Nortel Communication Server 1000

CP PM Co-resident Call Server and Signaling Server Fundamentals

Release: 6.0
Document Revision: 01.06

www.nortel.com

NN43001-509

Nortel Communication Server 1000
Release: 6.0
Publication: NN43001-509
Document release date: 5 October 2009

Contents

New in this release

The following sections detail what is new in the CP PM Co-resident Call Server and Signaling Server Fundamentals (NN43001-509) for Nortel Communication Server 1000 Release 6.0.

Navigation

Features

CS 1000 Release 6.0 introduces the Call Processor Pentium Mobile Co-resident Call and Signaling Server (CP PM Co-res CS and SS), which is capable of running the Call Server software, Signaling Server software, and System Management software on the same hardware platform operating under the RedHat Linux Operating System. The new system type for CP PM Co-res CS and SS is 4121.

For CS 1000 Release 6.0, the only supported hardware platform for the CP PM Co-res CS and SS Server is the Call Processor-Pentium Mobile (CP PM) platform.

Other

Revision History

October 2009

Standard 01.06. This is a new document created to support CP PM Co-res CS and SS for Nortel Communication Server 1000 Release 6.0

September 2009

Standard 01.05. This is a new document created to support CP PM Co-res CS and SS for Nortel Communication Server 1000 Release 6.0

July 2009
Standard 01.04. This is a new document created to support CP PM Co-res CS and SS for Nortel Communication Server 1000 Release 6.0.

June 2009
Standard 01.03. This is a new document created to support CP PM Co-res CS and SS for Nortel Communication Server 1000 Release 6.0.

May 2009
Standard 01.02. This is a new document created to support CP PM Co-res CS and SS for Nortel Communication Server 1000 Release 6.0.

May 2009
Standard 01.01. This is a new document created to support CP PM Co-res CS and SS for Nortel Communication Server 1000 Release 6.0.

How to get help

Introduction

This section contains the following topics:

Getting help from the Nortel Web site

The best way to receive 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 is a global document. Contact your system supplier or your Nortel representative to verify that support exists in your area for the hardware and software described in this document.

Subject

This document provides information about CP PM Co-res CS and SS for Nortel Communication Server 1000 Release 6.0.

Legacy products and releases

This document contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 6.0 software. For more information about legacy products and releases, click the Technical Documentation link under Support on the Nortel home page at www.nortel.com/support.

Applicable systems

This document applies to the following systems:

- CS 1000E
- MG 1000B Branch office
- MG 1000E Survivable Media Gateway

Intended audience

This document is intended for individuals who install, configure and maintain CP PM Co-res CS and SS in a Communication Server 1000 environment.

Only qualified personnel are to install CP PM Co-res CS and SS. To use this document, you must have a working knowledge of CS 1000E, CS 1000M, and Meridian 1 equipment and operation. Contact Nortel Training Centers for information on installation courses.

Conventions

Terminology

In this document, CS 1000E is referred to generically as system.

Related information

NTPs

The following list provides relevant information sources that this document references:

- *Communication Server 1000E Installation and Commissioning* (NN43041-310)
- *Communication Server 1000E: Planning and Engineering* (NN43041-220)
- *Element Manager System Administration* (NN43001-632)
- *Signaling Server IP Line Applications Fundamentals* (NN43001-125)
- *IP Peer Networking Installation and Commissioning* (NN43001-313)
- *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315)
- *Unified Communications Management*(NN43001-116)
- *Equipment Identification Reference* (NN43001-254)
- *Software Input Output Administration* (NN43001-611)
- *Software Input Output Reference - System Messages* (NN43001-712)
- *Software Input Output Reference - Maintenance* (NN43001-711)
- *Branch Office: Installation and Commissioning* (NN43001-314)
- *Security Management Fundamentals* (NN43001-604)

Overview

Introduction

A 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 CP PM Co-resident Call 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 Call Processor-Pentium Mobile (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.

Supported configurations

Overview

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

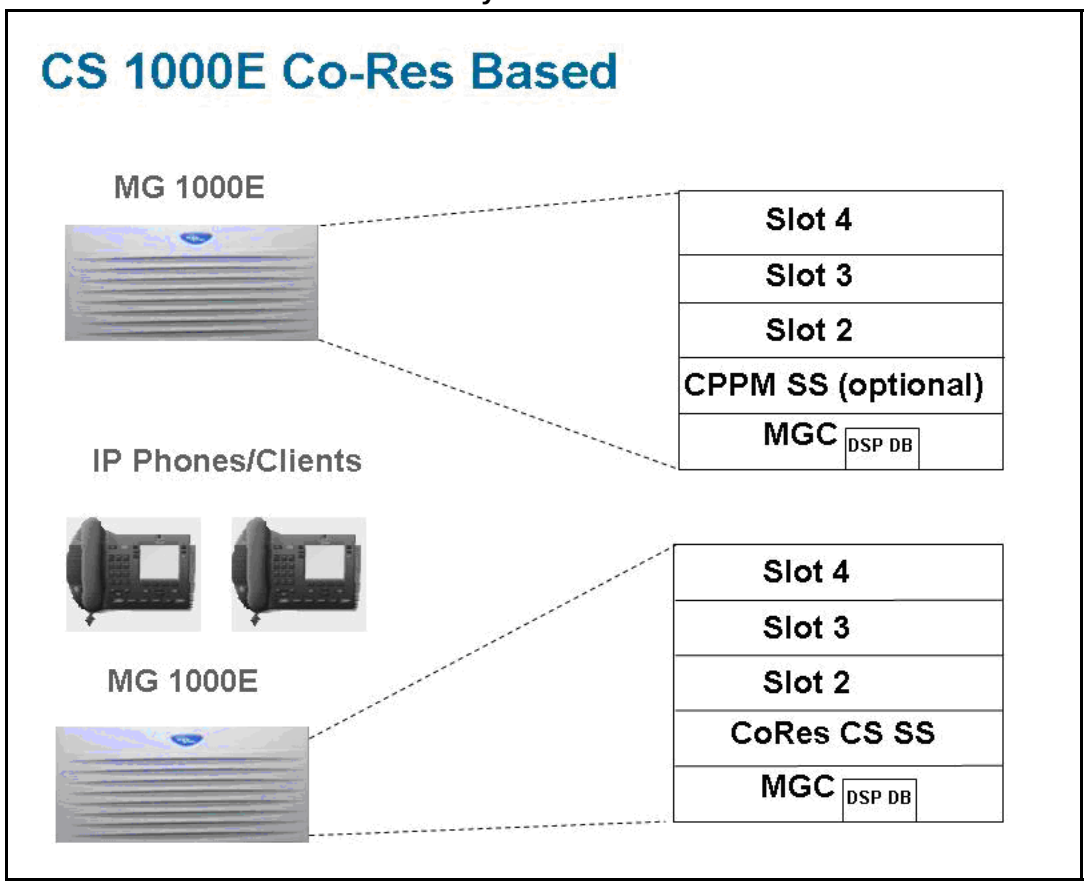
- CS 1000E
- MG 1000B Branch office
- MG 1000E Survivable Media Gateway
- CS 1000E TDM

Note: For details on CS 1000E Capacity limitations, see “Planning and engineering” (page 21)

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

Figure 1 "CS 1000E CP PM Co-res CS and SS System" (page 14) provides an example of a CS 1000E system with CP PM Co-res CS and SS.

Figure 1
CS 1000E CP PM Co-res CS and SS System



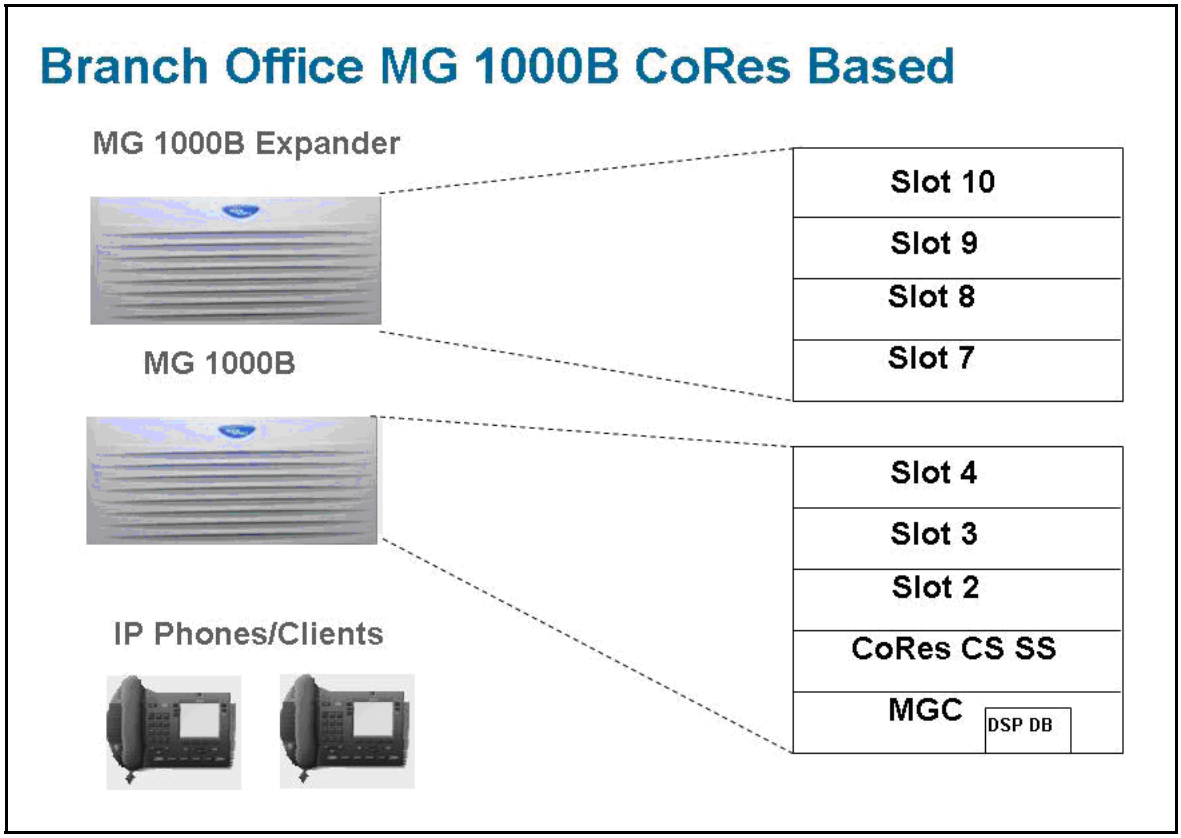
Optional second Signaling Server

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 2 "MG 1000B CP PM Co-res CS and SS System" (page 15) provides an example of the CS 1000 Release 6.0 CP PM Co-res CS and SS based Branch Office (MG 1000B) system.

Figure 2
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 + add-on)
- a maximum of 5 Media Gateways
- a maximum of 16 PRI cards
- a maximum of 200 ACD Agents
- 0 IP sets (no UniSTIM, no SipLine, no SipDect)
- 0 virtual trunks

Note: The CS 1000E TDM system does not support NRS.

CP PM Co-res CS and SS upgrade paths

CP PM Co-res CS and SS 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

  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

  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
- 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 to CS 1000 Release 6.0 CP PM Co-res CS and SS
- CS 1000 Release 4.5 or earlier CS 1000S Call Server to CS 1000 Release 6.0 CP PM Co-res CS and SS

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

NTM427CBE6 upgrade kit

The NTM427CBE6 CP PM Server Linux Upgrade kit includes the following items:

- NTDW6102E5 - CP PM Signaling Server Hard Drive kit (Linux OS preloaded)
- NTM42703 - 2 GB Compact Flash (CF) with Linux software, 2 GB blank CF
- NTDW6109E6 - 1 GB DDR SO-DIMM memory upgrade
- NTAK19ECE6 - CP PM Signaling Server 2 port SDI Cable assembly kit
- NTDU0606E6 - CP PM Signaling Server 25cm RJ45 Ethernet cable kit
- a DTE-DTE null modem cable (supplied)

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 GB 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 (FMD)

The CP PM card on a new CP PM Co-res CS and SS is shipped with a 40 GB internal hard disk FMD. For the CP PM Co-res CS and SS application to recognize that the FMD is a hard disk device (rather than a 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 (RMD)

The CP PM Co-res CS and SS supports two RMDs:

- CF card for installing Linux Base and CP PM Co-res CS and SS applications
- USB memory stick device, used to install CP PM Co-res CS and SS applications (cannot be used to install Linux Base)

  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).

Software applications

SIP Line Gateway and SIP DECT are not supported on CP PM Co-res CS and SS Server and require a separate Signaling Server.

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

- Linux Call Server
- 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 and Signaling Server (basic stand-alone CP PM Co-res CS and SS)
- Call Server and Signaling Server with NRS (CP PM Co-res CS and SS main with Branch Office support)

  Note: Support is available for SIP Line Gateway for SIP phones on a separate CP PM or COTS server.

High Availability (HA) support

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

IP Telephony Node Manager

This management interface includes the 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 *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Planning and engineering

Introduction

Complete all system engineering and planning activities before using this guide to install a CP PM Co-res CS and SS.

System parameter considerations

The CP PM Co-res CS and SS Call Server provides the same functionality as the existing VxWorks-based Call Server but with less capacity.

The CP PM Co-res CS and SS Signaling Server applications provide the same functionality as a CP PM or COTS Signaling Server that run one or more Signaling Server applications but with lower capacity.

Engineering of MG 1000E card placement and DSPs is the same as for a CS 1000E system. For details, see *Communication Server 1000E: Planning and Engineering* (NN43041-220).

When you plan an installation, consider the following information:

- The CP PM Co-res CS and SS is targeted for a CS 1000E, MG 1000B or MG 1000E Survivable Media Gateway (SMG) system with a capacity of up to 1000 IP (UniSTIM + Sip3 + SipN +SipDect) and 720 TDM users.
- The CP PM Co-res CS and SS supports up to 5 IP Media Gateways (IPMGs).
- The CP PM Co-res CS and SS supports up to 16 PRI (T1/E1) interfaces.
- The CP PM Co-res CS and SS supports up to 400 virtual trunks (split between H323 and SIP), 1000 PD users, up to 5 NRS endpoints and a total of 20 routing entries.

  Note: Converged Desktop: these numbers are targets for the CP PM Co-res CS and SS project, the actual numbers will be determined from Capacity testing.

Hardware requirements

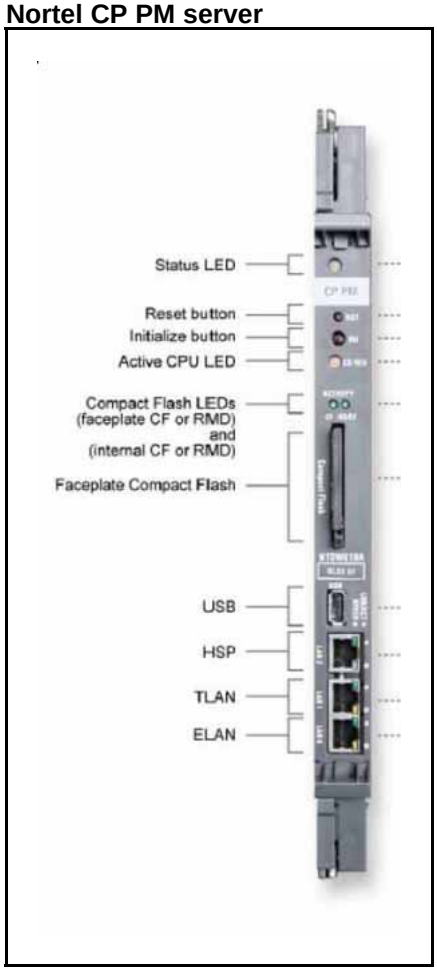
Nortel CP PM server

Note: CP PM Co-res CS and SS can only be installed on a NTDW61BAE5 CP PM server.

The Nortel NTDW61BAE5 CP PM server is a high performance server that can serve as both a stand alone or CoRes Call Server or Signaling Server in a CS 1000E system.

Figure 3 "Nortel CP PM server" (page 22) shows the faceplate of the NTDW61BAE5.

Figure 3
Nortel CP PM server



Features

The Nortel CP PM server provides the following features:

- Intel Pentium M processor (1.4 GHz)
- Fixed Media Device (FMD)
  - an internal hard drive (NTDW6102E5)
  - hosts all Call Server and Signaling Server software and applications
- Removable Media Device (RMD)
  - hot-pluggable Compact Flash (CF) card slot in the faceplate
  - used to back up and restore Call Server database
  - used for installing Nortel Linux Base
- 2 Gb of SDRAM
- One 1 GB/s Ethernet port (HSP)
  - not used when configured as a Signaling Server, not used in Co-resident CS and SS mode
- Two 100BaseT Ethernet ports
  - TLAN port to connect the server to a TLAN Layer 2 Ethernet switch port
  - ELAN port to connect the server to an ELAN Layer 2 Ethernet switch port
- Nortel NTDU0606E6 cabling kit
  - short length CAT5 cables to connect the Signaling Server to the TLAN/ELAN ports on a Media Gateway Card (MGC)
  - if the TLAN and ELAN Ethernet ports on the MGC are occupied, longer CAT5 cables are required (not supplied) to connect the Signaling Server directly to the TLAN and ELAN Ethernet switches
- Two serial ports
  - to connect a maintenance terminal to the server
- Nortel NTAK19EC cabling kit
  - to adapt the 50-pin MDF connector at the back of the CS 1000E Media Gateway or the CS 1000M Universal Equipment Module (UEM) to a 25-pin DB connector
  - a 25-pin to 9-pin straight-through serial cable (not supplied) is required to connect the 25-pin DB connector to a 9-pin serial port on the maintenance terminal

- One USB port
  - — used to backup and restore Linux Base and Application Data.
- A RST (Reset) button
  - — to cold-reboot the server
- An INI (Initialize) button
  - — to warm-reboot the Call Server application

Storage and memory

The CP PM Co-res CS and SS requires a minimum 40 GB hard drive and 2 GB of RAM.

Serial Data Interface (SDI)

The SDI ports of the CP PM platform are routed through the backplane of the shelf to the 50-pin MDF connector. The NTAK19EC cable adapts the 50-pin MDF to a 25-pin DB connector, to provide access to serial ports 0 and 1. A 25-pin null modem adapter is required to adapt the SDI port to a typical PC serial port.

The default TTY settings for port 0 are as follows:

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

LEDs

Two LEDs are on the faceplate of the CP PM card: the Status LED and the Active CPU LED. Use of the LEDs is described in Table 1 "Status LED for CP PM Co-res CS and SS " (page 24) and Table 2 "Active CPU LED for CP PM Co-res CS and SS" (page 25).

Table 1
Status LED for CP PM Co-res CS and SS

LED color	Description
Red	Hardware/BIOS
Yellow	Loading CP PM Co-res CS and SS applications

Green	CP PM Co-res CS and SS applications loaded and started successfully (Normal operation)
Off	No Power

Table 2
Active CPU LED for CP PM Co-res CS and SS

LED color	Description
Red	Single Core Call Server
Off	No Power

Note: The **`reboot`** or **`reboot -1`** Call Server PDT shell commands change the status LED to yellow. Upon reboot completion the Call Server application restarts and the status LED changes to green. Pushing the INI button on the CP PM faceplate also changes the status LED to yellow and then back to green.

CP PM BIOS requirements

The CP PM Co-res CS and SS requires CP PM BIOS Release 18 or later. To upgrade from CS 1000 Release 5.5 or earlier, see Procedure 2 "Automatically upgrading the CP PM BIOS with the Linux Base installer" (page 34).

Cabinet and Chassis support

Support exists for the CP PM Co-res CS and SS in the following chassis:

- Meridian 1 PBX 11C Cabinet (except for slot 0)
- Meridian 1 PBX 11C Chassis (except for slot 0 and slot 4 due to 48 port DLC)
- Meridian 1 PBX 11C Mini expander chassis
- MG 1000E main chassis (except for slot 0)
- MG 1000E expander chassis

Note: Slot 0 in the Meridian 1 PBX 11C Chassis or Cabinet main or expansion, Mini main, MG 1000E main chassis is reserved for the MGC.

The CP PM Co-res CS and SS is not supported in the following chassis:

- Large System IPE shelf
- 1U Call Server 1000S chassis due to power and card slot keying requirements

Ethernet port connections

The ELAN and TLAN ports on the CP PM Co-res CS and SS can be cabled by using the MGC (see Figure 4 "Cabling the CP PM Co-res CS and SS ELAN and TLAN ports by using the MGC" (page 26)).

Although the ELAN and TLAN ports connect directly to an external Layer 2 switch, Nortel recommends that you connect the ports to the MGC to provide ease of cabling and to take advantage of the dual-homing feature provided by the MGC.

Figure 4
Cabling the CP PM Co-res CS and SS ELAN and TLAN ports by using the MGC

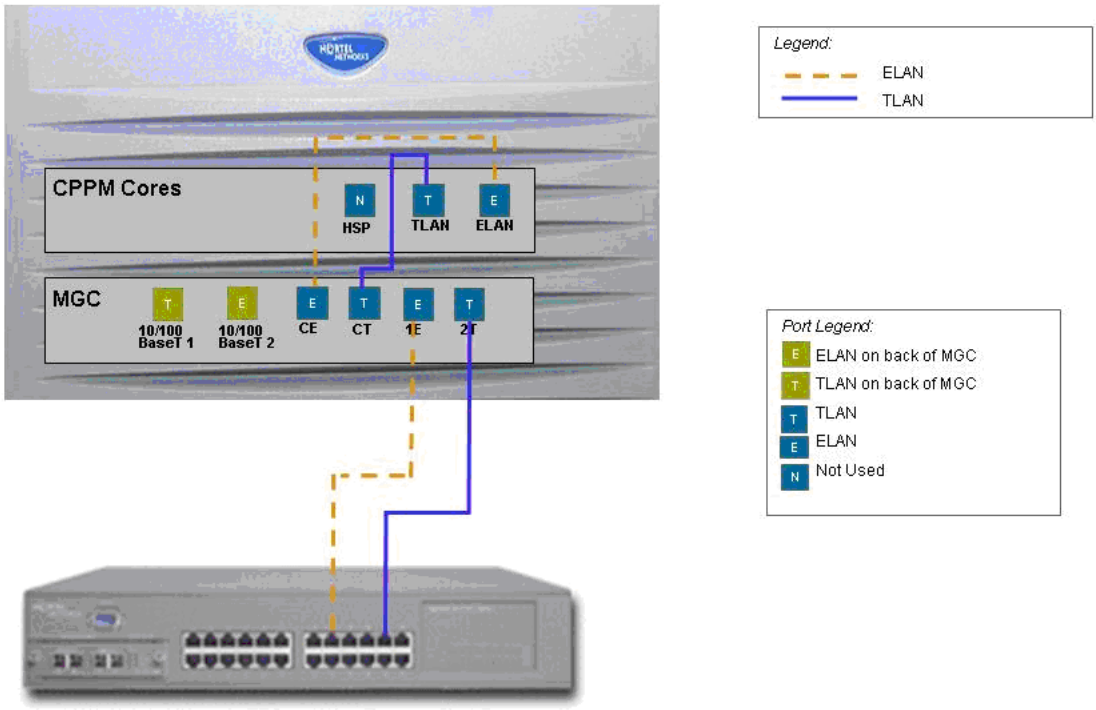
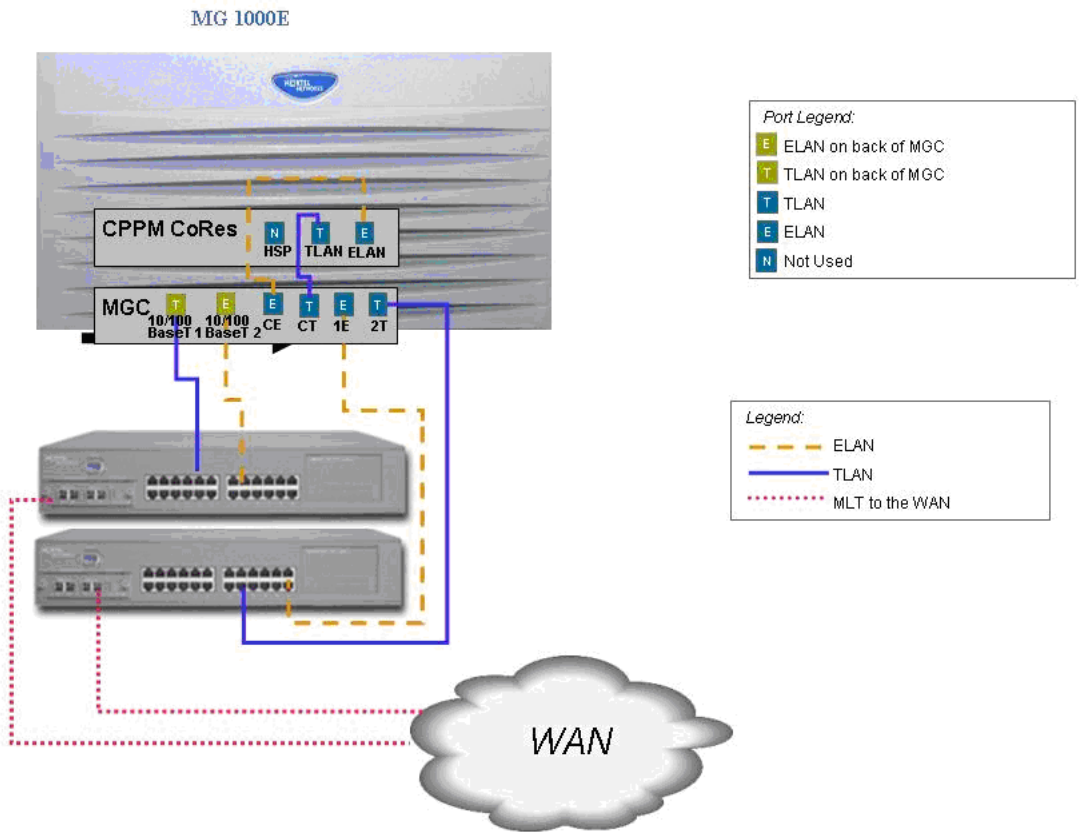


Figure 5 "Dual Homed ELAN and TLAN" (page 27) shows a CP PM Co-res CS and SS with dual-homed ELAN and TLAN ports. If one of the LAN links to the Layer 2 switch fails, or if the Layer 2 switch is out of service, the dual homing feature allows the CP PM Co-res CS and SS to continue

to function normally. In addition, using the Layer 2 switch MultiLink Trunking (MLT) feature provides redundancy and load sharing across the WAN.

Figure 5
Dual Homed ELAN and TLAN



WARNING
If the ELAN or TLAN ports (or both) are connected directly to a Layer 2 switch instead of the MGC CE or CT ports, autonegotiate must be set on the port settings on the Layer 2 switch to prevent Ethernet port duplex mismatching. Autonegotiation is enabled by default on the MGC CE and CT ports.

Routing Table configuration

The default gateway for a CP PM Co-res CS and SS server is the TLAN interface. To connect to any component in a different ELAN subnet, you must add a route to the CP PM Co-res CS and SS IP routing table.

The following are examples of scenario where route configuration is required:

- Geographic Redundancy (GR) system where the CP PM Co-res CS and SS server is the Primary Call Server (PCS), the Secondary Call Server (SCS) or the Survivable Media Gateway (SMG) and the PCS, SCS and the SMG are not in the same subnet.
- CS 1000E CP PM Co-res CS and SS system with distributed IPMGs This is a non-GR system with IPMGs that are in a different subnet than the CP PM Co-res CS and SS server.
- CS1000E CP PM Co-res CS and SS system where the Telephony Manager (TM) is in a different subnet than the CP PM Co-res CS and SS server.

CP PM Co-res CS and SS feature package requirements

No new feature packages are introduced for CP PM Co-res CS and SS. Table 3 "CS 1000E feature package requirements" (page 28), Table 4 "MG 1000B feature package requirements" (page 29), and Table 5 "MG 1000E SMG feature package requirements" (page 29) list the existing CS 1000 Call Server packages that are required for CP PM Co-res CS and SS.

Table 3
CS 1000E feature package requirements

Package mnemonic	Package number	Package description
SOFTSWITCH	402	Soft Switch Package
IPMG	403	IP Media Gateway Package
GRPRIM (optional, only required if an SMG is connected to the CP PM Co-res CS and SS system)	404	Geographic Redundancy Primary system
CPP_CNI	268	CP Pentium Backplane for Intel Machine
CORENET	299	CP Network

Table 4
MG 1000B feature package requirements

Package mnemonic	Package number	Package description
SOFTSWITCH	402	Soft Switch Package
IPMG	403	IP Media Gateway Package
CPP_CNI	268	CP Pentium Backplane for Intel Machine
CORENET	299	CP Network
BMG	390	Branch Office Package

Table 5
MG 1000E SMG feature package requirements

Package mnemonic	Package number	Package description
SOFTSWITCH	402	Soft Switch Package
IPMG	403	IP Media Gateway Package
CPP_CNI	268	CP Pentium Backplane for Intel Machine
CORENET	299	CP Network
GR_SEC	405	Geographic Redundancy

Table 6 "Disabled feature packages" (page 29)lists the packages that are disabled for CP PM Co-res CS and SS.

Table 6
Disabled feature packages

Package mnemonic	Package number	Package description
CPIO	298	Call Processor Input/Output (Option 81C)
FIBN	365	Fiber Network
HA	410	High Availability

CP PM Co-res CS and SS deployment configurations

The supported configurations for CP PM Co-res CS and SS are as follows:

- CS+SS
- CS+SS+EM
- CS+SS+EM+NRS
- CS+SS+EM+Subscriber Manager

Signaling Server deployment limitations

There are limitations when deploying other Signaling Servers with the CP PM Co-res CS and SS system:

- Installing a 2nd TPS (leader and follower) will not give true redundancy for the TPS. If the CoRes system itself fails, then the 2nd TPS has no place to register.
- Installing a CP PM Co-res CS and SS system means that the user has no redundancy on the Call Server or with the Signaling server applications. The only execption to this is the NRS.
- The following applications cannot be installed on the CP PM Co-res CS and SS system and must be installed on stand-alone signaling servers:
  - SLG (Sip Line)
  - Sip-Dect

System capacity

With the Call Server, Signaling Server, and System Management applications sharing the same hardware resources (CPU, memory, disk space), the CP PM Co-res CS and SS is targeted for a CS 1000E system with a capacity of up to:

- 1000 IP users (UniSTIM + SipN + Sip3 + SipDect), where (SipN + Sip3) <= 400
- 720 TDM sets
- 400 Virtual trunks
- 16 PRI spans
- 5 MG 1000E chassis
- maximum of 200 ACD agents
- 5 NRS endpoints with up to 20 total routing entries

An example system within the supported line size limit could contain 600 UniSTIM users, 300 SipLine (SipN) users and 100 SipDect users with a maximum 10,000 cph (total across Call Server and all Signaling Server applications, including NRS). For CPU usage calculations see *Communication Server 1000E: Planning and Engineering* (NN43041-220).

> ***Note:*** CPU usage or high call rates could limit the total number of supported sets for this system. If higher numbers of NRS endpoints, routing entries or call rates are required, then a stand-alone NRS is required. If higher numbers of sets, trunks, MG 1000Es, or a higher call rate is required, then a CS 1000E SA system is required.

SIP Line CP PM Co-res CS and SS requires a separate SIP Line server (either CP PM or COTS) and supports a maximum of 200 SIP Line users. Total IP user capacity is calculated using the following formula:

IP Users = UniSTIM + SipN + Sip3 + SipDect

Future growth considerations

You can upgrade a CP PM Co-res CS and SS- based system to a CS 1000E (VxWorks-based) SA with a stand-alone Signaling Server if the 1000 IP and 720 TDM users limit is exceeded. For details see *Communication Server 1000E Installation and Commissioning* (NN43041-310) and *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

IP address considerations

New systems

Prior to CS 1000 Release 6.0, System Management software communicated with the Call Server and Signaling server applications by using separate IP addresses with a common port number. In a CS 1000 Release 6.0 CP PM Co-res CS and SS system, the Call Server and Signaling Server applications share the same IP address, and System Management software is updated to account for the use of 2 port numbers.

This change is not backwards compatible. You cannot use Element Manager, in a pre-CS 1000 Release 6.0 system, to configure any Signaling Server.

Upgrades

When upgrading or migrating from a CS 1000E CP PM system or SSC-based Small System to a CP PM Co-res CS and SS, there are two options available for the ELAN IP address assignment:

- Assign the ELAN IP address of the Call Server from the originating system to the CP PM Co-res CS and SS. The IP Telephony node information must be updated on the Element Manager IP Telephony Nodes page in order for the Signaling Server applications to use the correct ELAN IP address. See *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).for details.
- Assign the ELAN IP of the Signaling Server from the originating system to the CP PM Co-res CS and SS. If upgrading from a CS 1000E CP PM system, all Call Server IP address fields in each MGC must be updated to reflect the new IP address. See *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).for details.

Installation and commissioning

Introduction

A CP PM Co-res CS and SS installation consists of two phases:

- Nortel Linux Base installation
- Application installation

Two separate installation media are provided. One contains the Linux Base image and the other contains the Call Server, Signaling Server, and system management application software.

Pre-installation checklist

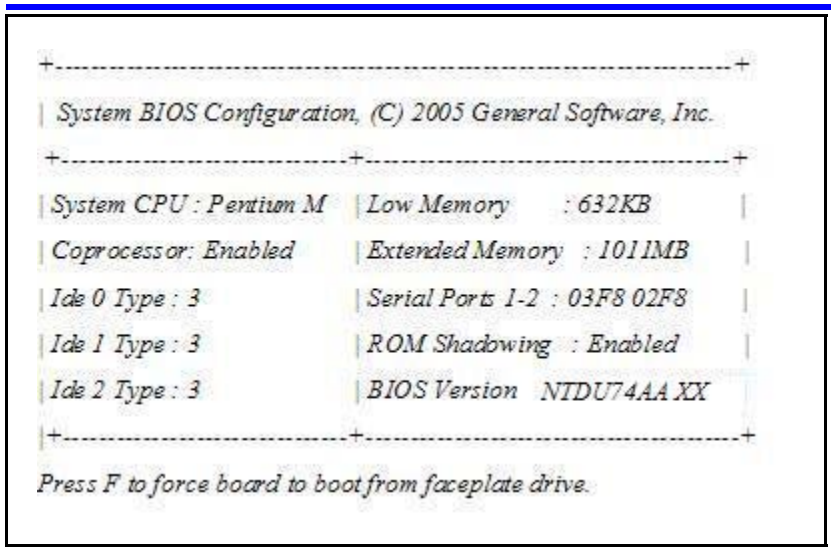
The CP PM Co-res CS and SS requires a CP PM hardware platform with a 40 GB hard drive and 2 GB of memory. The CP PM BIOS version must be Release 18 or later.

You must perform the following procedures before any installation to ensure CP PM hardware meet the preceding requirements.

> ***Note:*** The Call Server Overlay 135 **`stat mem`** command on a CP PM Co-res CS and SS does not show the actual physical memory size on the CP PM hardware. It displays the amount of memory that the Call Server application uses.

Procedure 1
Determining the CP PM BIOS version method 1

Step	Action
1	Power up the CP PM hardware.
2	Observe the CP PM BIOS version output from bootup screen.



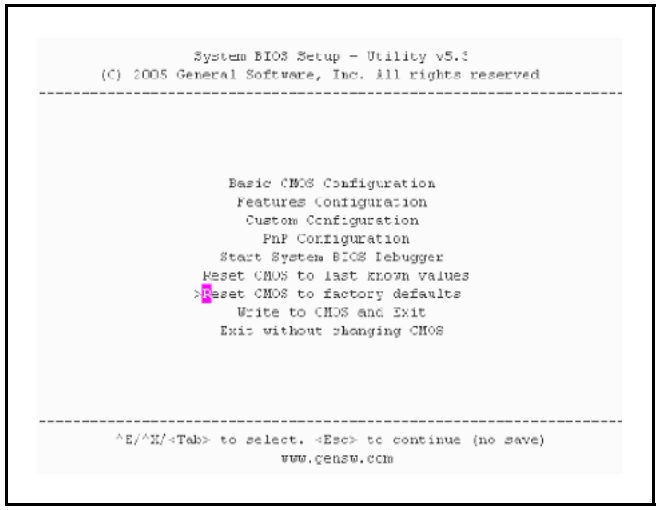
3 If the BIOS version is less than 18, complete Procedure 2 "Automatically upgrading the CP PM BIOS with the Linux Base installer" (page 34).

--End--

Procedure 2
Automatically upgrading the CP PM BIOS with the Linux Base installer

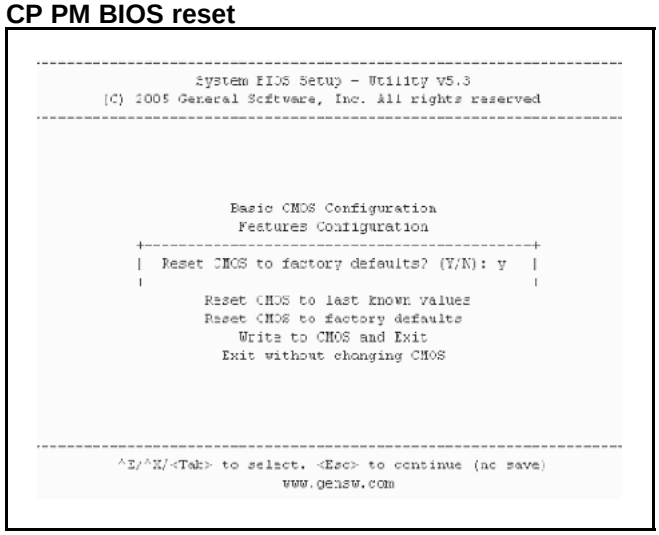
Step	Action
1	Connect to serial port 1 on the CP PM.
2	Insert the Linux Base installation CF card into the faceplate CF slot.
3	Power on the system.
4	During the reboot memory check, quickly press **CTRL C** to enter the CP PM BIOS.
5	Figure 6 "CP PM BIOS setup" (page 35) appears. Select **`Reset CMOS to factory defaults`** from the menu.

Figure 6
CP PM BIOS setup



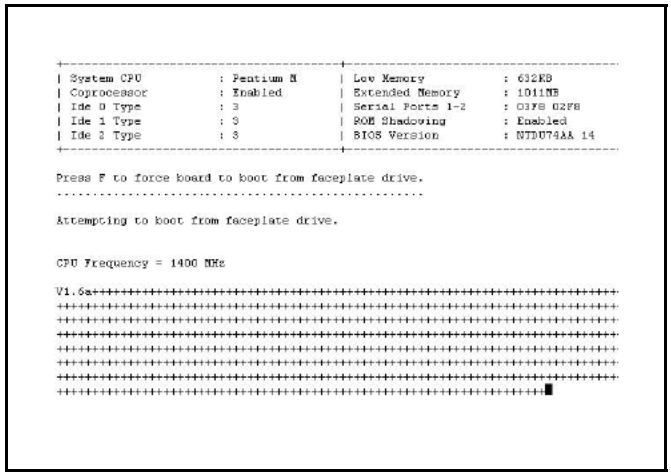
6 Figure 7 "CP PM BIOS reset" (page 35) appears. Press **y** to reset CMOS to factory defaults.

Figure 7
CP PM BIOS reset



7 Once the reboot and memory check completes, Figure 8 "CP PM faceplate drive boot" (page 36)appears. Press the **F** key to boot from the Linux Base installation faceplate CF card.

Figure 8
CP PM faceplate drive boot



8 The welcome screen appears. Press **ENTER** to direct the input and output to COM1.

9 Figure 9 "CP PM BIOS automatic upgrade" (page 37) appears if the CP PM card has a BIOS version less than 18. Press **y** to proceed with the automatic upgrade.

CAUTION
Do not interrupt the BIOS upgrade process. Damage to equipment may occur.

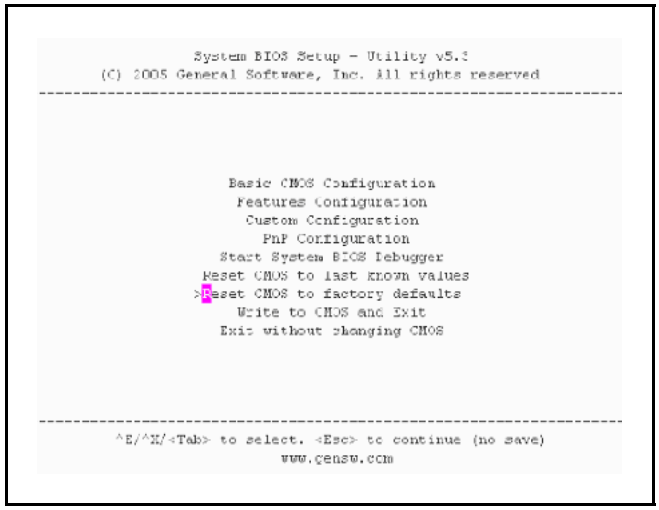
Figure 9
CP PM BIOS automatic upgrade

10 Verify that the BIOS upgrade is finished. Press **Enter** to reboot.

11 During the reboot memory check, quickly press **CTRL C** to enter the CP PM BIOS.

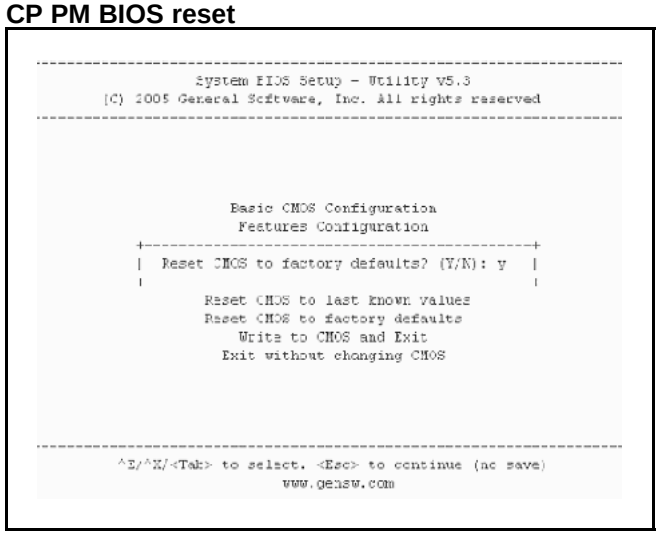
12 Figure 10 "CP PM BIOS setup" (page 38) appears. Select **`Reset CMOS to factory defaults`** from the menu.

Figure 10
CP PM BIOS setup



13 Figure 11 "CP PM BIOS reset" (page 38)appears. Press **y** to reset CMOS to factory defaults.

Figure 11
CP PM BIOS reset



14 The system reboots. Once the reboot is complete, the new BIOS version is displayed. Verify that the BIOS version is 18 or higher. You can now proceed with the Linux Base software installation.

--End--

Note: You must install the Nortel Linux Base before you complete the procedures described in the following sections.

Nortel Linux Base

Perform the Linux Base installation from the command line interface (CLI) using a bootable CF installation media card. Configure the ELAN, TLAN IP address, gateway, subnet masks, and date and time settings during the Linux Base installation.

For detailed information Linux Base installation information, see “Nortel Linux base installation” (page 63)

.

Note: Upon completion of the Linux base installation, the server must be configured as a primary, secondary or member server in the UCM security framework. This configuration is completed using the default Nortel userID and password when logging on to the Base Manager to perform the security configuration. For detailed information, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

CP PM Co-res CS and SS application installation

Note: The system must be a member of the UCM Security Domain before any applications can be installed. See *Unified Communications Management*(NN43001-116) for details.

Perform the application installation on the CP PM Co-res CS and SS (and stand-alone Linux-based CS 1000 servers) using the CS 1000 Software Deployment Manager, graphical user interface (GUI).

The Deployment Manager installs the Call Server, Signaling Server, and System Management applications as Linux Red Hat Package Manager (RPM) packages.

Deployment Manager access occurs through the Web-based CS 1000 UCM navigator.

The Deployment Manager can operate in two modes:

- Centralized Deployment Manager (Remote)

  the Deployment Manager runs on the UCM Primary Security Server. You must start the UCM navigator and log on to the UCM Primary Security Server. In this model, the Centralized Deployment Manager deploys application software to the target servers in the UCM security domain.

- Local Deployment Manager:

the Deployment Manager runs on the target server itself. Accessing the Deployment Manager is similar to the Centralized Deployment option except you must log on to the local target server by using the local Linux user ID and password
(ie: 'nortel'). This mode is typically used when you want to install software on the target server before it is configured to join the UCM security framework.

In both Centralized and Local modes, the application software Nortel Application Image (NAI) on the software delivery media is uploaded from the client workstation to the server where Deployment Manager runs:

- For the Centralized Deployment Manager, the application software image is transferred to the hard disk of the UCM primary security server.
- For the Local Deployment Manager, the application software image is transferred to the hard disk on the target server.

For details, see "Software loads" (page 81).

Note: For the Centralized Deployment Manager, you only need upload the application software once. You can then deploy the software image to multiple target servers in the UCM security domain.

The Deployment Manager supports new installation and upgrades. Both processes are similar but contain the following differences:

- For the upgrade, you cannot remove or add any new type of applications on the CP PM Co-res CS and SS, you must use the existing package configuration. The user can upgrade only the existing applications to a newer version.
- For the upgrade, existing data is backed up and restored when the new version of the application software is installed.

Note: If you change the package configuration, you must manually back up data on the target by using the **`sysbackup`** command before you use the Deployment Manager to install a new package configuration on the CP PM Co-res CS and SS.

For detailed information, see "Application installation using Deployment Manager" (page 76).

Call Server Keycode validation and pre-configuration

The Deployment Manager provides the following menus and pages specific to Call Server installation and deployment:

- Keycode Validation
- Call Server Database Selection
- Call Server PSDL Language Selection

Prior to deploying the application software to the CP PM Co-res CS and SS, the Deployment Manager performs the Call Server keycode validation to ensure that the keycode file used matches the software version and the security device on the target server. Table 7 "Keycode validation result " (page 41) describes the keycode validation results.

Table 7
Keycode validation result

Output message	Description	Action
The keycode file is validated successfully	Keycode validation passed.	Continue the installation.
File Access Error	Keycode file missing or cannot be read on target. The file transfer might not have succeeded.	Click on the Validate Keycode button again. If the problem persist, contact Nortel Support.
Software Release Error	Software version to install does not match version in keycode.	Make sure the keycode file matches the software version to be installed. Replace with the correct keycode file and Click the Validate Keycode button again.
Platform Error	Incorrect Keycode file: System Type in Keycode does not match actual platform.	Use correct keycode file for CP PM Co-res CS and SS Platform. Replace with the correct keycode file and Click on Validate Keycode button again.
Keycode Format Error	Keycode file is corrupt. The file transfer might not have succeeded.	Make sure you select the correct keycode file. Click on Validate Keycode button again. If problem persist, contact Nortel Support.

Dongle Error	Cannot detect Security Device. Device is missing or corrupted.	Make sure security device is inserted correctly. Re-seat the dongle device. Click on Validate Keycode button again. If problem persist, contact NT Support.
Keycode Validation Error	Keycode does not match Security Device.	Make sure the correct keycode file is selected. Make sure the correct dongle device is inserted. Click on Validate Keycode button again. If problem persist, contact NT Support.

You can use the Deployment Manager to select default, existing, or customer database. The existing database selection does not apply to new installations - only to upgrades. The customer database selection allows the user to upload a Call Server database that has been backed up using the LD 43 EDD command.

Note: After performing the LD 43 EDD command the CP PM Co-res CS and SS Call Server database is stored in the **`backup/single`** folder on the CF card. Click the browse tab and select the backup folder under the **`Customer Database`** option from Deployment Manager.

The Deployment Manager provides a menu to select the PSDL languages. The supported language sets are the same as those in CS 1000 Release 5.5.

For a detailed Deployment Manager keycode validation procedure, see .

Upgrades

Introduction

This section provides information on upgrading to a CS 1000 Release 6.0 CP PM Co-res CS and SS system.

Supported upgrade paths

For the Call Server application, the supported upgrade paths can be categorized as follows:

- migration from an SSC-based Small System. For details, see “Migration from an SSC-based small system” (page 47)
- upgrade from a CS 1000 Release 5.5 (or previous) CS 1000E CP PII, CP PIV or CP PM Call Server. For details, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315)
- upgrade from a CP PM Co-res CS and SS (application software version upgrade)

Hardware

- All CP PM Co-res CS and SS cards require a minimum 40 GB hard drive and 2 GB of memory.
- A CP PM Call Server running CS 1000 Release 5.5 or earlier requires an FMD of 1 GB.
- When upgrading from CS 1000 Release 5.X, the Call Server requires a 2 GB memory upgrade and an FMD replacement with a 40 GB hard drive. The Signaling Server requires a 2 GB memory upgrade.

  Note: When upgrading from a CS 1000 Release 5.x CP PM Call Server, the FMD CF card can be removed after installing the 40GB hard drive.

CP PM hard drive and memory upgrades

To perform a CP PM memory or hard drive upgrade, refer to *Circuit Card Reference* (NN43001-311).

CP PM Co-res CS and SS application software upgrade (6.0 to 6.x)

For the CP PM Co-res CS and SS application software upgrade, the following apply:

- You must use the existing package. You must use existing applications already installed on the CP PM Co-res CS and SS. When you perform an upgrade, the system does not allow you to install new packages.
- For the Call Server application:
  - — You require a keycode file for an upgrade.
  - — You can use the existing Call Server database or previously backed up (customer) database.
- Existing configuration data on the CP PM Co-res CS and SS is backed up, including all data for all applications installed on the CP PM Co-res CS and SS, not only the Call Server database. For centralized deployment, data is backed up to the centralized deployment server. For local deployment, data is backed up to a USB drive or to a remote SFTP server.
- The backed up data from the USB drive or remote SFTP server is restored on the CP PM Co-res CS and SS.

Backing up the CS 1000E CP PM Call Server database

Use existing backup and restore procedures to move the customer data from a CS 1000E CP PM Call Server to the new CS 1000E CP PM Co-res CS and SS. Back up the customer database to the RMD CF card by using the Overlay 43 EDD command.

Installing or upgrading the CP PM Co-res CS and SS using the CS 1000E CP PM Call Server database

Install the CS 1000E CP PM Call Server database on to the CP PM Co-res CS and SS by using the Deployment Manager. To deploy the Call Server application, the Deployment Manager provides a menu to select the default, existing or customer database. You must use the customer database selection, to allow the backed-up customer database on the RMD to be transferred to the CP PM Co-res CS and SS. For complete information, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Installing or upgrading the CP PM Co-res CS and SS without using the CS 1000E CP PM Call Server database

Complete the following procedure if the CP PM Co-res Call Server is upgraded or installed without using the CS 1000E CP PM Call Server database.

Procedure 3
Installing or upgrading the CP PM Co-res CS and SS without using the CS 1000E CP PM Call Server database

Step	Action
1	On the Call Server, leave the security domain. See *Security Management Fundamentals* (NN43001-604).
2	On the call server, enter LD 117 and disable secure transfer. See *Security Management Fundamentals* (NN43001-604).
3	On the Call Server, enter LD 143 and disable Centralized Software Download.
4	Perform a software upgrade or re-installation on the Call Server.
5	On the Call Server, enter LD 143 and perform a force upgrade on the MGC. ***Note:*** A transfer of account database error message and banner file are displayed on the end point terminal after the MGC reboots.
6	On the Call Server, join the security domain. See *Security Management Fundamentals* (NN43001-604).
7	On the Call Server, enter LD 117 and enable secure transfer. See *Security Management Fundamentals* (NN43001-604).
8	On the Call Server, perform a datadump to ensure SFTP is enabled using the updated token.
9	Check to ensure the account database and banner file is updated on the MGC.

--End--

Call Server installation support

Table 8 "VxWorks Call Server install program features not available for the CP PM Co-res CS and SS" (page 45) lists the features the Deployment Manager does not support in the VxWorks Call Server Installation program.

Table 8
VxWorks Call Server install program features not available for the CP PM Co-res CS and SS

Feature	CS 1000 Release 6.0 CP PM Co-res CS and SS Equivalent command	Notes
Main Menu Options:		--

Installing Call Server Database only	Call Server Overlay 43 RES command	--
Installing Call Server Keycode only	Call Server Overlay 143 KNEW command	--
Installing 3900 Set Languages	None	3900 Set Languages are installed as part of CP PM Co-res CS and SS Call Server Software and Database installation.
Configuring Centralized Software Upgrade options	Call Server Overlay 143 UPGMG command	Defaults to Centralized Software Upgrade enabled with sequential mode.
Tools Menu Options:		--
Set the system date and time	Linux Base datetimeconfig command	--
Partition the Fix Media Device	None	FMD should not be allowed to be repartitioned during application install. FMD is partitioned during Linux Base install.
Display the partition size of Fix Media Device	None	No longer required as all application directories reside in the same partition on Linux.
Reload default accounts	Linux Base Password reset	--
Print System S/W content on RMD	None	--
Print Keycode content	Call Server Overlay 143 KSHO	--
Print Security Device content	Call Server Overlay 137 SDID	--
Check the customer specific System S/W on the RMD	None	Feature no longer supported--not required.
Manually create Keycode on RMD.	None	Feature no longer supported--not required.
Install Keycode only.	Call Server Overlay 143 KNEW	--
Archive existing database	Call Server Overlay 43 EDD	--
Replace CPU board BIOS.	Linux Base BIOS upgrade command	--
Display media vendor information	Linux Base hdparm command	Feature no longer supported
Set the CP PM Core Location (Side/Loop/Shelf) Information.	Call Server Overlay 117 CHG LCL	--
Note: You can also configure the date and time in Element Manager. For details, see *Element Manager System Administration*.(NN43001-632).		

Migration from an SSC-based small system

Supported migration paths

Table 9 "Supported migration paths" (page 47)lists the supported migration paths from an SSC-based system to CP PM Co-res CS and SS-based CS 1000E system.

Table 9
Supported migration paths

CS 1000 Release 5.5 or earlier	CS 1000 Release 6.0 System
Option 11C Small System	CS 1000E CP PM Co-res CS and SS
CS 1000M Small System Cabinet	CS 1000E CP PM Co-res CS and SS
CS 1000M Small System Chassis	CS 1000E CP PM Co-res CS and SS
CS 1000S Small System	CS 1000E CP PM Co-res CS and SS

Note: The minimum software release supported for SSC migration is Release 23.10.

Backing up the Small System Call Server to an external drive

Note: For your convenience, the procedures required to back up the system database prior to the hardware upgrade are contained in this NTP.

The CP PM Co-res CS and SS Call Server supports converting the databases saved on the CS 1000 small system through the following methods:

- LD 43 EDD
- LD 143 archive database option (invoked from upgrade menus)
- LD 43 BKO

Note: The Customer Configuration Backup and Restore (CCBR) method of database backup is not supported for small system to large system database conversion.

By combining the EDD and archive methods, the database files are saved onto a Compact Flash (CF) card (with a PCMCIA card adapter when plugged into the SSC card) so that it can be inserted into the CP PM card during software deployment to perform the database conversion. LD 43 EDD updates the database on the internal drive (to ensure that the latest memory contents are backed up) and LD 143 backs up the database to the backup RMD (128 MB). Failure to perform a recent LD 43 (EDD) may result in the loss of any recent changes to the database.

Note 1: An alternative to the Archive command in LD 143 is the BKO command in LD 43. However; the Archive in LD 143 is the recommended method as it allows for multiple databases to be copied to the RMD. As a result, there is less risk of overwriting existing files using LD 143 to archive the database.

Note 2: You can upload the backup file from the UCM Client PC to the new CP PM Co-res CS and SS during the deployment.
There are 2 methods to provide a database to the CP PM Co-res CS and SS during software deployment, via the CP PM RMD or via the client machine.

There is a fundamental difference between the small system, running an SSC, and a CP PM Co-res CS and SS system. This difference is represented in how the format of the TN (Terminal Number) is displayed.

The small system TN is displayed to the administrator using a two-field format, or card-unit. In a CP PM Co-res CS and SS system, the TN is displayed using a four-field format, or loop-shelf-card-unit. This four-field TN format is the same as those used in current large systems.

The end result is that when a small system database is converted to a large system database, the TNs are re-mapped. The result is that the displayed TN changes during the conversion process. The administrator must be aware of the TN mapping. For example, a small system with an IP phone configured in TN 61-0 now has that same IP phone show up in 96-0-1-0 after the conversion process. For details, see *Communication Server 1000E Software Upgrades*.(NN43041-458).

LD 43 using EDD command

Procedure 4
Backing up the database using LD 43

Step	Action
1	To back up the customer database to the internal drive (to ensure the most recent database is copied to the backup RMD in LD 143), enter LD 43 at the command prompt.

2	Enter EDD. The following output is generated.
	`>`
	`LD 43`
	`EDD`
	`EDD000`
	`Backing up reten.bkp`
	`Internal backup complete`
	`All files are backed up!`
	`DATADUMP COMPLETE`
	`.`
	`EDD000`

3	The internal backup is complete.

--End--

LD 143 using the UPGRADE command

The second step involved in backing up the database involves moving the database from the hard drive to the RMD. This step is performed through the Utilities menu in LD 143.

Procedure 5
Archiving the database in LD 143

Step	Action

1	Insert the PCMCIA card in the card slot A. Enter LD 143 at the command prompt, then enter UPGRADE. The following screen appears.
	`SOFTWARE INSTALLATION PROGRAM **********`
	`**********`
	`Verify Security ID: XXXXXX`
	`**********`

2	The following menu appears. Enter 2 to select Call Server/Main Cabinet/Chassis.

```
Technology Software Installation Main Menu:
1.  Media Gateway/IPExpansion Cabinet
2.  Call Server/Main Cabinet
[q]uit, [h]elp or [?], <cr> - redisplay
Enter Selection :  2
```

The Call Server/Main Cabinet/Chassis Software Installation Main Menu appears. Enter 3 to select Utilities.

```
Call Server/Main Cabinet Software Installation Main Menu
:
1.  New Install or Upgrade from Option 11/11E - From
Software DaughterBoard
2.  System Upgrade
3.  Utilities
4.  New System Installation - From Software Delivery Card
[q]uit, [h]elp or [?], <cr> - redisplay
Enter Selection :  3
```

3 The Utilities menu appears. Enter 2 to select Archive Database Utilities.

```
Utilities Menu :
1.  Restore Backed Up Database
2.  Archive Database Utilities
3.  Install Archived Database
4.  Review Upgrade Information
5.  Clear Upgrade Information
6.  Flash Boot ROM Utilities
7.  Current Installation Summary
8.  Change 3900 series set languages.
9.  IP FPGA Utilities
[q]uit, [h]elp or [?], <cr> - redisplay
Enter Selection :  2
```

4 At the Customer Database Archives menu, enter 3 to select Archive a customer database.

```
Customer Database Archives:
1.  List customer databases.
2.  Remove customer database.
3.  Archive a customer database.
[q]uit, [h]elp or [?], <cr> - redisplay
Enter Selection :  3
```

5 At this point, you are prompted for a Customer name for your archived database. In this example, the name CS1000SU is entered as the Customer name.

```
Enter a Customer name for your customized data :
CS1000SU
Customer database created:  CS1000SU
Copying database from primary drive to CS1000SU
Archive copy completed.
```

6 The archive copy has been saved as CS1000SU. The Customer Database Archives menu appears. Enter 1 to select List customer databases.

```
Customer Database Archives:
1.  List customer databases.
2.  Remove customer database.
3.  Archive a customer database.
[q]uit, [h]elp or [?], <cr> - redisplay
Enter Selection :  1
```

The following list is generated:

```
Customer Database Archives available:
1.  450WBASE
2.  450W_CP
3.  CS1000SU
```

7 Enter q to quit LD 143, and then y to confirm your selection.

```
Customer Database Archives:
1.  List customer databases.
2.  Remove customer database.
3.  Archive a customer database.
[q]uit, [h]elp or [?], <cr> - redisplay
Enter Selection :  Q
Are you sure?  (y/n/[a]bort) :  Y
```

--End--

Once you have completed the backup and archive of the customer database, shut down the system and remove the PCMCIA card from slot. You are now ready to install the hardware.

Choosing the cabinet or chassis and slot locations

An MG 1000E performs functions under the control of the CS 1000E Core call server. Traditionally, this core call server was a CP II or CP IV in its own call server cabinet or chassis; however, the CP PM card sits in one of the MG 1000E Cabinet slots. Slot location is based on the type of system:

- For Cabinet systems, refer to “Cabinet” (page 52)
- For Chassis systems, refer to “Chassis” (page 53)
- For Communication Server 1000S systems, refer to “Communication Server 1000S” (page 55)

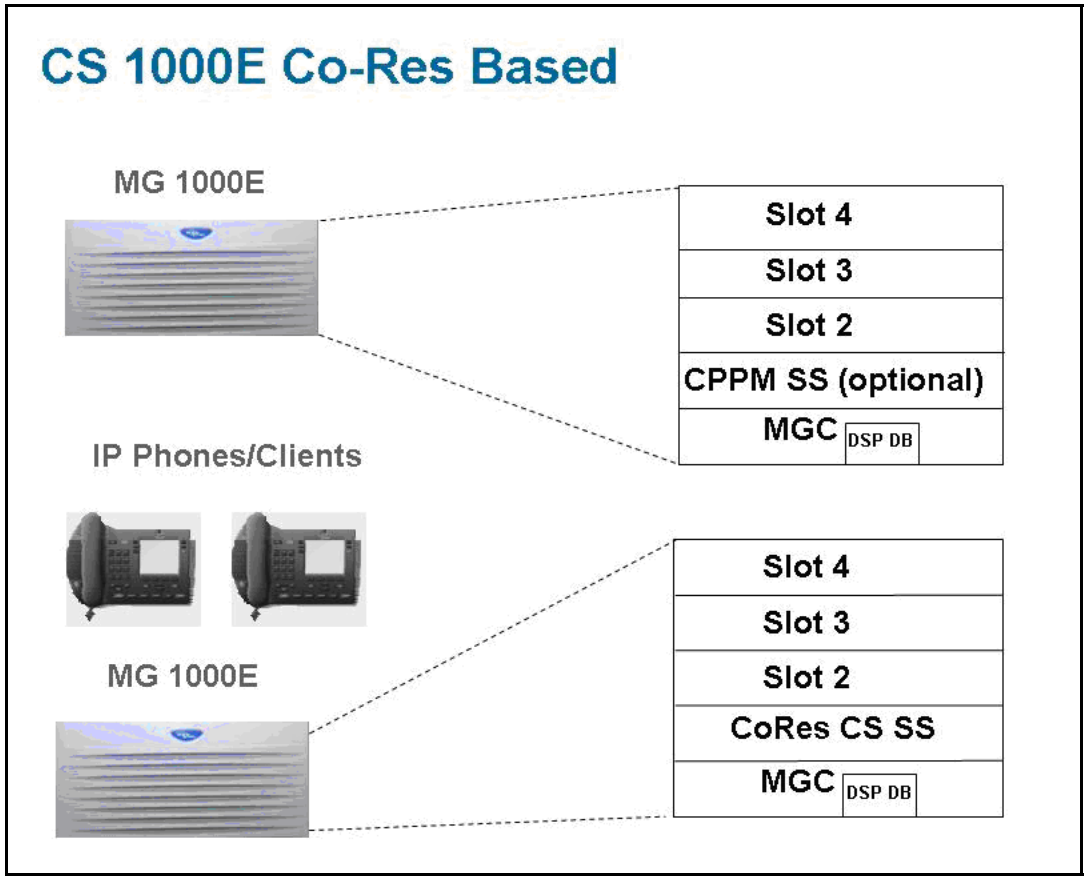
Cabinet

The CP PM card drives the MG 1000E through the MGC ELAN interface and therefore only uses the backplane for power. The following rules apply to the preferential placement of the CP PM card in the MG 1000E:

- The CP PM card cannot be placed in slot 0 of any MG 1000E. Slot 0 is reserved for the MGC.
- To allow for ease of cabling, the CP PM card may be placed in slots 1 through 10. The CP PM Signaling Server may be placed in slots 1 through 10 (see Figure 12 "CP PM Co-res CS and SS system" (page 53)) or in another cabinet if necessary.

Once the upgrade is complete, the CP PM Co-Res CS and SS system will have an MGC in slot 0 and a CP PM card in the main cabinet. The additional Media Gateways will contain MGCs, IPE cards, or another CP PM card running stand alone Signaling Server applications.

Figure 12
CP PM Co-res CS and SS system



To proceed with the upgrade, proceed to "Hardware Upgrade Task Overview" (page 56).

Chassis

The CP PM card drives the MG 1000E through the MGC ELAN interface and therefore only uses the backplane for power. The following rules apply to the preferential placement of the CP PM card in the MG 1000E:

- The CP PM card cannot be placed in slot 0 of any MG 1000E. Slot 0 is reserved for the MGC.
- To allow for ease of cabling, the CP PM card may be placed in slots 1 through 4 of the chassis, with the exception of the Option 11C Mini. The Option 11C Mini cannot have a CP PM card installed in slot 4 as this slot was originally allocated for the 48 port DLC only.

Figure 13 " Option 11C or Communication Server 1000M Chassis call server" (page 54) shows an existing Option 11C or Communication Server 1000M Chassis call server with the SSC card. Once the upgrade is complete, a CP PM Co-res CS and SS Chassis system will resemble Figure 14 "CP PM Co-res CS and SS system" (page 54) with an MGC in

slot 0, and a CP PM call server and signaling server in the main chassis. The additional media gateways would then contain MGC cards only for an CP PM Co-res CS and SS configuration. Additional Media Gateways can contain other IPE cards or a CP PM Server running standalone Signaling Server applications.

Figure 13
Option 11C or Communication Server 1000M Chassis call server

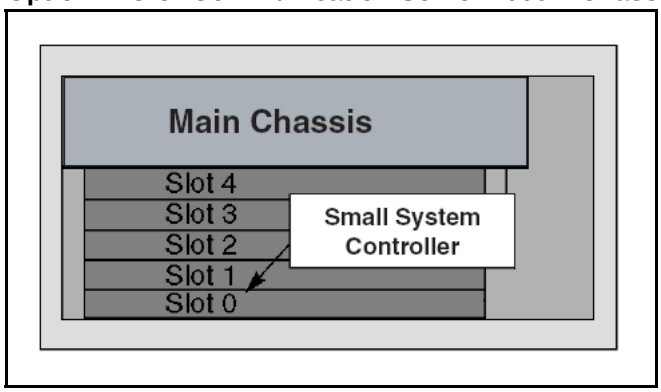
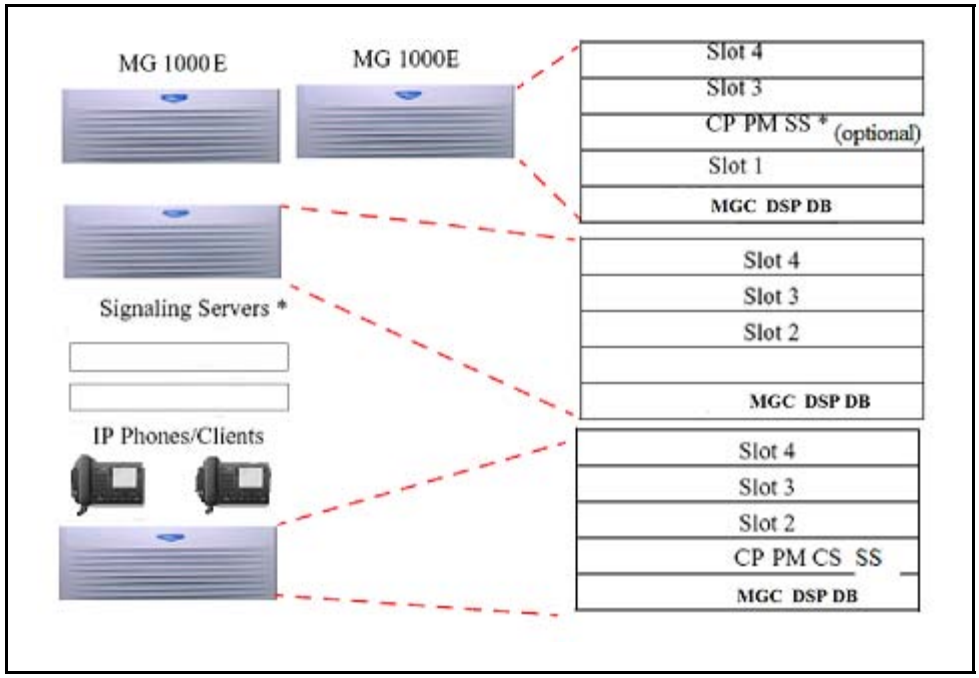


Figure 14
CP PM Co-res CS and SS system



*—Signaling Server may be one of the following:

- Nortel CP PM Signaling Server
- Dell R300 Commercial off-the-shelf (COTS) Signaling Server
- HP DL320 G4 COTS Signaling Server

- IBM x306m COTS Signaling Server
- IBM x3350 COTS Signaling Server

To proceed with the upgrade, proceed to “Hardware Upgrade Task Overview” (page 56).

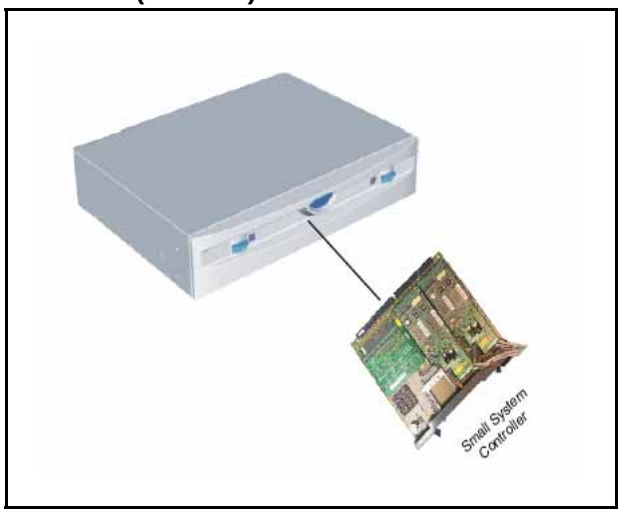
Communication Server 1000S

The CP PM card drives the MG 1000E through the MGC ELAN interface and therefore only uses the backplane for power. The following rules apply to the preferential placement of the CP PM call server in the MG 1000E:

- The CP PM card cannot be placed in slot 0 of any MG 1000E. Slot 0 is reserved for the MGC.
- To allow for ease of cabling, the CP PM card may be placed in slots 1 through 4 of the chassis, with the exception of the Option 11C Mini. The Option 11C Mini cannot have a CP PM card installed in slot 4 as this slot was originally allocated for the 48 port DLC only.

Figure 15 "CS 1000S (NTDU30) call server" (page 55) shows an existing CS 1000S Call Server with the SSC card. Once the upgrade is complete, a typical CP PM Co-res CS and SS Chassis system will resemble Figure 12 "CP PM Co-res CS and SS system" (page 53) with an MGC in slot 0, and a CP PM call server and signaling server in the MG1000E chassis. The additional media gateways would then contain MGC cards only for a CP PM Co-res CS and SS configuration. Additional Media Gateways can contain other IPE cards or a CP PM Server running standalone Signaling Server applications.

Figure 15
CS 1000S (NTDU30) call server



Hardware Upgrade Task Overview

To install the hardware for a Small System upgrade, perform the following steps:

- Power down the Main Cabinet or Chassis.
- Remove the SSC card as described in Procedure 6 “Removing the SSC card” (page 56).
- Install the DSP Daughterboard on the MGC card. See Procedure 7 “Installing a DSP Daughterboard” (page 58)
- Install the MGC card as described in Procedure 8 “Installing the MGC card” (page 59).
- Install the CP PM as described in Procedure 9 “Installing the CP PM card” (page 60).
- Cable the cards as shown in “Cabling the cards” (page 61).
- Power up the MG 1000E.
- Enter the ‘mgcsetup’ menu and configure the IP parameters. For details, see *Communication Server 1000E Installation and Commissioning* (NN43041-310)

  .
- Reboot the MGC

Installing the cards

The following sections describe the process required to install the MGC and CP PM cards.

Removing the SSC card

Procedure 6
Removing the SSC card

Step	Action
1	Power down the system.
2	Unlatch the SSC card.
3	Remove the SSC card from its slot.

--End--

ATTENTION
The SSC card and dongle should be preserved for a minimum of five days. It is illegal to continue to run the system software on the existing SSC card. Please DESTROY or RETURN the SSC dongle to your local Nortel Repairs/Returns center upon confirmation of a successful upgrade. No further orders will be accepted for the serial number since it will be decommissioned and tracked in Nortel's database. If the upgrade fails, you will not be able to revert back to the old system without the SSC card and dongle.

Installing a DSP Daughterboard onto an MGC card

Table 10 "DSP Daughterboard configurations" (page 57) lists the configuration options for Position 1 and 2.

Table 10
DSP Daughterboard configurations

Position 1 (DB1)	Position 2 (DB2)
NTDW62 DB32 (card slot 11)	None
None	NTDW62 DB32 (card slot 0)
NTDW62 DB32 (card slot 11)	NTDW62 DB32 (card slot 0)
NTDW64 DB96 (card slot 11, 12, & 13)	None
NTDW64 DB96 (card slot 11, 12, & 13)	NTDW62 DB32 (card slot 0)
Only the High Density PRI gateway can support two 96 port DSP daughter boards	

ATTENTION
Due to historical TN mapping for the Call Server software, even though the DSP channels will occupy Card 0 in the MG 1000Es, the TN (l s c u) 000 0 00 00 (ie unit 0 of card 0 in the first IPMG <supl sh> = 000 0) is not available.

A single channel (unit 0) is not available on the first IPMG ONLY if there is a 32 port DB installed in daughterboard position #2. If there is a 96 port DB installed in daughterboard position #1, all 96 channels are available. If there is a 32 port DB installed in daughterboard position #1, all 32 channels are available.

The following procedure describes how to install a DSP Daughterboard on an MGC card. See Figure 16 "DSP Daughterboard" (page 58).

Figure 16
DSP Daughterboard

Procedure 7
Installing a DSP Daughterboard

Step	Action
1	Place the MGC on a safe ESD surface.
2	Place the DSP DB in either DB position 1 (for DSP DB-32 or DSP DB-96) or DB position 2 (for DSP DB-32).
3	Ensure the DSP DB is securely attached to the MGC. (using supplied screws).

--End--

Installing the MGC card

To perform initial configuration of the MGC you need to connect via the MGC serial port. The 3-port SDI cable (NTBK48AA) is connected to the SDI (RS-232) port on the Chassis

Table 11 "MGC Serial Port Capabilities" (page 59) lists MGC Serial Port Capabilities.

Table 11
MGC Serial Port Capabilities

Port	Modem Support?	Used for initial Configuration?
SD10	Yes (requires null modem to connect to a TTY)	Yes
SD11	No (No hardware flow control)	No. Port 1 is not enabled during the initial configuration of the MGC.
SD12	No (No hardware flow control)	No. (Only available after FPGA is enabled. Not available during initial configuration menu display)

Procedure 8
Installing the MGC card

Step	Action
1	Insert the MGC into Slot 0 of the cabinet or chassis. The existing 3-port SDI cable (NTBK48AA) is reused. It connects to the SDI port on the cabinet or chassis.
2	This cabinet or chassis, the main cabinet or chassis in the system, is now known as IPMG 00.

--End--

ATTENTION
Please DESTROY or RETURN the SSC dongle to your local Nortel Repairs/Returns center upon confirmation of a successful upgrade. If the SSC system was using remote dongles for any expansion cabinets, please DESTROY or RETURN to your local Nortel Repairs/Returns center upon confirmation of a successful upgrade. If the upgrade fails, you will not be able to revert back to the old system without the SSC card and dongle. For the CP PM Card, you must use the dongle provided with the software kit. Chassis Expander dongles may be disposed of, as they are no longer needed.

Installing the CP PM card

The following procedure describes how to install the CP PM card in a Cabinet or Chassis.

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

The NTM427CBE6 CP PM Server Linux Upgrade kit includes the following items:

- NTDW6102E5 - CP PM Signaling Server Hard Drive kit (Linux OS preloaded)
- NTM42703 - 2 GB Compact Flash (CF) with Linux software, 2 GB blank CF
- NTDW6109E6 - 1 GB DDR SO-DIMM memory upgrade
- NTAK19ECE6 - CP PM Signaling Server 2 port SDI Cable assembly kit
- NTDU0606E6 - CP PM Signaling Server 25cm RJ45 Ethernet cable kit
- a DTE-DTE null modem cable (supplied)

Note: Save the packaging container and packing materials in case you must ship the product

Procedure 9
Installing the CP PM card

Step	Action
1	Ensure that the security dongle (the one that comes as part of the software kit) is inserted on the CP PM call processor. ***Note 1:*** This first step is applicable only when the CP PM card is used as a Call Server. ***Note 2:*** Remove the retainer clip from the FMD slot when the card is used as a Signaling Server. The clip must be removed to prevent it from shorting out adjacent cards.
2	Set switch S5 on the CP PM card to position 2.
3	Insert the 40 GB internal hard disk FMD.
4	Slide the CP PM call processor into Slot 1 (or higher) of the cabinet or chassis.
5	.Lock the card into the faceplate latches.
6	Attach the 2-port SDI cable (see Figure 17 "2-port SDI cable (NTAK19EC) cable" (page 61). The 50-pin Amphenol NTAK19EC connects to the back of the CP PM call server.

Figure 17
2-port SDI cable (NTAK19EC) cable

Note: To connect a terminal to the CP PM card, complete the following steps:

- ***Connect the NTAK19EC cable (shipped with the CP PM Signaling Server) to the 50 pin MDF connector on the back of the desired shelf of the IPMG.***
- ***Connect a 25 pin to 9 pin straight through serial cable to the 25 pin DB connector at the end of the NTAK19EC cable (a female to female gender changer may be required). These are customer provided.***
- ***Connect the other end of the 25 pin to 9 pin straight through serial cable to the serial port on the maintenance terminal. These are customer provided.***

--End--

The preceding procedures enable users to upgrade the system one MG 1000E at a time. For each additional IPMG, repeat Procedure 6 “Removing the SSC card” (page 56) to Procedure 8 “Installing the MGC card” (page 59).

.

Cabling the cards

The following sections describe the process required to cable the MGC and CP PM cards.

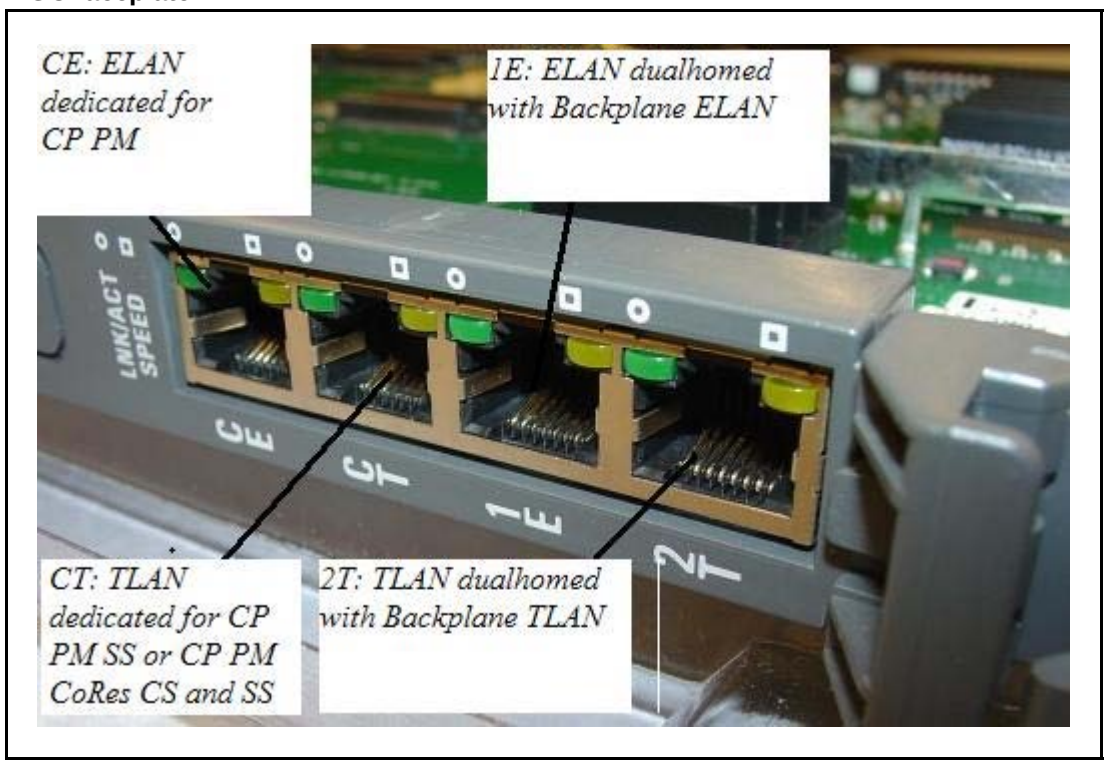
Cabling the MGC

The existing 3-port SDI cable (NTBK48AA) is reused. It connects to the SDI port on the cabinet or chassis. Figure 25 on page 107 shows the front of the MGC. The CE and CT ports are reserved for the CP PM card only. The CE connects to the ELAN port of the call server, while the CT connects to the TLAN port of the call server. The 1E and 2T ports must be attached to the external layer 2 switch that is dedicated to ELAN and/or TLAN traffic for the system.

MGC Ethernet Capabilities

An MGC features six Ethernet interfaces set to autonegotiate by default: four on the faceplate (see Figure 18 "MGC faceplate" (page 62)), and two on the expansion box connector using the breakout adaptor.

Figure 18
MGC faceplate



Cabling the CP PM card

The COM (SDI) port of the CP PM card is routed through the backplane of the shelf to the 50-pin Amphinol connector on the back of the shelf. A special cable is shipped with the CP PM card that adapts the 50-pin Amphinol to a 25-pin DB connector (NTAK19EC). Port 0 is used for maintenance access, and Port 1 is for an external modem connection.

Connect the ELAN of the CP PM card to the CE port of the MGC card or to the VLAN of the external layer 2 switch that is dedicated to ELAN traffic for the system. See Figure 3 "Nortel CP PM server" (page 22).

Nortel Linux base installation

Nortel Communication Server 1000 (CS 1000) Linux base introduces a two-stage installation procedure. The operating system is installed, and the applications are then deployed via UCM Deployment Manager after the Nortel Linux Base server joins the Primary UCM Security Domain. See “Application installation using Deployment Manager” (page 76).

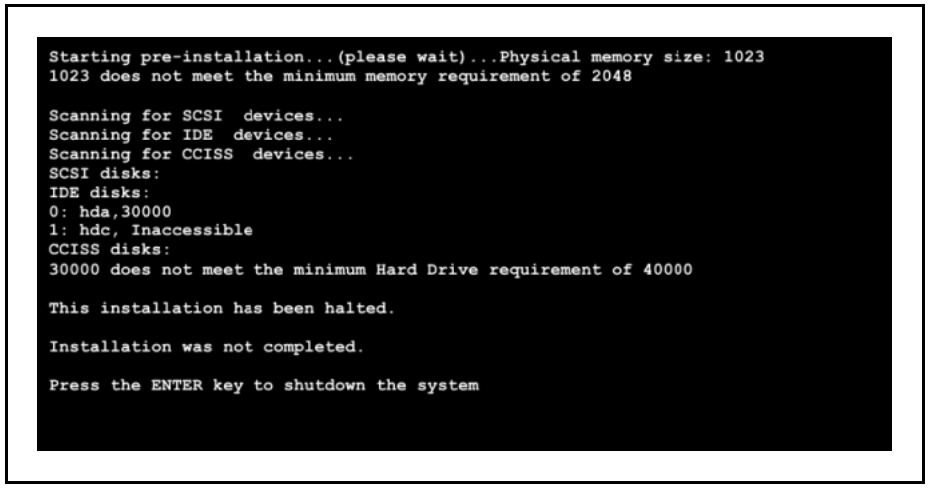
Each Linux server platform requires an installation of the base-level software. You start the installation from bootable installation media. The process includes the partitioning of hard disk drives, installation of the Linux kernel and the Linux root file system, associated device drivers, base system commands and utilities, and base applications. The process ends with a fully functional Nortel Linux base server.

Prerequisites

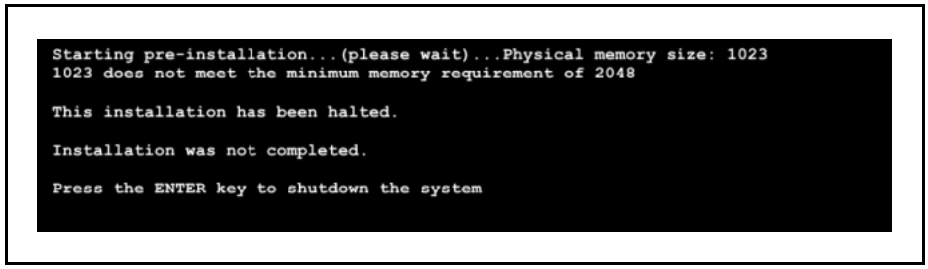
The server must meet the following requirements:

- The hard drive size must be at least 40 GB.
- There must be at least 2 GB of available memory.
- The CP PM BIOS must be Release 18 or higher.

If the hard drive is less than 40 GB, the following screen appears:



If there is less than 1 GB of memory available, the following screen appears:



If the platform does not meet the hard drive and memory requirements, the Linux base installation fails and the server returns to the previous state.

The compact flash card used for installation on a CP PM server must have a capacity of at least 1 GByte.

Before you install the Linux base you must complete the following tasks:

- Gather the following necessary customer information:
  - ELAN IP address
  - ELAN gateway IP address
  - ELAN netmask
  - The host name associated with the TLAN
  - The domain name

    Note 1: A Fully Qualified Domain Name (FQDN) consists of a host name and a domain name, and includes a top-level domain name. Using kwei.ca.nortel.com as an example, kwei is the host name, ca.nortel.com is the domain name, and .com is the top-level domain name. The FQDN must contain at least three fields separated by dots. If using an external DNS server, it is recommended to ping the FQDN to ensure that the DNS server is resolving your FQDN to the expected IP address.

    Note 2: If you are using a DNS server to resolve the FQDN to an IP address, ensure that prior to the installation of the Linux server that you can resolve the FQDN to the expected IP address. For example, attempt to ping the FQDN from a PC that uses the external DNS server, and it should resolve to the expected IP address.
  - TLAN IP address
  - TLAN gateway IP address
  - TLAN netmask
  - Timezone
  - IP address of the Primary Domain Name Service (DNS) server
  - Default system gateway associated with the network interface (ELAN or TLAN)

Note 1: The choice of ELAN or TLAN as the default gateway NIC can be influenced by the applications that you are going to deploy on the server and by network topology.

Note 2: The ELAN and TLAN ports on the CP PM CoRes CS and SS can be cabled via the Media Gateway Controller (MGC). Even though the ELAN and the TLAN ports can be connected directly to an external Layer 2 switch, it is recommended that the ports be connected to the MGC to provide ease of cabling and to take advantage of the dual-homing feature provided by the MGC.

Note 3: The CLI command **`routeconfig`** can be used to add routing entries. The choice of routing entries will depend upon the network topology and application deployment. For a list of Nortel Linux base CLI commands see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Additional Equipment

You may require the following additional equipment, depending on the installation options that you select.

- **PC**

  you can use a PC for the following installation tasks:

  — Run a program such as Putty to connect to the Linux server COM1 port. Use of the COM1 port is mandatory for installations on a CP PM server, and optional for installations on a COTS server.

  — Configure UCM primary, backup, and member servers.

  — Create a bootable compact flash card for installations on a CP PM server.

  — Launch Deployment Manager using a web browser to deploy Nortel deployment packages.

- **Keyboard, video card, and monitor (KVM)**

  KVM can be used for COTS server Linux base installation and password recovery.

  Note 1: KVM is no longer mandatory for password recovery; Linux base also supports COM port password recovery.

  Note 2: If you connect to the IBM x3350 server with a terminal for setup, the server does not function with the serial cable that was previously shipped with the ISP 1100 or other COTS platforms. The IBM x3350 server requires the new NTRX26NPE6 9 pin female to 9 pin female null modem cable. The NTRX26NPE6 9

pin female to 9 pin female null modem cable is displayed in Figure 19 "NTRX26NPE6 9 pin female to 9 pin female null modem cable" (page 66).

Figure 19
NTRX26NPE6 9 pin female to 9 pin female null modem cable

Installing the Linux base on a CP PM server

ATTENTION
This procedure documents the installation of Nortel Linux base on a CP PM server with no previous Nortel Linux base installation. If a Nortel Linux base installation exists on the server and you are upgrading to a newer Nortel Linux base version, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

ATTENTION
Before installing the Linux base, read all of the documentation provided by the server manufacturer.

WARNING
If you are installing Linux base on a CP-PM card and the CP PM card is currently running Signaling Server software from VxWorks, you must either press the faceplate reset button or reseat the card before you begin the Linux base installation. Failure to do so results in a watchdog reset during installation. This scenario occurs when you issue a reboot -1 from the pdt shell and then proceed directly to the Linux base installation. Reset the card using the faceplate button to disable the hardware watchdog and allow the installation to complete.

Step	Action
1	Connect to the CP PM server using the serial console.
2	Attach the Linux base compact flash installation media.

3 Reboot the server. Reseat the CP PM card to ensure a successful reboot.

When the server boots up, the CS 1000 Linux Base System Installer window appears as shown in Figure 20 "CS 1000 Linux base system installer (CP PM server)" (page 67).

Figure 20
CS 1000 Linux base system installer (CP PM server)

4 Type **com 1** to install using a serial console on COM1.

ATTENTION
If you log on to the COM 1 port, make sure that Caps Lock is turned off before you log on.

If you type `com 1`, the system will only install via the com port. If you install using kvm, the system will only install through a kvm.

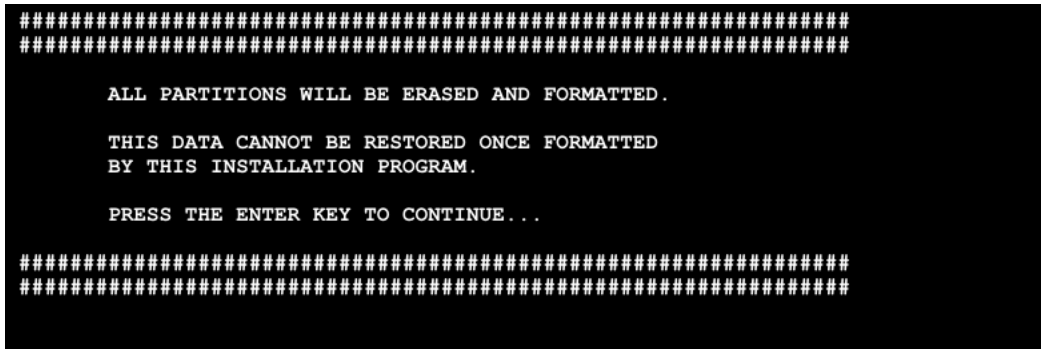
The CS 1000 Linux base system installer confirmation screen appears, as shown in Figure 21 "CS 1000 Linux base system installer confirmation window" (page 67).

Figure 21
CS 1000 Linux base system installer confirmation window

5 Type **Y** and press **Enter**. .

The Format all partitions screen appears, as shown in Figure 22 "Format all partitions window" (page 68).

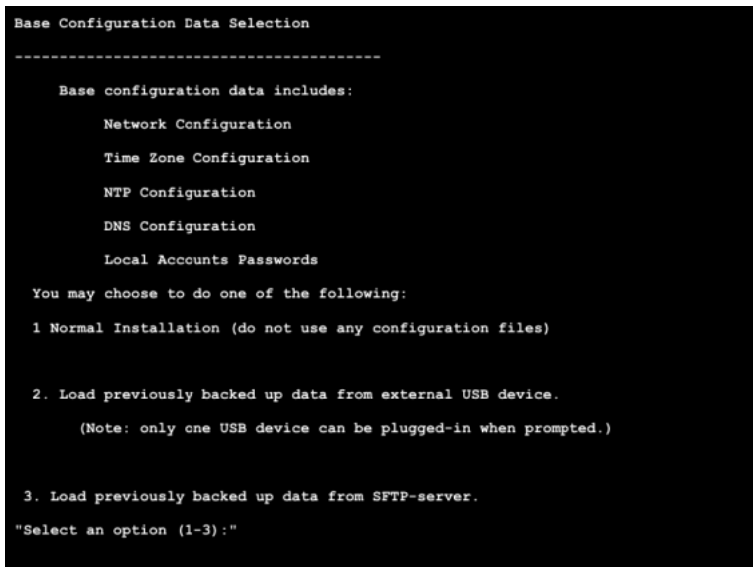
Figure 22
Format all partitions window



6 Press **Enter** to continue..

The Base Configuration Data Selection screen appears, as shown in Figure 23 "Base Configuration Data Selection window" (page 68).

Figure 23
Base Configuration Data Selection window

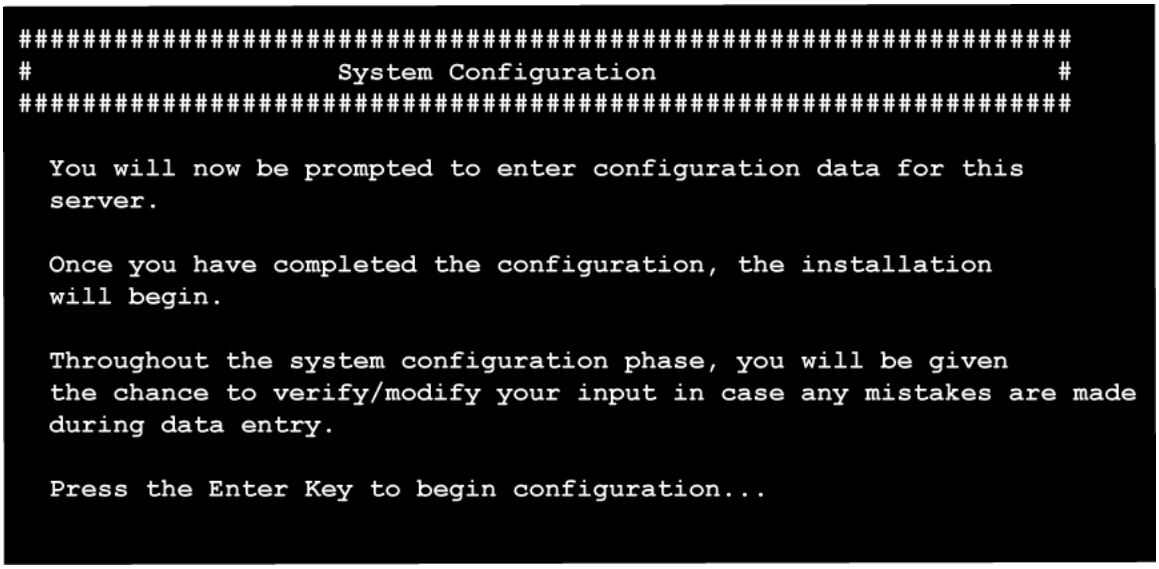


7 Type**1 Enter**..

Note: If you select option 2 or 3, the remainder of the process is the same as the upgrade procedure. See *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315) for details.

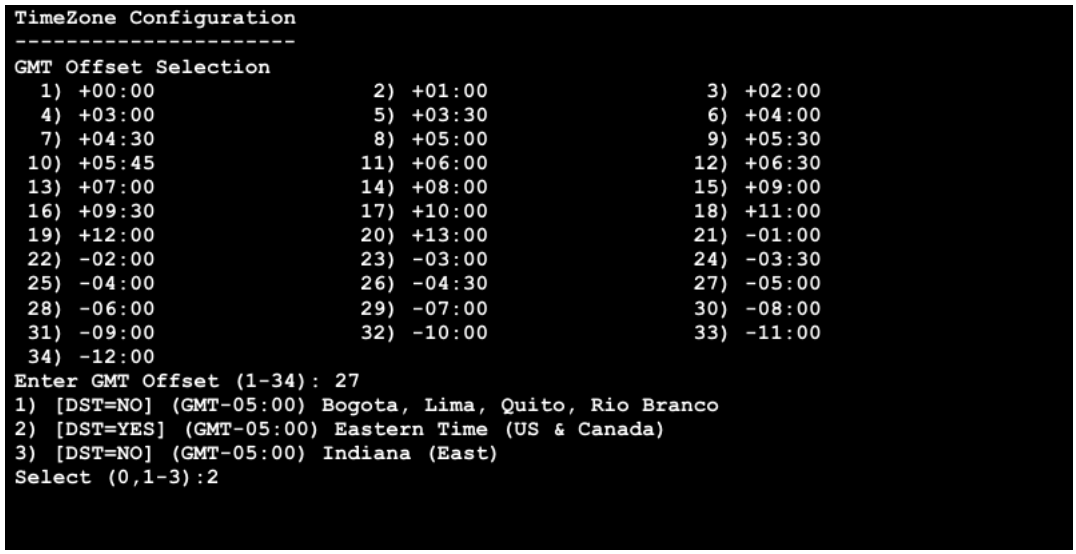
The System configuration window appears, as shown in Figure 24 "System configuration window" (page 69).

Figure 24
System configuration window



8 Press **Enter** to continue. The TimeZone Configuration screen appears, as shown inFigure 25 "TimeZone Configuration window" (page 69) .

Figure 25
TimeZone Configuration window



9 Type the number corresponding to the GMT offset you want to choose.

For example, to select a time in the United States Eastern time zone, type 27. For a listing of time zones and their corresponding Greenwich Mean Time (GMT) offsets, see Table 12 "GMT offset timezones" (page 70).

Table 12
GMT offset timezones

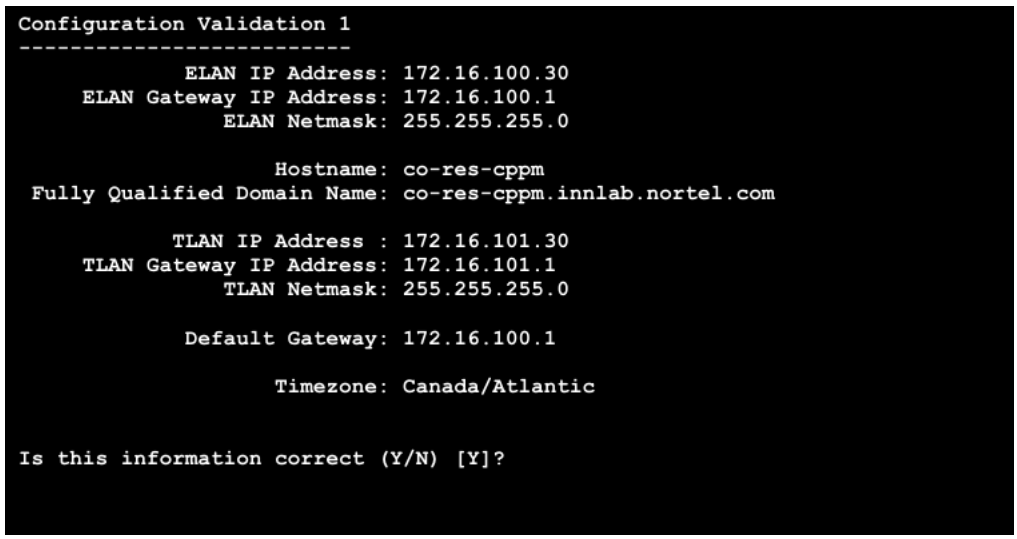
Name	Description	Relative to GMT
GMT	Greenwich Mean Time	GMT
UTC	Universal Coordinated Time	GMT
ECT	European Central Time	GMT+1:00
EET	Eastern European Time	GMT+2:00
ART (Arabic)	Egypt Standard Time	GMT+2:00
EAT	Eastern African Time	GMT+3:00
MET	Middle East Time	GMT+3:30
NET	Near East Time	GMT+4:00
PLT	Pakistan Lahore Time	GMT+5:00
IST	India Standard Time	GMT+5:30
BST	Bangladesh Standard Time	GMT+6:00
VST	Vietnam Standard Time	GMT+7:00
CTT	China Taiwan Time	GMT+8:00
JST	Japan Standard Time	GMT+9:00
ACT	Australia Central Time	GMT+9:30
AET	Australia Eastern Time	GMT+10:00
SST	Solomon Standard Time	GMT+11:00
NST	New Zealand Standard Time	GMT+12:00
MIT	Midway Islands Time	GMT-11:00
HST	Hawaii Standard Time	GMT-10:00
HST	Hawaii Standard Time	GMT-10:00
AST	Alaska Standard Time	GMT-9:00
PST	Pacific Standard Time	GMT-8:00
PNT	Phoenix Standard Time	PNT Phoenix Standard Time GMT-7:00
MST	Mountain Standard Time	GMT-7:00
CST	Central Standard Time	GMT-6:00
EST	Eastern Standard Time	GMT-5:00
IET	Indiana Eastern Standard Time	GMT-5:00

PRT	Puerto Rico and US Virgin Islands Time	GMT-4:00
CNT	Canada Newfoundland Time	GMT-3:30
AGT	Argentina Standard Time	GMT-3:00
BET	Brazil Eastern Time	GMT-3:00
CAT	Central African Time	GMT-1:00

10 Type the number that corresponds to the Daylight Saving Time (DST) value that you want to choose and press **Enter**.

The Configuration Validation 1 screen appears, as shown in Figure 26 "Configuration Validation 1 window" (page 71).

Figure 26
Configuration Validation 1 window



11 Review the configuration information, type **Y** to confirm the data, and press **Enter**.

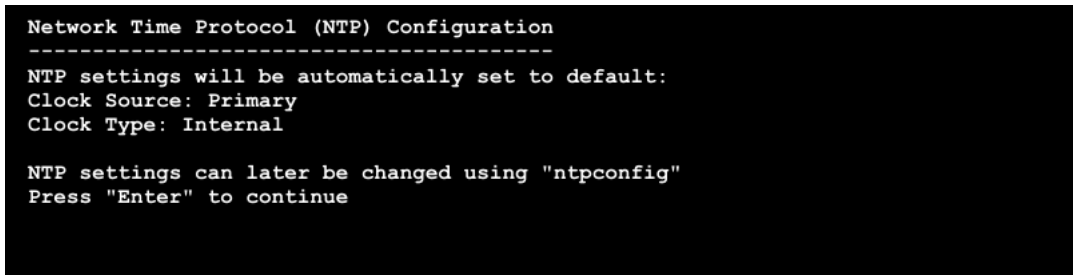
OR

Review the configuration information, type **N** and press **Enter** to re-enter the configuration information.

> ***Note:*** If you change the network parameters you can affect the configuration of applications. This can result in the loss of some services.

The Network Time Protocol (NTP) Configuration screen appears, as shown in Figure 27 "Network Time Protocol (NTP) Configuration window" (page 72) .

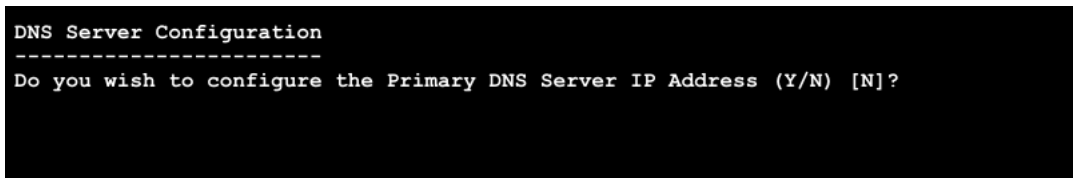
Figure 27
Network Time Protocol (NTP) Configuration window



12 Press **Enter**.

The DNS Server Configuration screen appears, as shown in Figure 28 "DNS Server Configuration window" (page 72).

Figure 28
DNS Server Configuration window



13 Type **Y** and press **Enter** to configure the Primary DNS server IP address.

OR

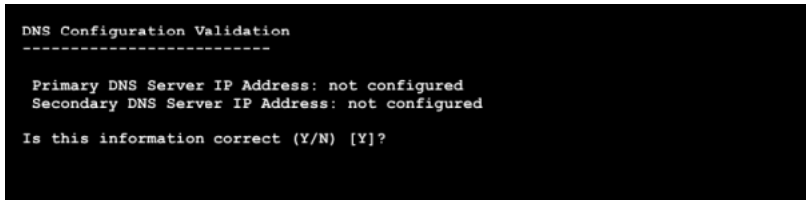
Type **N** and press **Enter** if you do not want to configure the Primary DNS server IP address.

Note 1: In this example we do not configure the Primary DNS server IP address. If you **Y** you are prompted to provide the Primary DNS server IP address.

Note 2: The CLI command **`hostconfig`** can be used to modify the static lookup table for host names. For a list of Nortel Linux base CLI commands see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

The Configuration Validation screen appears, as shown inFigure 29 "Configuration Validation window" (page 73) .

Figure 29
Configuration Validation window



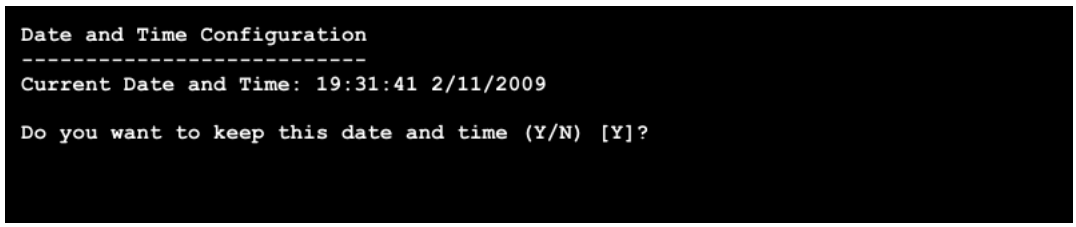
14 Type **Y** and press **Enter** to confirm the configuration.

OR

Type **N** and press **Enter** if the configuration information is not correct.

The Date and Time Configuration screen appears, as shown in Figure 30 "Date and Time Configuration window" (page 73).

Figure 30
Date and Time Configuration window



15 Type **Y** and press **Enter** to confirm the date and time.

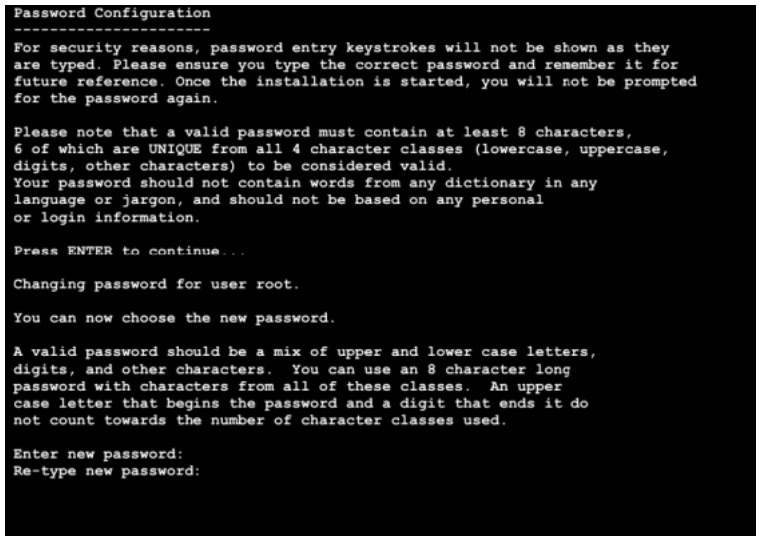
OR

Type **N** and press **Enter** if the configuration information is not correct.

> **ATTENTION**
> All Linux servers need to have accurate time. It is recommended to configure the time accurately on all servers on an external NTP server. Not doing so can result in failures to complete installation!

The root Password Configuration screen appears, as shown in Figure 31 "root Password Configuration window" (page 74).

Figure 31
root Password Configuration window

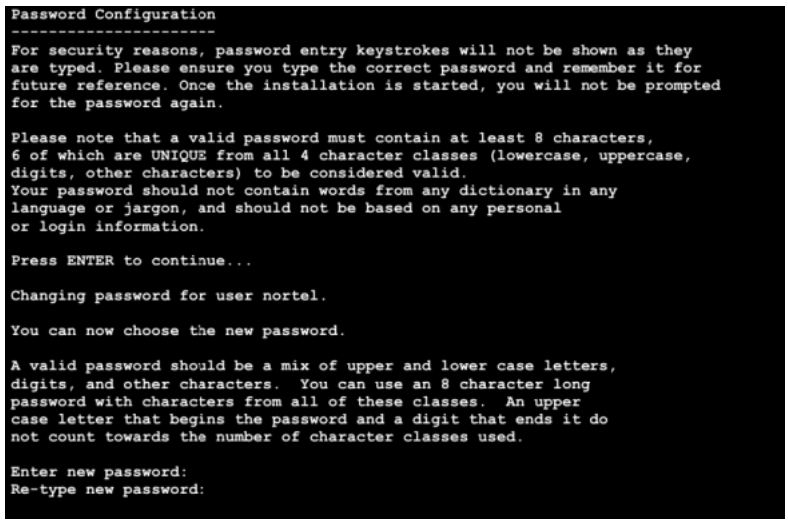


16 Enter a value for the root password.

17 Reenter the value for the root password and press **Enter**.

The nortel Password Configuration screen appears, as shown in Figure 32 "nortel Password Configuration window" (page 74).

Figure 32
nortel Password Configuration window

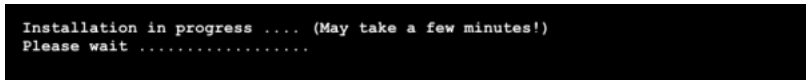


18 Enter a value for the nortel password.

19 Reenter a value for the nortel password and press **Enter**.

A pre-installation status screen appears as shown in Figure 33 "Pre-installation status window" (page 75).

Figure 33
Pre-installation status window



After approximately 15 to 20 minutes elapse, the Package Installation screen, Post System Configuration screen, and Status of Linux Hardening items screens appear, as shown in Figure 34 "Package Installation window" (page 75), Figure 35 "Post System Configuration window" (page 76), and Figure 36 "Status of Linux Hardening items window" (page 76).

Figure 34
Package Installation window

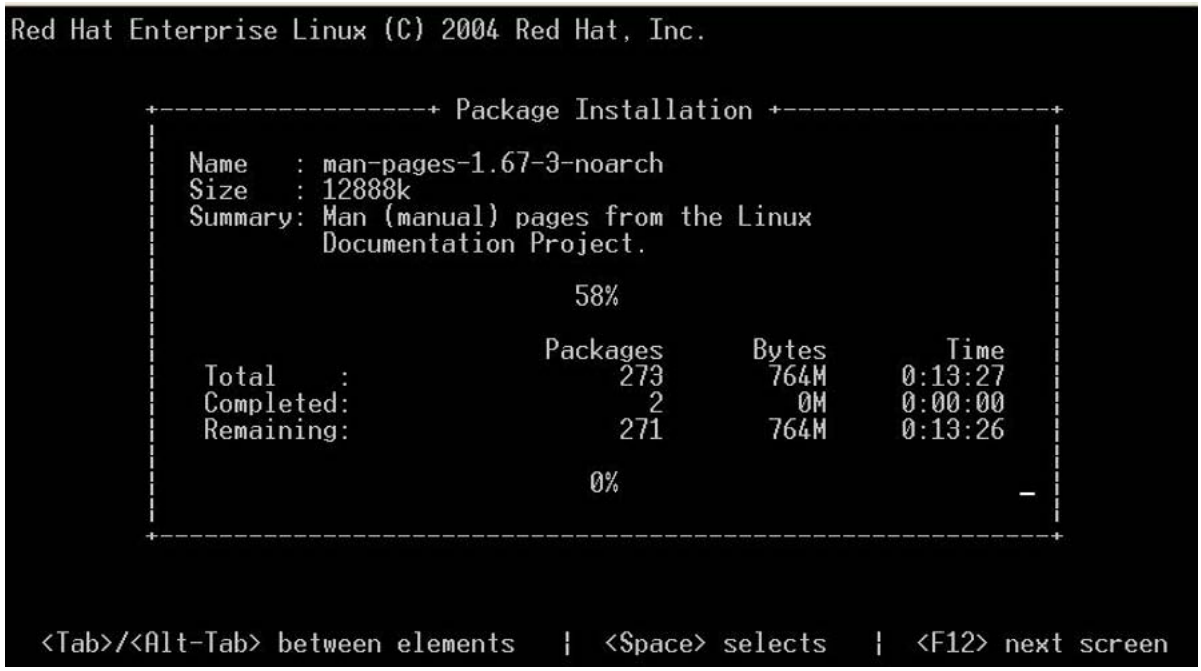


Figure 35
Post System Configuration window

Figure 36
Status of Linux Hardening items window

The CP PM Co-res CS and SS CP PM Card now has the Nortel Linux Base installed. You must complete the procedures in “Application installation using Deployment Manager” (page 76)to deploy the Call Server and Signaling Server Applications to this server using the UCM Deployment Manager.

--End--

Application installation using Deployment Manager

Nortel Linux platform uses Centralized 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.

Centralized Deployment Manager is a web-based framework. For details on how to create a primary security server in UCM, see *Unified Communications Management*(NN43001-116).

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 and Nortel 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 are installed using Centralized 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 CP PM Co-res CS and SS)
- Call Server, Signaling Server, and Network Routing Service (CP PM Co-res CS and SS with branch support)
- Session Initiation Protocol Line (SIPL)
- Element Manager (EM)
- Subscriber Manager (SubM)

Select a deployment package from the following list:

- SS
- NRS

- SS and NRS
- CS and SS
- CS, SS, and NRS
- EM

The deployment package selected represents the main purpose of the box. Once you select the initial deployment package you can add additional packages, as long as the packages are part of the supported configuration. The following is a list of supported configurations for CP PM Cores CS and SS:

Supported deployment configurations

- CS and SS
- CS, SS, and NRS
- EM
- NRS
- SS and NRS
- SIP Line
- Subscriber Manager

Access UCM

You must access the UCM Primary Security Server to perform application deployment using Centralized Deployment Manager. To join the UCM domain, or to create a UCM Primary Security Server if one does not exist, see *Unified Communications Management*(NN43001-116).

Procedure 10
Logging on to UCM

Step	Action
1	Open the Web browser.
2	Enter one of the following in the Address bar, and then press **Enter**: • FQDN for the UCM server. • UCM framework IP address—After you enter the UCM framework IP address, a Web page appears stating that you must access UCM by using the Fully Qualified Domain Name (FQDN) for the UCM server. Click the link on this Web page to use the FQDN for the UCM server.

3 Click **OK** or **Yes** to accept the security windows that appear.

The **UCM Login** Web page appears.

4 In the **User ID** field, enter your Primary UCM Security Server user ID, which has the appropriate rights to perform Software Deployment. See *Unified Communications Management*(NN43001-116).

5 In the **Password** field, enter your password.

6 Click **Log In**.

The default navigation Web page for UCM appears.

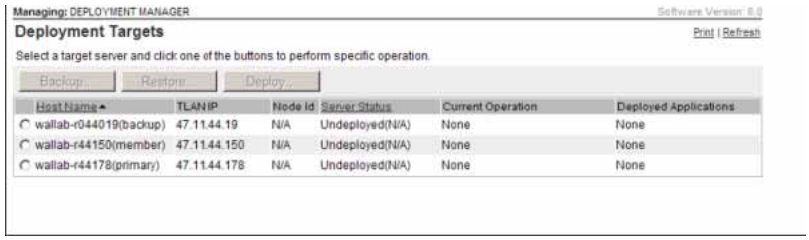
--End--

Access the centralized software Deployment Manager

Procedure 11
Accessing the centralized software Deployment Manager

Step	Action
1	Log on to UCM. See Procedure 10 “Logging on to UCM” (page 78).
2	In the navigation pane, click **Network**, **CS 1000 Servers**, **Software Deployment**. The Deployment Manager screen appears, as shown in Figure 37 "Deployment Manager window" (page 79).

Figure 37
Deployment Manager window



--End--

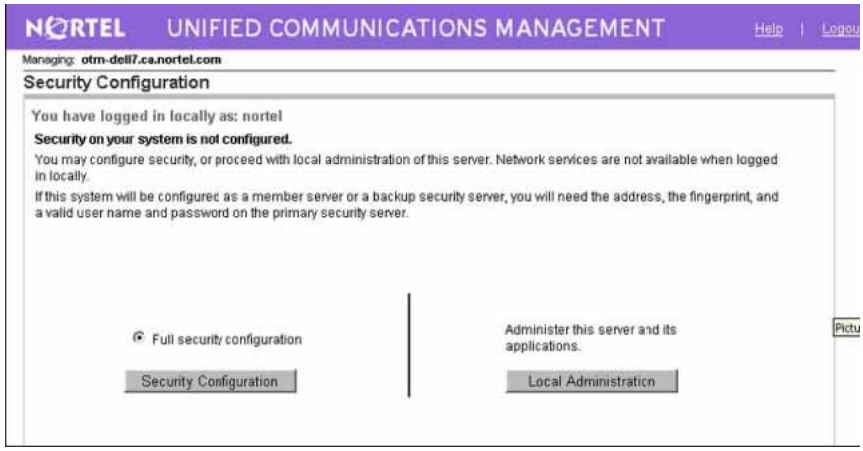
Access the Local Deployment Manager

Alternatively, application software can be deployed on a server before joining the security domain. To do this, you must log on to the local server and use the Deployment Manager to deploy the software locally. When the server does eventually join the security domain, local deployment information is recognized by the Central Deployment Manager.

Accessing the Local Deployment Manager

Step	Action
1	Log on to the linux base server using the nortel user ID and password. The Security Configuration screen appears, as shown in Figure 38 "Security Configuration window" (page 80).

Figure 38
Security Configuration window



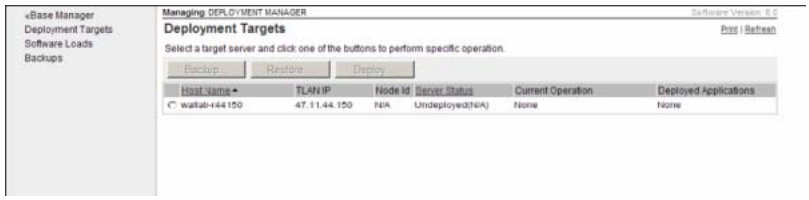
2	Click **Local Administration**. The Base Manager screen appears, as shown in Figure 39 "Base Manager window" (page 80).

Figure 39
Base Manager window

3	In the navigation pane click **Applications Deployment Manager**.

The Deployment Manager screen appears, as shown in Figure 40 "Deployment Manager window" (page 81).

Figure 40
Deployment Manager window



--End--

Software loads

There is a single application load file for CS 1000 Linux applications. The naming convention for the file is nortel-cs1000-linux-6xxyy.nai.

- 6.xx is the version number
- yy is the release number
- nai is the extension name (Nortel Application Image)

You can download the application load file directly to the hard drive of the client PC, or you can copy the application load file to a CD, DVD, compact flash (CF), or USB device and then attach the storage medium to the client PC and upload the application load file. Deployment Manager provides the functionality to transfer the application load file from the client PC to the server hard disk. The application load file must reside on the server hard disk before software deployment can be performed. There is also an additional method where the NAI file resides in the Server RMD (ie: Software Load Location "Deployment Server")

Note: In centralized deployment, you must upload the application load file to the primary security server, which deploys the software to other servers in the security domain.

Add a new software load to the Deployment Manager

Application software loads must reside on the hard drive of the server you are using to perform application deployment.

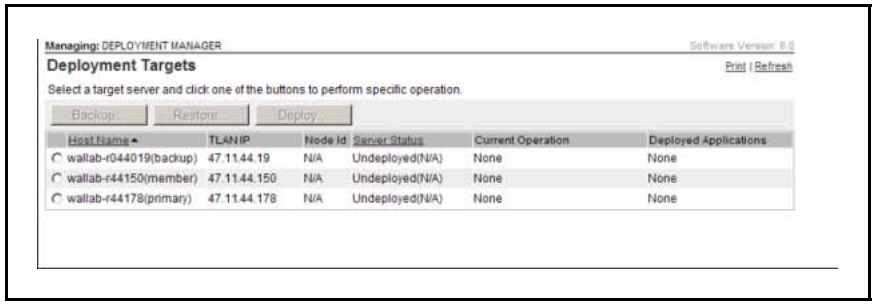
Centralized deployment requires that the application software load be loaded only once to the primary security server's hard drive. The primary security server can then deploy the software applications to other servers in the same security domain.

Local deployment requires that you upload the software load to each target server.

Procedure 12
Adding a new software load to the Deployment Manager

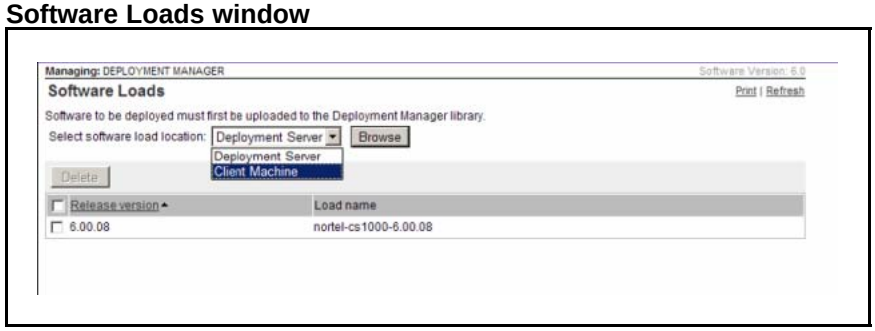
Step	Action
1	In the navigation pane, click **Software Deployment**. The Deployment Manager screen appears, as shown in Figure 41 "Deployment Manager window" (page 82).

Figure 41
Deployment Manager window



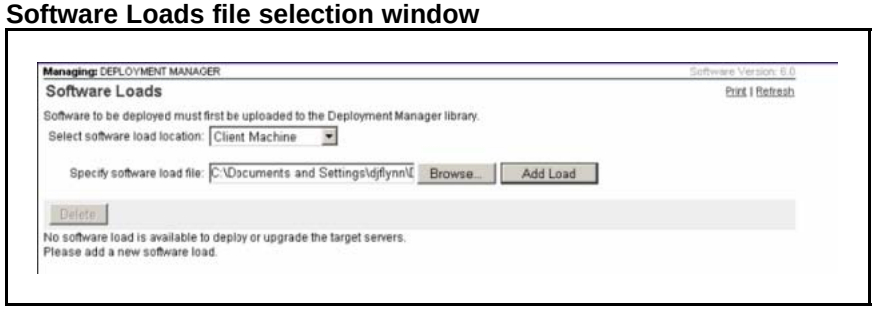
2	In the navigation pane, click **Software Loads**. The Software Loads page appears, as shown in Figure 42 "Software Loads window" (page 82).

Figure 42
Software Loads window



3	In the Select software load location list, select a software load location (Client Machine or Deployment Server).
4	If you selected Client Machine, in the Specify software load file field, type the file path for the software load file. **OR** Click **Browse** to browse to the location of the software load file. The **Add Load** button activates, as shown in Figure 43 "Software Loads file selection window" (page 83).

Figure 43
Software Loads file selection window



5 Click **Add Load**.

An upload progress screen appears, as shown in Figure 44 "Software upload progress window" (page 83)When the upload is complete the software load appears, as shown in Figure 42 "Software Loads window" (page 82).

Figure 44
Software upload progress window

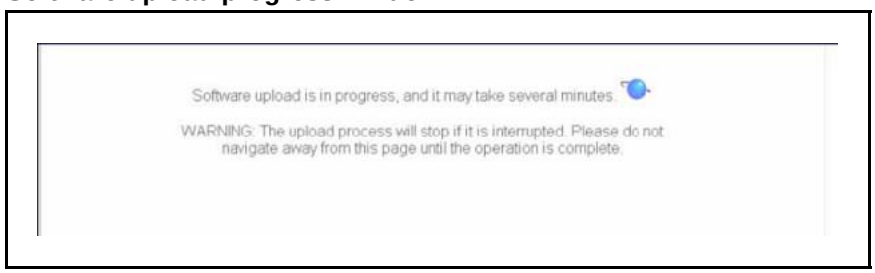
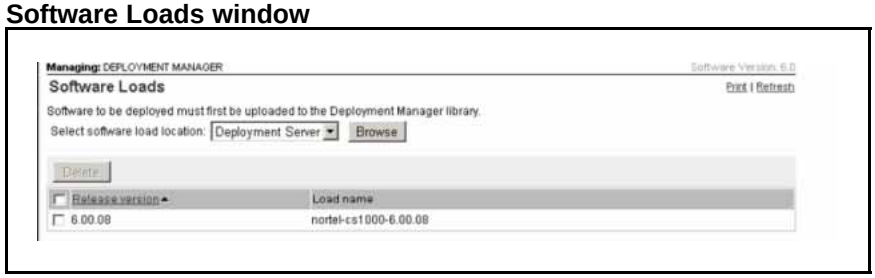


Figure 45
Software Loads window



--End--

Delete a software load from the Deployment Manager

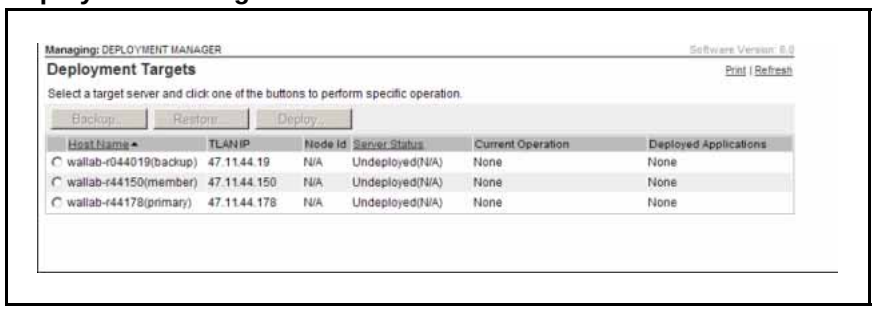
Deployment Manager can store a maximum of 3 software loads. If you want to add a software load after the maximum number of software loads has been reached, you must delete a software load.

Note: Nortel recommends that before the server joins the UCM security domain, you delete software loads added in a local deployment scenario. Software loads added during local deployment are not visible from Central Deployment Manager after the server joins the UCM security domain.

Procedure 13
Deleting a software load from the Deployment Manager

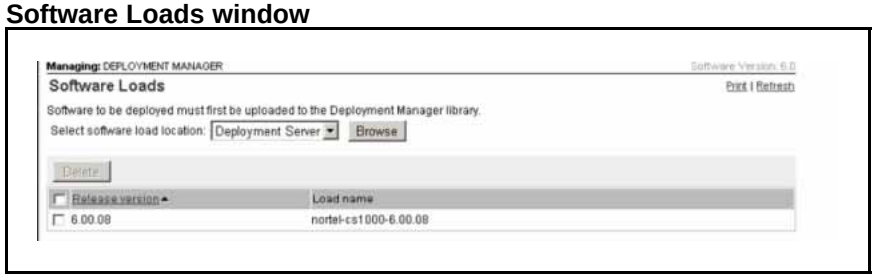
Step	Action
1	In the navigation pane, click **Network**, **CS 1000 Servers**, **Software Deployment**. The Deployment Manager screen appears, as shown in Figure 46 "Deployment Manager window" (page 84).

Figure 46
Deployment Manager window



2	In the navigation pane, click **Software Loads**. The Software Loads page appears, as shown in Figure 47 "Software Loads window" (page 84).

Figure 47
Software Loads window



3	Select the check box for the software load that you want to delete.

4 Click **Delete**.

--End--

Software deployment

Centralized Deployment Manager allows software application deployment from the primary security server to other Linux servers in the same security domain. The primary security server acts as the central repository for the software application load and deployment is done remotely, which eliminates the need to log on to each target server.

Deploy application software to a CP PM server

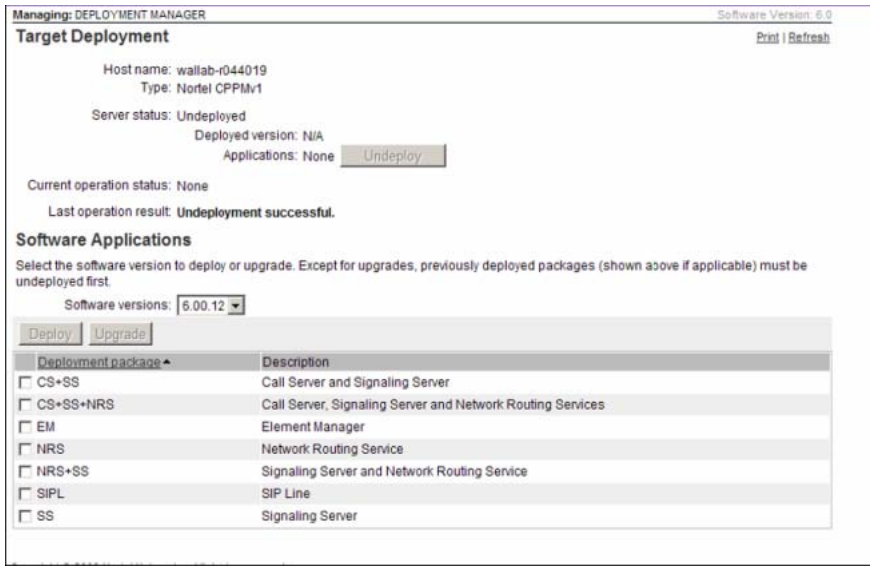
Prerequisites

- The status of the target server must be **Undeployed**.
- The Deployment Manager must contain a software load that matches the base version.

Procedure 14
Deploying application software to a CP PM server

Step	Action
1	In the navigation pane, click **Software Deployment**, **Deployment Targets**.
2	Select the target for deployment. ***Note:*** The target server must have a status of Undeployed.
3	Click **Deploy**. Target information and available software applications are displayed, as shown in Figure 48 "Target deployment and available software applications" (page 86).

Figure 48
Target deployment and available software applications



4 In the **Software versions** list select a value for software version.

5 Select a deployment package to deploy.

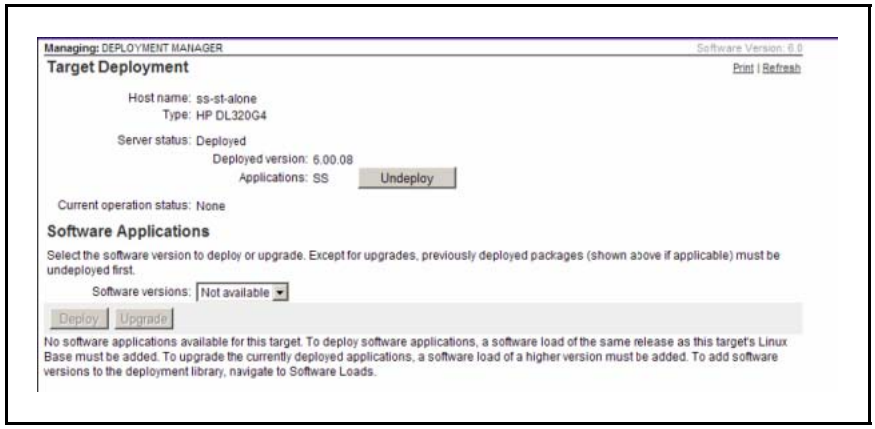
> ***Note:*** Deployment packages are platform dependant; the platform of the target server influences which deployment packages are available. For more information on deployment packages see Valid deployment package and server combinations.

6 Select any additional deployment packages that you want to deploy. Only deployment packages that are valid in combination with the previously selected deployment package are available for selection. For a list of supported deployment package configurations, see "Supported deployment package configurations" (page 78) .

7 Click **Deploy**.

ATTENTION
If you chose a deployment package that includes Call Server or Element Manager, or if a backup of the target server exists, proceed to steps 10-12. If you did not choose a deployment package that includes Call Server or Element Manager, or if a backup of the target server does not exist, the deployment completes and the deployed packages are displayed in the Target Deployment screen, as shown in Figure 49 "Target Deployment window" (page 87).

Figure 49
Target Deployment window



8 If you choose a package that includes Call Server, you are directed to the Call Server Configuration screen, as shown in Figure 50 "Call Server Configuration window" (page 87). For details on pre-configuring the Call Server, see

Figure 50
Call Server Configuration window

9 In the Keycode file box, type the path and filename for the keycode file.

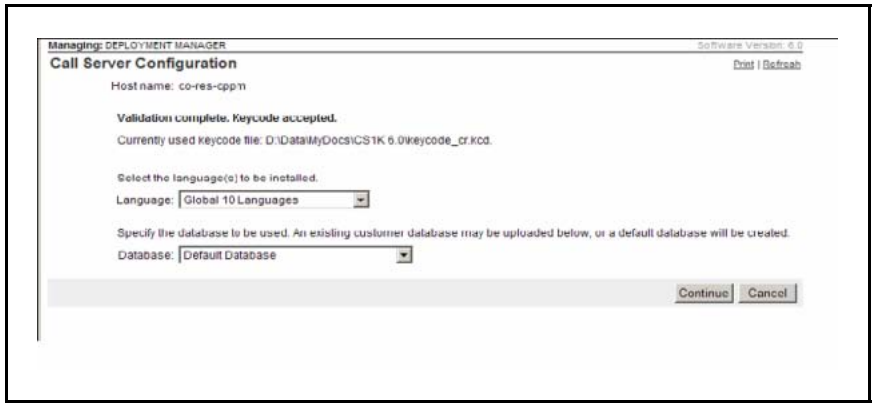
OR

Click **Browse** to browse for the keycode file.

10 Click **Validate** to validate the keycode.

After the keycode file validates successfully, language and database options are displayed, as shown in Figure 51 "Call Server Configuration language and database selection window" (page 88).

Figure 51
Call Server Configuration language and database selection window



11 In the **Language** list, select a value for language.

12 In the **Database** list, select a value for the database option.

If you want to select the default database, proceed to step 15.

If you want to select a customer database on the client machine, proceed to step 17.

If you want to select a customer database on the CP PM compact flash, proceed to step 25.

If you want to select an existing database, proceed to step 27.

> ***Note:*** The option to use an existing database is only available when you are performing an upgrade. The existing database option is not available during an initial deployment.

13 In the **Database** list, select **Default Database**.

14 Click **Continue**.

Proceed to step 29.

15 In the **Database** list, select **Customer Database on Client Machine**. The **Customer database directory** field appears, as shown in Figure 52 "Call Server Configuration customer database directory window" (page 89).

Figure 52
Call Server Configuration customer database directory window

16 In the **Customer database directory** box, type a value for the customer database directory.

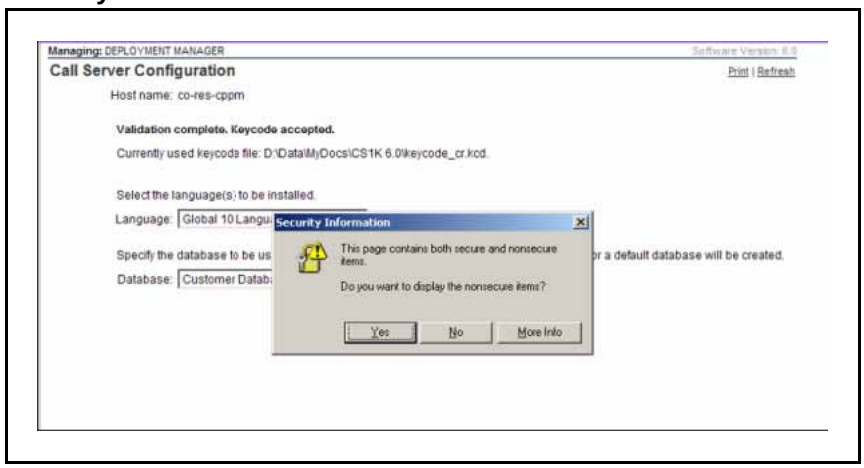
OR

Click **Browse** to browse for the customer database directory.

17 Click **Upload**.

The Security Information screen appears, as shown in Figure 53 "Security Information window" (page 89).

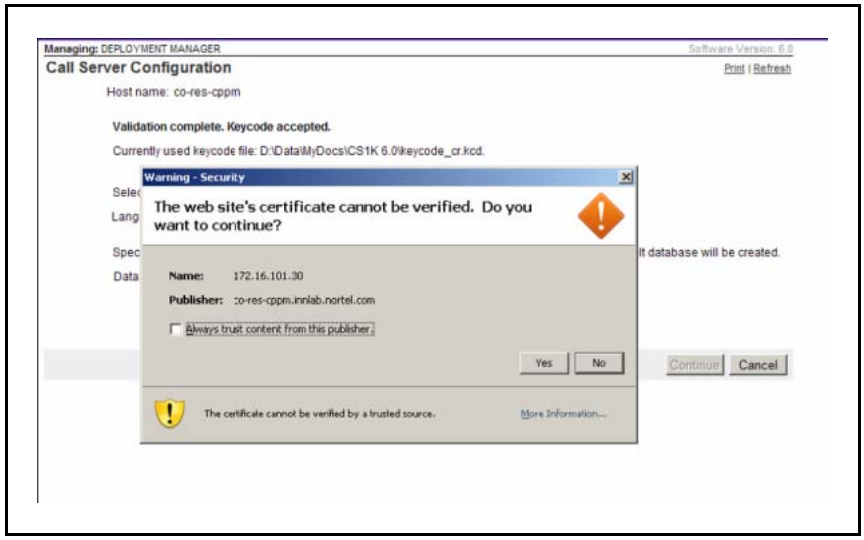
Figure 53
Security Information window



18 Click **Yes**.

The Security warning 1 screen appears, as shown in Figure 54 "Security warning 1 window" (page 90).

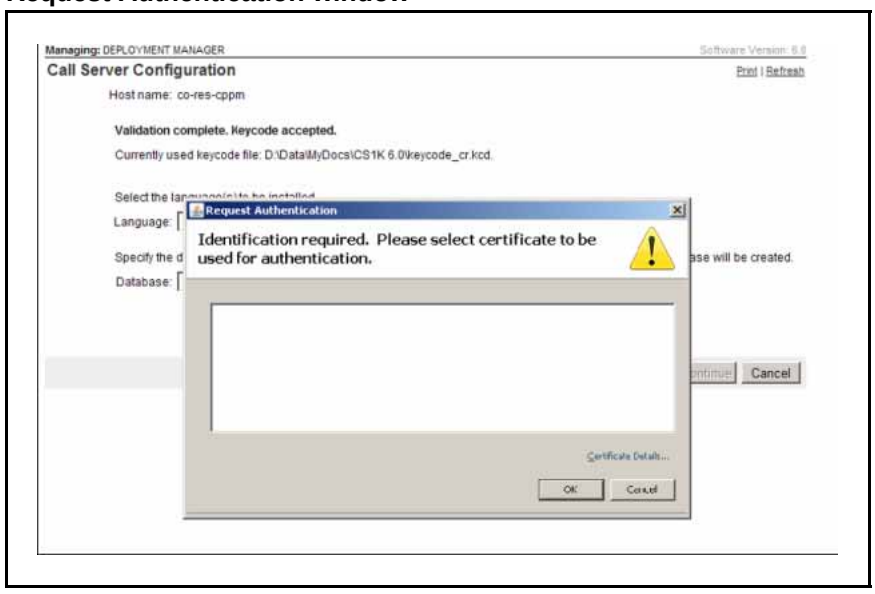
Figure 54
Security warning 1 window



19 Click **Yes**.

The Request Authentication screen appears, as shown in Figure 55 "Request Authentication window" (page 90).

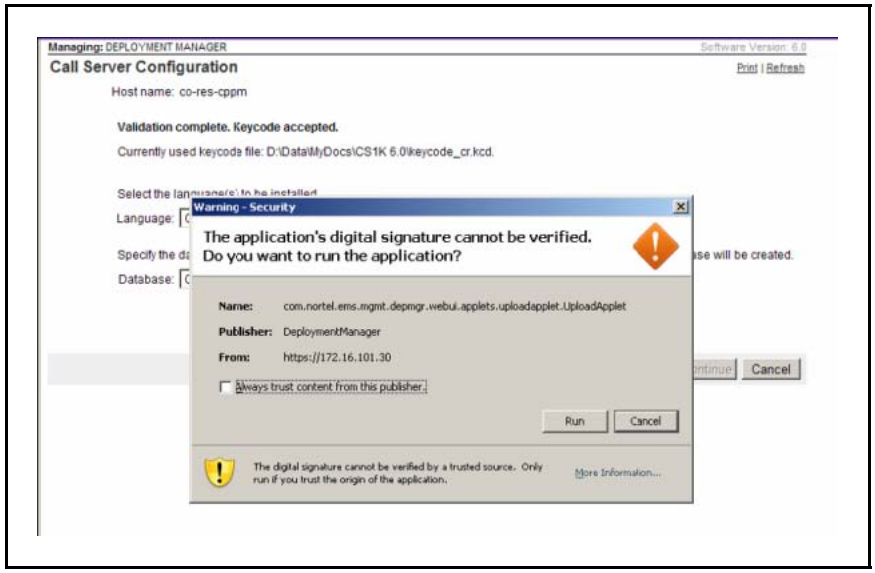
Figure 55
Request Authentication window



20 Click **OK**.

The Security warning 2 screen appears, as shown in Figure 56 "Security warning 2 window" (page 91).

Figure 56
Security warning 2 window



21 Click **Run**.

22 Click **Continue**.

Proceed to step 29.

23 In the **Database** list, select **Customer Database on Compact Flash**.

The **Database name list** appears, as shown in Figure 57 "Call Server Configuration database name window" (page 91).

Figure 57
Call Server Configuration database name window

24 Click **Continue**

Proceed to step 29.

25 In the **Database** list, select **Existing Database**.

26 Click **Continue**.

27 If you chose a deployment package that includes Element Manager and want to associate EM with an unmanaged Call Server in your security domain, proceed to step 30. If you chose a deployment package that includes Element Manager , and you are doing a local deployment or there is no Call Server in the security domain, proceed to step 33.

28 If you chose a package that includes Element Manager, the Element Manager Configuration screen appears, as shown in Figure 58 "Element Manager Configuration window" (page 92). For details on pre-configuring Element Manager, see .

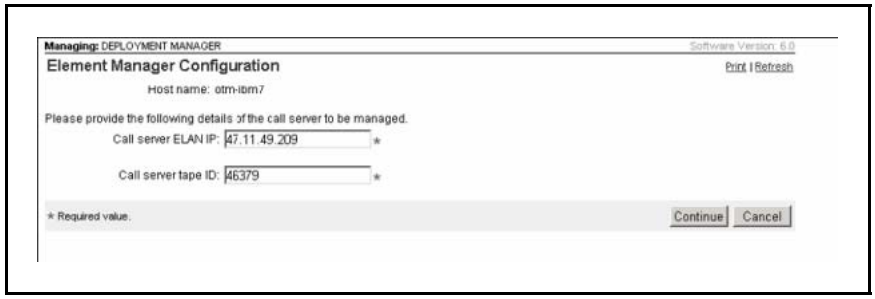
Figure 58
Element Manager Configuration window

29 In the **Call server ELAN IP list**, select the ELAN IP address of the call server that you want EM to manage.

30 Click **Continue**

31 If you chose a package that includes Element Manager , the Element Manager Configuration screen appears, as shown in Figure 59 "Element Manager Configuration window" (page 92)

Figure 59
Element Manager Configuration window



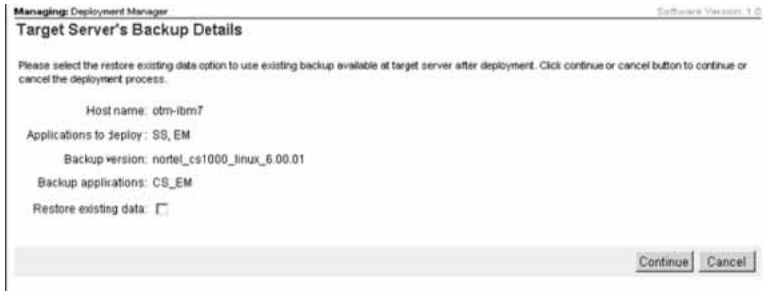
32 In the **Call server ELAN IP** field, enter a value for Call Server ELAN IP.

33 In the **Call server tape ID** field, enter a value for the Call Server tape ID.

34 Click **Continue**

35 If a backup of the target server exists, the Target Server Backup Details screen appears, as shown in Figure 60 "Target Servers Backup Details window" (page 93). For details on using an existing target server backup, see .

Figure 60
Target Servers Backup Details window



36 Select **Restore existing data** to deploy the application packages using existing data.

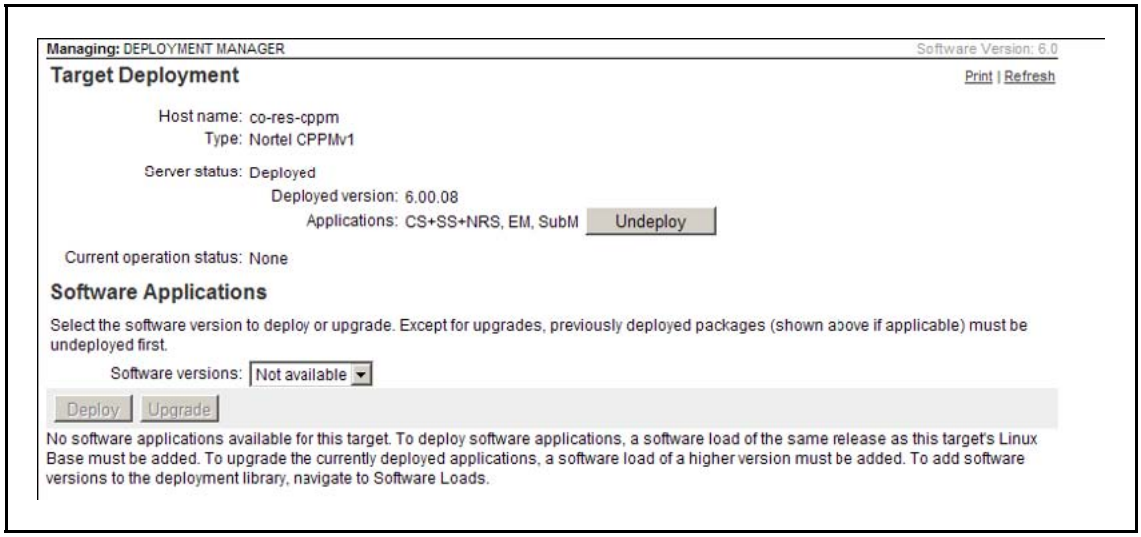
OR

37 Do not select **Restore existing data** to proceed without using pre-existing data.

38 Click **Continue**

The deployment completes. The Target Deployment screen appears, as shown in Figure 61 "Target Deployment window" (page 93). The screen displays the server deployment status and deployed packages.

Figure 61
Target Deployment window



--End--

Patching

Patching the CP PM Co-res CS and SS

Note: For detailed information on patching Linux components using Central Patching Manager and local patching by Base Manager, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Support is available for two patch types for the CP PM Co-res CS and SS:

- Call Server Binary patches are currently used in CS 1000 to patch the Call Server only. The file names for binary patches in VxELL for the Call Server have the pxxxxx_x.cpl format. VxWorks file names have the pxxxxx.x.cpm format.
- Linux patches are used to patch the Signaling Server, Linux Base and any other Linux based applications excluding the Call Server.

You can perform patching from the CLI or Element Manager. Patch files are transferred to the platform by using FTP/SFTP, a USB drive, or an RMD CF card. For detailed information on patching using Element Manager, see *Element Manager System Administration* (NN43001-632).

Patching Call Server binary patches

The method of deploying the Call Server binary patches on the Call Server using the CLI is similar to deploying patches using the previous release of CS 1000 Call Server. You patch by using the CLI. You must place the binary patch files in the /var/opt/nortel/cs/fs/u/patch folder. You must enter the **`pload`**, **`pins`**, **`poos`**, **`pstat`** and **`pout`** patching commands from the Call Server PDT shell.

Procedure 15
Patching Call Server binary patches

Step	Action
1	Ensure the patch file is in the /var/opt/nortel/cs/fs/u/patch directory.

2 Connect to the CP PM Co-res CS and SS remotely (ssh) or locally (serial port).

3 Log on to the CP PM Co-res CS and SS.

4 From the Linux bash shell, connect to the Call Server by using the cspdt (to Call Server pdt) or **csconsole** or **cslogin** command (Call Server overlays):

```
[nortel@ccName_cppm ~]$ cslogin

OVL111 000 IDLE
Logi admin2
PASS
```

5 You must enter **pdt1** to go to CS pdt. From pdt, issue the **pload** command and the filename for the patch to place the patch in service.

```
[nortel@ccName_cppm ~]$ cspdt

pdt> cd /u/patch

pdt> ll

Directory of 'ccName_cppm:/var/opt/nortel/cs/fs/u/patch':

4096 Feb-16-2008 20:03:52 <DIR>
4096 Feb-16-2008 20:14:22 <DIR>
4096 Feb-16-2008 20:14:42 reten <DIR>
4096 Feb-07-2008 22:02:04 pch_tmp <DIR>
4096 Feb-07-2008 22:02:04 deplist <DIR>
144000 Feb-16-2008 20:03:56 reten.bkp <DIR>
3829 Feb-15-2008 14:21:24 p12345_1.cpl <DIR>

pdt> pload -s 0 p12345_1.cpl
Loading patch from "/u/patch/p12345_1.cpl"
Patch handle is:  0
Patch Memory Total:  4083KB Used:  335KB Avail:  3747KB (
91% ) pdt> pins 0
function at 0x308be00 will be patched to jump to
0x35f78e60 (vtnProxyEvHandler)
Proceed with patch activation (y/n)?  [y] y
Patch 0 has been activated successfully.
pdt>
```

--End--

Element Manager patching

Support exists for Element Manager patching for Call Server binary patches and is applied by using the same procedures as the release of CS 1000 Call Server. See *Element Manager System Administration* (NN43001-632).

Linux patching

Support exists for Linux patching from Element Manager and from the CLI. Linux CLI patching requires that you log on to the Linux system and apply the patch from the Linux bash shell. See *Element Manager System Administration* (NN43001-632), *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315) , and *Unified Communications Management Common Services Fundamentals* (NN43001-116).

Call Server deplist

Support exists for Call Server deplist and is applied by using the same procedures as the previous release of CS 1000 Call Server.

Note: CP PM Co-res CS and SS supports installing a deplist from the FMD (hard drive) or RMD (USB, CF card).

Feature operation

Call Server

The Linux-based Call Server provides the same feature operation and feature management as the VXWorks-based, with the following exceptions:

- Configuration and management of Network Time Protocol (NTP) occurs within the Linux Base. Support is unavailable for Overlay 117 NTP management commands in CS 1000 Release 6.0.
- Support exists for CCBR backup and restore on MGC remote TTY ports. Support is unavailable for CCBR backup and restore on the CP PM serial port.
- Support exists for Xmodem **`sx`** and **`rx`** commands on the MGC remote TTY (from the Call Server PDT shell). Support is available for the **`sx`** and **`rx`** commands from the Linux Shell.
- Configuration of Time of Day (TOD) management occurs in Linux Base. Support is unavailable for Overlay 2 TOD configuration commands. Support is unavailable for Attendant Console Set Based Administration for TOD configuration and management. Support is only available for the Overlay 2 TOD print command.

Configuration management

OAM User Interface

While support exists for most of the existing CS 1000E Call Server and Signaling Server application user commands for CP PM Co-res CS and SS, some changes have been made to allow the Call Server and Signaling Server applications to co-reside and run as Linux applications. The new or modified user interfaces are focused in the following areas:

- Access to the CP PM Co-res CS and SS
- IP configuration and management
- NTP configuration management
- TOD configuration
- Point-to-Point Protocol (PPP) configuration
- File system layout for the CP PM Co-res CS and SS
- CP PM Co-res CS and SS restart
- Geographic Redundancy Survivable Media Gateway Configuration
- Serial port configuration
- CP PM Co-res CS and SS software version
- CP PM Co-res CS and SS configuration/database backup and restore
- Media Gateway Centralized Software Upgrade
- CP PM location (loop and shelf) configuration
- Overlay 137 Stat RMD commands
- Overlay 117 security configurations
- Accessing RMD and USB from Call Server PDT shell

Access to the CP PM Co-res CS and SS

CP PM Co-res CS and SS supports the following shells:

- Linux Bash Shell
- Call Server Overlay Shell
- Call Server PDT Shell

The Linux bash shell is used for Linux Base and Signaling Server applications.

The Call Server Overlay and PDT shells are used for the Call Server Overlay and PDT commands, respectively. These shells work the same as in the previous release of CS 1000 Call Server.

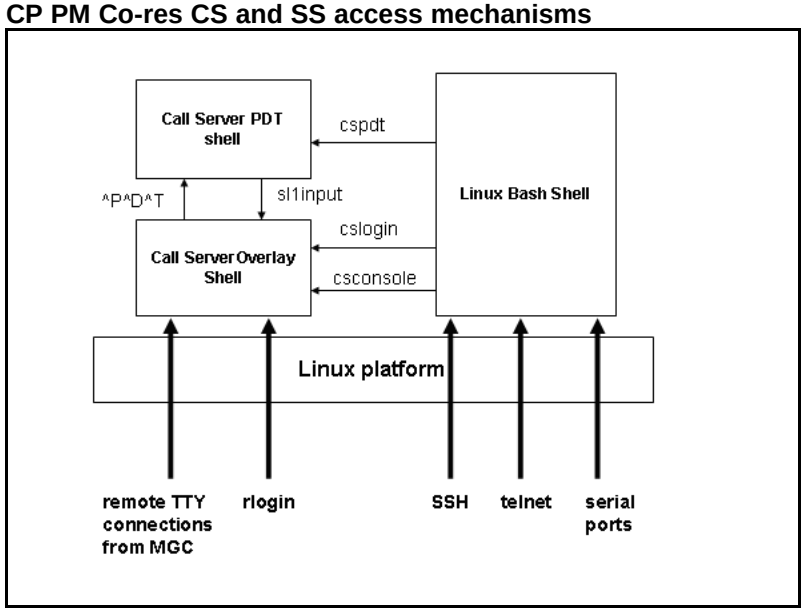
Table 13 "Shell commands" (page 102) lists the commands used to navigate between shells:

Table 13
Shell commands

From	To	Command to use
Linux Bash Shell	Call Server Overlay Shell	cslogin
Linux Bash Shell	Call Server Overlay Shell	csconsole
Linux Bash Shell	Call Server PDT shell	cspdt
Call Server Overlay Shell	Linux Bash Shell	if using cslogin to enter the overlay shell, type ~ . to exit if using csconsole to enter the overlay shell, type CTRL+AD to exit
Call Server Overlay Shell	Call Server PDT Shell	CTRL-PDT
Call Server PDT Shell	Call Server Overlay Shell	sl1input
Call Server PDT Shell	Linux Bash Shell	exit

Figure 62 "CP PM Co-res CS and SS access mechanisms" (page 103) provides the supported access mechanisms to the CP PM Co-res CS and SS.

Figure 62
CP PM Co-res CS and SS access mechanisms



Serial ports on CP PM

After connecting to the serial ports on the CP PM card and authenticating to the Linux Base bash shell, a user can issue Linux Base CLI commands and any appropriate Signaling Server application related commands.

You can also access the Call Server shell from the Linux bash shell using the **`cslogin`**, **`csconsole`** or **`cspdt`** commands.

Secure Shell (SSH)

Secure Shell access to the platform is supported. Upon successful authentication, you are connected to the Linux Bash Shell. You can then switch between different shells by using the commands listed in Table 13 "Shell commands" (page 102).

Telnet

Telnet access to the platform is optionally supported (depending on system security settings). Upon successful authentication, you are connected to the Linux Bash Shell. You can then switch between different shells by using the commands listed in Table 13 "Shell commands" (page 102).

Rlogin

Rlogin is supported but restricted to Call Server shell access. This is designed to support existing applications that require direct access to the Call Server overlays or PDT shell without any changes to the logon sequence.

Remote TTY from MGC

The CP PM Co-res CS and SS supports remote TTY connections. You can configure serial ports of the MGC to be remote TTYs for the Call Server. This connection directly links into the Call Server Overlay shell.

The cslogin command is used to log in to the TTY port configured for Call Server CPSI port 0. Nortel recommends accessing the Call Server overlays using cslogin.

The csconsole command is used to connect the user to any one of the TTY ports configured as the Call Server PTY ports.

In CS 1000 Release 6.0, the serial port is shared with other applications, therefore the output for the Call Server console port is redirected to **`/var/log/nortel/cs_console.log`** and is available to the user via the csconsole command.

Depending on how many PTY ports are configured, multiple cslogin sessions are supported. Multiple csconsole sessions are not supported.

Procedure 16
Connecting the Call Server using cslogin

Step	Action
1	Connect to the CP PM Co-res CS and SS remotely (ssh) or locally (serial port).
2	Log on to CP PM Co-res CS and SS.

3	Issue the cslogin command from Linux Bash Shell;
	`[nortel@ccName_cppm ~]$ cslogin`
	`OVL111 000 IDLE`
	`Logi admin2`
	`PASS`

--End--

Procedure 17
Connecting the Call Server using csconsole

Step	Action
1	Connect to the CP PM Co-res CS and SS remotely (ssh) or locally (serial port).
2	Log on to CP PM Co-res CS and SS.
3	Issue the csconsole command from Linux Bash Shell:

```
[nortel@ccName_cppm ~]$ csconsole

OVL111 000 IDLE
TTY 04 SCH MTC OSN TRF BUG 4:45
Logi admin2
PASS
```

--End--

Procedure 18
Connecting the Call Server using cspdt

Step	Action
1	Connect to the CP PM Co-res CS and SS remotely (ssh) or locally (serial port)
2	Log on to CP PM Co-res CS and SS
3	Issue the cspdt command from Linux Bash Shell

```
[nortel@ccName_cppm ~]$ cspdt
Username:  pdt2
PDT login on /pty/ptty00.S
Username:  pdt2
Password:

pdt>
```

--End--

IP Management for CP PM Co-res CS and SS

For CP PM Co-res CS and SS, the Linux Base software—not the Call Server application—handles network configuration and management. The network configuration and maintenance commands provided in Overlay 117 and Overlay 137 are blocked for the Call Server application running on the CP PM Co-res CS and SS. If you enter these commands in the Call Server overlays, you receive a warning message. In addition the IP network configuration will not be stored in the Call Server database.

Table 14 "Overlay 117 commands" (page 106) and Table 15 "Overlay 137 commands" (page 107) lists the Overlay 117 and 137 commands that do not apply to CP PM Co-res CS and SS.

Note: These commands are still applicable to VxWorks-based Call Servers.

Table 14
Overlay 117 commands

Command	Description
NEW HOST …	Add host name and IP address to network host table
OUT HOST …	Delete host from network host table
PRT HOST	Display network host table entries. (Command not Supported on Linux Call Server, please use Base Manager instead)
STAT HOST	Display host table status
ENL HOST …	Add a host entry to the run-time host table
DIS HOST …	Delete a host entry from the run-time host table
NEW ROUTE ….	Add new route to the network routing table
ENL ROUTE …	Add a new route to the runtime routing table
DIS ROUTE	Delete a route from the runtime routing table
PRT ROUTE	Display routing table entries stored in the database
STAT ROUTE	Display host and network routing table
CHG ELNK ACTIVE…	Set active ELAN IP address
CHG ELNK INACTIVE …	Set inactive ELAN IP address
PRT ELNK	Display active and inactive ELAN IP addresses. (Command not Supported on Linux Call Server, please use Base Manager instead)
RST ELNK ACTIVE	Reset active ELAN IP address to default.(Command not Supported on Linux Call Server, please use Base Manager instead)
RST ELNK INACTIVE	Reset inactive ELAN IP address to default. (Command not Supported on Linux Call Server, please use Base Manager instead)
PRT MASK	Display subnet mask. (Command not Supported on Linux Call Server, please use Base Manager instead)
CHG MASK …	Change subnet mask
SET MASK	Set run-time subnet mask to the configured value. (Command not Supported on Linux Call Server, please use Base Manager instead)
CHG HSP MASK	Change HSP subnet mask. (Command not Supported on Linux Call Server, please use Base Manager instead)

PRT HSP MASK	Display HSP subnet mask stored in database. (Command not Supported on Linux Call Server, please use Base Manager instead)
OUT HSP_MASK	Delete HSP subnet mask from database. (Command not Supported on Linux Call Server, please use Base Manager instead)
SET HSP_IP	Set HSP interface IP address and subnet mask to the configured values
UPDATE DBS	Update network database
PING	Ping an IP address

Table 15
Overlay 137 commands

Command	Description
STAT ELNK	Display the current active ELAN information. (Command not Supported on Linux Call Server, use **`ifconfig`** from Linux base)
ENL ELNK	Enable the current active ELAN interface. (Command not Supported on Linux Call Server, use **`ifconfig`** from Linux base)
DIS ELNK	Disable the current active ELAN interface. (Command not Supported on Linux Call Server, use **`ifconfig`** from Linux base)

Perform network configuration on the CP PM Co-res CS and SS by using Base Manager or with Linux Base CLI commands. See *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315) and *Unified Communications Management Common Services Fundamentals* (NN43001-116).

NTP and TOD configuration

For the CP PM Co-res CS and SS platform, the Linux OS controls and manages all system time related functions as well as the hardware timers. The Linux Base provides the user interface to the Linux OS for time and date-related configuration.

The system time related configuration and management commands are removed from the Call Server overlays for CS 1000 Release 6.0.

NTP configuration

The Network Time Protocol (NTP) feature is supported on the CP PM Co-res CS and SS platform. Configuration and management of NTP parameters occur at the Linux Base layer.

Table 16 "Obsolete Overlay 117 NTP commands" (page 108) lists the Call Server Overlay 117 NTP commands that are no longer supported for the CP PM Co-res CS and SS system.

Table 16
Obsolete Overlay 117 NTP commands

Command	Description
ENL NTP (Command not Supported on Linux Call Server, please use Base Manager instead)	Enable Network Time Protocol feature
DIS NTP (Command not Supported on Linux Call Server, please use Base Manager instead)	Disable Network Time Protocol feature
CHG NTP MODE <comm._mode>	Change NTP communication mode (Not applicable to Linux CS)
CHG NTP IPADDR <prim_ip><(sec_ip)>	Change IP address of Primary and Secondary NTP Server (Not applicable to Linux CS)
CHG UTCOFFSET <hour> <mins>	Change UTC offset applicable to the Call Server time zone
CHG NTP AUTHMODE <mode> <server>	Change NTP Secured mode of operation (Not applicable to Linux CS)
CHG NTP SECURE <server> <key_id>	Change NTP secured parameters (Not applicable to Linux CS)
CHG NTP TIMEINT time_int><offset>	Change NTP time interval and set the offset (Not applicable to Linux CS)
CHG NTP THRESH <min_thresh> <warn_thresh>. <max_thresh>	Change three NTP threshold levels (Not applicable to Linux CS
PRT NTP	Display NTP configuration (Command not Supported on Linux Call Server, please use Base Manager instead)
STAT NTP	Show the status of NTP. (Command not Supported on Linux Call Server, please use Base Manager instead)
SYNC NTP <sync_mode>	Synchronize in manual or background mode. (Command not Supported on Linux Call Server, please use Base Manager instead)
STOP NTP BACKGROUND	Abort the background synchronization operation. (Command not Supported on Linux Call Server, please use Base Manager instead)

Note: Perform NTP configuration on the CP PM Co-res CS and SS by using the Linux Base Manager or the Linux Base CLI command. See *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315) and *Unified Communications Management Common Services Fundamentals*(NN43001-116) for details.

TOD configuration

Table 17 "Obsolete Overlay 2 TOD commands" (page 109) lists the Call Server Overlay 2 time of day commands that are no longer supported.

Table 17
Obsolete Overlay 2 TOD commands

Command	Description
STAD	Set time and date
TDTA	Print daily time adjustment
SDTA	Set daily time adjustment
FWTM	Set the time and date to move forward for daylight savings time
BWTM	Set the time and date to move backward for daylight savings time
SDST	Enable or disable automatic daylight savings time adjustment
TDST	Query daylight savings time change information

Perform TOD configuration on the CP PM Co-res CS and SS by using Base Manager. See *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315) and *Unified Communications Management Common Services Fundamentals* (NN43001-116) for details.

Perform time and date configuration for the CP PM Co-res CS and SS platform by using the Linux Base Manager or the Linux Base CLI command. You can access this command if you are logged on to the server using an account with administrator privileges.

Note: Support is unavailable for TOD configuration using Attendant console.

PPP configuration

Support is available for the PPP protocol on the CP PM Co-res CS and SS. PPP configuration is no longer supported from the Call Server overlays. Configure PPP parameters using Linux Base commands.

Table 18 "Obsolete Overlay 117 PPP commands" (page 109) lists the PPP commands from Overlay 117 that are no longer supported:

Table 18
Obsolete Overlay 117 PPP commands

Command	Description
RST PTM	Reset PPP idle timer to default 30 minutes
CHG PTM <idletimer> [<cabNo>]	Change PPP idle timer value (0--60 minutes)

PRT PTM	Display current PPP idle timer settings
STAT PPP	Show PPP connection status
ENL PPP	Enable PPP for remote access
DIS PPP	Enable PPP for remote access

Xmodem on CP PM Co-res CS and SS

The Xmodem protocol is supported on CP PM Co-res CS and SS. The Xmodem rx and sx commands are available from Linux Bash shell and from the Call Server PDT shell.

Note: From the Call server PDT shell, the rx and sx commands are available only for the remote TTY connections from the MGC. These commands are blocked for any other connection types (ssh, serial port, cslogin and rlogin).

File System Layout

The file system for CP PM Co-res CS and SS is structured to support Call Server, Signaling Server, and System Management applications running on the same hardware platform.

All configuration and run-time data files for the Call Server that are used for normal operation reside in the folder /var/opt/nortel/cs/fs; for example:
All Call Server /p data will reside under /var/opt/nortel/cs/fs/p
All Call Server /u data will reside under /var/opt/nortel/cs/fs/u
All Call Server /e data will reside under /var/opt/nortel/cs/fs/e

Procedure 19
Accessing Call Server file system from Call Server PDT shell

Step	Action
1	Connect to the CP PM Co-res CS and SS remotely (ssh) or locally (serial port) .
2	Log on to CP PM Co-res CS and SS .
3	Issue the cspdt command from Linux Bash Shell:

```
[nortel@ccName_cppm ~]$ cspdt
pdt> cd /p
pdt> pwd
ccName_cppm:/var/opt/nortel/cs/fs/p
pdt>
```

--End--

Note: If the user works within the Linux bash shell or the VxWorks debug shell (as opposed to the PDT shell), the user must enter the complete path (no automatic prepending of the new file path).

CP PM Co-res CS and SS restart

Table 19 "Restart Commands" (page 111) lists the restart commands supported on the CP PM Co-res CS and SS.

Table 19
Restart Commands

From	Command	Description
Linux Bash Shell	Reboot	Shut down all processes and restart Linux OS End result for the Call Server is equivalent to a cold start.
Call Server Overlay 135	ini active	Invoke Call Server warm start only. No impact to other Linux processes.
	Sysload active	Invoke Call Server cold start No impact to other Linux processes.
Call Server PDT1/PDT2	Reboot	Invoke Call Server warm start No impact to other Linux processes.
	Reboot -1	Invoke Call server cold start No impact to other Linux processes.
Call Server VxWorks Shell (su)	Reboot	Invoke Call server warm start No impact to other Linux processes.
	Reboot -1	Invoke Call Server cold start No impact to other Linux processes.

WARNING
To warm start the Call Server only, you must issue the reboot command from the Call Server PDT shell, not from the Linux shell. Issuing the reboot command from the Linux shell shuts down all processes on the CP PM Co-res CS and SS and restarts the Linux OS.

Note: In Linux shell appstart cs warmstart can also be used to warmstart the Call Server.

INI Button

Pushing the INI button warmstarts the Call Server. All other Linux applications are not affected. The push button event is logged to the CP PM Co-res CS and SS system log files.

Note: Pushing the INI button changes the status LED to yellow. After the warmstart is completed and the Call Server application has restarted, the status LED changes to green.

Reset button

Pushing the RESET button initiates a board (hardware) reset. The Linux OS and all applications restart.

Reset Reason

Table 20 "CP PM Co-res CS and SS reset reasons" (page 112) lists the reset reasons and the corresponding code stored in the cppmRestart.dat.

Table 20
CP PM Co-res CS and SS reset reasons

Reset Reason Code	Description
0 Reset button	Reset PPP idle timer to default 30 minutes
2	Power-up reset
3	Reboot from Linux shell
5	Hardware watchdog (stage 2) reset
6	INI button
7	Software reboot: • reboot or reboot -1 from pdt • using appstart facility to restart Call Server

GR N-way configuration

The Call Server can be the Primary Call Server, Secondary Call Server, or the Alternate Call Server in a CS 1000 GR N-way system. Previous CS 1000E Call Server Overlay 117 GR N-way configuration is supported; however, for CS 1000 Release 6.0 the GR N-way is enhanced to

implement secure file transfer methods for database replication between the Main Call Server and the SMGs, replacing the FTP protocol used in CS 1000 Release 5.5 and 5.0.

> ***Note:*** The default route for CP PM Co-res CS and SS is the TLAN port, therefore route configuration is required for CS 1000 system components assigned to a different subnet than the CP PM Co-res CS and SS.

Upgrading a CS 1000 Release 5.5 or 5.0 GR N-way system to CS 1000 Release 6.0 requires that you upgrade all SMGs before the main Call Server to ensure successful GR N-way database replication. For details, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Serial Port configuration

For CP PM Co-res CS and SS, the serial ports on the CP PM card are no longer managed from the Call Server overlays. Serial ports must be configured from the Linux shell. See *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

The following Overlay 17 serial port setting prompts are disabled on the CP PM Co-res CS and SS CP PM card:

- BPS: baudrate setting
- BITL: Data Length
- STOP: number of stop bits
- PARY: Parity
- FLOW: flow control

The prompts display only the current settings; you cannot enter new values.

Table 21
Overlay 17 serial port settings

Prompt	Response	Comment
REQ	CHG	Request
TYPE	ADAN	Action Device and Number
ADAN	chg tty 5	Change an I/O Device
CTYP	CPSI	Card Type
PORT	1	Port Number
DES	<cr>	
BPS	9600	Bits Per Second

Table 21
Overlay 17 serial port settings (cont'd.)

Prompt	Response	Comment
BITL	8	Data Bit Length
STOP	1	Number of Stops
PARY	NONE	Parity Type
FLOW	NO	Flow Control
BCST	<cr>	

Displaying CP PM Co-res CS and SS software version

Procedure 20
Displaying CP PM Co-res CS and SS software version

Step	Action
1	Connect to the CP PM Co-res CS and SS remotely (ssh) or locally (serial port).
2	Log on to CP PM Co-res CS and SS .
3	Issue the swVersionShow command from the Linux Bash Shell:

```
[nortel@ccName_cppm ~]$
```

```
swVersionShow
```

```
Base configuration:  Base Applications
Configuration version 6.00.20
base 6.00.20
Snmp-Daemon-TrapLib 6.00.20
NTAFS 6.00.20
nortel-Radius 6.00.20
Jboss-Quantum 6.00.20
cnd 6.00.20
lhmonitor 6.00.20
kcv 6.00.20
pcap 6.00.20
cppmUtil 6.00.20
oam-logging 6.00.20
dmWeb 6.00.20
baseWeb 6.00.20
ipsec 6.00.20
tap 6.00.20
ISECSH 6.00.20
ipsec 6.00.20
ipsec 6.00.20
```

```
Application configuration:  CS+SS+NRS_EM
Packages:
CS+SS+NRS
EM
NRS
CS
LTPS
Configuration version:  6.00.20


cs 6.00.T
dbcom 6.00.20
cslogin 6.00.20
sigServerShare 6.00.20
csv 6.00.20
tps 6.00.20
vtrk 6.00.20
pd 6.00.20
sps 6.00.20
ncs 6.00.20
gk 6.00.20
nrsm 6.00.20
nrsmWebService 6.00.20
emWeb_6-0 6.00.20
csmWeb 6.00.20
bcc_6-0 6.00.20
csoneksvrmgr 6.00.20
ftrpkg 6.00.20
cs1000WebService_6-0 6.00.20
```

--End--

Displaying Call Server Software Version using Overlay 22 iss command

Procedure 21
Displaying Call Server software version using Overlay 22 iss command

Step	Action
1	Connect to the CP PM Co-res CS and SS remotely (ssh) or locally (serial port).
2	Log on to CP PM Co-res CS and SS.
3	From Linux bash shell, connect to the Call Server by using the csconsole or cslogin command:
4	Login to SL1 and issue the LD 22 iss command `[nortel@ccName_cppm ~]$`

```
cslogin


>
OVL000
>ld 22
PT2000

REQ iss

VERSION 4121

System type is - Communication Server 1000E/CPPM Linux
CP PM - Pentium M 1.4 GHz
PMGs Registered:  2 IPMGs
Unregistered:  0 IPMGs Configured/unregistered:  3

RELEASE 6
ISSUE 00 A
IDLE_SET_DISPLAY NORTEL
IPMG TYPE CSP/SW MSP APP FPGA BOOT DBL1 DBL2
```

--End--

Displaying the Call Server software version from PDT

Procedure 22
Displaying the Call Server Software version from PDT

Step	Action
1	Connect to the CP PM Co-res CS and SS remotely (ssh) or locally (serial port).
2	Log on to CP PM Co-res CS and SS.
3	From Linux bash shell, connect to the Call Server by using the cspdt (to PDT) or csconsole or cslogin command (to CS overlays).
4	Login to Call Server Overlay:
5	Enter ^P^D^T if required to go to CS PDT
6	Issue the osversion and sl1Version commands

```
[nortel@ccName_cppm ~]$
```

```
cspdt
```

```
pdt> osVersion
OS: Date = Apr 24 2009, Time = 13:28:13, Base = x210600a
value = 0 = 0x0
pdt> sl1Version
SL1:  Date = Apr 24 2009, Time = 13:28:15, Base = x210600a
X21 Version:  4121
```

--End--

CP PM Co-res CS and SS configuration and database backup and restore

Note: The sysbackup and sysrestore commands only support USB. CF is not supported.

The Linux Base sysbackup and sysrestore commands provide back up and restore of all configuration data from Linux Base and all Linux applications running on the CP PM Co-res CS and SS.

CP PM Co-res CS and SS does support the existing Call Server backup and restore commands, but these commands back up and restore the Call Server configuration data only.

Local Call Server database Backup and Restore

The following existing commands are supported: **EDD**, **BKO**, and **RES**.

For CP PM, two removable storage devices are supported:

- RMD CF card
- USB drive

By default, if only one device is detected, EDD and BKO will store the backup data on to that device (USB or RMD). The RES command restores data from that device. If both devices are detected, the USB device is used by default.

Two new options are available for the BKO command:

- BKO RMD: Database is backed up to the RMD
- BKO USB: Database is backed up to the USB
- RES RMD: Database is restored from the RMD
- RES USB: Database is restored from the USB

Note: The BKPR command supports rule type USB

Procedure 23
Backing up Call Server data to RMD

Step	Action
1	Connect to the CP PM Co-res CS and SS remotely (ssh) or locally (serial port).
2	Log on to CP PM Co-res CS and SS.
3	From Linux bash shell, connect to the Call Server by using the cspdt (to PDT) or csconsole or cslogin command (to CS overlays).
4	Login to Call Server Overlay:
5	Issue LD 43 BKO RMD command

```
[nortel@ccName_cppm ~]$
cslogin


logi admin2
PASS?
<login banner>
OVL000
>ld 43
EDD000
BKO RMD
Starting CCBR backup to "/var/opt/nortel/cs/fs/u/ccbr/c
cbr.gz":
.
CCBR backup Complete!  100 percent completed
Backing up reten.bkp
Starting database backup to local Removable Media Device
.
Backing up reten.bkp to "/var/opt/nortel/cs/fs/cf2/back
up/single"
Database backup Complete!
TEMU207 Backup process to local Removable Media Device
ended successfully.
.
EDD000
```

--End--

Backing up Call Server data to USB

Procedure 24
Backing up Call Server data to USB

Step	Action
1	Connect to the CP PM Co-res CS and SS remotely (ssh) or locally (serial port).
2	Log on to CP PM Co-res CS and SS.
3	From Linux bash shell, connect to the Call Server by using the cspdt (to PDT) or csconsole or cslogin command (to CS overlays).
4	Login to Call Server Overlay:
5	Issue the LD 43 BKO USB command

```
logi admin2
PASS?
<login banner>
OVL000
>ld 43
EDD000
BKO USB
Starting CCBR backup to "/var/opt/nortel/cs/fs/u/ccbr/c
cbr.gz":
.
CCBR backup Complete!  100 percent completed
Backing up reten.bkp
Starting database backup to local Removable Media Device
.
Backing up reten.bkp to "/var/opt/nortel/cs/fs/usb/back
up/single"
Database backup Complete!
TEMU207 Backup process to local Removable Media Device
ended successfully.
.
EDD000
```

--End--

Note: Two new options are available for the RES command:

- ***RES RMD: Restore database from the RMD***
- ***RES USB: Restore database from USB***

Restoring Call Server data from RMD

Procedure 25
Restoring Call Server data from RMD

Step	Action
1	Connect to the CP PM Co-res CS and SS remotely (ssh) or locally (serial port).
2	Log on to CP PM Co-res CS and SS.
3	From Linux bash shell, connect to the Call Server by using the cspdt (to PDT) or csconsole or cslogin command.
4	Login to Call Server Overlay:
5	Issue LD 43 RES RMD command

```
[nortel@ccName_cppm ~]$
cslogin
```

```
Logi admin2
PASS? ld 43
EDD000 .RES RMD
Starting database restore from "/var/opt/nortel/cs/fs/c
f2/backup/single"
CONFIG
DATA
HI
ZONE
ESET1
ESET2
SYSCFG
SMPCONF
ACCOUNTS
ERL
CDM
NZON
ELIN
SUBNET
NTP
MGC
SYSTEM_PARAMS
PORT_CUSTOM
PORT_STATE
Database restore Complete!
TEMU138 Restoring Process ended successfully.
System Restart required to activate restored database.
.
EDD000
```

--End--

Restoring Call Server data from USB

Procedure 26
Restoring Call Server data from USB

Step	Action
1	Connect to the CP PM Co-res CS and SS remotely (ssh) or locally (serial port).
2	Log on to CP PM Co-res CS and SS.
3	From Linux bash shell, connect to the Call Server by using the cspdt (to PDT) or csconsole or cslogin command (to Call Server overlays).
4	Login to Call Server Overlay:
5	Issue LD 43 RES USB command

```
[nortel@ccName_cppm ~]$
cslogin


logi admin2
PASS?
<login banner>
OVL000
>ld 43
EDD000 .RES USB
Starting database restore from "/var/opt/nortel/cs/fs/u
sb/backup/single"
CONFIG
DATA
HI
ZONE
ESET1
ESET2
SYSCFG
SMPCONF
ACCOUNTS
ERL
CDM
NZON
ELIN
SUBNET
NTP
MGC
SYSTEM_PARAMS
PORT_CUSTOM
PORT_STATE
Database restore Complete!
TEMU138 Restoring Process ended successfully.
System Restart required to activate restored database.
.
EDD000
```

--End--

Remote Call Server database backup and restore

The following existing CCBR commands are supported:

- XBK: backing up the database to an external host using the xmodem File Transfer Protocol (FTP)
- XRT: restoring the database from an external host using the xmodem FTP

Note: These commands are supported on the remote TTY connections only. Overlay 117 bkpr commands also allow a database backup to a remote ftp server.

Complete platform backup and restore

The Nortel Linux Base provides two backup and restore commands for configuration data from all applications running on the platform and the Call Server database. These commands are sysbackup and sysrestore. For details, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Note: Nortel recommends performing a data dump (EDD command) before executing the sysbackup command.

Call Server backup using Overlay 117 backup rules

In previous releases, the bkpr commands in Overlay 117 allowed users to configure a backup rule for backing up the Call Server database to a Secondary Call Server, the FMD, an RMD or an external remote FTP server. In addition to these targets, CP PM Co-res CS and SS supports backing up to a USB device as follows:

- new bkpr <ruleNumber> <ruleType> [N of Version] [Name]
- chg bkpr <ruleNumber> <ruleType> [N of Version] [Name]

where ruleType = <SCS | FTP | FMD |RMD | USB>

Media Gateway Centralized Software Upgrade

The CP PM Co-res CS and SS supports the existing Centralized IP Media Gateway (IPMG) software upgrade feature for upgrading the loadware on the MGC IPMG. The option to select the sequential or simultaneous upgrade method is no longer available during the CP PM Co-res CS and SS installation. The default setting for Centralized Software Upgrade is enabled and sequential upon completion of the CP PM Co-res CS and SS system installation.

You can use the existing Overlay 143 UPGMG command to disable the Centralize Software Upgrade feature. Use the same command to select the sequential or simultaneous upgrade options.

Note 1: If you add additional IPMGs to the system after you enable the Centralized Software Upgrade feature, the CP PM Co-res CS and SS automatically downloads the current IPMG loadware to the newly added IPMGs.

Note 2: The Centralized Software Upgrade settings are not backed up during Call Server Overlay 43 EDD or Linux Base sysbackup. These settings must be re-entered using the Overlay 143 UPGMG command after a CP PM Co-res CS and SS installation or upgrade.

CP PM location (loop and shelf) configuration

In order for the CP PM Co-res CS and SS to respond correctly to the Inventory and STAT CPU commands in overlays 117 and 137 respectively, the CP PM card location information must be configured correctly.

On the CP PM Co-res CS and SS, the CP PM card location configuration can only be performed using the Overlay 117 CHG LCL commands. Unlike the CP PM VxWorks-based Call Server, the CP PM Co-res CS and SS does not support configuring the loop, shelf and side settings during the install process.

Configuration files

The network database file (inet.db) is not used in the CP PM Co-res CS and SS and is not backed up as part of the Call Server database. You must use the Nortel Linux Base **`sysbackup`** and **`sysrestore`** commands to back up the network configuration information.

Security configuration

UCM configuration

IP Security configuration is no longer supported for the CP PM Co-res CS and SS Call Server. Instead, IP Security parameters must be configured from UCM. See *Unified Communications Management Common Services Fundamentals (NN43001-116)* for details.

Table 22 "Overlay 117 IPSSS commands not supported on the CP PM Co-res CS and SS Call Server" (page 125)lists the ISSS commands from LD 117 not supported on the CP PM Co-res CS and SS Call Server.

Table 22
Overlay 117 IPSSS commands not supported on the CP PM Co-res CS and SS Call Server

Command	Description
CHG ISEC	Change ISEC pre-shared key or security level (ISEC--Intra System Signaling Security)
COMMIT ISEC	Commit for ISEC profile changes
CONFIRM ISEC	Used to confirm PSK between Active Call Server and other elements
DIS ISEC	Disables system security (ISEC--Intra System Signaling Security)
DIS ISECTAR	Disables target security for ISEC
ENL ISEC	Enables system security (ISEC--Intra System Signaling Security)
ENL ISECTAR	Enables target security for ISEC
NEW ISECTAR	Adds a new target to ISEC target list
OUT ISECTAR	Deletes a target from ISEC target list
PRT ISEC	Shows system ISEC status. There are three options: ALL, EXCEP and TARGET
PRT ISECTAR	Display all targets information

Centralized authentication

UCM provides a centralized, GUI-based interface for individual account administration for the CS 1000 network. When a user logs into a Linux server CLI they are prompted for a user name and password. First the user name and password are authenticated locally. The user name and password are then encrypted and sent to the centralized UCM security server via the radius protocol for verification. If the user is defined in the UCM database they are granted access to the proper Linux shell with the roles defined in the UCM database.

UCM can function as a Radius server, providing authentication for Radius clients.

For more information on UCM role creation, see *Unified Communications Management* (NN43001-116).

CS 1000 Access Restrictions

You can use access restrictions to prevent port-based attacks on system components by configuring port blocking rules. These rules are installed during initial Communication Server 1000 software installation and are preconfigured with factory default settings. A port blocking state indicating

file indicates whether the feature is currently active or not. The rules are automatically propagated from the Call Server to dependent VGMC platforms.

You can configure the port blocking rules using LD 117 or Element Manager, but there are a few mandatory rules that cannot be modified or deactivated. The mandatory rules are considered system essential and remain in an activated state regardless of whether the port access is configured with default or customized settings.

The port access rules can only be activated on servers with VxWorks platforms (MGC, MC32S, CP PIV and CP PM). CP PM Co-res CS and SS uses a Linux-based platform with a shell application called VxWorks (VXELL) Call Server. As a result, you cannot enable the port access restrictions rules directly for this type of server, but you can administer the port access for other VxWorks components. The access restrictions feature is not supported on the SSC, CP PII, ITG-P, ITG-SA, MIXX, and ISP1100 platforms.

> ***Note:*** The Call Server component of this feature is directly related to the Call Server software release. If an upgrade is performed and the software is later backed out or downgraded, reinstalling a previous release will overwrite the access restrictions default and state files.

The directory structures for storing access files are different for VxWorks and Linux platforms. Table 23 "Port blocking file locations for VxWorks and Linux systems" (page 126) lists the file names and locations for each platform.

Table 23
Port blocking file locations for VxWorks and Linux systems

VxWorks systems	
File	**Location**
default	/p/accres/defaultport.xml
state	/u/db/portstate.txt
custom	/u/db/customport.xml
Linux systems (CP PM Co-res CS and SS)	
File	**Location**
default	/var/opt/Nortel/cs/fs/p/accres/defaultport.xml
state	/var/opt/Nortel/cs/fs/u/db/portstate.txt
custom	/var/opt/Nortel/cs/fs/u/db/customport.xml

cspdt and cslogin

The **cslogin** command starts an overlay shell on the local or remotely located Call Server. The **cspdt** command starts a pdt shell on the local or remotely located Call Server.

Both the **cslogin** and **cspdt** commands require that the user has a role via the UCM web page with Linux Base Maintenance Administrator privileges. The user name used to login to the Linux server need not be the same as the user name used to further login to the Call Server pdt or overlay shell.

If central authentication is enabled on the Call Server, the user name used to logon to the respective Call Server shell is required to have a UCM role with the appropriate CS 1000 privileges, Overlay Options for cslogin, and Diagnostic (PDT) access for cspdt.

> ***Note:*** If a user has both PDT and admin privileges and enters the cspdt command at the Call Server CLI prompt, the Overlay shell is started by default.

If central authentication is disabled on the Call Server, UCM accounts will not work for either pdt or overlay access. Only usernames local to the Call Server and having the appropriate permissions can login to the respective shells.

Central authentication It is enabled and disabled via the Call Server overlay LD117 commands **register ucmsecurity device** and **unregister ucmsecurity device**, respectively.

Shell and transfer commands

CP PM Co-res CS and SS supports enabling and disabling secure and insecure access protocols such as SSH, SFTP, TELNET, RLOGIN and FTP. These settings are configured using the Linux Base harden commands. See *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)*.

Overlay 117 commands for secure and insecure shells or transfers are still supported for CP PM Co-res CS and SS, however these commands are only used for configuring the secure and insecure shell and transfers on the MGCs and Media Cards that are registered to the CP PM Co-res CS and SS Call Server. The Overlay 117 commands do not affect the secure and insecure shells or transfers on the CP PM Co-res CS and SS itself or any Signaling servers that are registered to the CP PM Co-res CS and SS Call Server.

Table 24 "Overlay 117 Shell and Transfer commands" (page 128) lists the shell and transfer commands supported for CP PM Co-res CS and SS.

Table 24
Overlay 117 Shell and Transfer commands

Command	Description
ENL SHELLS SECURE	Enables all secure shells. This includes SSH, sFTP, and SCP sessions. This command will not affect the secure shell settings on the CP PM Co-res CS and SS but it will enable secure shells on all the MGCs and Media Cards that are registered to the CP PM Co-res CS and SS Call Server.
DIS SHELLS SECURE	Disables all secure shells in the system. This includes SSH, sFTP, and SCP sessions This command will not affect the secure shell settings on the CP PM Co-res CS and SS but it will disable secure shells all the MGCs and Media Cards that are registered to the CP PM Co-res CS and SS Call Server.
STAT SHELLS SECURE	Shows whether secure shell access is enabled or disabled on all the MGC and Media Cards that are registered to the CP PM Co-res CS and SS Call Server.
ENL TRANSFERS SECURE	Enables all secure transfers in the system. This includes SFTP sessions. This command will not affect the secure transfer settings on the CP PM Co-res CS and SS but it will enable secure transfers on all the MGCs and Media Cards that are registered to the CP PM Co-res CS and SS Call Server.
DIS TRANSFERS SECURE	Disables all secure transfers in the system. This includes SFTP sessions. This command will not affect the secure transfer settings on the CP PM Co-res CS and SS but it will disable secure transfers all the MGCs and Media Cards that are registered to the CP PM Co-res CS and SS Call Server.
STAT TRANSFERS SECURE	Shows whether secure transfer is enabled or disabled on all the MGC and Media Cards that are registered to the CP PM Co-res CS and SS Call Server.
ENL SHELLS INSECURE	Enables all insecure shells in the system. This includes TELNET, RLOGIN, and FTP sessions. This command will not affect the insecure shell settings on the CP PM Co-res CS and SS but it will enable insecure shells on all the MGCs and Media Cards that are registered to the CP PM Co-res CS and SS Call Server.

DIS SHELLS INSECURE	Disables all insecure shells in the system. This includes TELNET, RLOGIN, and FTP sessions. This command will not affect the insecure shell settings on the CP PM Co-res CS and SS but it will disable insecure shells all the MGCs and Media Cards that are registered to the CP PM Co-res CS and SS Call Server.
STAT SHELLS INSECURE	Shows whether insecure shell access is enabled or disabled on all the MGC and Media Cards that are registered to the CP PM Co-res CS and SS Call Server.
ENL TRANSFERS INSECURE	Enables all insecure transfers in the system. This includes FTP sessions. This command will not affect the insecure transfer settings on the CP PM Co-res CS and SS but it will enable insecure transfers on all the MGCs and Media Cards that are registered to the CP PM Co-res CS and SS Call Server.
DIS TRANSFERS INSECURE	Disables all insecure transfers in the system. This includes FTP sessions. This command will not affect the insecure transfer settings on the CoRes Server but it will disable insecure transfers all the MGCs and MCs that are registered to the CoRes Call Server.
STAT TRANSFERS INSECURE	Shows whether insecure transfer is enabled or disabled on all the MGC and Media Cards that are registered to the CoRes Call Server.

SSH Commands

CP PM Co-res CS and SS Call Server Overlay support for SSH Key configuration is limited. The SSH Key must be configured from UCM. See *Unified Communications Management Common Services Fundamentals (NN43001-116)* for details.

Table 25 "Overlay 117 SSH Key commands" (page 129) lists the SSH commands.

Table 25
Overlay 117 SSH Key commands

Command		Description
SSH Key commands supported on CP PM Co-res CS and SS		
SSH KEY ACTIVATE CABINET		Activate the ssh key for the specified cabinet or all or the cabinets

SSH KEY ACTIVATE INACTIVE		Activate the ssh key for the inactive core
SSH KEY CLEAR CABINET		Delete the public ssh keys for the specified cabinet or all of the cabinets
SSH KEY GENERATE CABINET		Generate the ssh key for the specified cabinet or all of the cabinets
SSH KEY SHOW CABINET		Display the ssh key finger prints for the specified cabinet or all or the cabinets
SSH Key commands not supported on CP PM Co-res CS and SS		
SSH KEY ACTIVATE ACTIVE		Activate the ssh key for the active core
SSH KEY CLEAR ACTIVE		Delete the public ssh keys for the active core
SSH KEY CLEAR INACTIVE		Delete the public ssh keys for the inactive core
SSH KEY GENERATE ACTIVE		Generate the ssh key for the active core
SSH KEY GENERATE INACTIVE		Generate the ssh key for the inactive core
SSH KEY SHOW ACTIVE		Display the ssh key finger prints for the active core
SSH KEY SHOW INACTIVE		Display the ssh key finger prints for the inactive core

Procedure 27
Accessing RMD and USB from Call Server PDT shell

Step	Action
1	Connect to the CoRes Server remotely (ssh) or locally (serial port).
2	Log in to CoRes server.

3	Log in to Call Server PDT shell using cspdt:
	`pdt> cd /cf2`
	`cf2 mounted Successfully.`
	`Please call unmount /cf2 before removing device`
	`pdt> unmount /cf2`

--End--

IP Sec

Use IPSec for network-wide policy implementation and synchronization of pre-shared keys across network targets. IPSec is enabled and configured after installing UCM. For more information about using IPSec, see *Security Management Fundamentals (NN43001-604)*.

Maintenance

Power up and power down procedures

The existing CP PM based Call Server power up and power down procedure is supported for CP PM Co-res CS and SS, however the bootup sequence is different from the existing VxWorks-based servers. On power up, system boot time is longer due to the Linux OS loading before all applications.

Diagnostic logs

Call Server RPT log viewer

The CP PM Co-res CS and SS uses both the existing CS 1000 RPT report log and the Linux syslog facilities. The RPT report log is used for the Call Server application running on the Call Server. All other Linux applications use the Linux syslog for event logging.

The Call Server report log can be viewed from the Call Server PDT shell or from Element Manager. The Call Server RPT report log viewer is also available for viewing the report log files from the Linux bash shell. This allows the display of the RPT report log without logging in to the Call Server PDT shell or using Element Manager.

Procedure 28
Viewing the Call Server report log using rpt

Step	Action
1	Connect to the CP PM Co-res CS and SS remotely (ssh) or locally (serial port).
2	Log on to CP PM Co-res CS and SS using the default emergency account or Nortel account.
3	Issue the rpt command from Linux bash shell: `[nortel@davecppm3 dev]# rpt`

```
Reading /var/opt/nortel/cs/fs/e/rpt/LOG00000.RPT Newes
t File Name "/var/opt/nortel/cs/fs/e/rpt/LOG00000.RPT"
File being viewed :  "/var/opt/nortel/cs/fs/e/rpt/LOG00
000.RPT"
Capacity in bytes :  1000000
Capacity in records :  980
Number of records = 104
Oldest record = 0, logged at 31/12/1969 19:00:00
Newest record = 103, logged at 06/05/2008 09:22:06
Current Record = 103
Display Increment = 10 records
...
375e00c4:375dff80 eeeeeeee 00000000 00000000 00a7dff4
375dff80 00000000 375dff58

Please enter rptReport command:  rdhelp for help quit(q)
to exit
```

--End--

Call Server csconsole log

On startup the Call Server application is run as a background process on the CP PM Co-res CS and SS. To access the Call Server use the csconsole, cspdt and cslogin commands.

All console output for the Call Server process is logged and stored in the /var/log/nortel/cs_console.log file.

System messages

CP PM Co-res CS and SS system messages

The following new system messages are added for CP PM Co-res CS and SS.

SCH2338 CPSI Port 1 not supported on Linux Call Server

Action:

Severity: **Critical to Monitor:** **SNMP trap:**

SCH2284 Time and Date changes are not supported on Linux Call Server

Action:

Severity: **Critical to Monitor:** **SNMP trap:**

TFC0006 Command not supported on Linux Call Server

Action:

Severity: **Critical to Monitor:** **SNMP trap:**

TFC0007 Time and Date changes are not supported on Linux Call Server

Action:

Severity: **Critical to Monitor:** **SNMP trap:**

Technical assistance service

Contents

This section contains information on the following topics:

Nortel Technical Assistance Centers

To help customers obtain maximum benefit, reliability, and satisfaction from their CS 1000E system s, Nortel provides technical assistance in resolving system problems. Table 26 "Customer Technical Services (CTS)" (page 137) lists the centers that provide this service.

Table 26
Customer Technical Services (CTS)

Location	Contact
Nortel Global Enterprise Technical Support (GETS) PO Box 833858 2370 Performance Drive Richardson, TX 75083 USA	North America Telephone: 1 800 4NORTEL
Nortel Corp. P.O. Box 4000 250 Sydney Street Belleville, Ontario K8N 5B7 Canada	North America Telephone: 1 800 4NORTEL

Table 26
Customer Technical Services (CTS) (cont'd.)

Location	Contact
Nortel Service Center - EMEA	EMEA Telephone: 00 800 8008 9009 or +44 (0)870 907 9009 E-mail: emeahelp@nortel.com
Nortel 1500 Concord Terrace Sunrise, Florida 33323 USA	Brazil Telephone: 5519 3705 7600 E-mail: entcts@nortel.com English Caribbean Telephone: 1 800 4NORTEL Spanish Caribbean Telephone: 1 954 858 7777 Latin America Telephone: 5255 5480 2170
Network Technical Support (NTS)	Asia Pacific Telephone: +61 28 870 8800 Australia Telephone:1800NORTEL (1800 667835) or +61 2 8870 8800 E-mail: asia_support@nortel.com People's Republic of China Telephone: 800 810 5000 E-mail: chinatsc@nortel.com Japan Telephone: 010 6510 7770 E-mail: supportj@nortel.com Hong Kong Telephone: 800 96 4199 E-mail: chinatsc@nortel.com Taiwan Telephone: 0800 810 500 E-mail: chinatsc@nortel.com

Table 26
Customer Technical Services (CTS) (cont'd.)

Location	Contact
	Indonesia Telephone: 0018 036 1004 Malaysia Telephone: 1 800 805 380 New Zealand Telephone: 0 800 449 716 Philippines Telephone: 1 800 1611 0063 or 632 917 4420 Singapore Telephone: 800 616 2004 South Korea Telephone: 0079 8611 2001 Thailand: Telephone: 001 800 611 3007

Services available

Services available through the Technical Assistance Centers include:

- diagnosing and resolving software problems not covered by support documentation
- diagnosing and resolving hardware problems not covered by support documentation
- assisting in diagnosing and resolving problems caused by local conditions

There are several classes of service available. Emergency requests (Class E1 and E2) receive an immediate response. Service for emergency requests is continuous until normal system operation is restored. Non-emergency requests (Class S1, S2, and NS) are serviced during normal working hours. Table 27 "Technical service emergency classifications" (page 140) and Table 28 "Technical services non-emergency classifications" (page 140) describe the service classifications.

Table 27
Technical service emergency classifications

Class	Degree of failure	Symptoms
E1	Major failure causing system degradation or outage	System out-of-service with complete loss of call-processing capability. Loss of total attendant console capability. Loss of incoming or outgoing call capability. Loss of auxiliary Call Detail Reporting (CDR) in resale application. Call processing degraded for reasons such as trunk group out-of-service: • 10% or more lines out-of-service • frequent initializations (seven per day or more) • inability to recover from initialization or SYSLOAD • consistently slow dial tone (eight seconds or more delay)
E2	Major failure causing potential system degradation or outage	Standby CPU out-of-service. Frequent initializations (one per day or more). Disk drive failure. Two sets of disks inoperative.

Table 28
Technical services non-emergency classifications

Class	Degree of failure	Symptoms
S1	Failure that affects service	Software or hardware trouble directly and continuously affecting user's service or customer's ability to collect revenue. Problem that seriously affects service at in-service or cut-over date.

Table 28
Technical services non-emergency classifications (cont'd.)

Class	Degree of failure	Symptoms
S2	Intermittent failure that affects service	Software or hardware faults that intermittently affect service. System-related documentation errors that directly result in or lead to impaired service.
NS	Failure that does not affect service	Documentation errors. Software inconsistencies that do not affect service. Hardware diagnostic failures (not previously defined) that cannot be corrected by resident skills. Test equipment failures for which a backup or manual alternative can be used. Any questions concerning products.

Except as excluded by the provisions of warranty or other agreements with Nortel, a fee for technical assistance may be charged, at rates established by Nortel. Information on rates and conditions for services are available through Nortel sales representatives.

Requesting assistance

Collect the information listed in Table 29 "Checklist for service requests" (page 141) before you call for service.

Table 29
Checklist for service requests

Name of person requesting service	_____
Company represented	_____
Telephone number	_____
System number/identification	_____
Installed software generic and issue (located on data disk)	_____
Modem telephone number and password (if applicable)	_____

Table 29
Checklist for service requests (cont'd.)

Seriousness of request (see Table 27 "Technical service emergency classifications" (page 140) and Table 28 "Technical services non-emergency classifications" (page 140))	_____
Description of assistance required	_____
_____	
_____	

Nortel Communication Server 1000

CP PM Co-resident Call Server and Signaling Server Fundamentals

Release: 6.0
Publication: NN43001-509
Document revision: 01.06
Document release date: 5 October 2009

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com

NORTEL