services system administration group (systemadmin).

The database administration commands are accessible only by users belonging to the UCM Common Services database administration group (dbadmin).

For more information about NRS enhancements, see *Network Routing Service Fundamentals* (NN43001-120).

Patching Manager

Overview

Patching Manager supports patching for all Linux-based elements in CS 1000 Release 6.0. This includes patching of all Linux bases and applications on these elements (except for Call Server on the Co-resident Call Server and Signaling Server).

> ***Note:*** Patching for the Call Server (on VxWorks or Linux) and other VxWorks devices (such as media cards) is supported by Element Manager.

Linux base supports three patch categories:

- Patch—This category of patch changes program behavior for a period of time. Patches are used to fix bugs or for diagnostic purposes. In some instances, you can apply this category of patch without a program restart.
- Serviceability update—A serviceability update (SU) is a cumulative update of patches. A serviceability update is a full-application Red Hat Package Manager (RPM) package distribution that contains all patches that you apply to a specific application, and replaces previous serviceability updates.
- Service packs—A service pack (SP) is a single file that contains a bundle of multiple patches and serviceability updates for a specific product release.

The Patching Manager provides a graphical user interface (GUI) to upload and manage patches and service packs on the Linux targets in the enterprise network. The Patching Manager facilitates the centralized deployment of patches to all target Linux systems within the Unified Communications Management (UCM) security domain. For more information about UCM, see *Unified Communications Management Common Services Fundamentals* (NN43001-116).

You can use Patching Manager on the primary security server to remotely deploy patches from a central location to other Linux servers on the same security domain (using the Central Patching Manager). You can also install patches locally. Local patching is accessible from the Base Manager of each Linux Element (using the Local Patching Manager).

Two interfaces support patch management:

- Central Patching Manager—The Central Patching Manager is accessible from Primary UCM server. Central Patching Manager obtains the list of all Linux servers (or Linux Base Elements) in the same security domain from the UCM framework and can patch all Linux elements in the same security domain.
- Local Patching Manager—The Local Patching Manager is accessible from the UCM Base Manager of each Linux element. Base Manager can be accessed using a central UCM login or a local login to the element.

Patching Manager does not support patching of the Call Server, Media Gateway Controllers, and media cards. Element Manager supports Call Server and media card patching.

For more information about Patching Manager, see *Patching Fundamentals* (NN43001-407).

Base Manager

Overview

The Base Manager is a new interface to the element level Linux base. Base Manager is used for lower level configuration of Linux elements.

Base Manager allows you to manage the base system in the following functional areas:

- Base System
  - Networking (Network Identity, DNS and Hosts, Route Table)
  - Explicit Congestion Notification
  - Date and Time
- Software
  - Applications
  - Deployment
  - Patches
- Tools
  - Logs

Click Element in the UCM Element list to access the Base Manager interface.

For more information about Base Manager, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Deployment Manager

Overview

Deployment Manager is introduced in CS 1000 Release 6.0 Unified Communications Management (UCM) Common Services. Deployment Manager is used to deploy software applications from a central location. Every Linux server that is installed on the network is learned by UCM Common Services where Deployment Manager is running. Centralized software deployment is the Nortel recommended solution for deployment but local deployment remains an option. Deployment Manager provides the following benefits:

- centralized application deployment and upgrades
- backup and restore capabilities
- GUI front end to Linux base features

Application installation using Deployment Manager

Nortel Linux platform uses Deployment Manager to remotely deploy application software from the primary security server to other Linux servers located in the same security domain.

The primary security server acts as a central repository for the application software loads. Application software is deployed from the primary security server to other Linux servers in the security domain on a per host basis. Deployment Manager is a web-based framework.

You can also use the Local Deployment Manager to deploy application software to a server before it joins the security domain, however centralized deployment is the preferred method.

There are 2 types of applications.

- Base applications
- Nortel applications

Base applications

Base applications provide necessary system functionality and must be successfully installed in order for Nortel applications to function. Base applications reside on the Linux base installation media and are installed automatically the first time the system boots up after base installation. The success or failure of the base applications installation is shown in an on-screen message. If the base application installation fails, the Linux base must be reinstalled.

The following is a list of base applications:

- Unified Communications Management (UCM)
- Nortel Simple Network Management Protocol (SNMP)
- Deployment Manager

Nortel applications

Nortel applications are installed using Deployment Manager. Nortel applications are deployed in the following predefined deployment packages:

- Signaling Server (SS)
- Network Routing Service (NRS)
- Signaling Server and Network Routing Service
- Call Server (CS) and Signaling Server (basic stand-alone Co-resident [CoRes] system)
- Call Server, Signaling Server, and Network Routing Service (CoRes system with branch support)
- Session Initiation Protocol Line (SIPL)
- Element Manager (EM)
- Subscriber Manager (SubM)

For more information about Deployment Manager, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Unicode Name Directory Server

Overview

CS 1000 caller or called party name appears in up to seven other languages with the Unicode Name Directory feature. This feature enhances the functionality of IP Phones that can display Unicode. The Unicode Name Directory feature provides localized names on a subscriber base and generates the Calling Line IDs and Uniform Resource Identifiers (URI) on a subscriber telephony account on a network level to serve the Unicode Name Directory server.

The Unicode Name Directory provides the following features:

- display of localized name in UTF-8 Unicode character encoding for incoming and outgoing calls
- storage for up to seven localized names in the database for a particular subscriber
- support for Korean, traditional and simplified Chinese, Japanese and other Unicode languages for called or caller party name display
- ability to work with IP Phone 2007, IP Softphone 2050 (version 3.1), IP Phone 1210, IP Phone 1220, IP Phone 1230, IP Phone 1110, IP Phone 1120E, IP Phone 1140E, and IP Phone 1150E.
- a Web interface for Unicode Name Directory server configuration

Unicode Name Directory integrates with Personal Directory (PD) as part of the Personal Directory installation. The Unicode Name Directory is enabled in the Call Server only if Personal Directory is configured. For information about configuring Unicode Name Directory, see *Element Manager System Reference—Administration* (NN43001-632).

In CS 1000 Release 6.0, Personal Directory and Unicode Name Directory can be installed as a part of Local software deployment or Centralized software deployment. For more information about deployment options, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

For more information about Unicode Name Directory Server, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

SNMP Linux

Overview

Fault management is implemented in Element Manager and hosted on the Unified Communications Management (UCM) Common Services framework. UCM provides a generic launch point, common user interface, and generic infrastructure for all applications.

For more information about Simple Network Management Protocol (SNMP) fault management, see *Communication Server 1000 Fault Management—SNMP* (NN43001-719).

SNMP trap and Management Information Base enhancements

Communication Server 1000 Release 6.0 introduces the following enhancements to SNMP trap handling and Management Information Base (MIB):

- new commands in LD 117 and Element Manager for enabling or disabling the sending of traps for any network element
- suppression of traps for network elements based on severity
- ability to configure trap destination ports is extended to all elements
- Linux command line tool for sending SNMP traps
- QOSTRAFFIC-MIB for Call Server
- SNMP MIB support for Linux-based Call Server and Signaling Server
- changes in the procedure to query Quality of Server (QOS) MIB on Signaling Server
- new command in LD 117 to synchronize SNMP parameters (EDD no longer synchronizes SNMP Parameters)

SNMP Profile Manager

Communication Server 1000 Release 6.0 introduces the concept of SNMP profiles. The SNMP Profile Manager page in Unified Communications Manager (UCM) provides a common interface to configure SNMP parameters on all Communication Server 1000 Network Elements.

The SNMP Profile Manager runs on the UCM Primary Security Server. It performs SNMP configuration at the security domain level. You can add, modify, and delete SNMP profiles using the SNMP Profile Manager. You can configure and assign profiles to the following types of UCM managed elements:

- Communication Server 1000 Call Servers
  - The configuration settings applied to the Call Server are propagated to all system elements associated with the Call Server, such as Signaling Servers, Voice Gateway Media Cards, and Media Gateway Controllers. These elements are all running CS 1000 applications, such as SIP Line.
- Linux elements running UCM Common Services, but not running Communication Server 1000 applications
  - Examples of these types of elements are standalone NRS elements, the UCM Primary Security Server, or an element running Element Manager, where in all cases there are no other CS 1000 applications installed (such as SIP Line, Signaling Server applications, and so on).

  You can add only one profile at a time, but you can delete multiple profiles at one time. A newly added profile is assigned version 1.0. When you update or modify the profile, the version number of the profile increments by one.

For more information about SNMP profiles, see *Communication Server 1000 Fault Management—SNMP* (NN43001-719).

Web Services API Administration

Overview

The Web services feature allows remote management and configuration of CS 1000 and Network Routing Service (NRS) systems. Web services allow application developers to write custom management applications, to accomplish custom or specialized tasks for CS 1000.

Four web services are available depending on what management applications (EM or NRSM) are deployed on a UCM CS server. The following table displays the types of services deployed depending on the type of server that is installed. The deployment type can be Element Manager (EM) or Network Routing Service (NRS) irrespective of whether the server is primary, backup, or member.

Service	Description	Deployment type
CS 1000	Provides access to functionality available on the CS 1000. This includes overlay access and selected Signaling Server and Media Card CLI command access.	Element Manager
Phone Provisioning	Provides a programmable way of configuring phones.	Element Manager
Network Routing Service (NRS)	Provides access to functionality available through NRS Manager (NRSM).	NRS
Managed Element Registry	Provides access to query managed elements available in UCM that support one of the other services.	Element Manager and NRS

In this table, the deployment types (as per the Deployment Manager application) are listed, not the hardware type. The web services are deployed when the corresponding management applications (EM or NRSM) are deployed on a server. The web services can be deployed to any server type on which the corresponding management application can be deployed.

All services are deployed using industry-standard features and are compliant with the following standards:

- Web Services Interoperability (WS-I) Basic Profile 1.1
- WSDL 1.1
- Simple Object Access Protocol (SOAP) 1.1 and 1.2

Each service is exposed using document/literal wrapped binding style. As a result, it is possible to write client application that uses these web services in any language, using any toolkit that is compliant to the same standards. However, all examples in this document are written in Java and use the Java API for XML Web Services (JAX-WS) toolkit, available from Sun, in combination with Apache Ant. Procedures to create clients using other toolkits can vary drastically.

For more information about Web services, see *Web Services API Administration* (NN43001-640).

OAM Transaction Activity and Security Event Logging

Overview

The primary purpose of the Operation, Administration, and Maintenance (OAM) Transaction Activity and Security Event Logging feature is to securely maintain an audit trail of all system administrator OAM activities and security related events in a centralized location on CS 1000 management framework, with the ability to forward the log files to external Operational Support System (OSS) using SYSLOG.

In order to be effective, security audit logs must contain sufficient information for after-the-fact investigation or analysis of security incidents. These audit logs provide a means for accomplishing several security-related objectives including individual accountability, reconstruction of past events, intrusion detection and problem analysis.

The centralized UCM primary security server uses the log viewer tool to view Security and OAM related audit logs. When logged on as a security administrator, the following functions can be performed:

- Filter the log based on the query string and event types.
- View the log for a specific date.
- Configure the remote SYSLOG server for forwarding audit logs in real time to the third party Operational Support System (OSS)
- Export the log as a comma-separated value (csv) file.

This feature has dependencies on all the other applications running in the UCM in the form of adding the OAM audit log statements. The applications include the following:

- Unified Communication Management
- Element Manager (including Phone Provisioning)
- Network Routing Service Manager
- Subscriber Manager

- Web Services
- Base Manager
- LTPS
- SIP Line Gateway
- SIP Signaling Gateway
- NRS Routing Bundle (NCS, H323 GK, SIP Redirect Server)
- Co-res Signaling Server
- Linux Base Log

Log configuration

The following table shows the logs files stored in the /var/log/nortel/OAM folder of the UCM primary security server.

Table 33
UCM primary security server log files

Log file type	Description
OAM logs are stored in two files based on the type of logging event:	
Audit logs: oam.log	Storage location of all OAM administration events that occur from the CS 1000 management applications running on a Linux platform: • Operational events—captures the query for status and enabling or disabling resources. • Configuration events—captures all the feature or functional provisioning and modifications. • Maintenance events—captures all the upgrades, backups, restores and patching.
Security logs: security.log	Storage location of all security related events: • Security policy changes • Logon success and failures • Certificate changes • User account creation and illegal (failed) login events • Any OAM security event where network administrator privilege (or flag) is enabled or required

Log file type	Description
Application logs are generated using the Syslog framework at a Linux operating system level. View Application logs stored on a local system by using the Log Viewer tool from the base manager.	
Application logs	These applications include the following: • LTPS • SIP Line Gateway • SIP Signaling Gateway • NRS Routing bundle (NCS, H323, and SIP Redirect Server) • Management bundle • Linux Base log • CP PM Co-resident Signaling Server • Any other Nortel specific application log

For more information about OAM Transaction Audit Logs, see *System Management Reference* (NN43001-600)and *Unified Communications Management Common Services Fundamentals* (NN43001-116).

Linux Security Hardening

Overview

Linux security hardening is divided into two categories, basic hardening and enhanced hardening. During the Linux base installation, the generic Linux base components are installed, then the basic and enhanced hardening items are applied. The enhanced hardening items are set to their default values when they are applied during the installation process.

When a Linux base upgrade takes place, the generic Linux base components are installed, then the basic hardening and enhanced hardening items are applied. If backed up data exists for the enhanced hardening items, then the values from the backed up data are used. If there are no backup values for enhanced hardening the default values are used.

Basic Linux security hardening includes all hardening items that do not affect the performance of Nortel applications. Basic hardening items are turned on by default and they are not configurable. Although basic hardening items are turned on by default, there can be instances where you reapply basic hardening values. For example, you can reapply basic hardening after the installation of third-party applications to ensure that all basic hardening items are in secure status. Use the CLI command harden basic reapply to perform this task.

Enhanced hardening items include all hardening items that can affect the performance of Nortel applications, or hardening items that require configuration. Enhanced hardening items that do not affect Nortel applications performance are turned on by default, enhanced hardening items that affect performance are turned off by default. Enhanced hardening items are configurable using Command Line Interface (CLI) commands

A security administrator performs the following security hardening tasks:

> ***Note:*** UCM has various user roles. You must have a user role of security administrator to use hardening commands.

- Apply basic hardening.
- Enable or disable source filtering for SSH connections, and modify the filtering list.

  If you manipulate the SSH filter, ensure the IP and subnet values are correct. Incorrect IP and subnet values causes you to lose connectivity. If connectivity is lost, you must reestablish your connection using the console. If you configure SSH filtration, ensure that the main members of the security domain are in the filtration list.
- Modify the pre-login logon banner.
- Modify the variables related to password lifetime.
- Configure the core dumps creation process; core dumps are available by default.
- Enable or disable the Linux Audit daemon.
- Enable or disable Trivial File Transfer Protocol (TFTP) service.
- Enable or disable File Transfer Protocol (FTP) service.
- Enable or disable telnet service.
- Enable or disable network tools (ethereal/wireshark, tcpdump, tracepath, traceroute).
- Retrieve the status of enhanced hardening options.

The following existent operations are extended to support Linux security hardening:

- Application of enhanced hardening options during Linux base installation
- Backup of system wide configured application data
- Restoration of system wide configured application data

All security hardening options are managed using CLI commands. These commands are available to the user immediately after the installation of the Linux base.

For more information about Linux Security Hardening, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Element Manager Phone Provisioning Enhancement

Overview

With CS 1000 Release 6.0, Element Manager is only deployed on Unified Communications Management (UCM), which provides all users access to Phone Provisioning. The following functional enhancements are additions to Phone Provisioning for this release:

- Graphical interface for Phone Key Programming
- Terminal Number (TN) enhancements to provide the ability to span TNs beyond a single card.
- Publish additional phone attributes in Subscriber Manager.
- Support for employee reference in import and export of phones.
- Ability to create a new phone template from an existing phone configuration.
- Export and Import for phone templates.
- Ability to migrate phone data from Element Manager to Subscriber Manager.

For more information about new and updated features in this chapter for Element Manager, see *Element Manager System Reference - Administration* (NN43001-632).

Phone Key Programming

This feature allows you to program phone keys using a graphical image of the phone.

You can program telephone keys from the Phone Details Web page by using the graphical image of the telephone, which appears when you click on the telephone image at the top left of the page.

Terminal Number enhancements

Terminal Number (TN) enhancements provide bulk phone provisioning functionality in Element Manager providing the ability to span TNs beyond a single card.

Publish additional phone attributes in Subscriber Manager

With CS 1000 Release 6.0, the Electronic Switched Network (ESN) number is published in Subscriber Manager. The ESN number is the combination of Home Location Code (HLOC) field and the prime Directory Number (DN) of the phone.

Subscriber Manager displays whether a Prime Directory Number (DN) has Multiple Appearance Redirection Prime (MARP) applied to it or not.

Employee reference field

This feature is required when you upgrade Element Manager to a later release. You can export and the import employee reference fields along with other supported telephone fields. The employee reference field stores the ID of the subscriber who owns the telephone. This field is the link between a telephone in EM Phone Provisioning and a subscriber in Subscriber Manager.

Create a template from existing phone

This feature provides you with the ability to define a new template from an existing phone configuration and quickly create a phone template.

Export and Import of Templates

The objective of this feature is to support export and import of templates in CSV format.

Template data configured at one Element Manager is not available for every Element Manager in the UCM Common Services framework. You must perform a manual export and import procedure to share this data between various Element Managers.

Migrate the Element Manager Phone Provisioning database from Solid to MySQL

With CS 1000 Release 6.0, UCM uses MySQL as the RDBMS. Because of this change, Element Manager Phone Provisioning must migrate data to MySQL

Element Manager Phone Provisioning uses MySQL to store the following data:

- System data: Properties associated with the call server required for phone provisioning and phone validation.
- Phone data: Collection of phone features and keys.
- Phone Template data: Template data for phones.

IP security for Intra System Signaling Security

Overview

IP security for Communication Server 1000 networks is centrally managed from the Unified Communications Management Primary Security Server using the IPsec for Intra System Signaling Security (ISSS) management interface. ISSS employs IPsec to provide security services, including confidentiality, authentication, and anti-replay to application layer protocols.

Communication Server 1000 provides simplified, automated IPsec policy configuration and avoids the complex configuration requirements inherent in many other implementations of IPsec.

ISSS elements are classified into the following two categories:

- UCM Targets—these elements automatically belong to the Unified Communications Management security domain without the need to add them using the Unified Communications Management ISSS management interface. An example of a Unified Communications Management target is a Call Server.
- Manual targets—these elements must be manually configured using the Unified Communications Management ISSS management interface before ISSS can be enabled. An example of a manual target is Call Pilot.

When a new device is installed and configured as part of the UCM security domain it is automatically listed in the UCM targets table. Devices that are not part of the UCM security domain must be added as Manual targets from the ISSS user interface.

ISSS can manage up to a maximum of 1000 combined Unified Communications Management and manual targets.

ISSS/IPsec only secures IP traffic on the ELAN. At Full security level, the AML protocol is protected on the TLAN of Linux-based elements for manual targets. You can protect any feature within the ELAN depending on the Security Level.

- Optimal (OPTI)—ELAN traffic over pbxLink and Xmsg between this host and its known IPsec targets is protected by IPsec. IPsec is required for both pbxLink and Xmsg. For unknown IPsec targets, traffic using the pbxLink and Xmsg protocols is denied.
- Full (FULL)—For known IPsec targets, all ELAN protocols except HTTPS, LDAPS, RADIUS, BOOTP, SSH/SFTP, SSL/TLS, and DTLS, are protected by IPsec. For unknown IPsec targets, all protocols are denied IPsec, except HTTPS, LDAPS, RADIUS, BOOTP, SSH/SFTP, SSL/TLS, and DTLS. If Full security is configured on the CS 1000 system, all external devices such as CallPilot and TM must have IPsec configured in order to communicate with the CS 1000 system. These auxiliary devices can communicate without IPsec if they are configured as ISSS Disabled in UCM.

ISSS/IPsec

ISSS provides an IP Security (IPsec) solution that works with all IP protocols. IPsec works at a low layer of the network (Layer 3 of the OSI 7-Layer Model). This makes it possible for software applications to engage in secure communications without the need to add additional communications security code to each application.

IPsec encrypts the data stream between the two endpoints of a connection. A preshared key (PSK) is used to authenticate the two endpoints, and an encryption key is negotiated by using IKE.

ISSS/IPsec is managed and configured using the Unified Communications Management ISSS interface. The settings are propagated throughout the system by the Primary Security Server to all Unified Communications Management-registered targets.

Communication Server 1000 Release 6.0 includes several system components, including a Call Server, Signaling Servers, Voice Gateway Media Cards, Media Gateway Controllers and Element Managers. In certain configurations, these components can be co-resident on the same element, for example, a Signaling Server co-resident with a Call Server. Communications between these elements is primarily through the ELAN.

Communication between certain auxiliary systems (such as Call Pilot, Symposium Contact Center, or Telephony Manager) is normally through the ELAN interface on the Communication Server 1000 elements; however, in the case of the AML protocol, communication may also occur through the TLAN interface.

ATTENTION
Previous versions of ISSS/IPsec are not supported in Communication Server 1000 Release 6.0. When a Communication Server 1000 system is upgraded to Release 6.0, IPsec must be reconfigured using the ISSS interface on the Unified Communications Management Primary Security Server.

In addition to Communication Server 1000 system components, Communication 1000 supports the UCM Primary and Backup Security Server and Network Routing Service (NRS) elements. Although these elements can be configured to be co-resident with elements of a particular Communication Server 1000 system component, they are not specifically protected by ISSS/IPsec because they communicate using application secured protocols or through their TLAN interfaces.

Unified Communications Management IPsec ISSS management

From the ISSS interface on the Unified Communications Management Primary Security Server, you can administer several aspects of IP security, such as the configuration of a domain-wide security policy, the adding and removing of IPsec targets, and the enabling or disabling of IPsec for network elements.

WARNING
If you configure a network element as Enabled, it must communicate using IPsec as defined by the current level (OPTI or FULL). If you configure the element as Disabled, it continues to communicate with the other elements without IPsec protection. This is not recommended as it may create a security vulnerability.

Elements that are managed by ISSS require a centrally-configured password or preshared key (PSK) to allow for the detection of devices that do not have the correct credentials and to prevent unauthorized access.

The ISSS configuration page contains two main sections, the Configuration and Status area and the Targets table. The Configuration and Status area displays the current security level, synchronization status, and activation status for all targets. You can edit and synchronize these configurations by clicking the Edit, Synchronize, or Activate buttons.

ISSS synchronization and activation

When configuring ISSS parameters, two steps are required to put the new configurations into effect. The synchronization phase, which delivers the new parameters to the UCM members, and the activation phase, which instructs the UCM members to place the new parameters into effect.

There are two activation modes, Graceful and Forced. Graceful activation results in a seamless activation of the new parameters to unaffected targets in most situations; however, changes to the PSK do not take effect until existing sessions expire, which in some cases can take up to three days.

Forced activation causes immediate use of a newly configured PSK; however, messaging traffic is disrupted, causing a service interruption that can last for several minutes. Nortel recommends that you only use Forced activation during scheduled maintenance periods.

For more information about the ISSS feature, see *Security Management Fundamentals* (NN43001-604).

IP Telephony nodes

In Communication Server 1000 Release 6.0, the IP Telephony Nodes page has been updated in Element Manager.

The Node management in CS 1000 Release 6.0 introduces a new work flow on the User Interface (UI) with Add and Modify functions of the Node. The Nodes also provide scalability (by deploying multiple Nodes) and optionally Load sharing (by distributing processing to other Node members. Each Node belongs to a Call Server and has a one-to-many relationship with Call Server. The IP Nodes resides on two LAN subnets: ELAN and TLAN.

The SIP Line application in CS 1000 Release 6.0 cannot co-reside with LTPS or any other virtual trunk applications like SIPGw or H323Gw. The Node management interface does not allow the user to configure SIP Line service any other application services.

The gateway application services operate on a service IP address configured to be on the TLAN of the network and this IP address floats between active and standby servers. The standby server takes over this IP address when the active instance goes down. The active and standby roles are dynamically assigned through a service specific election process that runs on the servers.

Each Node belongs to a Call Server and has a one-to-many relationship with Call Server. The IP Nodes resides on two LAN subnets: ELAN and TLAN.

In CS 1000 Release 6.0, the Deployment Manager, deploys software applications from Unified Communication Management (UCM).

The Node management interface adds servers in to a Node from the list of servers that UCM has learned. Before you add the servers to a Node, it is required that the Deployment Manager deploys the necessary software application to each of the Linux servers.

The IP Telephony Nodes Web page in Element Manager shows the following information:

- Node ID
- Server components or elements
- Configured applications
- IP address information (ELAN and TLAN)
- Overall status of the Node

The IP Telephony Nodes page in Element Manager is used to enable and configure the Signaling Server application services such as the UNIStim Line Terminal Proxy Server (LTPS), the SIP Gateway (SIPGw), the H.323 Gateway (H23Gw), and the new SIP Line application.

> ***Note:*** In CS 1000 Release 6.0, the SIP Line application cannot co-reside with LTPS or virtual trunk applications like SIPGw or H323Gw. In Element Manager, the IP Telephony Node interface does not allow you to configure SIP Line service with any other application services.

For more information about IP Telephony nodes, see *Element Manager System Reference—Administration* (NN43001-632). For more information about configuring the SIP Line Gateway application, see *SIP Line Fundamentals* (NN43001-508).

Vacant Number Routing and MCDN Alternate Routing

Overview

Vacant Number Routing (VNR) is a default route used for routing untranslatable, invalid or unassigned dialed numbers (DN). IP networks usually contain only a subset of the numbers that can be used to reach them. An enterprise network rarely has sufficient data to route calls based on prefixes. Therefore, calls to the IP network need to be able to reroute to alternate routes, while maintaining the ability to receive vacant number treatment when the called destination is an unassigned number. The main purpose of the VNR enhancement feature is to provide appropriate call clearing treatment for 'vacant number' calls over IP domain.

This feature combines the functionality of VNR and Meridian Customer Defined Network Alternate Routing (MALT) for calls routed over IP, to route the call to the correct destination and provide appropriate vacant number treatment.

This feature also allows the user to configure predefined cause values to perform MALT, using Element Manager. The feature interacts with the Element Manager to determine whether to provide MALT for a particular cause. Element Manager provides ten causes to perform MALT for VNR calls. .

The MALT and VNR on IP feature uses Call to Vacant Number (CTVN) to provide treatment for the VNR call, but does not change any of the CTVN functionality.

There are no specific requirements for upgrade. However, when a system is downgraded from CS 1000 Release 6.0, ensure that the lower release systems have the correct patches to build reason header when interacting with higher releases.

There are two sections of this feature:

- Configurable MALT causes for different vendors IP Gateways
- MALT calls routed to the IP domain

For more information about VNR and MALT, see *ISDN Primary Rate Interface Features Fundamentals* (NN43001-569). For more information about configuring MALT VNR, see *Element Manager System Reference—Administration* (NN43001-632).

Telephony Manager 4.0

Overview

Telephony Manager 4.0 for CS 1000 Release 6.0 introduces the following enhancements:

- Web Report Scheduling
- Common Network Directory (CND) synchronization
- Concurrency support

Web Report Scheduling

The Telephony Manager 4.0 Web Report Scheduling feature enables you to schedule Web Station Reports. You can schedule the generation of HyperText Markup Language (HTML) and Comma-separated values (CSV) format reports. The scheduled reports are generated in CSV format , based on the scheduled time. Each report is generated with time stamp information to identify the unique time scheduled for that report. The generated reports are stored in the Telephony Manager home directory. A log file is created for each generated report. The log file contains the information about the CSV Report, such as the site and system, the criteria selected, and the number of records added. You can view the generated report and its corresponding log file in the Telephony Manager Web Station Reports page. A separate log file is generated in the common data path indicating whether or not the scheduled report generation has been successful.

CND synchronization

In Telephony Manager 4.0, Common Name Directory (CND) synchronization uses the entryUUID field (UUID) of CND as a primary key to identify an employee from the CND server. For an upgrade version of TM from previous releases, the UUID is compared first to find the matching entries during CND synchronization. If a matching UUID is not found then the matching "cn" is found. In Telephony Manager 4.0, the UUID of CND is used to identify an employee during CND synchronization.

A log file in comma separated values (CSV) format is generated for assigning Employee to the telephones that are not built during CND synchronization.

For more information about CND synchronization, see *Telephony Manager 4.0 System Administration* (NN43050-601).

Concurrency support

Telephony Manager 4.0 supports the following:

- IPL 6.0 node retrieval and OM Report Generation
- CP PM Co-resident Call Server and Signaling Server is displayed for CS 1000E and CS 1000 M systems for CS 1000 Release 6.0.
- System Data Report and ESN Report
- Minimum support for UEXT SIPL Phone type
- Zone Based Dialing
- Service DN (ARDN/SDN)

For more information about Telephony Manager 4.0, see *Telephony Manager 4.0 System Administration* (NN43050-601).

Instant Messaging and Presence Application

CS 1000 Release 6.0 introduces the Instant Messaging (IM) and Presence Application to the CS 1000. The CS 1000 IM and Presence Application provides IM capability and phone presence information for all CS 1000 users. CS 1000 users can view presence information and exchange Instant Messaging using Nortel's IP Softphone 3456 (IPSP 3456), or Web Client (browser-based IM and Presence client).

A new plug-in is added to an open source IM and Presence platform to enable "CS 1000 Telephony Presence". Its function is to accept SIP-Publish messages from the CS 1000 Presence Publisher component and then broadcast presence updates using the IM and Presence Application to all users.

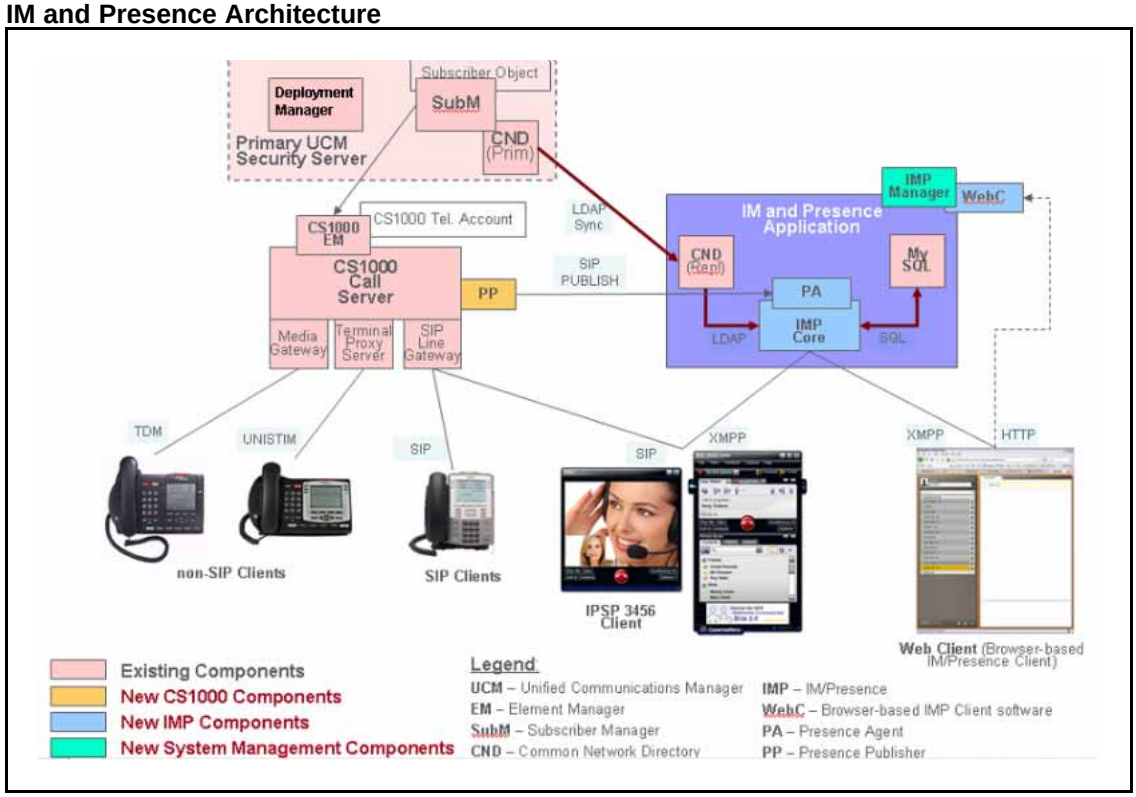
A COTS2 server is added to the network to handle the IM and Presence functionality. This is a single server that does not provide redundancy at this time.

For more information see *Instant Messaging and Presence Application* (NN43001-141).

Deployment model

The following diagram shows the system components and architecture used to support the IM and Presence Application.

Figure 24
IM and Presence Architecture



System Component Description

The following table provides an overview of the a description of the system components used to support the IM and Presence Application.

Table 34
Presence Component Overview

Component	Description
Primary UCM Security Server	Overall system management is coordinated by this management system. On this server the Deployment Manager, Subscriber Manager, and CND reside.
Deployment Manager	The Deployment Manager is used to deploy or upgrade application software.
Subscriber Manager Application	Provisioning of a user's service and accounts is managed by this application.
CS 1000 Element Manager	The Call Server provisioning and other telephony nodal functions are managed by this application.
IM and Presence Application	This new network wide application runs on the new COTS2 (Dell R300 or IBM x3350) and handles instant messaging, contact list and presence updates.

IM and Presence Manager	IM and Presence Manager is used to configure the IM and Presence Application
Nortel CS 1000 Call Server	The CS 1000 Call Server provides service for Nortel telephones.
Nortel CS 1000 Presence Publisher	A new software application running on the Signaling Server works with the CS 1000 Call Server to provide telephony presence updates to the IM Presence server.
Personal Agent	An end-user Web application to manage IM and Presence Application passwords.

Supported IM and Presence clients

The following clients are supported for telephony presence:

- IP Softphone (IPSP) 3456 - has dual accounts (one account for SIP, that can be used as SIPL client on CS 1000, and one account for IM and Presence activity)
- Web Client - browser-based client used for IM and Presence

Supported telephony Publishing Presence clients

Nortel telephones (Analog, Digital, VoIP-Unistim, SIP Line, MobileX, and MC 3100 and IP softphone) controlled by the CS 1000 Call Server - their phone activity triggers presence update.

Software Input/Output prompts, responses and commands

Overview

The tables in this chapter outline the new, changed, or retired information in the Software Input/Output Reference documents (NN43001-611 and NN43001-711) for Communication Server 1000 Release 6.0.

Numerical list of new packages

Number	Mnemonic	Name
417	SIP_Lines	SIP Line Service
420	ZBM_Package	Zone Based Dialing

LD 02: Traffic

The following prompts in LD 2 include a statement to indicate that they are not available to the Call Server in the new Co-resident Call Server and Signaling Server system configuration.

- STAD
- TDTA
- SDTA
- FWTM
- BWTM
- SDST
- TDST

Basic commands

Command	Description
BWTM	Set the date and time for the clock to move backward. This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Time of Day is controlled from the Linux Base layer.
FWTM	Set the date and time for the clock to move forward This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Time of Day is controlled from the Linux Base layer.
SDTA X X Y	Set the time of day adjustment This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Time of Day is controlled from the Linux Base layer.
SDST	Enable or disable the automatic daylight savings time adjustment This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Time of Day is controlled from the Linux Base layer.
STAD	Set the time and date This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Time of Day is controlled from the Linux Base layer.
TDST	Query the daylight savings time adjustment information This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Time of Day is controlled from the Linux Base layer.
TDTA X	Print the current time of day adjustment This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Time of Day is controlled from the Linux Base layer.

LD 10: Analog (500/2500) Telephone Administration

The following prompt is introduced to support Zone Based Dialing feature: NUMZONE.

Prompts and Responses

Prompt	Response	Comment
NUMZONE	0-1023	Numbering zone. Package 420 (Zone Based Dialing) must be equipped.

LD 11: Digital Telephone Administration

The following changes are made in LD 11:

- New prompt to support Zone Based Dialing prompt
  - NUMZONE
- New response is added to UXTY
  - SIPL—to support SIP Line Services
- New prompts to support SIP Line Services are added:
  - MCCL
  - SUPR
  - NDID
- New response for KEY prompt is added
  - xx HOT U (Access Code used to make and receive calls between the SIP client and the universal extension (UXTY = SIPL). The SIP Line Gateway (SLG) application is the only entity that makes use of this key. Package 417 (SIP Lines Services) must be equipped.)

Alphabetical list of prompts

Prompt	Response	Comment	Pack/Rel
KEY			basic-1
	xx aaa yyyy (cccc or D) zz..z		
		Telephone function key assignments. Key assignments determine calling options and features available to a telephone ***Note:*** The **KEY** prompt is presented in a loop until just a **<CR>** is entered at the prompt.	
	xx HOT U <UADN>		
		Access Code used to make and receive calls between the SIP client and the universal extension (UXTY = SIPL). The SIP Line Gateway (SLG) application is the only entity that makes use of this key. Package 417 (SIP Lines Services) must be equipped.	basic-6.00

Prompt	Response	Comment	Pack/Rel
		Where: • xx = any key except 0 (key 0 is reserved for the Primary DN) • <UADN> = a 1-7 digit number representing a User Agent DN If a User Agent prefix (UAPR) is provisioned in the Customer Data Block (CDB), after the primary DN (PDN) is configured on key 0, the system automatically generates a UADN (PDN + UAPR) and displays it on the TTY. You can enter **<CR>** to accept the system-generated UADN, or enter a different UADN. If a UAPR is not provisioned in the CDB, you must enter a UADN. ***Note:*** The UADN must conform to the customer's dialing plan.	
MCCL	x y z u	Number of clients per supported SIP Line type for a Universal Extension designated as a SIP Line. Where: • x = number of clients on Nortel SIP lines (SIPN type) • y = number of clients on 3rd party SIP lines (SIP3 type) • z = number of clients on fixed mobile convergence SIP lines (FMCL type) • u = number of clients on telephony service SIP lines (TLSV type) Package 417 (SIP Lines Services) must be equipped.	basic-6.00
NDID	xxxx	The SIP Lines Gateway (SLG) node identifier. Package 417 (SIP Lines Services) must be equipped.	basic-6.00

Prompt	Response	Comment	Pack/Rel
SUPR	(NO)/YES	SIP Line super user. Package 417 (SIP Lines Services) must be equipped. Where: • NO = SIP line user is not a super user • YES = SIP Line user is a super user	basic-6.00

LD 12: Attendant Consoles

The following change is made in LD 12:

- New prompt to support Zone Based Dialing prompt
  - NUMZONE

Prompts and Responses

Prompt	Response	Comment
NUMZONE	0-1023	Numbering zone Package 420 (Zone Based Dialing) must be equipped.

LD 15: Customer Data Block

The following changes are made in LD 15:

- New prompts are added to support Zone Based Dialing
  - ZBD
  - DIALPLAN
- New prompts are added to support SIP Line Services
  - SLS_DATA
  - SIPL_ON
  - SIPD
  - UAPR
  - NMME
- New datablock is added to support SIP Line Services
  - SLS_DATA

Data block: SLS (SIP Line Services)

Prompt	Response	Comment
REQ:	CHG	Change existing data block
TYPE:	SLS_DATA	SIP Line Services
CUST	xx	Customer number
SIPL_ON	(NO)/YES	Enable SIP Line Services.
SIPD	x...x	SIP Line domain name.
UAPR	x...x	Prefix used to auto-generate the User Agent DN (UADN) for SIPL clients of the specified customer.
NMME	(NO)/YES	Enable Multimedia Service.

Alphabetical list of prompts

Prompt	Response	Comment	Pack/Rel
ZBD	(NO) YES	Enable/disable the Zone Based Dialing (ZBD). Package 420 (Zone Based Dialing) must be equipped.	basic-6.00
DIALPLAN	aaa	Configure the on-net dial plan (public or private) when ZBD feature is enabled (controls DN/CLID processing). Where: • aaa = PUB (public on-net dial plan) E.164 CLID is displayed on a terminating telephone • aaa = PRV (private on-net dial plan) 7-digit DN/CLID is displayed on a terminating telephone Package 420 (Zone Based Dialing) must be equipped.	basic-6.00
NMME	(NO)/YES	Enable/disable Multimedia Services for SIP Lines.	basic-6.00

Prompt	Response	Comment	Pack/Rel
SIPD	x...x	Configure SIP domain name, where x...x = 1-16 characters. Allowable values: • 0-9 • A-Z • a-z • . (period)	basic-6.00
SIPL_ON	(NO)/YES	Enable/disable SIP Line Services. Where: • NO = disable SIP Lines Services • YES = enable SIP Line Services	basic-6.00
	SLS_DATA	SIP Lines services	basic-6.00
UAPR	x...x	SIP Line User Agent prefix.	basic-6.00

LD 16: Route Data Block, Automatic Trunk Maintenance

The following changes are made in LD 16

- New response to the PCID prompt to support SIP Line Services
  - SIPL
- New response to the PII prompt of the Route Data Block to support the Enhance Override CLID Presentation Restriction
  - AUXP

Alphabetical list of prompts

Prompt	Response	Comment	Pack/Rel
AUXP		Auxiliary processor applications.	cppe-6.0

	YES	Send the Calling Line Identification and Calling Party Name (if available) to auxiliary applications like Contact Center Manager (CCM). If the Calling Line Identification (CLID) Presentation Indicator and the Calling Party name Display (CPND) Indicator for an incoming ISDN call are received as "restricted/denied", they are changed to "allowed". If the Privacy Indicator Ignore (PII) prompt is configured to YES, the AUXP prompt is configured to YES automatically by the system, and cannot be changed.	
	(NO)	Do not send the Calling Line Identification and Calling Party Name to auxiliary applications like Contact Center Manager (CCM). If the Calling Line Identification (CLID) Presentation Indicator and the Calling Party Name Display (CPND) Indicator for an incoming ISDN call are received as "restricted/denied", they remain as such	
PCID	xxxx	Protocol ID for the route. Where xxxx: • H323 = non-SIP route • SIP = SIP route • SIPL = SIP Line route	basic-2 basic-4.0 basic-6.00
PII		Privacy Indicator Ignored	cpp-23
	(NO)	Calling Party Privacy Indicator is honored and the existing functionality is maintained.	
	YES	The Calling Party Privacy Indicator is ignored. When PII is set to YES, the CLID Presentation Indicator field in the Calling Party Number IE is changed from restricted to allowed and the CPND Indicator field in the Display IE is changed from denied to allowed.	

[CR]	Leave the feature setting as it was prior to the active service change. ***Note:*** The PII prompt applies to all ISDN interfaces. • ***Euro ISDN (All variants)*** • ***APAC (All variants)*** • ***QSIG (ISO and ETSI)*** • ***MCDN Enterprise networking variants (including the peer-to-peer variant-SL1 and the enterprise UNI variant- SL100)*** • ***H323 and SIP (they use the MCDN peer-to-peer variant-SL1 between the call server and the signaling server)***	cppe-6.0

LD 17: Configuration Record 1

The following prompts in LD 17 include a statement to indicate that they are not available to the Call Server in the new Co-resident CP PM Call Server and Signaling Server system configuration.

- BPS
- BITL
- STOP
- PARY
- FLOW
- FLOW_TYPE

Alphabetical list of prompts

Prompt	Response	Comment	Pack/Rel
BITL	(5), 6, 7, 8	Bit length. Prompted for asynchronous ESDI ports. For Small System, BITL is not prompted for CARD 0 PORT 0 or when TTY_TYPE = PTY. ***Note:*** This prompt is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Serial port configuration is controlled from the Linux Base layer. The prompt displays the current BITL configuration on the system. For example, **BITL 8**.	cls-7

	5 / 6 / 7 / (8)	For release 5.0: Default data bit length for all three remote TTYs on an MGC is 8.	basic-5.0
BPS		Asynchronous baud rates (bits per second): ***Note:*** This prompt is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Serial port configuration is controlled from the Linux Base layer. The prompt displays the current BPS configuration on the system. For example, **BPS 9600**.	cls-7
FLOW	(NO) YES	Flow control capability This prompt appears for Options: 51C, 61C, and 81C. For Small System, FLOW is not prompted when TTY_TYPE = LSL.	csl-7
FLOW_TYPE		Flow control type for Small System. FLOW_TYPE is prompted when TTY_TYPE = LSL. ***Note:*** This prompt is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Serial port configuration is controlled from the Linux Base layer. The prompt displays the current FLOW_TYPE configuration on the system. For example, **FLOW_TYPE NONE**.	basic-22
	NONE	No flow control	
	XON	XON/XOFF flow control	
	MAIL	Mail style flow control protocol	
	HWR	Hardware flow control protocol FLOW_TYPE must be MAIL for the LSL used for Meridian Mail administration / maintenance access. When TTY_TYPE = LSL and CARD = 0, only NONE and XON are valid responses.	

PARY		Parity type. Prompted for asynchronous ESDI ports. For Small System, PARY is not prompted for CARD 0 PORT 0 or when TTY_TYPE = PTY. ***Note:*** This prompt is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Serial port configuration is controlled from the Linux Base layer. The prompt displays the current PARY configuration on the system. For example, **PARY NONE**.	basic-19
	(NONE)	No parity bit	
	ODD	Odd parity bit	
	EVEN	Even parity bit Default parity type for all three remote TTYs on a IPMG is NONE.	
STOP		Number of stop bits ***Note:*** This prompt is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Serial port configuration is controlled from the Linux Base layer. The prompt displays the current STOP configuration on the system. For example, **STOP 1**.	cls-19
	(1)-2	Large Systems. Prompted for asynchronous ESDI ports.	
	(1)-1.5-2	Small Systems. To enter 1.5, use 1X5. STOP is not prompted for CARD 0 PORT 0 or when TTY_TYPE = PTY. Default number of stop bits for all three remote TTYs on an MGC is 1.	

LD 20: Print Routine 1

The following new prompt provides support for Zone Based Dialing:

- NUMZONE

Prompts and Responses

Prompt	Response	Comment
NUMZONE	0-1023	Numbering zone Package 420 (Zone Based Dialing) must be equipped.

LD 21: Print Routine 2

The following new prompts support the Zone Based Dialing

- ZBD
- DIALPLAN

Alphabetical list of prompts

Prompt	Response	Comment	Pack/Rel
ZBD	(NO) YES	Print status of Zone Based Dialing feature. Package 420 (Zone Based Dialing) must be equipped.	basic-6.00
DIALPLAN	aaa	The type of on-net dial plan (public or private) in use for the ZBD feature. Where: • PUB = public on-net dial plan E.164 CLID is displayed on a terminating telephone • PRV = private on-net dial plan 7-digit DN/CLID is displayed on a terminating telephone Package 420 (Zone Based Dialing) must be equipped.	basic-6.00

LD 22: Print Routine 3

The following change is made in LD 22:

- In the report generated by the existing SLT response to the PRT prompt, the ISMs for Analogue Telephones, Class Telephones and Digital Telephones are combined into a new Traditional Telephones ISM counter as follows:

  ```
  TRADITIONAL TELEPHONES 9999 LEFT 9848 USED 151
  ```

LD 81: Features and Station Print

The following changes are made in LD 81

- New prompt is prompt is added to support Zone Based Dialing
  - NZON
- New response is added to FEAT
  - NZON—to support Zone Based Dialing

Prompts and Responses

Prompt	Response	Comment
NZON	0-1023 0-1023	Numbering zone or range of numbering zones Package 420 (Zone Based Dialing) must be equipped.

LD 83: Terminal Number Sort and Print

The following new prompt is added to support the Zone Based Dialing

- NUMZONE

Prompts and Responses

Prompt	Response	Comment
NUMZONE	x...x	Numbering zone or range of numbering zones

LD 117: Ethernet and Alarm Management

The following changes are made in LD 117

- New command to support UNIStim Security with DTLS
  - STIP DTLS
- New commands to support Access Restrictions
  - PORT ACCESS CUSTOM/DEFAULT/OFF
  - PORT ACCESS SHOW CUSTOM/DEFAULT
  - PORT ACCESS STATUS
- New commands to support Secure Transport
  - ENL TRANSFERS INSECURE/SECURE
  - DIS TRANSFERS INSECURE/SECURE
  - STAT TRANSFERS INSECURE/SECURE
  - SECURITY DOMAIN JOIN/LEAVE/STAT
- New commands to support Zone Based Dialing
  - NEW/CHG/OUT/PRT NUMZONE
  - CHG/PRT ZPARM
  - CHG/PRT NZDES
  - NEW/CHG/OUT/PRT ZFDP
  - NEW/CHG/OUT/PRT ZDID
- New command to support SNMP Fault Management
  - SNYC/STAT CNMPCONF

- New command to support SIP Line Services
  - SIP SIPLUA
- New commands to support Unicode Name Directory
  - CHG/PRT NDAPP
  - CHG/PRT LDAPSYNC
- Commands are updated to support SNMP Fault Management
  - SNYC SYS
  - SET/PRT ENABLE_TRAPS
- Commands are retired to support ISSS Synchronization
  - ENL/DIS/CHG/PRT/COMMIT/CONFIRM ISEC
  - NEW/OUT/ENL/DIS/PRT ISECTAR
- A note is added to the following commands to support the Co-resident Call Server and Signaling Server configuration
  - NEW/OUT/PRT/STAT/ENL/DIS/HOST
  - NEW/ENL/DIS/PRT/STAT ROUTE
  - CHG ELNK ACTIVE/INACTIVE
  - PRT ELNK
  - RST ELNK ACTIVE/INACTIVE
  - PRT/CHG/SET MASK
  - CHG/PRT/OUT HSP_MASK
  - SET HSP ID
  - UPDATE DBS
  - PING
  - CHG INP IPADDR/THRESH/SECURE/AUTHMODE/TIMEINT/MODE
  - CHG UTCOFFSET
  - ENL/DIS/SYNC/STAT/PRT NTP
  - STOP NTP BACKGROUND
  - RST/CHG/PRT PTM
  - ENL/DIS/STAT PPP
- A note is added to the following commands to support SNMP Fault Management
  - PRT ADMIN_COM
  - PRT NAV_SITE

— PRT NAV_SYSTEM

— PRT OPEN_ALARM

— PRT SNMP_SYSGRP

— PRT SYSMGMT_COMM

Alphabetical list of Administration commands

Command	Description	Pack/Rel
CHG ADMIN_COMM n aa...a	Change the admin groups community name string, where: • n = a number from 1 to 3 • aa...a = a string with a maximum length of 32 characters, where: — Default(1) = admingroup1 * — Default(2) = admingroup2 * — Default(3) = admingroup3 * * = case-sensitive These communities are used for accessing different SNMP objects on the Call Server, Signaling Servers, Voice Gateway Media Cards and Media Gateway Controllers.	basic-4.0
	In CS 1000 Release 6.0, if administration group community strings are added or modified in LD 117, they are stored in an "OVLY 117 Configuration" area pending activation. When the SYNC SNMPCONF command is executed, the "OVLY 117 Configuration" changes are activated and become part of the "ACTIVE Configuration" on the system.	basic-6.00
CHG ELNK ACTIVE hostname	Set system active Ethernet interface IP address (set active ELAN IP address). ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
CHG ELNK INACTIVE hostname	Set system inactive Ethernet interface IP address (set inactive ELAN IP address) ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	

Command	Description	Pack/Rel
CHG HSP_MASK <subnet mask>	Modify the manually-configured subnet mask, if it exists; otherwise, the subnet mask to the Call Server is added. ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	basic-4.50
CHG LDAPSYNC <ldapsync> [<timeOfDay> [<ldapserver> <userid> <password> [<security> [<secure port> [insecure port>]]]]]	Enable/disable the scheduled synchronization of the Unicode Name Directory data with the CND LDAP server data, or change the parameters for the scheduled synchronization task. Where: • <ldapsync> = disable/enable scheduled synchronization of the Unicode Name Directory data with the CND LDAP server data — 0 = disable — 1 = enable • <timeOfDay> = the time of day for scheduled LDAP synchronization Format = hh:mm • <ldapserver> = IP address or FQDN of the CND LDAP server • <userid> = username required for access to the CND LDAP server • <password> = password required for access to the CND LDAP server • <security> = enable/disable secure SSL connection to the CND LDAP server • <secure port> = port used for secure SSL connection to CND LDAP server. Default port = 636. • <insecure port> = port used for insecure connection to CND LDAP server. Default port = 389. ***Note:*** <userid> and <password> must always be specified as a pair.	basic-6.00
CHG MASK nnn.nnn.nnn.nnn		

Command	Description	Pack/Rel
	Change subnet mask. ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
CHG NAV_SITE aa... a		basic-4.0
	Change the navigation site name (MyCity, for example), where: • aa...a = a string with maximum length of 32 characters • default = Navigation Site Name ***Note:*** Use a single X to clear the field.	
	In CS 1000 Release 6.0, if the navigation site name is modified in LD 117, it is stored in an "OVLY 117 Configuration" area pending activation. When the SYNC SNMPCONF command is executed, the "OVLY 117 Configuration" changes are activated and become part of the "ACTIVE Configuration" on the system.	basic-6.00
CHG NAV_SYSTEM aa... a		basic-4.0
	Change the navigation system name (Station Switch, for example) where: • aa...a = a string with a maximum length of 32 characters • default = Navigation System Name ***Note:*** Use a single X to clear the field.	
	In CS 1000 Release 6.0, if the navigation system name is modified in LD 117, it is stored in an "OVLY 117 Configuration" area pending activation. When the SYNC SNMPCONF command is executed, the "OVLY 117 Configuration" changes are activated and become part of the "ACTIVE Configuration" on the system.	basic-6.00
CHG NTP AUTHMODE <Secure | Insecure> <Primary | Secondary | All>		basic-5.0
	Configure the security mode for the Primary, Secondary, or both, NTP servers. ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	
CHG NTP IPADDR <primary_ip_addr> <secondary_ip_addr>		basic-5.0

Command	Description	Pack/Rel
	Configure the IP addresses for the Primary and Secondary NTP Servers. ***Note 1:*** When you are configuring the IP address for the secondary NTP server, enter the IP address of the primary NTP server, followed by the IP address of the secondary NTP server. ***Note 2:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	
CHG NTP MODE CS	Configure Router as the mode of communication between the NTP server and the CS. ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	basic-5.0
CHG NTP MODE SS	Configure Signaling Server as the mode of communication between the NTP server and the CS. ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	basic-5.0
CHG NTP SECURE <primary_ip_add> <secondary_ip_addr> <key_id>	Configure the parameters used by the Primary and/or Secondary NTP servers in secure mode of operation. Where: • <primary_ip_add> = IP address of primary NTP server • <secondary_ip_addr> = IP address of secondary NTP server • <key_id> = private key with values = 1 - 4294967295. The system prompts for the private key if not entered. ***Note:*** For security reasons, the private key does not show in the command line as you enter it. ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	basic-5.0

Command	Description	Pack/Rel
CHG NTP THRESH <Minimum> <Warning> <Maximum>	Configure the 3 NTP threshold levels. Where: • <Minimum> = (0)-5 seconds • <Warning> = (6)-15 seconds • <Maximum> = (16)>15 seconds ***Note 1:*** Enter values for all three threshold levels when you use this command. ***Note 2:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	basic-5.0
CHG NTP TIMEINT <time interval in hours> <offset in minutes>	Configure both the time interval for background synchronization and the offset from other background routines. Where: • <time interval in hours> = 1, 2, 6, 12, (24), 30 • <offset in minutes> = 15, (30), 45 ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	basic-5.0
CHG NUMZONE <numbering zone> <ZBD numbering zone parameters>	Change the parameters of a ZBD numbering zone. Package 420 (Zone Based Dialing) must be equipped. Where: • <numbering zone> = new numbering zone number A number from 1-1023. • <ZBD zone parameters>: — <PREF> = site prefix A number from 0-9999. — <CC> = country code A number from 0-9999. — <NPA> = area code (used for dialing through ZFDP)	basic-6.00

Command	Description	Pack/Rel
	A number from 0-9999. — <AC1> = trunk access code 1 A number from 0-99. — <AC2> = trunk access code 2 A number from 0-99. — <NATC> = national dial code A number from 0-9999. — <INTC> = international dial code A number from 0-9999. — <DAC> = flag to delete NPA for a local subscriber call A number from (0)-1. — <TTBL> = tone table A number from (0)-32.	
CHG NZDES <numbering zone> <"description">	Change the description of a ZBD numbering zone. Package 420 (Zone Based Dialing) must be equipped. Where: • <numbering zone> = 1-1023 • <"description"> = 1-128 characters Description of numbering zone.	basic-6.00
CHG UTCOFFSET <Time Offset>>	Configure the time offset (from UTC) for the local time zone. Where <Time Offset> = +/-hh:mm (+00:00). ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	basic-5.0
CHG ZDID <numbering zone> <matching string> <replacement string> [<"description">]		basic-6.00

Command	Description	Pack/Rel
	Change a ZBD numbering zone-based call translation table entry. Package 420 (Zone Based Dialing) must be equipped. Where: • <numbering zone> = 1-1023 • <matching string> = 1-16 digit “best match” numeric string Unique inside a numbering zone. • [<replacement string>] = string that replaces the matching string If <type> = SPN, CDP or ESDN, 1-16 numeric digits; if <type> = INTL, LOC, REG1, NPA, REG2 or NXX, 1-16 alphabetic characters. If <replacement string> is not specified, the matching string is deleted and not replaced. • <description> = 1-32 character textual description for the numbering zone-based call translation (ZDID) table entry If not specified, the ZDID table entry remains unchanged.	
CHG ZFDP <numbering zone> <matching string> <type> [<replacement string>] [LEN <max length>] ["<description>"]		basic-6.00
	Change a ZBD numbering zone-based flexible dialing plan table entry. Package 420 (Zone Based Dialing) must be equipped. Where: • <numbering zone> = 1-1023 • <matching string> = 1-16 digit “best match” numeric string Unique inside a numbering zone. • <type> = values specified in the LD 15 AC1 and AC2 prompts After stripping the matching string, save the CLID type and take the following actions depending on <type> specified: — If <type> = INTL (International E.164 number), insert AC1/AC2+replacement string. — If <type> = LOC (UDP Location Code), insert AC1/AC2+ replacement string. — If <type> = REG1 (Regional Level 1), insert AC1/AC2+ZC C+replacement string. — If <type> = NPA (North American NPA), insert AC1/AC2+1, then replacement string. — If <type> = REG2 (Regional Level 2), insert AC1/AC2+ZCC +ZNPA+replacement string	

Command	Description	Pack/Rel

— If <type> = NXX (North American NXX), insert AC1/AC2+ZCC+ZNPA+replacement string

— If <type> = SPN (Special Number), insert AC1/AC2+replac ement string

— If <type> = CDP (Coordinated Dial Plan), insert replacement string

— If <type> = ESDN (Emergency Service DN), insert replacement string

- [<replacement string>] = string that replaces the matching string
  If <type> = SPN, CDP or ESDN, 1-16 numeric digits; if <type> = INTL, LOC, REG1, NPA, REG2 or NXX, 1-16 alphabetic characters.
  If <replacement string> is not specified, the matching string is deleted and not replaced.
- [LEN <max length>] = maximum number of dialed digits expected to match
  If not specified, default is to match digits for all multiple matches.
- [<"description">] = textual description of the numbering zone-based flexible dialing plan (ZFDP) table entry
  If not specified, the ZFDP table entry has no textual description.

CHG ZPARM <numbering zone> <parameter name> <value> basic-6.00

Change the value of a ZBD numbering zone parameter.
Package 420 (Zone Based Dialing) must be equipped.

Where:

- <numbering zone> = 1-1023
- <parameter name> = name of numbering zone parameter
  Where:
  — PREF = site prefix
  — CC = country code
  — NPA = area code (used for dialing through ZFDP)
  — AC1 = trunk access code 1
  — AC2 = trunk access code 2
  — NATC = national dial code
  — INTC = international dial code
  — DAC = flag to delete NPA for a local subscriber call
  — TTBL = tone table
- <value> = new value for specified parameter

Command	Description	Pack/Rel
	— If <parameter name> = PREF, <value> = 0-9999. — If <parameter name> = CC, <value> = 0-9999. — If <parameter name> = NPA, <value> = 0-9999. — If <parameter name> = AC1, <value> = 0-99. — If <parameter name> = AC2, <value> = 0-99. — If <parameter name> = NATC, <value> = 0-9999. — If <parameter name> = INTC, <value> = 0-9999. — If <parameter name> = INTC, <value> = 0-9999. — If <parameter name> = DAC, <value> = (0)-1. — If <parameter name> = TTBL, <value> = (0)-32.	
DIS TRANSFERS INSECURE	Disable FTP (insecure File Transfer Protocol) on the system. Call server sends a related message through pbxLink to all connected devices and IPMG devices. ***Note 1:*** SFTP must be enabled. FTP and SFTP cannot both be disabled at the same time. ***Note 2:*** Command cannot be issued within 5 minutes of a previously issued ENL TRANSFERs or DIS TRANSFERS command.	basic-6.00
DIS TRANSFERS SECURE	Disable SFTP (secure File Transfer Protocol). Call server sends a related message through pbxLink to all connected devices and IPMG devices. ***Note 1:*** FTP must be enabled. FTP and SFTP cannot both be disabled at the same time. ***Note 2:*** Command cannot be issued within 5 minutes of a previously issued ENL TRANSFERs or DIS TRANSFERS command.	basic-6.00
ENL / DIS NTP	Enable / Disable NTP. ***Note:*** These commands are blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	basic-5.0
ENL TRANSFERS INSECURE		basic-6.00

Command	Description	Pack/Rel
	Enable FTP (insecure File Transfer Protocol) on the system. Call server sends message through pbxLink to all connected devices and IPMG devices. ***Note:*** Command cannot be issued within 5 minutes of a previously issued ENL TRANSFERs or DIS TRANSFERS command.	
ENL TRANSFERS SECURE		basic-6.00
	Enable SFTP (secure File Transfer Protocol) on the system. Call server sends message through pbxLink to all connected devices and IPMG devices. ***Note:*** Command cannot be issued within 5 minutes of a previously issued ENL TRANSFERs or DIS TRANSFERS command.	
NEW HOST DEV_SIDE0_HSP <ip address>		basic-4.50
	Configure the HSP ip address ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
NEW HOST DEV_SIDE1_HSP <ip address>		basic-4.50
	Configure the HSP ip address ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
NEW HOST <hostname> <IPaddress>		
	Configure a new host entry, where; • host name must exist in the host table • default setting for the Primary IP address is: 137.135.128.253 • default setting for Primary Host Name is: PRIMARY_ENET	

Command	Description	Pack/Rel
	• default setting for the Secondary IP address is: 137.135.128.254 • default setting for the Secondary Host Name is: SECONDARY_ENET. ***Note 1:*** **Host Name Syntax:** A host name can be up to 16 characters in length. The first character of a host name must be a letter of the alphabet. A character can be a letter, number, or underscore(_). A period is used as a delimiter between domain names. Spaces and tabs are not permitted. No distinction is made between upper and lower case. ***Note 2:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
NEW NUMZONE <numbering zone> [ZBD numbering zone parameters]	Configure a new numbering zone with specified (optional) ZBD zone parameters. Package 420 (Zone Based Dialing) must be equipped. Where: • <numbering zone> = new numbering zone number A number from 1-1023. • <ZBD zone parameters>: — <PREF> = site prefix A number from 0-9999. — <CC> = country code A number from 0-9999. — <NPA> = area code (used for dialing through ZFDP) A number from 0-9999. — <AC1> = trunk access code 1 A number from 0-99. — <AC2> = trunk access code 2 A number from 0-99. — <NATC> = national dial code A number from 0-9999. — <INTC> = international dial code A number from 0-9999. — <DAC> = flag to delete NPA for a local subscriber call A number from (0)-1. — <TTBL> = tone table	basic-6.00

Command	Description	Pack/Rel
	A number from (0)-32. ***Note:*** Default values (hard-coded) are used for the ZBD numbering zone parameters, if they are not specified.	
NEW ROUTE <network IP address> <gateway IP address>	Configure a new routing entry <IP address>= valid IP address ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
NEW ZDID <numbering zone> <matching string> <replacement string> [<"description">]	Configure a ZBD numbering zone-based call translation table entry. Package 420 (Zone Based Dialing) must be equipped. Where: • <numbering zone> = 1-1023 • <matching string> = 1-16 digit “best match” numeric string Unique inside a numbering zone. • [<replacement string>] = string that replaces the matching string If <type> = SPN, CDP or ESDN, 1-16 numeric digits; if <type> = INTL, LOC, REG1, NPA, REG2 or NXX, 1-16 alphabetic characters. If <replacement string> is not specified, the matching string is deleted and not replaced. • <description> = 1-32 character textual description for the numbering zone-based call translation (ZDID) table entry If not specified, the ZDID table entry has no textual description.	basic-6.00
NEW ZFDP <numbering zone> <matching string> <type> [<replacement string>] [LEN <max length>] ["<description>"]		basic-6.00

Command	Description	Pack/Rel
	Create a ZBD numbering zone-based flexible dialing plan table entry. Package 420 (Zone Based Dialing) must be equipped. Where: • <numbering zone> = 1-1023 • <matching string> = “best match” string of 1-16 digits Unique inside a numbering zone. • <type> = values specified in the LD 15 AC1 and AC2 prompts After stripping the matching string, save the CLID type and take the following actions depending on <type> specified: — If <type> = INTL (International E.164 number), insert AC1/AC2+replacement string. — If <type> = LOC (UDP Location Code), insert AC1/AC2+ replacement string. — If <type> = REG1 (Regional Level 1), insert AC1/AC2+ZC C+replacement string. — If <type> = NPA (North American NPA), insert AC1/AC2+1, then replacement string. — If <type> = REG2 (Regional Level 2), insert AC1/AC2+ZCC +ZNPA+replacement string — If <type> = NXX (North American NXX), insert AC1/AC2+ZCC+ZNPA+replacement string — If <type> = SPN (Special Number), insert AC1/AC2+replac ement string — If <type> = CDP (Coordinated Dial Plan), insert replacement string — If <type> = ESDN (Emergency Service DN), insert replacement string • [<replacement string>] = string that replaces the matching string If <type> = SPN, CDP or ESDN, 1-16 numeric digits; if <type> = INTL, LOC, REG1, NPA, REG2 or NXX, 1-16 alphabetic characters. If <replacement string> is not specified, the matching string is deleted and not replaced. • [LEN <max length>] = maximum number of dialed digits expected to match If not specified, default is to match digits for all multiple matches. • [<"description">] = textual description of the numbering zone-based flexible dialing plan (ZFDP) table entry If not specified, the ZFDP table entry has no textual description.	

Command	Description	Pack/Rel
OUT HOST nnn	Delete configured host entry (delete host from network host table). ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
OUT HSP_MASK	Removes the configured HSP subnet mask from the Call Server and replaces it with the default HSP subnet mask ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	basic-4.50
OUT NUMZONE <numbering zone)	Remove a ZBD numbering zone, where <numbering zone) = a number from 1-1023. Package 420 (Zone Based Dialing) must be equipped.	basic-6.00
OUT ZDID <numbering zone> <matching string>	Delete a ZBD numbering zone-based call translation. Package 420 (Zone Based Dialing) must be equipped. Where: • <numbering zone> = 1-1023 • <matching string> = “best match” string of 1-16 digits Unique inside a numbering zone.	basic-6.00
OUT ZFDP <numbering zone> <matching string>	Delete a ZBD numbering zone-based flexible dialing plan. Package 420 (Zone Based Dialing) must be equipped. Where: • <numbering zone> = 1-1023 • <matching string> = “best match” string of 1-16 digits Unique inside a numbering zone.	basic-6.00

Command	Description	Pack/Rel
PORT ACCESS CUSTOM	Configures a custom Access Restrictions ruleset defining port access rules for the system. Issuing this command results in the following actions by the system: 1. Check to ensure a custom Access Restrictions rules file exists in the appropriate directory structure. If not, an error is displayed and the command aborted. 2. Displays a warning that enabling a custom Access Restrictions rules file could possibly have detrimental effects on the system, and prompts the user to confirm the action (Y or N). 3. Check to ensure that the custom Access Restrictions rules file loads. If not, an error is displayed and the command aborted. 4. If the VxWorks firewall state indicates that the Access Restrictions feature is already enabled, disable the existing Access Restrictions rules, including mandatory Access Restrictions rules. 5. If the VxWorks firewall state indicates that the Access Restrictions feature is not already enabled, enable it and set the default Access Restrictions rule to ACCEPT ALL. Any old Access Restrictions statistics are cleared. 6. Load the mandatory Access Restrictions rules file. 7. Load the custom Access Restrictions rules file. If a problem is encountered when loading the custom Access Restrictions rules file, the system displays an error, aborts the command, and returns the Access Restrictions feature to its previous state. 8. Change the VxWorks firewall state on the Call Server to Custom. An information message is logged on the Call Server indicating that the Access Restrictions feature is operating with a custom Access Restrictions rules file. 9. Send a VxWorks firewall state change message to all endpoints with the mandatory and custom Access Restrictions rules files version numbers.	basic-6.00

Command	Description	Pack/Rel
	An information message is logged on each endpoint indicating that the Access Restrictions feature is operating with a custom Access Restrictions rules file. ***Note:*** When a PORT ACCESS command (CUSTOM, DEFAULT, OFF) is entered, all other PORT ACCESS commands are suspended for a pre-determined or incremental amount of time depending on the number of endpoints, to allow sufficient time to propagate the state change to all endpoints.	
PORT ACCESS DEFAULT	Configures the default Access Restrictions ruleset defining port access rules for the system. Issuing this command results in the following actions by the system: 1. Check to ensure a default Access Restrictions rules file exists in the appropriate directory structure. Errors are not expected to occur when processing the default Access Restrictions rules file. 2. If the VxWorks firewall state indicates that the Access Restrictions feature is already enabled, delete the existing Access Restrictions rules, including mandatory Access Restrictions rules. 3. If the VxWorks firewall state indicates that the Access Restrictions feature is not already enabled, enables it and sets the default Access Restrictions rule to ACCEPT ALL. Any old Access Restrictions statistics are cleared. 4. Load the mandatory Access Restrictions rules file. 5. Load the default Access Restrictions rules file. 6. Change the VxWorks firewall state on the Call Server to Default. An information message is logged on the Call Server indicating that the Access Restrictions feature is operating with a default Access Restrictions rules file. 7. Send a VxWorks firewall state change message to all endpoints with the default and custom Access Restrictions rules files versions as zeros. An information message is logged on each endpoint indicating that the Access Restrictions feature is operating with a default Access Restrictions rules file. ***Note:*** When a PORT ACCESS command (CUSTOM, DEFAULT, OFF) is entered, all other PORT ACCESS commands are suspended for a pre-determined or incremental amount of time depending on the number of endpoints, to allow sufficient time to propagate the state change to all endpoints.	basic-6.00

Command	Description	Pack/Rel
PORT ACCESS OFF	Disables all Access Restrictions rules in the system. Issuing this command results in the following actions by the system: 1. Disable all enabled Access Restrictions rules. 2. Deactivate the VxWorks firewall facility. 3. Change the VxWorks firewall state on the Call Server to OFF. An information message is logged on the Call Server indicating that the Access Restrictions feature is not operational. 4. Send a VxWorks firewall state change message to all endpoints with the default and custom Access Restrictions rules files versions as zeros. An information message is logged on each endpoint indicating that the Access Restrictions feature is not operational. ***Note:*** When a PORT ACCESS command (CUSTOM, DEFAULT, OFF) is entered, all other PORT ACCESS commands are suspended for a pre-determined or incremental amount of time depending on the number of endpoints, to allow sufficient time to propagate the state change to all endpoints.	basic-6.00
PORT ACCESS SHOW CUSTOM	Display the Access Restrictions rules in the CUSTOM Access Restrictions rules file in tabular format.	basic-6.00
PORT ACCESS SHOW DEFAULT	Display the Access Restrictions rules in the DEFAULT Access Restrictions rules file in tabular format.	basic-6.00
PORT ACCESS STATUS [ALL]	Display the global state of the Access Restrictions feature. If the [ALL] parameter is specified, the system polls all endpoints to determine their local Access Restrictions state: • If there are any cards that don't have matching file signatures, or that can't be contacted, they are displayed. A list of the possible failures is as follows: — CS local state incorrect: <CS state> — <endpoint IP> <endpoint type> state not received — <endpoint IP> <endpoint type> has incorrect state of <bad state>	basic-6.00

Command	Description	Pack/Rel
	— <endpoint IP> <endpoint type> has incorrect default and custom file — <endpoint IP> <endpoint type> has incorrect default file — <endpoint IP> <endpoint type> has incorrect custom file • If all cards have matching file signatures, a message is displayed indicating that all endpoints match.	
PRT ADMIN_COMM		basic-4.0
	Print the administration group read-only community name strings.	
	If administration group community strings have been added or modified in LD 117 since the last execution of the SYNC SNMPCONF command, the PRT ADMIN_COMM command prints the added and modified strings in an "OVLY 117 Configuration" area and the existing community strings in an "ACTIVE Configuration" area. When the SYNC SNMPCONF command is executed, the "OVLY 117 Configuration" changes are activated and become part of the "ACTIVE Configuration" on the system.	basic-6.00
PRT ENABLE_TRAPS		basic-6.00
	Display the enabled/disabled parameter for all SNMP traps.	
PRT ELNK	Display active and inactive Ethernet interface IP addresses (display active and inactive ELAN IP addresses). ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
PRT HOST	Display network host table entries (enabled and disabled hosts). ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
PRT HSP_MASK		

Command	Description	Pack/Rel
	Retrieves the manually configured HSP mask from the Call Server if it exists and outputs it to the screen, otherwise it prints the default HSP subnet mask (255.255.255.0) ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
PRT LDAPSYNC		basic-6.00
	Display the parameters of the Unicode Name Directory <-> CND LDAP scheduled data synchronization task.	
PRT MASK		basic-5.0
	Display subnet mask stored in database. ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
PRT NAV_SITE		basic-4.0
	Print the navigation site name	
	If the navigation site name has been modified in LD 117 since the last execution of the SYNC SNMPCONF command (not activated), the PRT NAV_SITE command prints the modified navigation site name in an "OVLY 117 Configuration" area and the existing navigation site name in an "ACTIVE Configuration" area. When the SYNC SNMPCONF command is executed, the "OVLY 117 Configuration" changes are activated and become part of the "ACTIVE Configuration" on the system.	basic-6.00
PRT NAV_SYSTEM		basic-4.0
	Print the navigation system name	
	If the navigation system name has been modified in LD 117 since the last execution of the SYNC SNMPCONF command (not activated), the PRT NAV_SYSTEM command prints the modified navigation system name in an "OVLY 117 Configuration" area and the existing navigation system name in an "ACTIVE Configuration" area. When the SYNC SNMPCONF command is executed, the "OVLY 117 Configuration" change is activated and becomes part of the "ACTIVE Configuration" on the system.	basic-6.00

Command	Description	Pack/Rel
PRT NUMZONE <numbering zone)	Print a table of information for a ZBD numbering zone, where <numbering zone> = 1-1023. Package 420 (Zone Based Dialing) must be equipped. Output: • <PREF> = site prefix A number from 0-9999. • <CC> = country code A number from 0-9999. • <NPA> = area code (used for dialing through ZFDP) A number from 0-9999. • <AC1> = trunk access code 1 A number from 0-99. • <AC2> = trunk access code 2 A number from 0-99. • <NATC> = national dial code A number from 0-9999. • <INTC> = international dial code A number from 0-9999. • <DAC> = flag to delete NPA for a local subscriber call A number from (0)-1. • <TTBL> = tone table A number from (0)-32. ***Note:*** If <numbering zone> is not specified, all numbering zones are printed.	basic-6.00
PRT NZDES [<numbering zone>]	Print the description for a specified ZBD numbering zone. Package 420 (Zone Based Dialing) must be equipped. ***Note:*** Descriptions for all numbering zones are printed if <numbering zone> is not specified.	basic-6.00
PRT OPEN_ALARM	Display SNMP open alarm trap settings.	

Command	Description	Pack/Rel
	If SNMP open alarm trap settings have been added or modified in LD 117 since the last execution of the SYNC SNMPCONF command, the PRT OPEN_ALARM command displays the new (not yet activated) SNMP open alarm trap settings in an "OVLY 117 Configuration" area, and the existing (currently active) SNMP open alarm trap settings in an "ACTIVE Configuration" area. When the SYNC SNMPCONF command is executed, the "OVLY 117 Configuration" open alarm changes are activated and become part of the "ACTIVE Configuration" on the system.	basic-6.00
PRT ROUTE	Display routing table entries stored in the database. ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
PRT SYSMGMT_COMM		basic-4.0
	Print the system management Read/Write/Trap community name strings	
	If system management read/write/trap community strings have been added or modified in LD 117 since the last execution of the SYNC SNMPCONF command (not activated), the PRT SYSMGMT_COMM command prints the added and modified system management read/write/trap community strings in an "OVLY 117 Configuration" area and the existing system management read/write/trap community strings in an "ACTIVE Configuration" area. When the SYNC SNMPCONF command is executed, the "OVLY 117 Configuration" changes are activated and become part of the "ACTIVE Configuration" on the system.	basic-6.00
PRT ZDES [<DESMatchString>]		
	Print a table of the zone description entries.	
PRT ZDID [<numbering zone>] [<matching string>]		basic-6.00

Command	Description	Pack/Rel
	Print a table of ZBD numbering zone-based call translations. Package 420 (Zone Based Dialing) must be equipped. Where: • <numbering zone> = 1-1023 • <matching string> = “best match” string of 1-16 digits Unique inside a numbering zone. Only numbering zone-based call translations with the specified 1-16 digit numeric matching string are printed If not specified, all numbering zone-based call translations are printed.	
PRT ZFDP [<numbering zone>] [<matching string>]	Print a table of ZBD numbering zone-based flexible dialing plans. Feature 420 (Zone Based Dialing) must be equipped. Where: • <numbering zone> = 1-1023 If not specified, all numbering zone-based flexible dialing plans are printed. • <matching string> = 1-16 digit numeric string Unique inside a numbering zone. Only numbering zone-based flexible dialing plans with the specified 1-16 digit matching string are printed. If not specified, all numbering zone-based flexible dialing plans are printed.	basic-6.00
PRT ZPARM [<numbering zone>]	Print the parameters of a ZBD numbering zone, where <numbering zone> = 1-1023. Package 420 (Zone Based Dialing) must be equipped. ***Note:*** When no numbering zone is specified, parameters for all ZBD numbering zones are printed.	basic-6.00
RST ELNK ACTIVE		

Command	Description	Pack/Rel
	Reset Meridian 1 active Ethernet interface IP address to default value (reset active ELAN IP address to default). ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
RST ELNK INACTIVE		
	Reset Meridian 1 inactive Ethernet interface IP address to default value (reset inactive ELAN IP address to default). ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
RST PPP LOCAL		
	Reset local Point-to-point Protocol interface IP address to default value	
RST PPP REMOTE		
	Reset remote Point-to-point Protocol interface IP address to default value	
SECURITY DOMAIN JOIN		basic-6.00
	Establish mutual trust with the UCM Primary Security Server.	
SECURITY DOMAIN LEAVE		basic-6.00
	Remove the UCM Primary Security Server mutual trust information from the device.	
SECURITY DOMAIN MODE [MANUAL | USER | AUTO]		basic-6.00

Command	Description	Pack/Rel
	Configure the UCM security domain management mode on the Call Server. Where: • MANUAL = all devices must join the UCM security domain using local CLI commands • USER = the user is prompted with a list of all currently active devices and is asked to confirm their addition to the UCM security domain • AUTO = The credentials for the user accounts assigned the necessary role are cached on the Call Server so that they can be sent at a later time to any device that the Call Server requires to join the UCM security domain	
SECURITY DOMAIN STAT		basic-6.00
	Display the IP address and fingerprint of the UCM Primary Security Server.	
STAT NTP		basic-5.0
	Check status of NTP. Status information displays in four categories—current NTP configuration, last NTP configuration, last synchronization error, and counters—and includes the following fields: • NTP enabled or disabled (if disabled, the report includes no further information) • IP addresses of the primary and secondary NTP servers • local time zone offset from UTC • time difference (delta) between system time and NTP server • current threshold level: Minimal, Warning, Maximum • secure mode of operation set to secure or insecure • packets sent • packets received ***Note 1:*** NTP status information also appears on the Date and Time page in Element Manager, under the Network Time Protocol field. ***Note 2:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	

Command	Description	Pack/Rel
STAT SNMPCONF	Display the status of the SYNC SNMPCONF command. The result indicates whether the SNMP parameters configured through LD 117 ("OVLY 117 Configuration") are synchronized with the CS. There are two possible results: • SNMP Configuration is in progress When SNMP parameters are added or modified in overlay 117 and the SYNC SNMPCONF command is not executed, the new SNMP parameters are pending activation. • SNMP Configuration is completed When SNMP parameters are added or modified in overlay 117 and the SYNC SNMPCONF command is executed (new SNMP parameters are activated).	basic-6.00
SYNC SNMPCONF	Update the "ACTIVE Configuration" (current) SNMP parameters on the CS with "OVLY 117 Configuration" SNMP parameters, and propagate the updated SNMP parameters to all system elements that have an established pbxlink with the CS.	basic-6.00
SYNC SYS	Propagates Dbconfig and QOS parameters on the CS to all system elements that have an established pbxlink with the CS.	
STAT TRANSFERS SECURE	Display the status of the secure File Transfer Protocol (SFTP).	basic-6.00
STIP DTLS <Node> <Connection_Type> <DTLS_Capability>	Display IP Phones based on signaling encryption related values, namely the type of connection currently in use by each IP Phone and their capability to make DTLS connections. Where: • <Node> = the node ID of the node the subject IP phones belong to, or “ALL” to omit node-based filtering • <Connection_Type> = type of signaling encryption used — INSECURE = no signaling encryption — SECURE” = USec or DTLS — DTLS = DTLS	basic-6.00

Command	Description	Pack/Rel
	— USEC = UNIStim Security — ALL = all encryption types • <DTLS_Capability> = capability to make DTLS connections — YES = able to make DTLS connections — NO = not able to make DTLS connections — ALL = both capabilities	
STOP NTP BACKGROUND	Stop background synchronization from running. ***Note 1:*** You cannot stop a background synchronization if no background routine is running. Attempts to do so result in an error message. ***Note 2:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	basic-5.0
SYNC NTP <Manual | BACKGROUND>	Synchronize with NTP server in manual or background mode. ***Note 1:*** Manual synchronization places LD 117 on hold for 15 seconds. During that time, you cannot abort from the overlay. ***Note 2:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). NTP configuration and management are controlled from the Linux Base layer.	basic-5.0
UPDATE DBS	Rebuild INET database and renumber host and route entry ID (update network database). ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	

Alphabetical list of Maintenance commands

Command	Description	Pack/Rel
DIS BUF ALL	Disable buffering for all data types	
DIS BUF CDR		

Command	Description	Pack/Rel
	Disable buffering for CDR data	
DIS BUF TRF	Disable buffering for TRF data	
DIS DBK	Display database disaster recovery's backup & restore	
DIS HOST n	Remove a host from the run time host table, where n = host entry number. ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
DIS PPP	Disable Point-to-point Protocol access (this enables PPPD)	
DIS ROUTE n	Remove a route from the run time routing table, where n = route entry number. ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
DIS ZALT <zone>	Disable ACR for zone, where: • zone = 0-255 ***Note:*** Branch Office is configured at the Main Office	basic-4.50
DIS ZBR <Zone> [ALL] [LOC] [ESA] [TIM] [ALT]	Disable a Zone's Branch Office behavior, if no specific features are specified, then ALL is assumed, where: • zone = 0-255 • ALL = all features • LOC = Local Dialing Access • ESA = Emergency Service Access • TIM = Time Adjustment • ALT = Alternate Routing for Branch	basic-4.0 basic-4.50

Command	Description	Pack/Rel
DIS ZCAC <Zone>	Disable Call Admission Control (CAC) for the identified zone, where: • Zone = 0-255 ***Note:*** Disables the feature on a zone by zone basis.	zcac-4.50
DIS ZONE 0-255	Disable a Zone, No new calls is established inside the disabled zone, from or towards this Zone.	
ENL BUF ALL	Enable buffering for all data types	
ENL BUF CDR	Enable buffering for CDR data	
ENL BUF TRF	Enable buffering for TRF data	
ENL DBK	Enable database disaster recovery's backup & restore	
ENL HOST n	Add a host to run time host table, where n = host entry number. ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
ENL PPP	Enable Point-to-point Protocol access (Enables PPPD command)	
ENL ROUTE n	Add a route to run time routing table, where n = route entry number . ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	

Command	Description	Pack/Rel
ENL ZALT <zone>	Enable ACR for zone, where: • zone = 0-255 ***Note:*** Branch Office zone is configured at the Main Office	basic-4.50
ENL ZBR <zone> [ALL] [LOC] [ESA] [TIM] [ALT]	Enable a Zone's Branch Office behavior, if no specific features are specified, then ALL is assumed, where: • zone = 0-255 • ALL = all features • LOC = Local Dialing Access • ESA = Emergency Service Access • TIM = Time Adjustment • ALT = Alternate Routing for Branch	basic-4.0 basic-4.50
ENL ZCAC <Zone>	Enables Call Admission Control (CAC) for the identified zone, where: • Zone = 0-255 ***Note:*** Enables the feature on a zone by zone basis.	zcac-4.50
ENL ZONE 0-255	Enable a Zone	
PING	Ping an IP address to test the network settings. ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
SET ENABLE_TRAPS (ON) | OFF	Enable/disable the sending of SNMP traps. Where: • ON = enabled • OFF = disabled	basic-6.00

Command	Description	Pack/Rel
SET HSP_IP	Activates the HSP IP addresses and subnet mask ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	basic-4.50
SET MASK	Set ELNK subnet mask to configured value (set runtime subnet mask to the configured value). ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
SET OPEN_ALARM <slot> <IP address> [<port>]	Add an SNMP (Simple Network Management Protocol) trap destination. Where: • <slot> = 0-7 • <IP Address> = any valid value in an x.x.x.x format (TCP/IP) • <port> = destination port for the SNMP trap ***Note:*** When <port> is not specified, SNMP traps are routed to port 162 by default. ***Note:*** To clear an SNMP trap destination, specify appropriate <slot> value and set <IP Address> = 0.0.0.0. When SNMP open alarm trap destinations are added or modified in LD 117, they are stored in an "OVLY 117 Configuration" area pending activation. When the **SYNC SNMPCONF** command is executed, the "OVLY 117 Configuration" SNMP open alarm changes are activated and become part of the "ACTIVE Configuration" (current) on the system.	basic-6.00
STAT AUTONEG IPM	Display auto-negotiate status of Main Cabinet ports.	

Command	Description	Pack/Rel
	The following report is displayed: AUTO-NEGOTIATE LINK PARTNER STATUS - MAIN/CALL SERVER PORTS ---------- PORT Bandwidth Duplex Mode AutoNegotiate ========== IPR 1 UNKNOWN UNKNOWN ON IPR 2 UNKNOWN UNKNOWN IPR 3 100 Mbps full duplex ON IPR 4 UNKNOWN UNKNOWN If the auto-negotiation process is successful, it returns " 100 Mbps full duplex". Otherwise UNKNOWN is reported, indicating a failure in negotiating 100 Mbps full duplex bandwidth.	
STAT AUTONEG IPR	Display auto-negotiate status of Expansion Cabinet ports. The following report is displayed: AUTO-NEGOTIATE LINK PARTNER STATUS - EXPANSION/MEDIA GATEWAY PORTS ---------- PORT Bandwidth Duplex Mode AutoNegotiate ========== IPR 1 UNKNOWN UNKNOWN ON IPR 2 UNKNOWN UNKNOWN IPR 3 100 Mbps full duplex ON IPR 4 UNKNOWN UNKNOWN If the auto-negotiation process is successful, it returns " 100 Mbps full duplex". Otherwise UNKNOWN is reported, indicating a failure in negotiating 100 Mbps full duplex bandwidth.	
STAT BUF	Display buffer info (data type, % full, not ready)	
STAT DBK	Display status of disaster recovery (enabled, disabled)	
STAT ELIN [ALL] / <erl>		basic-5.0

Command	Description	Pack/Rel
	Print current status of all ELINs in all / specified ERLs.	
STAT ELIN ACTIVE [<erl>]		basic-5.0
	Print active mappings for specified ERL, or all ERLs if none is specified.	
STAT HOST	Display current runtime host table status (enabled hosts). ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
STAT LINK APP <applicationType>		
	Display the link information status of the server for the specified application, where: • applicationType, where: — LTPS = Line TPS — VGW = Voice Gateway — H323 = H.323 Virtual Trunk — GK = GateKeeper — MC32S = 32 port Mindspeed VGMC	
STAT LINK IP <IP address>		
	Display the link information status of the server for the specified IP address, or IP addresses of the specified subnet, where: • IP address = the ELAN IP address of the Signaling Server or Voice Gateway Media Card ***Note:*** The IP address can be in full or partial IP address format. For example, "10.11.12.13" or "10.11".	
STAT LINK NAME <hostName>		
	Display the link information status of the servers based on the supplied host nam, where: • hostName = MAINSERVER	
STAT LINK NODE <nodeID>		
	Display the link information status of the specified node, where:	

Command	Description	Pack/Rel
	• nodeID = 0-9999 ***Note:*** The nodeID identifies the node number assigned to a group of Voice Gateway Media Cards and Signaling Server equipment.	
STAT LINK SRV <serverType>	Display the link information status of the servers for the specified server type, where: • serverType, is: — ITGP = ITG Pentium — SMC = Media Card — SS = Signaling Server — MC32S = 32 port Mindspeed VGMC	
STAT PPP	Display Point-to-point Protocol connection status.	
STAT ROUTE	Display host and network routing table. ***Note:*** This command is blocked for co-resident Call Server applications (Call Server and Signaling Server applications co-located on a CP PM server). Network configuration and management are controlled from the Linux Base layer.	
STAT SERV APP <applicationType>	Display the link information status of the server for the specified application, where: • applicationType is: — LTPS = (Line TPS) — VGW = Voice Gateway — H323 = H.323 Virtual Trunk — GK = GateKeeper — SIP (Session Initiated Protocol) — MC32S = 32 port Mindspeed VGMC — SLG = SIP Lines Gateway	
STAT SERV IP <IP address>		

Command	Description	Pack/Rel
	Display the link information status of the server for the specified IP address, or IP addresses contained in the specified sub-net, where: • IP address = the ELAN IP address of the Signaling Server or Voice Gateway Media Card. ***Note:*** The IP address can be in full or partial IP address format. For example, "10.11.12.13" or "10.11".	
STAT SERV NAME <hostName>	Display the link information status of the servers based on the supplied host name, where: • hostName = MAINSERVER	
STAT SERV NODE <nodeID>	Display the link information status of the specified node, where: • nodeID = 0-9999 ***Note:*** The nodeID identifies the node number assigned to a group of Voice Gateway Media Cards and Signaling Server equipment.	
STAT SERV TYPE <serverType>	Display the server information of the specified server type, where: • serverType is: — ITGP = ITG Pentium — SMC = Media Card — SS = Signaling Server — MC32S = 32 port Mindspeed VGMC	
STAT SS	Display the server information of the specified Signaling Server.	
STAT ZBR [<Zone>]	Display status of branch office zones, where: • Zone = 0-255	
STAT ZONE [<Zone>]	Display zone status table, where:	

Command	Description	Pack/Rel
	• Zone = 0-255	
STIP ACF	Displays status for all ACF calls	basic-4.50
STIP ACF <status>		basic-4.50
	Displays Active Call Failover (ACF) status information, where: • UNREG = unregistered calls • HREG = half-registered calls • REB = rebuilt calls • HREB = half-rebuilt calls • PREB = partial-rebuilt calls	
STIP HOSTIP <IP address>		
	Display information contained in the resource locator module table corresponding to the specified HOSTIP address, or HOSTIP addresses contained in the specified sub-net, where: • IP address = the ELAN IP address of the Signaling Server or Voice Gateway Media Card. ***Note:*** IP address can be in full or partial IP address format. For example, "10.11.12.13", or "10.11".	
STIP NODE <nodeID>		
	Display information contained in the resource locator module table corresponding to the specified node ID, where: • nodeID = 0-9999 ***Note:*** The nodeID identifies the node number you have assigned to a group of VGMC and Signaling Server equipment.	
STIP SIPLUA <UA string>		basic-6.00
	Display SIP Line Services TNs with the specified User Agent string.	
STIP TERMIP <IP address>		
	Display information contained in the resource locator module table corresponding to the specified TERMIP address, or TERMIP addresses contained in the specified sub-net, where:	

Command	Description	Pack/Rel
	• IP address = the TLAN IP address of the IP Phone or Voice Gateway Media Card. ***Note:*** IP address can be in full or partial IP address format. For example, "10.11.12.13", or "10.11".	
STIP TN <l s c u>	Display the resource locator module information for the specified TN, or group of TNs, as denoted by the l s c u and c u parameters.	
STIP TYPE <aaa>	Display the resource locator module information for the specified TN type. Where valid values for <aaa> are: • I2002 = IP Phone 2002 • I2004 = IP Phone 2004 • I2050 = IP Phone 2050 • ISET = all IP sets • VGW = Voice Gateway resources • IPTI = Virtual Trunk and IP Trunks • MC32S = 32 port Mindspeed VGMC Where valid values for <aaa> are: • 1210 = IP Phone 1210 • 1220 = IP Phone 1220 • 1230 = IP Phone 1230 ***Note:*** Up to 3 TN types can be specified.	basic 5-5
STIP ZONE <zone>	Display the resource locator module information for the specified zone number, or range of zones, where: • zone = 0-255	
TEST ALARM [aaaannnn]		basic-4.0

Command	Description	Pack/Rel
	Generate an alarm. Where: • aaaa = any character sequence. However, to test how an existing system message category (for example, BUG, ERR, INI) appears in an alarm browser, use an existing system message. • (nnnn) = any numeric sequence Defaults to 0000. The output shown on the TTY is the system message used as the parameter. The actual trap sent to the trap destination list has the same severity as an existing message defined in the EDT and EPT. Nonexistent system messages have a severity of `Info`. The following items are found in the details section of the trap output: • `commonMIBDateAndTime` = the time when the test is generated • `commonMIBSeverity`= defined by the EDT and EPT or Info(5) • `commonMIBComponentID` = the configured value of the Navigation system name: Navigation site name: CS (component type) • `commonMIBNotificationID` = 0 • `commonMIBSourceIPAddress`= IP Address of Call Server • `commonMIBErrCode` = AAAANNNN • `commonMIBAlarmType` = 8 (indicating unknown) • `commonMIBProbableCause` = 202 (indicating unknown) • `commonMIBAlarmData` = Contains textual description The rest of the variable bindings are NULL.	
TEST SUBNETLIS <IP address>	Return the location data for the subnet entry that matches the specified IP address.	basic-5.0

LD 43: Equipment Datadump

The following changes are made for LD 43

- New parameter for BKO and RES commands to support the Co-resident CP PM Call Server and Signaling Server system configuration
- A statement added to EDD command in support of the Zone Based Dialing enhancement to indicate that the ZBD configuration and parameter database are now included in the CS 1000 backup and restore functionality.

Alphabetical list of commands

Command	Description	Pack/Rel
BKO xxx	The file holding the MIB-II variables, System Navigation variables, and community name strings is copied from the primary device to the backup (external storage) device.	basic-19
	Where xxx = removeable storage device type. • RMD = Compact Flash device • USB = USB memory stick ***Note:*** This parameter only applies when the Call Processor and SS applications are co-resident on a CP PM server.	basic-6.00
RES xxx	The file created to store the MIB-II variables, System Navigation variables, and community name strings is restored from the backup (external storage) device to the primary device.	basic-19
	Where xxx = removeable storage device type. • RMD = Compact Flash device • USB = USB memory stick ***Note:*** This parameter only applies when the Call Processor and SS applications are co-resident on a CP PM server.	basic-6.00

LD 96: D-channel Diagnostic

The following new commands are added for LD 96

- DCT
- DCT CLR
- DCT HELP
- DCT DCH n
- DCT x…x

- DCT I x…x
- DCT > n
- DCT ON/OFF

D-channel call trace commands

All LD 96 DCT commands and variants are listed below.

DCT xxxxxxxx	Set the monitor digits (part or all of a DN) for trace operation .
DCT on/off	Turn the DCT monitor on and off.
DCT I xxxxxxxx	Set several occurrences of monitor digits (part or all of multiple DNs) for trace operation.
DCT > n	Change the DCT monitor message threshold.
DCT clr	Clear all DCT monitor settings.
DCT I xxxxxxxx <NPI> <TON> <MsgRecv> <MsgSend>	Specify specific types of calls for monitoring.
DCT dch n	Specify the DCHs to monitor.
DCT dch clr	Remove monitoring for all DCHs.
DCT	Display DCT settings.
DCT help/?	Display DCT commands syntax.
Note: For the monitor digits with 3 or fewer digits, only the DCH message with a match is recorded (not any associated messages). This prevents excessive messaging.	

LD 135: Core Common Equipment Diagnostic

The following update is made to LD 135

- A note is added to the following command to support Co-resident CP PM Call Server and Signaling Server system configuration
  - STAT MEM

Alphabetical list of commands

Command	Description	Pack/Rel
STAT MEM	Get the status of SIMMs on both Call Processors. ***Note:*** On a Co-res Call Server, the command does not show the actual physical memory size of the CP PM hardware. It shows the memory size that the Call Server application is using.	cpp_cni-25

System messages

The following system messages are introduced for Communication Server 1000 Release 6.0. The new messages are sorted by the following message categories:

- "AUD: Software Audit (LD 44)" (page 230)
- "BUG: Software Error Monitor" (page 231)
- "CCBR: Customer Configuration Backup and Restore" (page 240)
- "DCH: D-channel Diagnostic (LD 96)" (page 240)
- "ELAN: Ethernet Local Area Network" (page 241)
- "ERR: Error Monitor (Hardware)" (page 242)
- "ESA: Emergency Services Access" (page 244)
- "HWI: Hardware Infrastructure Maintenance" (page 245)
- "IOD: Input/Output Diagnostic (LD 37)" (page 245)
- "ITG: Integrated IP Telephony Gateway" (page 245)
- "MGMT: Management messages." (page 245)
- "NBWM: Network Bandwidth Management" (page 246)
- "NPR: Network and Peripheral Equipment Diagnostic (LD 32)" (page 247)
- "PRI: Primary Rate Interface Diagnostic (LD 60)" (page 249)
- "SCH: Service Change" (page 249)
- "SEC: Security Notification Monitor" (page 267)
- "SRPT: System Reports" (page 281)
- "SYS: System Loader" (page 287)
- "TEMU: Tape Emulation" (page 290)
- "TFC: Traffic Control (LD 2)" (page 291)

The following information is available for each system message:

- message description
- action (if applicable)
- message severity
- whether the message is critical to monitor
- whether the message is sent as an SNMP trap

AUD: Software Audit (LD 44)

Message	Description	Action	Severity	Monitor	SNMP
AUD0120	ACTIVECR of SIP Line Trunk differs from ACTIVECR of corresponding Universal Extension. Procedure TRK _AUDIT_DONE.	No action required.	Major	Yes	Yes
AUD0121	tntrans failed for TRK_UEXT TN. Procedure TRK_AUDIT_DONE.	No action required.	Major	Yes	Yes
AUD0122	Timer Call Register used for ROD/SAVE key is not cleared properly. Timer Call Register is idled.	Contact your technical support group.	Minor	No	Yes
AUD0123	Timer Call Register is not cleared properly during the ROD/SAVE key usage, as the Call register is not the same as the one saved in the keylink of the set. Timer Call Register is idled.	Contact your technical support group.	Minor	No	Yes
AUD0124	Marked DCT channel/trunk found in IDLE state.	If the problem persists contact your technical support.	Minor	No	No

Message	Description	Action	Severity	Monitor	SNMP
AUD0125	Son call register has an invalid Father call register.		Minor	No	Yes
AUD0126	Physical TN is detected as busy but not involved in any call. Physical TN is idled. Parameters: <PTN>, <VITN_ VTNLINK>, <VITN _PTN_COUNT>, <ACTIVECR>	Contact your technical support.	Minor	No	No

BUG: Software Error Monitor

Message	Description	Action	Severity	Monitor	SNMP
BUG0673	SIPL trunk configuration counter corruption happened. The counter is reset to 0.	Check the database. Contact your technical support	Info	No	No
BUG0674	ZBD: Incorrect configuration for DAPC. ZBD option and route-based DAPC cannot be enabled at the same time. The set displays an invalid DN or blank field.	Check ZBD and DAPC configuration. If the problem persists contact your next level support organization.	Major	Yes	Yes
BUG0678	DNXLPTR is corrupt. Parameters: DN, DNPTR, DNXLPTR. The CPND block associated with DN will not be dumped.	Contact your technical support group.	Major	Yes	Yes

Message	Description	Action	Severity	Monitor	SNMP
BUG0679	DIGITLOAD or DIGITUNLOAD not correctly set during a call from UEXT TN. . DIGITLOAD is less than DIGITUNLOAD. DIGITLOAD should be greater than or equal to DIGITUNLOAD. The call will fail.	SW defect. Please contact the next level of support in your organization	Major	Yes	Yes
BUG0686	Failed to open %s file. HI and HA modules are dependent on this file. The system may not behave as expected.	1. Check the permission with the /etc/opt/nortel/cppmUtil directory. 2. Check for the existence of the file in the same directory.	Major	Yes	Yes
BUG0692	CM: Cannot init HSP Server : Bind server socket failed due to invalid [%s]. The [%s] assigned is corrupt due to a previous bind failure.	Try to reuse or reassign the [%s].	Major	Yes	Yes
BUG0699	CM: Cannot init HSP Server : Bind server socket failed due to invalid [%s]. The [%s] assigned is corrupt due to a previous bind failure.	Try to reuse or reassign the [%s].	Major	Yes	Yes
BUG0723	Pointer is out of range in the RFC_IPDN_HDLR procedure.		Minor	No	No

Message	Description	Action	Severity	Monitor	SNMP
BUG0724	Failed to get the Internet address of a network interface %s<PRIMARY _ETHERNET_I NTERACE>The Call Server will fail to send an arp request to registered MGCs.	Check if the primary ethernet interface is defined.	Minor	No	No
BUG0734	Failed to map an interface %s<PRIMARY_ ETHERNET_IN TERACE> to an interface structure pointer.The Call Server will fail to send an arp request to registered MGCs.	Check if the primary ethernet interface is defined.	Minor	No	No
BUG0736	LOGIN_CNT does not equal the number of active sessions. Parameters: LOGIN_CNT, the number of active sessions, PORT_ID[.MAX_ TTY_LOGINS], OVL_PROG_ ARY[.MAX_T TY_LOGINS], OVLTIMER_ARY The LOGIN_CNT value will be recalculated.	If the problem persists, contact your technical support group.	Minor	No	No
BUG0737	ORIGTN = 0 before calling REMOVETONE. Procedure REMO VE_IEES_PATH.	Contact your technical support group.	Minor	No	Yes

Message	Description	Action	Severity	Monitor	SNMP
BUG0738	MAINPM = .REORDER before calling REMOVETONE. Procedure REMOVE_IEES_PATH.	Contact your technical support group.	Minor	No	Yes
BUG0739	DCHI ring buffer full message is not applicable for CS1000E.		Minor	No	No
BUG0746	Error setting Linux Call Server hardware platform type. Linux Call Server functionality is dependent on the platform type. Failing to set platform type will impact the system critically.	Contact the Nortel technical support staff.	Critical	Yes	Yes
BUG0747	Incoming SETUP message had a CREF that may belong to a completely separate call. The channel requested in the SETUP message was a TN associated to the MSG CR for that call reference. The ACTIVECR of this TN had both ORIGTN and a TERTN, one of which was the trunk TN and the other was not NULL.	Capture the bug message along with d-channel traces and provide it to the design community to investigate further.	Minor	No	No

Message	Description	Action	Severity	Monitor	SNMP
BUG0748	Incoming SETUP message had a CREF that the local system determined belongs to a completely separate call. The channel requested in the SETUP message is neither the ORIGTN nor the TERTN allocated to the MSG CR for that call reference.	Capture the bug message along with d-channel traces and provide it to the design community to investigate further.	Minor	No	No
BUG0749	ACTIVECR of the PTN is not NIL.	If the problem persists, contact your technical support.	Info	No	No
BUG0751	CTE_CMD_PM is out of range. PROCEDURE: CTE_EXECUTE. Parameters: 2 words of memory adjacent to CTE_CMD_PM. Corruption of local pool data in ld 80. Corruption of local pool data in ld 80.	Contact your technical support group.	Major	Yes	Yes
BUG0753	CEMUXOPENCONN fails either due to invalid card number/cab number/ivalid buffer value, or invalid app_id. The connection will not come up; the result is the MSDL card will not enable.	If the problem persists, contact your technical support.	Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
BUG0754	LCS: taskSpawn failed. Failure when spawning SshSync task .	Contact your technical support	Critical	Yes	Yes
BUG0756	Task (%s) ID get error. It is safe to write to log file when there is error trying to get a taskId.		Minor	No	No
BUG0757	Semaphore (sbbmsgXmitSem) give error. It is safe to write to log file, when cmSemGive fails. This will make debugging easier.		Minor	No	No
BUG0758	CNI access error, slot=%d. CNI cannot be accessed when the CNI card is pulled out or during tSL1 restart.		Minor	No	No
BUG0761	Problem storing secured data. (Type: ttttt Error code: eeee) Secured data is used for passwords and keys. If there is a problem storing the password or key, there will likely be a failure of the feature needing the secured data.	This indicates a system or softw are malfunction where a resource is temporarily unavailable and so it may be possible to try the feature again. If the problem persists, contact your technical support.	Warning	No	No

Message	Description	Action	Severity	Monitor	SNMP
BUG0762	Problem retrieving secured data. (Type: ttttt Error code: eeee) Secured data is used for passwords and keys. If there is a problem retrieving the password or key, there will likely be a failure of the feature needing the secured data.	This indicates a system or softw are malfunction where a resource is temporarily unavailable and so it may be possible to try the feature again. If the problem persists, contact your technical support.	Warning	No	No
BUG0835	ZBD: ZBD prefix is 0 in IE message. There is an invalid value in the message field. The set displays an invalid DN or blank field.	Contact your next level support organization.	Major	Yes	Yes
BUG0836	ZBD: TNTRANS fails for given TN. An error occurred while processing a TN. The set displays an invalid DN or blank field.	Check if this TN is configured on the Call Server. If the problem persists contact your next level support organization.	Major	Yes	Yes
BUG0837	ZBD: Unable to get country code. Unable to get country code for given numbering zone. The set displays an invalid DN or blank field.	Check if the country code is configured for given numbering zone. If the problem persists contact your next level support organization.	Major	Yes	Yes
BUG0838	ZBD: Invalid ZBD digits count in DN. DN contains too many digits. The set displays an invalid DN or blank field.	Check if the configured DN is valid. If the problem persists contact your next level support organization.	Major	Yes	Yes

Message	Description	Action	Severity	Monitor	SNMP
BUG0839	ZBD: Incorrect configuration. Called plan is E164/public but called type is not for E164. The set displays an invalid DN or blank field.	Check your dialing plan configuration. If the problem persists contact your next level support organization.	Major	Yes	Yes
BUG0861	ZBD: incorrect numbering zone. Some zone-based features may not work.	Check that correct numzone is used for the set. Check the ZBD zone configuration in LD 117. If the problem persists contact your technical support.	Major	No	Yes
BUG0862	Zone prefix cannot be found in DGT_MANIPULATIONS. Asterisk in DMI Will not be replaced for the zone prefix.	Check that the numbering zone and zone prefix are configured correctly.	Major	No	Yes
BUG0863	* in DMI is not allowed in SBO/SMG. Asterisk in DMI Will not be replaced for the zone prefix.	Correct the DMI.	Warning	No	Yes
BUG0864	Empty Zone Prefix in ZBD IE. Pd: INS_ZBD_PREFIX. Asterisk in DMI Will not be replaced for the zone prefix.	Contact your technical support.	Warning	No	Yes
BUG0865	BUILD_ZBD: incorrect DN of originator. Some of the ZBD features may not work for trunk calls	Check the DN of the originating set. It should be a 7-digit DN.	Major	No	Yes

Message	Description	Action	Severity	Monitor	SNMP
BUG0866	BUILD_ZBD_TE RTN: TNTRANS fails. Possible data corruption.	Contact your technical support.	Major	No	Yes
BUG6507	ACTIVECR of the PTN is updated with the wrong Call Register.	If the problem persists, contact your technical support.	Info	No	No
BUG7210	ZBD: failed to find the zone-based CC. CLID may be incorrect on set display for international calls.	Check that correct ZBD zone is used for the set. Check the ZBD zone configuration in ld 117. If the problem persists contact your technical support.	Major	No	Yes
BUG7211	The SOURCE is incorrect in ZBD_HANDLER.	Contact your technical support.	Major	No	Yes
BUG7212	Required para meter(s) is(are) not specified. Data corruption is possible.	Contact your technical support.	Major	No	Yes
BUG7213	The TYPE is incorrect for SOURCE = ZBD _ADD_ZPARM in ZBD_HANDLER. CLID may be incorrect on set display.	Contact your technical support.	Major	No	Yes
BUG7214	ZBD: Unsuppo rted unit type. Cannot obtain a zone number. Some zone-based features may not work.	Contact your technical support.	Major	No	Yes

Message	Description	Action	Severity	Monitor	SNMP
BUG7215	ZBD: CC is incorrect. ESA call went to wrong BO. Incorrect ANI will be sent to PSAP.	Check the dial plan configuration on Call Server and Network Routing Service. If the problem persists contact your technical support.	Major	No	Yes
BUG7216	ZBD: NPA is incorrect. ESA call went to wrong BO. Incorrect ANI may be sent to PSAP.	Check the dial plan configuration on Call Server and Network Routing Service. If the problem persists contact your technical support.	Major	No	Yes

CCBR: Customer Configuration Backup and Restore

Message	Description	Action	Severity	Monitor	SNMP
CCBR0030	Semaphore create failed.	Contact your technical support.	Major	No	Yes
CCBR0031	RMD/USB device not responding.	Check the device, or check the csProxy status on Linux. If the problem persists, contact your technical support.	Major	No	Yes

DCH: D-channel Diagnostic (LD 96)

Message	Description	Action	Severity	Monitor	SNMP
DCH0058	The DCT monitor is now off. DCT DCH message monitoring has stopped.	To turn the DCT monitor back on use the DCT command in OVL96:- DCT on	Info	No	No
DCH0059	DCH message printing has been stopped. DCH message print queue cleared.	To reset DCH message printing use the monitor command in OVL96:- rst mon	Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
DCH0060	DCT DCH mes sage threshhold exceeded. The DCT monitor has turned itself off.	To change the threshhold value use the DCT command in OVL96:- dct > <1-60>	Info	No	No
DCH0061	<DCT_ERROR> <ERR_INFO> DCT_ERROR can have the following values:- 1 The syntax of the DCT command is:- dct help OR dct ? 2 The syntax of the DCT command is:- dct 3 The syntax of the DCT command is:- dct on 4 The syntax of the DCT command is:- dct of	Check the command that you entered.	Info	No	No

ELAN: Ethernet Local Area Network

Message	Description	Action	Severity	Monitor	SNMP
ELAN0031	An ELAN host route has been removed (for hhhh IP address xxx.xxx.xxx.xxx.).		Info	No	No
ELAN0032	A new ELAN host route has been configured (for hhhh IP address xxx.xxx.xxx.xxx.). The default route on some devices is normally the TLAN interface, but routing to the reported device is being changed to use the ELAN interface.		Info	No	No

ERR: Error Monitor (Hardware)

Message	Description	Action	Severity	Monitor	SNMP
ERR0127	Both UADN and HOT U key are not provided. The target pointer is NIL.	Configure a valid UADN and retry the call.	Major	Yes	Yes
ERR0128	Invalid Target DN used to route the call.	Configure a valid Target DN and retry the call.	Major	Yes	Yes
ERR0129	Call dropped due to detection of closed far-end port. Check VGMC logs.Parameters: <Active CR bugprint>CP - for Call Pilot call <Active CCR_IV R_CR>MG - for Media Gateway callTR - for trunk call IP - for local call to IP set <DSPTN>	Contact your next-level technical support. To assist in diagnosing the problem gather the following information: • logs from the Call Server • logs from the VGMC • logs from the Signaling Server • TNB information using LD 20 for the TNs in the output	Major	No	Yes
ERR0131	The SIP Line Universal Extension TN linked to this trunk TN is null <trunk TN>.		Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
ERR0132	The ACTIVECR of this SIP Line Universal Extension TN is not equal to CRPTR <UEXT TN> <ACTIVECR> <TRUNK TN> <CRPTR>.		Info	No	No
ERR0133	TERTN of the incoming call is not equal to the SIP Line Universal Extension TN <TERTN> <UEXT TN> <incoming call register>.	Check the univ ersal extension configuration in overlay 11.	Major	Yes	Yes
ERR0134	TNTRANS failed for the real originator TN behind this SIP Line universal extension <real originator TN> <UEXT TN> <call register of real originator>.	Check the univ ersal extension configuration in overlay 11, or the SIP Line route /trunk configuration in overlay 16/14.	Major	Yes	Yes
ERR0135	The MSGCR of this SIP Line Trunk is NIL. <SIP Line Trunk TN>.		Info	No	No
ERR0136	Cannot get call register from the call id of the incoming call to SIPL universal extension <call id> <UEXT TN>.	Turn on AML message printing on Call Server (LD 48) or Signaling Server (slgAmlTrace) to check if the incoming call is disconnected.	Major	Yes	Yes
ERR0137	This error mes sage indicates potential packet loss/delay on CS ELAN.	Ensure that the CS ELAN connection is working properly.	Warning	No	No

Message	Description	Action	Severity	Monitor	SNMP
ERR0138	ORIGTN or TERTN is ZERO.	Please report the issue to Field Support to investigate the root cause.	Major	Yes	Yes
ERR0139	MAINPM is equal to REORDER.	Please report the issue to Field Support to investigate the root cause.	Major	Yes	Yes
ERR0141	ZBD: Incorrect configuration for DAPC. ZBD option and route-based DAPC cannot be enabled at the same time.	Check ZBD and DAPC configuration. If the problem persists, contact your technical support.	Major	Yes	Yes
ERR0144	<packed TN> <NUMZONE number> <PREF> <DN> PREF of NUMZONE is not equal to the beginning of a DN for the TN. PREF is not cut off from a DN.	Check configu ration of PREF in NUMZONE and DN of a set. If the problem persists, please contact your next level support organization.	Info	No	No

ESA: Emergency Services Access

Message	Description	Action	Severity	Monitor	SNMP
ESA0070	SIP Client for UEXT TN <tn> and IP <ip> was not located by Subnet LIS - will use ESA defaults.	'Consider adding the phone's location to Subnet LIS.	Info	No	No
ESA0071	Unable to find a SIP Client for UEXT TN <tn> and ESA SIPL ID <id>.	Check the ESA ID values stored in RLM and SLG, mis match happened. To be investigated.	Info	No	No

HWI: Hardware Infrastructure Maintenance

Message	Description	Action	Severity	Monitor	SNMP
HWI0012	HWI: Spurious NMI event. The HWI event initiates a cold start.	Contact your technical support.	Minor	No	No

IOD: Input/Output Diagnostic (LD 37)

Message	Description	Action	Severity	Monitor	SNMP
IOD0008	Interrupt: checkNonConfigDevs: unconfigured card in slot 2 generated unexpected CEMUX interrupt.		Minor	No	No

ITG: Integrated IP Telephony Gateway

Message	Description	Action	Severity	Monitor	SNMP
ITG0127	SLG Application is not ready: <AML Link is down>.The SLG application will not be able to register the clients if the AML link is down.	Check the AML link for SLG application.	Major	Yes	Yes

MGMT: Management messages.

Message	Description	Action	Severity	Monitor	SNMP
MGMT0002	DTLS policy has been modified from <DTLS policy original value> to <DTLS policy changed value> for node <node id>. The DTLS policy controls which ports are open on the elements of the node and		Info	No	Yes

Message	Description	Action	Severity	Monitor	SNMP
	whether the elements will attempt to switch DTLS-capable pho				

MSDL: Multi-purpose Serial Data Link

Message	Description	Action	Severity	Monitor	SNMP
MSDL0109	No response from the card. Card will not enable due to response timeout	If the problem persists, please contact your technical support.	Info	No	No
MSDL0504	CEMUX link to the IPMG cabinet is down.	Try the command after the link is re-established.	Minor	No	No

NBWM: Network Bandwidth Management

Message	Description	Action	Severity	Monitor	SNMP
NBWM0001	NBWM peer system has changed its status to stand-alone.	No action required. Note that Network Bandwidth Management is disabled.	Info	No	Yes
NBWM0002	NBWM peer system has changed its status to registered.	No action required. Note that Network Bandwidth Management is enabled.	Info	No	Yes
NBWM0003	NBWM peer system has changed its status to registration request.	No action required.	Info	No	Yes
NBWM0004	The link to NBWM master is lost.	Contact your technical support group.	Major	Yes	Yes

NPR: Network and Peripheral Equipment Diagnostic (LD 32)

Message	Description	Action	Severity	Monitor	SNMP
NPR0058	This comm and is not applicable to ENET cards. When you try to check the card ID of an ENET card (DTI/PRI /DTI2/PRI2), you should get this NPR message; because IDC procedure does not support ENET cards.	If the problem persists, please contact your technical support.	Minor	No	No

OSM: Operating System Messaging

Message	Description	Action	Severity	Monitor	SNMP
OSM0030	<MEMORY_S IZE> does not meet the minimum system memory requirement of <MIN_MEMORY _SIZE>.Where:< MEMORY_SIZE> - actual installed system memory size, <MIN_ME MORY_SIZE> - minimal required system memory size.The system will not be operational due to insuffi	Add more system memory to comply with minimal hardware requirements.	Critical	Yes	Yes

Message	Description	Action	Severity	Monitor	SNMP
OSM0031	<HDD_SIZE> does not meet the minimum HDD requirement of <MIN_HDD_SIZE> Where:<HDD_SIZE> - actual installed HDD size, <MIN_HDD_SIZE> - minimal required HDD size.The system will not be operational due to insufficient HDD size.	Replace the installed HDD to comply with minimal hardware requirements.	Critical	Yes	Yes
OSM0032	IP address is not assigned for eth0/eth1. The issue is caused by incorrect network topology and/or configuration. For example,. the system with the same IP address does actually exist in the same subnet or it was registered on the nearest switch/hub/rout	Ensure that no one uses the same IP address. Then restart network interface.	Major	Yes	Yes
OSM0033	NIC settings for eth0/eth1 do not comply with the minimal system requirements. Speed/half-duplex setting is caused due to some assumptions made by network equipment on the Ethernet level. Two devices (Ethernet card on our system and	You must reboot the system.	Major	Yes	Yes

Message	Description	Action	Severity	Monitor	SNMP
	Ethernet port on the				

PRI: Primary Rate Interface Diagnostic (LD 60)

Message	Description	Action	Severity	Monitor	SNMP
PRI0009	Crossing messages during establishment phase.	Capture the PRI message along with d-channel traces and provide it to the design community to investigate further.	Minor	No	No
PRI0390	Version of ZBD ISDN IE is incorrect. Some of the ZBD features may not work for trunk calls.	Contact your technical support.	Major	No	Yes

SCH: Service Change

Message	Description	Action	Severity	Monitor	SNMP
SCH2251	SIPL trunks ISM exhausted/ Insufficient.	Increase the ISM parameter for SIPL trunks. Contact your technical support.	Info	No	No
SCH2261	SIP Lines package is not equipped.	Unrestrict the SIP Lines package (package number 417).	Info	No	No
SCH2262	The SIP domain name (SIPD) is not configured.	The SIPD has to be configured in LD 15, under the SIP Lines Services (SLS) gateway.	Info	No	No
SCH2263	Invalid input for the SIP Domain name (SIPD).	The SIPD must be alpha numeric or a '.' character, and the maximum length is 16 characters.	Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
SCH2264	Cannot delete SIP domain name (SIPD) input.	You cannot the SIPD. Delete the Customer Data Block (CDB) and reconfigure.	Info	No	No
SCH2265	Cannot delete UAPR input. At least 1 TN is using UAPR for a UADN prefix.	To delete the UAPR, configure UADN for all of the TNs or delete the TNs without UADN.	Info	No	No
SCH2266	Invalid input for SIP Client List (SCTL).	Valid inputs for the SCTL prompt in LD 11 are FMCL, TLSV, SIP3, and SIPN.	Info	No	No
SCH2267	The SIP user name (SIPU) in LD 11 cannot be blank.	Configure a valid username. A username must be alphabetic and the maximum length is 16 characters.	Info	No	No
SCH2268	Invalid input for the SIP user name (SIPU).	You can configure the user name at the SIPU prompt in LD 11. Configuration of the user name does not include the @ sign or the domain name.. The username must be alphabetic and the maximum length is 16 characters.	Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
SCH2269	The SIP user name (SIPU) that you entered already exists.	The SIPU input must be unique for each user. The SIPU value that you entered is already configured for the TN printed in this SCH message. Input a different SIPU, or modify the conflicting TN's SIPU and then configure the current TN.	Info	No	No
SCH2270	NDID prompt in LD 11 cannot take NULL input. Configuring a valid node input for the NDID prompt is mandatory.	Configure a valid node input for the NDID prompt in LD 11.	Info	No	No
SCH2271	Invalid user level entered for super user (SUPR).	Valid inputs for the SUPR prompt in LD 11 are: • YES – The user is a super user • NO – The user is not a super user	Info	No	No
SCH2272	Invalid input for NDID prompt. Input for the NDID prompt can only be ascii values and cannot exceed 4 digits in length.	Configure a valid node input for the NDID prompt in LD 11.	Info	No	No
SCH2273	Invalid input. SIPL can only be used for the PRT command.	Enter a valid input.	Info	No	No
SCH2274	UADN is not configured. HOT U input cannot be null.	Configure UADN or enter a valid input for the HOT U key.	Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
SCH2275	Cannot CHG the UXTY FROM or TO MOBX.	UXTY prompt value in LD 11 cannot be changed from or to MOBX, because the UXID value must be unique. The TN must be deleted and configured again to create a new UXTY configuration.	Info	No	No
SCH2276	SLS gateway is not configured.	Configure SLS (SIP Lines Service) gateway in CDB (LD 15), before configuring SIPL TNs.	Info	No	No
SCH2277	HOT U key cannot be configured for non-SIPL TNs	HOT U key (in LD 11) is allowed only for the SIPL TNs. Do not configure it for non-SIPL TNs.	Info	No	No
SCH2278	PDN (Primary DN) not configured.	Configure PDN (Primary DN) for KEY 0 (in LD11) before configuring UADN.	Info	No	No
SCH2279	HOT U key not configured.	Configure HOT U key (in LD 11) for the SIPL TN before completing the TN configurations.	Info	No	No
SCH2280	Invalid UAPR.	Input configured for the UAPR (UADN prefix) in LD 15 is not valid. Input must be a unique DN and must pass the DNTrans.	Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
SCH2281	Redirection DN is UADN.	FDN or HUNT (LD 11) cannot be configured with any SIPL TN's UADN. Configure a different DN.	Info	No	No
SCH2282	SCTL cannot be blank.	SCTL (Sip ClienT List) prompt in LD 11 cannot be blank. At least 1 client should be configured for the SIPL TN. The valid inputs are FMCL, TLSV, SIP3 and SIPN.	Info	No	No
SCH2283	Command not supported on Linux Call Server.		Minor	No	No
SCH2284	Time and Date changes privileges are not supported on Linux Call Server.		Minor	No	No
SCH2285	DN cannot be in MARP with other SIP Line TN.	LD 11 DN, for a SIP Line TN, cannot be in MARP with any other SIP Line TNs. Configure a different DN.	Info	No	No
SCH2286	ROD and SAVE key can be configured only if CLS is ICRA. These keys are for call recording purposes.		Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
SCH2287	ROD and SAVE keys are not supported for this set type. ROD and SAVE keys can be configured only on IP sets supporting Call Recording.		Info	No	No
SCH2288	ROD and SAVE keys are functional only with CCMS 7.0 or later.		Info	No	No
SCH2289	ROD and SAVE keys will be removed if CLS is changed from ICRA to ICRD. ROD and SAVE keys can be configured only if CLS is ICRA because these keys are for call recording.		Info	No	No
SCH2290	Database has not finished loading - try again in a minute. New entries cannot be configured until the database is loaded.	Try the operation again.	Info	No	No
SCH2291	ZBD package (420) is restricted. The action cannot be performed because the ZBD package is not equipped.	Contact your next level support organization.	Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
SCH2292	FDP <zone number> <matching string> does not exist.The entry does not exist and cannot be changed, deleted or printed.	No action required.	Info	No	No
SCH2293	DID <zone number> <matching string> does not exist.The entry does not exist and cannot be changed, deleted, or printed.	No action required.	Info	No	No
SCH2294	FDP <zone number> <matching string> is already configured.The entry already exists and cannot be added.	Change the entry using another command.	Info	No	No
SCH2295	DID <zone number> <matching string> is already configured.The entry already exists and cannot be added.	Try the operation again. If the problem persists, contact your next level support organization.	Major	Yes	Yes
SCH2296	Failed to create FDP <zone number> <matching string>.The entry was not created.	Try the operation again. If the problem persists, contact your next level support organization.	Major	Yes	Yes
SCH2297	Failed to create DID <zone number> <matching string>.The entry was not created.	Try the operation again. If the problem persists, contact your next level support organization.	Major	Yes	Yes

Message	Description	Action	Severity	Monitor	SNMP
SCH2298	Invalid Matching String <matching string>.The input characters are not valid.	Try the operation again with correct parameters.	Info	No	No
SCH2299	Invalid Length <number>.The input parameter is wrong.	Try the operation again with correct parameters.	Info	No	No
SCH2300	Invalid Description <description>.The input parameter is wrong.	Try the operation again with correct parameters.	Info	No	No
SCH2301	LD 11, SCTL prompt (for SIPL user) change/remove invalid (cannot change/remove this client type as its registered).	Unregister all clients of this type and then try to change/remove the client type(SCTL promt).	Info	No	No
SCH2302	LD 15, UAPR prompt can take 4 digits input at the maximum.	Configure input up to 4 digits for the UAPR prompt in LD 15.	Info	No	No
SCH2303	DB32 cannot be configured on this type of IPMG.		Info	No	No
SCH2304	DB96 can only be configured in card slots 8,9.10,11,12,13.		Info	No	No
SCH2305	CTYP does not match IPMG type.		Info	No	No
SCH2306	CTYP of XSM is only allowed on IPMG type of MGX.		Info	No	No
SCH2307	CE-Mux cards are not supported on this type of IPMG.		Info	No	No
SCH2308	Cannot change IPMG type.		Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
SCH2309	Invalid Input for NDID prompt in LD 11. Input for NDID prompt in LD 11 cannot exceed 4 digits in length.	Configure NDID input using a maximum of 4 digits.	Info	No	No
SCH2310	PDN (Primary DN) and UADN (User Agent DN) cannot be the same DNs. For a SIP Line TN, the PDN and UADN cannot be the same.	Configure a different DN, which does not conflict with PDN, for UADN.	Info	No	No
SCH2311	SIP Lines Pack age is restricted, therefore the SIPL services will not be available. SIPL trunks cannot be configured on the system because the SIP Lines Package is restricted.	Enable the SIP Lines package and reconfigure the SIPL trunks.	Major	No	No
SCH2312	IP Phone has reached End of Life status. IP Phone reached End of Life status in 2007.		Major	No	No
SCH2313	Value cannot be changed if ZBD option is disabled. NUMZONE value is not changed.	Enable ZBD option in LD 15. If the problem persists contact your technical support.	Info	No	No
SCH2314	HOT P cannot be configured for SIPL UEXT TN. In LD 11, HOT P is allowed only for non-SIP line UEXt TNs and cannot be present for SIPL TNs.	Remove the HOT P configured for this TN.	Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
SCH2315	Security domain unreachedable. Unable to get a response when pinging the primary security server.	This could be a networking problem, but some network configurations may not ever allow ICMP messages, such as PING. Check the IP address and network configuration if you are getting this message while unable to join the security domain.	Info	No	No
SCH2316	Unable to find security domain. Attempt to get details of security domain when the system is not part of a security domain.	You should attempt to join a security domain before performing a status or leave operation.	Info	No	No
SCH2317	SCPW cannot be removed for SIP Line. SIP Line will not be able to register if SCPW is removed.	Do not remove SCPW for SIP Line.	Info	No	No
SCH2318	Must configure SCPW for SIP Line. SIP Line will not be able to register if SCPW is not configured.	Configure SCPW for SIP Line.	Info	No	No
SCH2319	Name Directory cannot be enabled when application server is not configured.	Enable the application server before Name Directory configuration.	Minor	No	No

Message	Description	Action	Severity	Monitor	SNMP
SCH2320	Invalid input for MCCL. n LD 11, MCCL (Max Client Count List) can be configured only as YES or NO.	Configure MCCL=YES (to allow the user to configure the number of clients of each client type) or NO (for default client type).	Info	No	No
SCH2321	MCCL cannot be blank. In LD 11, MCCL (Max Client Count List) MUST be configured only as YES or NO.	Configure MCCL as Yes or No.	Info	No	No
SCH2322	Both SIPN and SIP3 cannot be NULL for SIP Line TN. In LD 11, either SIPN client or SIP3 client MUSt be configured for SIP Line TN.	Configure either SIPN or SIP3.	Info	No	No
SCH2323	Invalid input for SIPN client. In LD 11, configure a valid numeric value for the SIPN client.	Configure a valid numeric value for SIPN client.	Info	No	No
SCH2324	Invalid input for SIP3 client. In LD 11, configure a valid numeric value for the SIP3 client.	Configure valid Numeric value for SIP3 client.	Info	No	No
SCH2325	Invalid input for FMCL client. In LD 11, configure a valid numeric value for the FMCL client.	Configure a valid numeric value for FMCL client.	Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
SCH2326	Invalid input for TLSV client. In LD 11, configure a valid numeric value for the TLSV client.	Configure a valid numeric value for TLSV client	Info	No	No
SCH2327	Both SIPN and SIP3 cannot be 1 for SIP Line TN. In LD 11, either SIPN client or SIP3 client only can be configured for SIP Line TN.	Configure either SIPN or SIP3, but not both.	Info	No	No
SCH2328	Pointer is NIL. Pointer used to access the SIP Line template is NIL. Configuration cannot be made.	Pointer corruption occurred. Exit the overlay and try to reconfigure.	Info	No	No
SCH2329	UXTY=SIPL cannot be configured as all the related client packages are restricted. n LD 11, UXTY=SIPL configuration is not accepted as the packages for all the 4 supported clients - SIPN, SIP3, FMCL, TLSV are all restricted.	Unrestrict at least one of the supported clients package and then configure SIP Line TN.	Info	No	No
SCH2330	ZBD Zone already exists. New CM Zone cannot be configured.	Try the operation again.	Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
SCH2331	ZBD Zone has IP set registered - ZBD zone number <zone number>.The ZBD Zone cannot be deleted, because there are several IP sets registered with it.	Remove all IP sets from ZBD Zone and try again.	Info	No	No
SCH2332	ZBD Zone parameter value is out of range. New ZBD Zone parameter(s), cannot be applied.	Try the operation again with a proper value.	Info	No	No
SCH2333	ZBD Zone number is incorrect. ZBD Zone cannot be changed/added/deleted.	Try the operation with a proper ZBD Zone number.	Info	No	No
SCH2334	ZBD Zone cannot be created. There appear to be system issues.	Contact your next level support organization.	Info	No	No
SCH2335	Cannot delete an IPMG that is not configured.		Minor	No	No
SCH2336	No custom file available at the moment. If the custom rules file does not exist in the system, access restrictions that use custom rules cannot be turned on.	Upload the custom rules file, then turn on access restrictions.	Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
SCH2337	Resource busy, please try again after 2 minutes. When one of the PORT ACCESS OFF/DEFAU LT/CUSTOM access restrictions commands are given, some access restrictions commands will be locked out and unable to execute for 2 minutes to allow sufficient time for	Wait for 2 minutes and then try the command again.	Info	No	No
SCH2338	CPSI Port 1 not supported on Linux Call Server.	Only CPSI Port 0 can be configured on Linux Call Server.	Minor	No	No
SCH2339	Trunk config uration in LD 14 cannot be changed to/from SIPL trunk. SIPL trunk cannot be changed to SIP/H323 Trunk, and H323/SIP trunk cannot be changed to SIP trunk.	Trunk CHG is not valid. Create a new trunk of the required type.	Info	No	No
SCH2340	Invalid card number. Physical cards cannot be configured on logical slots. The valid physical slots for MGC IPMG are 1 to 10.	The valid card numbers range from 1 to 10.	Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
SCH2341	ZBD Zone has FDP entry configured - ZBD zone number <zone number>.The ZBD Zone cannot be deleted, because there is an FDP entry configured for this zone.	Remove all FDP entries from CDP zone and try again.	Info	No	No
SCH2342	Tone table does not exist - Table <table>. Tone table does not exist and cannot be assigned to a numbering zone.	Create a tone table and try the operation again.	Info	No	No
SCH2343	ZBD zone does not exist - zone <zone>.ZBD zone is not configured.	Configure ZBD zone in overlay 117.	Info	No	No
SCH2345	WARNING! X -zone usage is not 0. The change in X -zone bandwidth configuration can cause incorrect calculation of the X -zone traffic report. Where X is intra or inter.	Contact your technical support.	Info	No	No
SCH2346	Model sets are not supported, beginning in Release 6.0. You cannot create model sets as of Release 6.0.		Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
SCH2347	PREF already exist (shorter, longer or the same) -- PREF <>, conflicting NUMZONE 400, PREF 400. Shorter, longer or the same PREF exists in other NUMZONE. PREF is empty if NEW NUMZONE is used or not changed if CHG command is used	Use another PREF. If the problem persists, contact your technical support.	Info	No	No
SCH2348	The default numbering zone cannot be removed. The default (0) numbering zone should be always configured and cannot be removed; this zone is available for changing the configuration.	Do not remove the default numbering zone.	Info	No	No
SCH2349	Input numbering zone is not configured.	Configure numbering zone in Overlay 117.	Info	No	No
SCH2350	The TN has to be in a Virtual Loop		Info	No	No
SCH2351	WARNING: IP address must be configured for this IPMG because TNs are configured.	Configure an IP address for this IPMG.	Warning	No	No
SCH2352	Do not configure more than one node ID for each DCH.		Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
SCH2353	MCCL cannot be changed for the TN if it has an ACD key configured. SIP IVR UEXT agents are always configured as type SIPN, so other client types such as SIP3 or TLSV are not supported.	Continue using the default value of MCCL and list other prompts for the TN.	Info	No	No
SCH2354	Configuration of an ACD key for PBX agents is not allowed as SIPQ prompt is set for the associated ACD queue. SIP IVR agents are configured only as UEXT TNs which requires the SIPQ prompt to be set for the associated queue. Other types of units/sets are	Disable the SIPQ prompt on the associated ACD queue and configure the PBX unit as a normal ACD agent.	Info	No	No
SCH2355	Configuration of an ACD key for non SIP Line agents is not allowed as the SIPQ prompt is set for the associated ACD queue. SIP IVR agents are configured only as UEXT TNs which requires the SIPQ prompt to be set for the associated queue. Other types of un	Disable the SIPQ prompt on the associated ACD queue and configure the non-SIP Line unit as a normal ACD agent.	Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
SCH2356	Configuration of an ACD key for SIP Line UEXT IVR agents is not allowed as the SIPQ prompt is not set for the associated ACD queue. ACD key is not supported for normal UEXT TNs.Only SIP IVR UEXT agents support ACD key but it requires the SIPQ prompt to b	Enable the SIPQ prompt on the associated ACD queue and configure the SIP Line unit as an IVR ACD agent.	Info	No	No
SCH2357	Configuration of an ACD key for SIP Line UEXT IVR agents is not allowed as the unit is not configured as a SIPN client. ACD key is not supported for other SIP Clients (such as SIP3 or TLSV).Only SIPN clients are allowed to be configured with an ACD key	Set the SIPN prompt in the TN block and configure the SIP Line unit as an IVR ACD agent with an ACD key.	Info	No	No
SCH2358	Modification of an SIPQ prompt is not allowed, as agents are already available for this ACD queue. SIPQ prompt for the ACD queue can be changed only if this queue is not served by any agents. This is to ensure that the SIPQ prompt is not deactivated for	Disable and remove all the agents associated with the queue and then alter the SIPQ prompt for the ACD queue.	Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
SCH2359	Up to 1024 DTR/ TDET/ DTD units can be defined in each system.		Info	No	No
SCH2361	LD 11, HOT U DN (UADN) for SIPL users has to be unique and cannot have MARP with any pre-configured DN. User would not be able to configure any pre-configured DN as UADN.	Enter a unique DN.	Info	No	No
SCH2362	The ELAN which has been removed has at least one resource in acquired status.	Remove all of the resources on this ELAN.	Minor	No	No
SCH2363	Applicable for redundant systems only. Midnight SCPU is not possible for non-redundant system.		Info	No	No

SEC: Security Notification Monitor

Message	Description	Action	Severity	Monitor	SNMP
SEC0037	Security domain membership has been granted. (Centralized authentication with primary security server xxx.xxx.xxx.xxx is now enabled). The user's request to join the security domain was successful. The local accounts are	This is a confirmation of an action initiated by a user. No action is required so long as the action was authorized.	Info	Yes	Yes

Message	Description	Action	Severity	Monitor	SNMP
	now disabled in favour of the				
SEC0038	Security domain membership has been revoked. (Centralized authentication is now disabled.) The user's request to leave the security domain was successful.	This is a confirmation of an action initiated by a user. No action is required so long as the action was authorized.	Info	Yes	Yes
SEC0039	More than one security domain file has been found. Only one security domain may be authorized at a time, but somehow more than one authorization file is present in the system.	This is an abnormal operation; contact your technical support.	Major	Yes	Yes
SEC0060	SSH source filtering is enabled. Only trusted hosts are allowed to connect to the Linux base system.	Check that only trusted hosts are in the SSH filtration list.	Cleared	No	Yes
SEC0061	SSH source filtering is disabled SSH connections are allowed for all hosts. This is a potential security exposure.	Check that the filtration was disabled by an authorized person.	Major	Yes	Yes

Message	Description	Action	Severity	Monitor	SNMP
SEC0062	The host [host/subnet] is added to the list of allowed hosts for SSH connection. The added host is considered trustworthy and is permitted to connect to the Linux base system by SSH.	Check that the changes were done by an authorized person.	Warning	No	Yes
SEC0063	The host [host/subnet] is removed from the list of allowed hosts for SSH connection. The host is not permitted to connect to the Linux Base system by SSH.	Check that the changes were done by an authorized person.	Warning	No	Yes
SEC0064	The host [host/subnet] is added to the list of denied hosts for SSH connection. The host is not allowed to connect to the Linux base system by SSH.	Check that the changes were done by an authorized person.	Warning	No	Yes
SEC0065	The host [host/subnet] is removed from the list of denied hosts for SSH connection. The host is permitted to connect to the Linux base system by SSH.	Check that the changes were done by an authorized person.	Warning	No	Yes

Message	Description	Action	Severity	Monitor	SNMP
SEC0066	The Linux audit daemon is started. The Linux audit daemon started inspecting the Linux system calls.	Inspect the audit logs regularly for security-critical events.	Cleared	No	Yes
SEC0067	The Linux audit daemon is stopped. The Linux audit daemon stopped inspecting the Linux system calls. This is a potential security exposure.	Check that the changes were done by an authorized person.	Major	Yes	Yes
SEC0068	The maximum number of days a password can be used is set to the new value <value>.	Check that the changes were done by an authorized person.	Warning	No	Yes
SEC0069	The minimum number of days permitted between password changes is set to the new value <value>.	Check that the changes were done by an authorized person.	Warning	No	Yes
SEC0070	The FTP service is permitted. This is a potential security exposure.	Check that the changes were done by an authorized person.	Major	Yes	Yes
SEC0071	The FTP service is forbidden.	Check that the changes were done by an authorized person.	Cleared	No	Yes
SEC0072	The FTP service is started. This is a potential security exposure.		Major	Yes	Yes
SEC0073	The FTP service is stopped.		Cleared	No	Yes

Message	Description	Action	Severity	Monitor	SNMP
SEC0074	Core dump files are permitted. This is a potential security exposure.	Check that the changes were done by an authorized person.	Major	Yes	Yes
SEC0075	Core dump files are forbidden.		Cleared	No	Yes
SEC0076	Core file size is changed to <value>.		Warning	No	Yes
SEC0077	The TFTP service is permitted. This is a potential security exposure.	Check that the changes were done by an authorized person.	Major	Yes	Yes
SEC0078	The TFTP service is forbidden.		Cleared	No	Yes
SEC0079	The TFTP service is started. This is a potential security exposure.		Major	Yes	Yes
SEC0080	The TFTP service is stopped.		Cleared	No	Yes
SEC0081	The Telnet service is permitted. This is a potential security exposure.	Check that the changes were done by an authorized person.	Major	No	Yes
SEC0082	The Telnet service is forbidden.		Cleared	No	Yes
SEC0083	The Telnet service is started. This is a potential security exposure.		Major	Yes	Yes
SEC0084	The Telnet service is stopped.		Major	No	Yes
SEC0085	The pre-login banners are turned off.	Check that the changes were done by an authorized person.	Major	No	Yes

Message	Description	Action	Severity	Monitor	SNMP
SEC0086	The text of the pre-login banner is changed.	Check that the changes were done by an authorized person.	Warning	No	Yes
SEC0087	Secure transfers have been enabled. When secure transfers are enabled, the CS1K applications can transfer data based on the seucre transfer protocol, such as SFTP.	This is an informational message; no action is required.	Major	Yes	Yes
SEC0088	Secure transfers have been disabled. When secure transfers are disabled, the CS1K applications cannot transfer data based on the seucre transfer protocol, such as SFTP.	This is an informational message; no action is required.	Major	Yes	Yes
SEC0089	Insecure transfers have been enabled. When insecure transfers are enabled, the CS1K applications can transfer data based on the inseucre transfer protocol, such as FTP.	This is an informational message; no action is required.	Major	Yes	Yes

Message	Description	Action	Severity	Monitor	SNMP
SEC0090	Insecure transfers have been disabled. When insecure transfers are disabled, the CS1K applications cannot transfer data based on the inseucre transfer protocol, such as FTP.	This is an informational message; no action is required.	Major	Yes	Yes
SEC0091	The pre-login banners are turned on.		Cleared	No	Yes
SEC0092	Network tools are disabled. The following network tools are disabled: Ethereal, tcpdump and gryphon, traceroute and tracepath commands.		Cleared	No	Yes
SEC0093	Network tools are enabled. The following network tools are enabled: Ethereal, tcpdump and gryphon, traceroute and tracepath commands. This is a potential security exposure.	Check that the changes were done by an authorized person.	Major	Yes	Yes
SEC0094	Another Security Domain command may be in progress. The system detected another security domain manage ment command is already in progress.	Multiple user commands to manage the security domain should not be issued in parallel.	Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
SEC0095	rlogin to the Call Server by external client is permitted. rlogin access to the Linux server from the network is enabled. The server's firewall has been opened for the standard rlogin port 513. rlogin requests will handled by the Call Server application.	No action is required. Issue the Linux CLI command "harden rlogin off" to disable external rlogin access. Only users with a Security Admin role are permitted to issue this command.	Major	Yes	Yes
SEC0096	rlogin to the Call Server by external client is forbidden. rlogin access to the Linux server from the network is disabled. The server's firewall has been closed for the standard rlogin port 513.	No action is required. Issue the Linux CLI command "harden rlogin on" to enable external rlogin access. Only users with a Security Admin role are permitted to issue this command.	Cleared	No	Yes
SEC0097	This element has successfully requested membership in the security domain. The user's request to have the device join the security domain was successful.	This is a confirmation of an action initiated by a user. No action is required so long as the action was authorized.	Info	Yes	Yes

Message	Description	Action	Severity	Monitor	SNMP
SEC0098	This element has failed to request membership in the security domain. The user's request to have the device join the security domain was not successful.	The device encountered an error while attempting to join the security domain. Its possible that the wrong credentials were used. If proper credentials were used and it fails, then it may be necessary to contact support.	Info	No	No
SEC0099	This element has successfully removed security domain membership credentials. The user's request to have the device leave the security domain was successful.	This is a confirma tion of an action initiated by a user. No action is required so long as the action was authorized.	Info	Yes	Yes
SEC0100	This element has failed to remove security domain membership credentials. The user's request to have the device leave the security domain was not successful.	The device encountered an error while attempting to clean up its security domain credentials. This is an abnormal situation, so assistance from support may be required.	Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
SEC0101	Element xxx.xxx.xxx.xxx sucessfully requested membership in the security domain. The user's request to have the device join the security domain was successful.	This is a confirmation of an action initiated by a user. No action is required so long as the action was authorized.	Info	No	No
SEC0102	Element xxx.xxx.xxx.xxx failed to request membership in the security domain. The user's request to have the device join the security domain was not successful.	The device encountered an error while attempting to join the security domain. Its possible that the wrong credentials were used. If proper credentials were used and it fails, then it may be necessary to contact support.	Info	No	No
SEC0103	Element xxx.xxx.xxx.xxx sucessfully removed its security domain membership credentials. The user's request to have the device leave the security domain was successful.	This is a confirmation of an action initiated by a user. No action is required so long as the action was authorized.	Info	No	No
SEC0104	Element xxx.xxx.xxx.xxx failed to remove its security domain membership credentials. The user's request to have the device leave the security	The device encountered an error while attempting to clean up its security domain credentials. This is an abnormal situation, so	Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
	domain was not successful.	assistance from support may be required.			
SEC0105	User=<User> SRC = <source> DST = <shell> EVT=<scope> port access state change to <state>, RESULT = <success/ failure>User can have the following values:1. The actual user name for a manual change.2. “initialization” from system bootup.3. “CS Update” on		Info	No	Yes
SEC0106	Unable to request security domain membership because SSH transfers are disabled. Joining the security domain requires the usage of SSH transfers. SSH transfers are currently disabled, so it will not be possible to join the security domain.	Issue the ENL TRANSFERS SECURE command to enable secure transfers.	Info	No	No
SEC0107	The PPP service is forbidden.		Cleared	No	Yes
SEC0108	The PPP service is permitted. This is a potential security exposure.		Major	Yes	Yes
SEC0109	The firewall is enabled.		Cleared	No	Yes

Message	Description	Action	Severity	Monitor	SNMP
SEC0110	The firewall is disabled. There is a potential security exposure.		Major	Yes	Yes
SEC0111	REGISTER UCMSECURITY SYSTEM command is not supported for STDBY Call Server. Only the active Call Server has control of the media gateways and media cards, so issuing the REGISTER UCMSECURITY SYSTEM command does not make sense on the STDBY Call Server.	Use the REGISTER UCMSECURITY DEVICE command instead.	Info	No	No
SEC0112	UNREGISTER UCMSECURITY SYSTEM command is not supported for STDBY Call Server. Only the active Call Server has control of the media gateways and media cards, so issuing the UNREGISTER UCMSECURITY SYSTEM command does not make sense on the STDBY Call Server	Use the UNREGISTER UCMSECURITY DEVICE command instead.	Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
SEC0113	Issuing the CUTOVR command may invalidate the security domain membership. Re-establishing security domain membership is required. The SSH keys used to enable security domain membership can be lost under certain failure situations. CUTOVR is often used	The message is a reminder to issue the REGISTER UCMSECURITY DEVICE if the SSH keys of the Call Server were impacted. (The SSH keys must remain unchanged to maintain the mutual trust implicit in security domain membership.)	Warning	No	No
SEC0114	Establishing security domain membership from STDBY Call Server will require re-establishing security domain membership after issuing CUTOVR or JOIN commands. If any security domain changes were done when the cores were not redundant then it is necessary	The message is a reminder that security domain membership becomes invalidated on the STDBY Call Server when the active core switches or when redundant mode is restored.	Warning	No	No
SEC0115	Issuing the JOIN command may invalidate the security domain membership. Re-establishing security domain membership is required. If security domain memberhip was altered when	If any security domain changes were done when the cores were not redundant then it is nece ssary to issue the REGISTER UCMSECURITY DEVICE comma nd to ensure both of the redundant	Warning	No	No

Message	Description	Action	Severity	Monitor	SNMP
	redundancy was disabled, re-establishing security domain membership will be requ	Call Server cores have current security domain membership credentials.			
SEC0116	User uuuuuuu has been allowed to log in using an emergency account.	Contact technical support; inves tigate to see if there is a possible network outage.	Critical	Yes	Yes
SEC0117	Central account <username> conflicts with local account. Local account will be deleted.		Warning	No	No
SEC0118	Central account <username> conflicts with local account. Local permissions will be used.A central authentication account conflicts with a local account . The local account permissions will be used instead of the central auth permissions		Warning	No	Yes
SEC0119	< Local or Centra l> authentication is being used. An information message to inform whether the system is set to use local or central authentication		Warning	No	No

Message	Description	Action	Severity	Monitor	SNMP
SEC0120	Default accounts have been loaded into memory, perform EDD to make them persistent. Central authentication is being turned off, and local accounts are being restored, but there are no local accounts with the permission to manage the accounts. Rather th	Use the default ADMIN2 account to manage the accounts and change default passwords. Perform EDD to allow the acco unts to become permanent.	Warning	Yes	Yes

SRPT: System Reports

SRPT0295	Failed to access locked FDP <zone number> <procedure name>.The FDP table is locked and it is not accessable.	Try the operation again. If the problem persists, contact your next level support organization.	Major	Yes	Yes
SRPT0296	Failed to access locked DID <zone number> <procedure name>.The DID table is locked and it is not accessable.	Try the operation again. If the problem persists, contact your next level support organization.	Major	Yes	Yes

SRPT0297	ZBDInit:<explanation>.Semaphores are not created to acces FDP/DID tables, or the database load task is not spawned. The FDP/DID tables are not accessable.	Contact your next level support organization.	Critical	Yes	Yes
SRPT0298	Failed to take FDP table semaphore <procedure name>.The FDP node is not added or deleted.	Try the operation again. If the problem persists, please contact your next level support organization.	Major	Yes	Yes
SRPT0299	Failed to take DID table semaphore <procedure name>.The DID node is not added or deleted.	Try the operation again. If the problem persists, please contact your next level support organization.	Major	Yes	Yes
SRPT0300	Failed to allocate memory <explanation>.The FDP/DID node was not created. It is possible that there is no free memory.	Try the operation again. If the problem persists, please contact your next level support organization.	Major	Yes	Yes
SRPT0301	ZBDZoneInit:<explanation>.Semaphore is not created to access ZBD Numbering Zones table. ZBD Numbering Zones Table is not accessible.	Contact your next level support organization.	Critical	Yes	Yes

SRPT0302	Failed to take ZBD Numbering zones table semaphore <procedure name>.The ZBD Numbering Zone not added or deleted.	Try the operation again. If the problem persists, contact your next level support organization.	Major	Yes	Yes
SRPT0303	[%s]:expected AFS application type [%d] is not equal to the application type [%d] return from call back function. The call back function will not execute the required operation.	No action. This should never happen unless there is corruption in the AFS Publisher structure.	Info	No	No
SRPT0304	Failed to connect to SSD Server. Return Status[error number]	Analyze the failure; this error can be caused by Call Server SYSLOAD/INI. If the problem persists, contact technical support.	Major	No	Yes
SRPT0305	ERROR reading SSD Client socket. Socket <socket number> ERROR <error number>	Analyze the failure; this error can be caused by Call Server SYSLOAD/INI. If the problem persists, contact technical support.	Major	No	Yes
SRPT0306	SSD Client socket closed.	Analyze the failure; this error can be caused by Call Server SYSLOAD/INI. If the problem persists, contact technical support.	Major	No	Yes
SRPT0307	SSD Client re-started.		Minor	No	No

SRPT0308	<CemuxIOLink Mgmt> / Cemux MaintLinkMgmt: Connection closed. Return Status <error number>	Analyze the failure; this error can be caused by Call Server SYSLOAD/INI. If the problem persists, contact technical support.	Major	No	Yes
SRPT0309	The <IO> / <Ma int> connection is already UP with Call Server / IPMG <IPMG number>		Minor	No	No
SRPT0310	Remote TTY: <ttyServer>/<tty Client> :Socket <socket number> for cabinet <IPMG number> is closed.	Analyze the failure; this error can be caused by Call Server SYSLOAD/INI. If the problem persists, contact technical support.	Major	No	Yes
SRPT0311	Remote TTY: <ttyServer>/<tty Client> :Failure reading socket <socket number> for cabinet <IPMG number> Return Status <error number>	Analyze the failure; this error can be caused by Call Server SYSLOAD/INI. If the problem persists, contact technical support.	Major	No	Yes
SRPT0313	TOD: <description of error> [yy/m m/dd hh:mm:ss] errno [nn] where <description of error> could be either (a) Failed to spawn task to update time; or (b) CS PROXY reported failure to set time. The update date and time will be printed along with the internal	Check the current system time and date and adjust, if necessary, using the Base Manager or Linux Base CLI command. If this message persists, please contact Nortel Support for further investigation.	Info	No	Yes

SRPT0314	Heartbeat Link Mismatch between CS and cabinet <x>. Trying to recover HB Link.		Minor	No	No
SRPT0315	CS is not able to recover link between CS and cabinet <x>.	Check the CS Heartbeat connection. If the problem persists, contact your technical support.	Major	No	Yes
SRPT0317	Central Authentication with UCM for user accounts is turned on. Local user accounts are disabled.	Start using user accounts created on the UCM primary server.	Info	No	No
SRPT0318	INI signal (%d) received, warmstart CS.		Info	No	No
SRPT0319	Coldstart signal (%d) received, coldstart CS.		Info	No	No
SRPT0320	REMOTE TTY: ttyclient:ERROR writing to socket 39 for cabinet 3. There is no socket on the Call Server to receive messages.	You must create a remote TTY.	Minor	No	No
SRPT0321	Failure writing to SSD socket.Session <session number> socket <socket number> nBytesToSend <bytes to send> nBytesSent <bytes sent> Return status <errno>	Analyze the failure. This might be because of Call Server SYSLOAD/INI. If the problem persists contact your technical support.	Major	No	No

SRPT0322	Ignore the watchdog timeout value greater than 32. for CP P4 system type, watchdog timeout (SYS_SANITY_ TIMEOUT_MA) value is 32; anything greater than that should be ignored.		Warning	No	No
SRPT0323	System recovered using backup files from /p/hidir. Ungraceful switchover in the middle of disk sync operation can leave files on the inactive core corrupted. This situation can result in continous sysload on the inactive core during ungraceful switchover	No action required.	Major	Yes	Yes
SRPT0324	The CNI network is enabled and call processing is resumed. After all CNI interrupts are enabled, the call processing will be resumed.		Minor	No	No
SRPT0325	The system switchover is complete; the attempt to disconnect the CNI card is aborted. Once the cpu switchover is done, any attemp to disconnect the CNI card will be aborted.		Minor	No	No

SRPT0326	Task (%s) is resumed. Previously suspended task is resuming again.		Minor	No	No
SRPT0327	The CNI network is disabled and call processing is suspended. When CNI card is disabled, call processing is suspended.		Minor	No	No

SYS: System Loader

Message	Description	Action	Severity	Monitor	SNMP
SYS0160	Error loading ZBD database <file name>.The ZBD database is not loaded, or is partially loaded. An error occurred during the load.	Contact your next level support organization.	Critical	Yes	Yes
SYS0161	SIP Lines Pack age is restricted, therefore the SIPL trunks cannot be sysloaded. SIPL trunks configured on the system is lost.	Enable SIP Lines package and reconfigure the SIPL trunks.	Critical	Yes	Yes
SYS0162	SIP Lines Pack age is restricted, therefore the SIPL route cannot be sysloaded. SIPL route configured on the system is lost.	Enable SIP Lines package and reconfigure the SIPL route.	Critical	Yes	Yes

Message	Description	Action	Severity	Monitor	SNMP
SYS0163	SIP Lines Package is restricted, therefore the SIP Line TN is removed. SIP Line TN configured on the system is lost.	Enable SIP Lines package and reconfigure the SIP Line TN.	Critical	Yes	Yes
SYS0164	SIP Lines Service (SLS) Gateway is not ON, therefore the SIP Line TN is removed. SIP Line TN configured on the system is lost.	Turn ON SLS Gateway and reconfigure the SIP Line TN.	Critical	Yes	Yes
SYS0165	PCA package is restricted, therefore the PCA TN is removed. PCA TN configured on the system is lost.	Enable PCA package and reconfigure the PCA TN.	Critical	Yes	Yes
SYS0166	MobileX package is restricted, therefore the MobileX route is changed to a non-Mobile route. The route can still be used, but not for Mobile X.	Order the Mobile X package 412 and either sysload with the original database or reconfigure the route for Mobile X.	Major	Yes	Yes
SYS0167	Universal Extension for Mobile X is not loaded because the corresponding package is unequipped.	Order a new keycode that enables package 412.	Major	No	Yes
SYS0168	Universal Extension for Telephony Services is not loaded because the corresponding package is unequipped.	Order a new keycode that enables package 413.	Major	No	Yes

Message	Description	Action	Severity	Monitor	SNMP
SYS0169	Universal Extension for Fixed Mobile Convergence is not loaded because the corresponding package is unequipped.	Order a new keycode that enables package 414.	Major	No	Yes
SYS0170	Universal Extension for Nortel SIP is not loaded because the corresponding package is unequipped.	Order a new keycode that enables package 415.	Major	No	Yes
SYS0171	Universal Extension for Third Party SIP is not loaded because the corresponding package is unequipped.	Order a new keycode that enables package 416.	Major	No	Yes
SYS0172	Error loading ZBD Numbering Zone database <file name>.The ZBD database is not loaded or loaded partially. Some error occurred during load.	Contact your next level support organization.	Critical	Yes	Yes
SYS0173	ITG Trunk cards are not supported. All the related data blocks are removed from the database.		Info	No	No
SYS0174	The mode of communication has been changed from SS to CS. SS mode for NTP is not supported in Rls 6.0, so the mode has been	Use Element Manager to set up appropriate NTP configuration for the system and perform EDD once	Info	No	No

Message	Description	Action	Severity	Monitor	SNMP
	changed to CS on upgrade.	configurations are done.			

TEMU: Tape Emulation

Message	Description	Action	Severity	Monitor	SNMP
TEMU0026	Error dumping ZBD database <file name>.The ZBD database is not dumped or is partially dumped. An error occurred during the dump.	Contact your next level support organization.	Critical	Yes	Yes
TEMU0027	Error dumping ZBD Numbering Zone database <file name>.The ZBD database is not dumped or dumped partially. Some error occurred during dump.	Contact your next level support organization.	Critical	Yes	Yes
TEMU0031	Attempt to send GR Database Replication request through the use of afsAp pPublish failed. GR Database Replication failed for the selected Secondary Call Server.	Check whether the AFS API is up and running and the GR application is registering correctly with the AFS Publisher. If the problem persists, contact your next level support organization.	Major	Yes	Yes
TEMU0033	RMD/USB device not responding.	Check the device, or check the csProxy status on Linux. If the problem persists, contact your technical support.	Major	No	Yes

TFC: Traffic Control (LD 2)

Message	Description	Action	Severity	Monitor	SNMP
TFC0006	Command not supported on Linux Call Server.		Minor	No	No
TFC0007	Time and Date changes privileges are not supported on Linux Call Server.		Minor	No	No
TFC0017	NTP is enabled. NTS slave cannot be activated.	Disable NTP to activate NTS slave.	Info	No	No

TTY: Teletype Error Reports

Message	Description	Action	Severity	Monitor	SNMP
TTY0018	FD %d is not valid for TTYs. An invalid FD initiates INI.	Contact your technical support.	Major	No	Yes

Nortel Communication Server 1000

New in this Release

Release: 6.0
Publication: NN43001-115
Document revision: 03.14
Document release date: 19 February 2010

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com