Nortel Communication Server 1000 Co-resident Call Server and Signaling Server Fundamentals

7.0
NN43001-509, 02.04

July 2010

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

Copyright

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/Copyright/.

Preventing toll fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://www.avaya.com/support/. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Chapter 1: New in this release

The following sections detail what is new in this document for Nortel Communication Server 1000 Release 7.0.

Navigation

- Features on page 7
- Other on page 9

Features

This section describes new features or hardware introduced in Communication Server 1000 Release 7.0.

Hardware platforms

CS 1000 Release 7.0 Co-resident Call Server and Signaling Server (Co-res CS and SS), is capable of running the Call Server software, Signaling Server software, and System Management software on a hardware platform running the Linux Base Operating System.

For CS 1000 Release 7.0, various hardware platforms support the Co-res CS and SS configuration. For information about the supported hardware roles, see Table 2: Hardware platform supported roles on page 16.

Table 1: Co-res CS and SS system types

Server hardware for Co-res CS and SS	System types for VxELL Servers
CP PM	4121
CP DC	4221
CP MG 32	4321
CP MG 128	4421
COTS2	4521

Common Processor Dual Core (CP DC) card

The Common Processor Dual Core (CP DC) card is introduced. The CP DC is a Server card for use in a Communication Server 1000E system. The CP DC card contains a dual core AMD processor and upgraded components which can provide improvements in processing power and speed over existing Server cards.

The CP DC card is available in two versions:

- NTDW53AAE6 - single slot metal faceplate CP DC card for CS 1000E systems
- NTDW54AAE6 - double slot metal faceplate CP DC card for CS 1000M systems

The CP DC card requires the Linux Base Operating System, and supports Co-resident Call Server and Signaling Server, or stand-alone Signaling Server configurations. The CP DC card does not support the standard or high availability Call Server configuration.

Common Processor Media Gateway (CP MG) card

The Common Processor Media Gateway (CP MG) card is introduced. The hardware for the CP MG card consists of integrating a Common Processor, a Gateway Controller, and non-removable Digital Signal Processor (DSP) resources into a single card for use in a Communication Server 1000E system.

The CP MG card is available in two versions:

- NTDW56BAE6 - CP MG card with 32 DSP ports
- NTDW59BAE6 - CP MG card with 128 DSP ports

The CP MG card provides improvements in port density and cost reductions by functioning as a Call Server or Application Server and a Gateway Controller with DSP resources while occupying slot 0 in a Media Gateway. The CP MG card requires the Linux Base Operating System. The CP MG 128 supports the Co-resident Call Server and Signaling Server, and CS 1000E TDM configurations. The CP MG 32 supports the SIP Survivable Media Gateway (SSMG), and Branch Office configurations. The CP MG card does not support the standard or high availability Call Server configuration.

128-port DSP daughterboard

The 128-port Digital Signal Processor (DSP) daughterboard (DB-128) for the Media Gateway Controller (MGC) card is introduced. An MGC card populated with one NTDW78 DB-128 can provide 128 DSP ports.

The CS 1000E Peripheral Rate Interface (PRI) Media Gateway (PRI Gateway) can support a MGC card populated with two DB-128 for a maximum of 256 DSP ports. The Extended Media

Gateway PRI (MGP) package 418 is required to support MGC cards populated with two DB-96 or two DB-128.

Other

Revision History

July 2010 Standard 02.04. This document is up-issued to update planning and engineering content.

July 2010 Standard 02.03. This document is up-issued to include recommended USB memory stick support.

June 2010 Standard 02.02. This document is up-issued to include CP PM version 2 content.

June 2010 Standard 02.01. This document is issued to support the Co-resident Call Server and Signaling Server for Nortel Communication Server 1000 Release 7.0.

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.

Chapter 2: 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: http://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: http://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: http://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.

Chapter 3: 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 Co-resident Call Server and Signaling Server (Co-res CS and SS) for Nortel Communication Server 1000 Release 7.0.

Legacy products and releases

This document contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 7.0 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:

- Communication Server 1000E
- Branch office Media Gateway
- Survivable Media Gateway

Intended audience

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

Only qualified personnel are to install 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.

Co-res CS and SS task flow

The following graphic shows the task flow to deploy a Co-res CS and SS system.

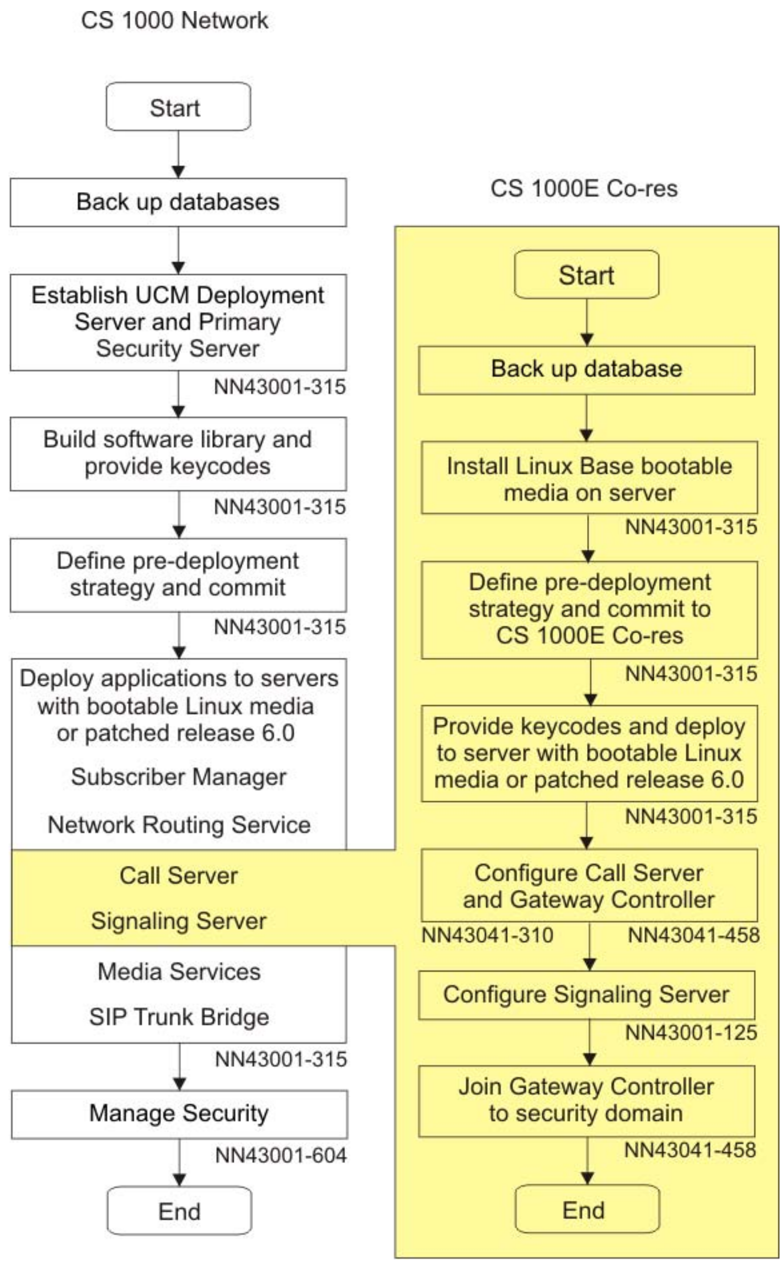

CS 1000 Network
Start
Back up databases
Establish UCM Deployment Server and Primary Security Server
NN43001-315
Build software library and provide keycodes
NN43001-315
Define pre-deployment strategy and commit
NN43001-315
Deploy applications to servers with bootable Linux media or patched release 6.0
Subscriber Manager
Network Routing Service
Call Server
Signaling Server
Media Services
SIP Trunk Bridge
NN43001-315
Manage Security
NN43001-604
End
CS 1000E Co-res
Start
Back up database
Install Linux Base bootable media on server
NN43001-315
Define pre-deployment strategy and commit to CS 1000E Co-res
NN43001-315
Provide keycodes and deploy to server with bootable Linux media or patched release 6.0
NN43001-315
Configure Call Server and Gateway Controller
NN43041-310
NN43041-458
Configure Signaling Server
NN43001-125
Join Gateway Controller to security domain
NN43041-458
End

Figure 1: Co-res CS and SS task flow

Conventions

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

In this document, the following Chassis or Cabinets are referred to generically as Media Gateway:

- Option 11C Mini Chassis (NTDK91) and Chassis Expander (NTDK92)
- Option 11C Cabinet (NTAK11)
- MG 1000E Chassis (NTDU14) and Expansion Chassis (NTDU15)
- Media Gateway 1010 (MG 1010) (NTC310)

In this document, the following hardware is referred to as Gateway Controller:

- Media Gateway Controller (MGC) card (NTDW60 and NTDW98)
- Common Processor Media Gateway (CP MG) card (NTDW56 and NTDW59)

In this document, the following hardware is referred to generically as Server:

- Common Processor Pentium Mobile (CP PM) card
- Common Processor Media Gateway (CP MG) card
- Common Processor Dual Core (CP DC) card
- Commercial off-the-shelf (COTS) servers
    - IBM x306m server (COTS1)
    - HP DL320 G4 server (COTS1)
    - IBM x3350 server (COTS2)
    - Dell R300 server (COTS2)

In this document, the generic term COTS refers to all COTS servers. The term COTS1 or COTS2 refers to the specific servers in the preceding list.

Co-res CS and SS is not supported on COTS1 servers. You can deploy a COTS1 server as a stand-alone Signaling Server.

The following table shows CS 1000 Release 7.0 supported roles for hardware platforms.

Table 2: Hardware platform supported roles

Hardware platform	VxWorks Server	Linux Server	Co-res CS and SS	Gateway Controller
CP PIV	yes	no	no	no
CP PM	yes	yes	yes	no
CP DC	no	yes	yes	no
CP MG	no	no	yes (see note)	yes (see note)
MGC	no	no	no	yes
MG XPEC	no	no	no	yes

Hardware platform	VxWorks Server	Linux Server	Co-res CS and SS	Gateway Controller
COTS1	no	yes	no	no
COTS2	no	yes	yes	no

Note:

The CP MG card functions as the Co-resident Call Server and Signaling Server, and the Gateway Controller while occupying slot 0 in a Media Gateway.

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)

Chapter 4: Overview

Introduction

A Communication Server 1000 (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.

The CS 1000 Release 7.0 Co-resident Call Server and Signaling Server (Co-res CS and SS) runs the Call Server software, the Signaling Server software, and System Management software on one hardware platform running the Linux Base Operating System. For CS 1000 Release 7.0, the Co-res CS and SS supports various hardware platforms, see Table 2: Hardware platform supported roles on page 16.

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 Co-res CS and SS in the following configurations:

- Communication Server 1000E (CS 1000E)
- Branch Office Media Gateway (MG 1000B)
- Survivable Media Gateway (SMG)
- Survivable SIP Media Gateway (SSMG)
- Communication Server 1000E TDM (CS 1000E TDM)

You can deploy a Co-res CS and SS as a Main Office, Branch Office, or SSMG.

Note:

For details on CS 1000E Capacity limitations, see Planning and engineering on page 27

Co-res CS and SS based CS 1000E system

Figure 2: CS 1000E CP PM Co-res CS and SS System on page 20 provides an example of a CS 1000E system with a CP PM based Co-res CS and SS in a MG 1000E chassis. You can also use a COTS2 server, or an MG 1010, chassis, or cabinet with a CP DC or CP MG card to deploy a Co-res CS and SS.

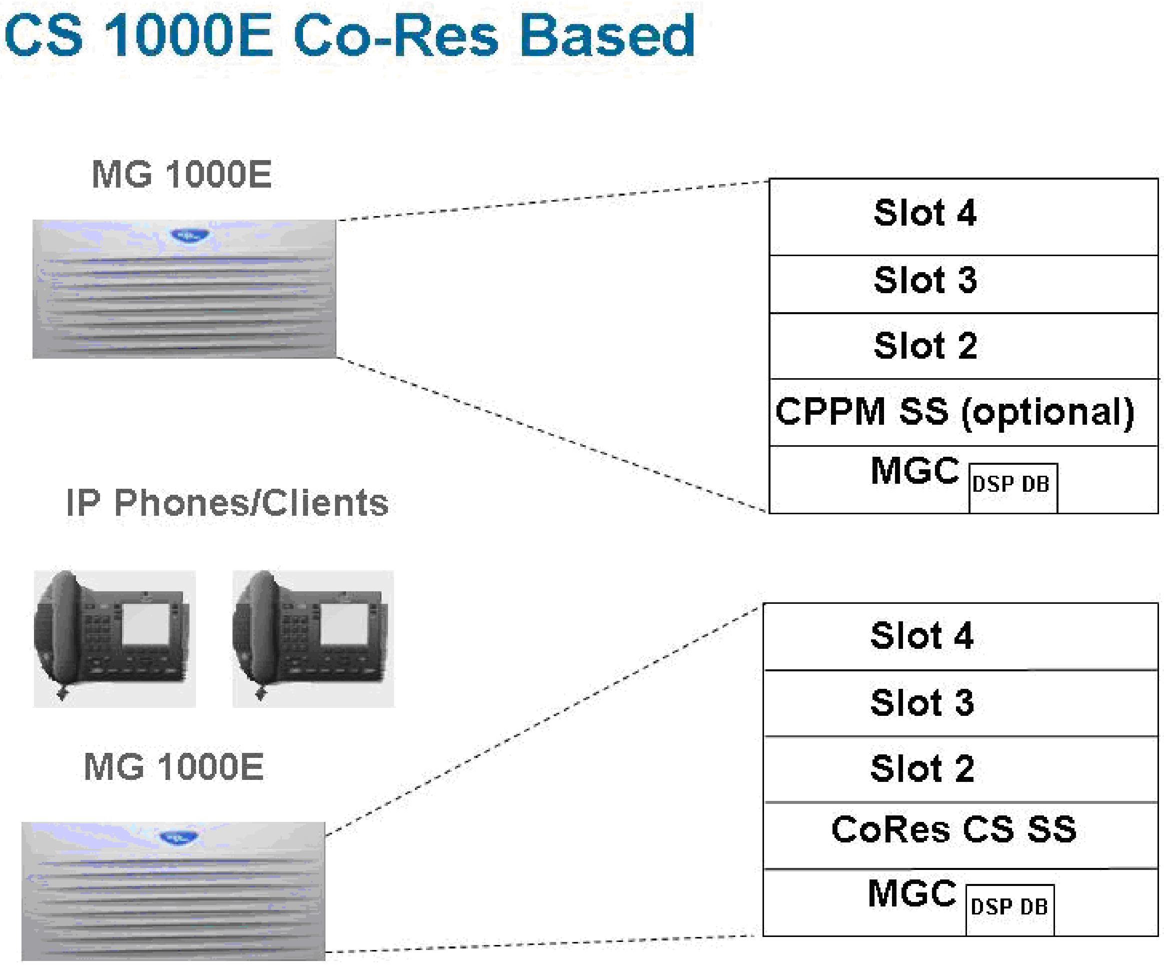


Figure 2: CS 1000E CP PM Co-res CS and SS System

Optional second Signaling Server

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

Co-res CS and SS based Branch Office Media Gateway

Figure 3: MG 1000B CP PM Co-res CS and SS System on page 21 provides an example of a Co-res CS and SS based Branch Office Media Gateway (MG 1000B) system.

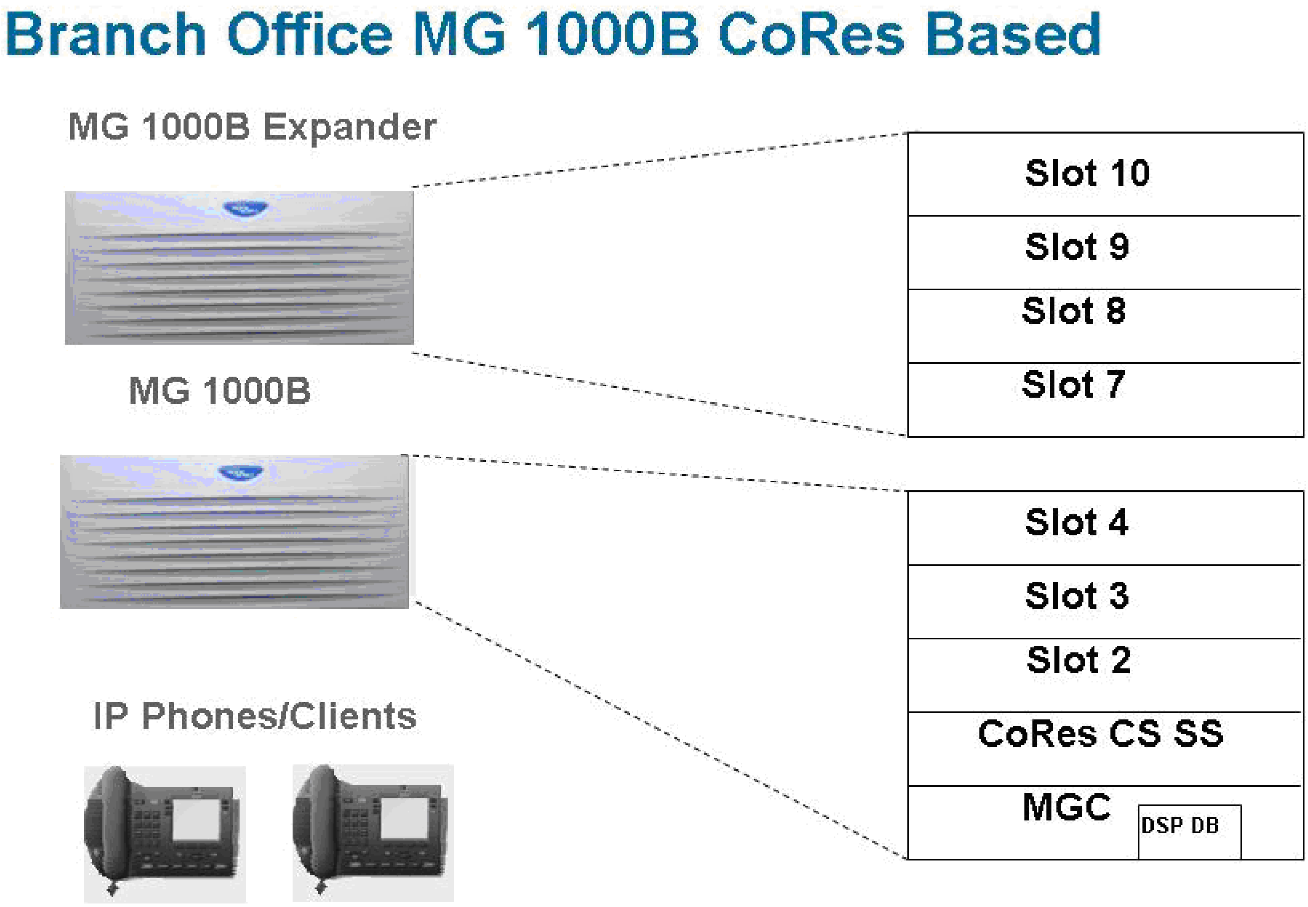


Figure 3: MG 1000B CP PM Co-res CS and SS System

CS 1000E TDM

CS 1000 Release 7.0 supports a TDM only version of the Co-res CS and SS on CP PM, CP DC, and CP MG 128 platforms. The CS 1000E TDM system has the following capacity limitations:

- 720–800 combined TDM users (Traditional, CLASS, DECT users, including installed plus 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. The CS 1000E TDM system does not support CP MG 32 or COTS platforms.

TDM user range of 720–800 is based on Cabinet or Chassis card slot limits.

High Availability (HA) support

The 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, you must deploy a VxWorks-based CS 1000 system.

Co-res CS and SS upgrade paths

The following upgrade paths are supported for Communication Server 1000 systems.

- CS 1000 Release 6.0 or earlier CP PM based CS 1000E with Standard Availability (SA) to a CS 1000 Release 7.0 Co-resident Call Server and Signaling Server.
- CS 1000 Release 6.0 or earlier CP PM based CS 1000E Signaling Server to CS 1000 Release 7.0 Co-res CS and SS

- CS 1000 Release 6.0 or earlier CP PM based Meridian 1 Option 11C, CS 1000M, or CS 1000S to CS 1000 Release 7.0 Co-res CS and SS
- CS 1000 Release 6.0 or earlier CP PM based Meridian 1 Option 11C to CS 1000 Release 7.0 CS 1000E TDM.

Note:

Minimum CS 1000 Release for Small System migration to Co-res CS and SS is Release 23.10.

Note:

If you upgrade from a non-CP PM based CS 1000E Server, you must replace your old Server hardware with either a CP PM card, CP MG card, CP DC card, or COTS2 server and upgrade the software.

Hardware

The Communication Server 1000 Release 7.0 Co-resident Call Server and Signaling Server is supported on CP PM cards, CP MG cards, CP DC cards, and COTS2 servers running the Linux base Operating System.

The Co-res CS and SS can run on the CP PM hardware platform introduced in Communication Server 1000 Release 5.0, however the software changes from VxWorks to Linux, and a CP PM Linux upgrade kit is required. The CP PM card requires BIOS version 18 or later, 2 GB memory, and a 40 GB hard drive to support the Co-res CS and SS configuration.

For more information about the hardware platforms, see *Circuit Card Reference, NN43001-311*

CP PM upgrade kit

The CP PM Server Linux Upgrade kit can include the following items:

- 2 GB Compact Flash (CF) with Linux software
- 1 GB DDR SO-DIMM memory
- 40 GB Hard Drive kit , Linux OS preloaded (optional, provisioned if required)

CP PM Media Storage

For CP PM cards configured with an internal hard drive Fixed Media Drive (FMD), you must ensure switch S5 on the CP PM card is in position 2. Position 2 configures the CP PM card to boot from the hard drive FMD. Switch S5 in position 1 configures the CP PM card to boot from the internal Compact Flash (CF) FMD. The hard drive FMD is required for Linux deployments. The CF card FMD is required for VxWorks deployments.

The CP PM card supports two types of Removable Media Drives (RMD)

- CF card, supports the installation of Linux Base and Linux applications
- USB memory stick device, supports the installation of Linux applications (cannot use to install Linux Base)

Note:

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

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

CP MG, CP DC, and COTS2 media storage

The CP MG card, CP DC card, and COTS2 servers require an internal hard drive Fixed Media Drive (FMD). The FMD contains the Linux Base Operating System. The CP MG and CP DC card use a 160 GB SATA FMD. The COTS2 servers contain different sizes of SATA FMD based on your purchase configuration.

The CP MG, CP DC, and COTS2 support USB 2.0 storage devices as Removable Media Drives (RMD). A bootable USB 2.0 storage device can be used to install or patch the Linux Base Operating System. The CP MG, CP DC and COTS2 hardware platforms do not support CF cards as RMD.

Note:

The N0220961 USB memory stick is supported for Communication Server 1000 Release 7.0. Not all USB memory sticks are supported.

For information about installing hard drives on circuit cards, see *Circuit Card Reference, NN43001-311*. For information about installing hard drives on COTS servers, see your manufacturers COTS server user manual.

Software applications

The Co-res CS and SS supports the following software applications

- Linux Call Server
- Line Telephony Proxy Server (LTPS)

- Unicode Name Directory (UND)
- Signaling Server Gateway including H.323 Gateway and SIP Gateway
- SIP Line Gateway
- Failsafe SIP Proxy Service, Gatekeeper
- Personal Directory (PD)
- Network Routing Service (NRS)
    - You can configure the NRS as Primary, however you can only configure NRS as a Secondary if the Primary is also running on a Co-res CS and SS.
    - The CP PM based Co-res CS and SS does not support a Secondary or backup NRS to capacity higher than the Primary NRS due to the small disk size and low call rates on a CP PM based Co-res CS and SS.
- Element Manager
- Unified Communications Management (UCM) Primary Security Server in limited deployment. For detailed UCM Primary Security Server procedures, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*

Element Manager

The Element Manager (EM) 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 EM, see *Element Manager System Reference - Administration, NN43001-632*.

Chapter 5: Planning and engineering

Introduction

Complete all system planning and engineering activities before using this guide to install a Co-resident Call Server and Signaling Server (Co-res CS and SS).

System parameter considerations

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

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

Engineering of Media Gateway card placement and DSPs is the same as for a CS 1000E system. For details, see *Communication Server 1000E Planning and Engineering, NN43041–220*.

Hardware requirements

The Co-res CS and SS can be deployed on various hardware platforms. For CS 1000 Release 7.0, the Co-res CS and SS supports the following Servers:

- Common Processor Pentium Mobile (CP PM) card
- Common Processor Media Gateway (CP MG) card
- Common Processor Dual Core (CP DC) card
- IBM x3350 and Dell R300 Commercial off-the-shelf (COTS) servers (COTS2)

The Server cards install in Media Gateway IPE slots, the COTS servers install in standard 19 inch racks.

One Gateway Controller is required in each Media Gateway cabinet or chassis. The Gateway Controller can be an MGC card or a CP MG card.

Note:

The CP MG card functions as a Gateway Controller and a Co-resident Call Server and Signaling Server while occupying slot 0 in a Media Gateway. The CP MG card is available with 32 or 128 DSP ports. The CP MG 32 supports the Survivable SIP Media Gateway (SSMG) or Branch Office (MG 1000B) configuration only.

For more information about the CP PM, CP DC, CP MG, MGC, and COTS2 hardware, see *Circuit Card Reference, NN43001-311*.

Security dongle

Server hardware you configure for Co-res CS and SS requires a security dongle for Call Server software and keycode validation. Server cards provide an internal security dongle holder on the circuit card. To determine the security dongle location on various Server cards, see *Circuit Card Reference, NN43001-311*.

COTS2 servers require an NTRH9220E5 USB security dongle adapter (the adapter is provided with the software kit), see Figure 4: NTRH9220E6 USB security dongle adapter for COTS2 servers on page 28. For increased security, ensure the USB security dongle adapter is hidden from plain view. Do not insert the USB security dongle adapter into a front USB port. Nortel recommends you insert the USB security dongle adapter into the internal USB port on the Dell R300 server, and into a rear USB port on the IBM x3350 server.

For the security dongle to be recognized on COTS2 servers, you must insert the USB security dongle adapter with security dongle into a USB port before you boot the COTS2 server .

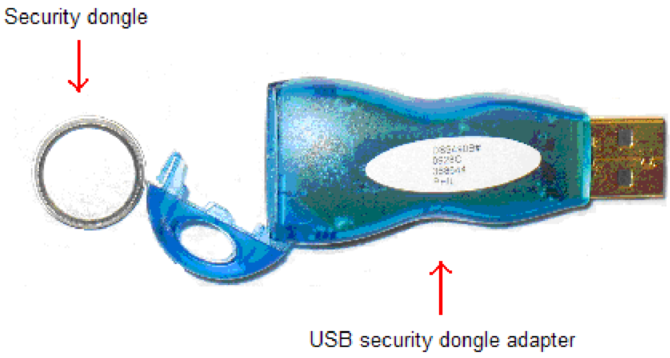


Figure 4: NTRH9220E6 USB security dongle adapter for COTS2 servers

Ethernet port connections

The Server and Gateway Controller Ethernet ports must connect to the ELAN and TLAN subnets of the CS 1000E network. For Co-res CS and SS systems with an MGC card, see Server and MGC connections on page 29for cabling options.

For Co-res CS and SS systems with a CP MG card, you can connect the IE (ELAN port) on the CP MG faceplate to the ELAN subnet of the CS 1000E network, and connect the 2T (TLAN port) on the CP MG faceplate to the TLAN subnet of the CS 1000E network. The CP MG Ethernet connections between the Server and the Gateway Controller are embedded into the CP MG card, so no cabling is necessary to connect the Ethernet ports of the Server to the Gateway Controller.

Server and MGC connections

The ELAN and TLAN ports on the Server card of a Co-res CS and SS can be cabled by using the MGC (see Figure 5: Cabling the CP PM Co-res CS and SS ELAN and TLAN ports by using the MGC on page 30for an example with a CP PM and an MGC card).

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.

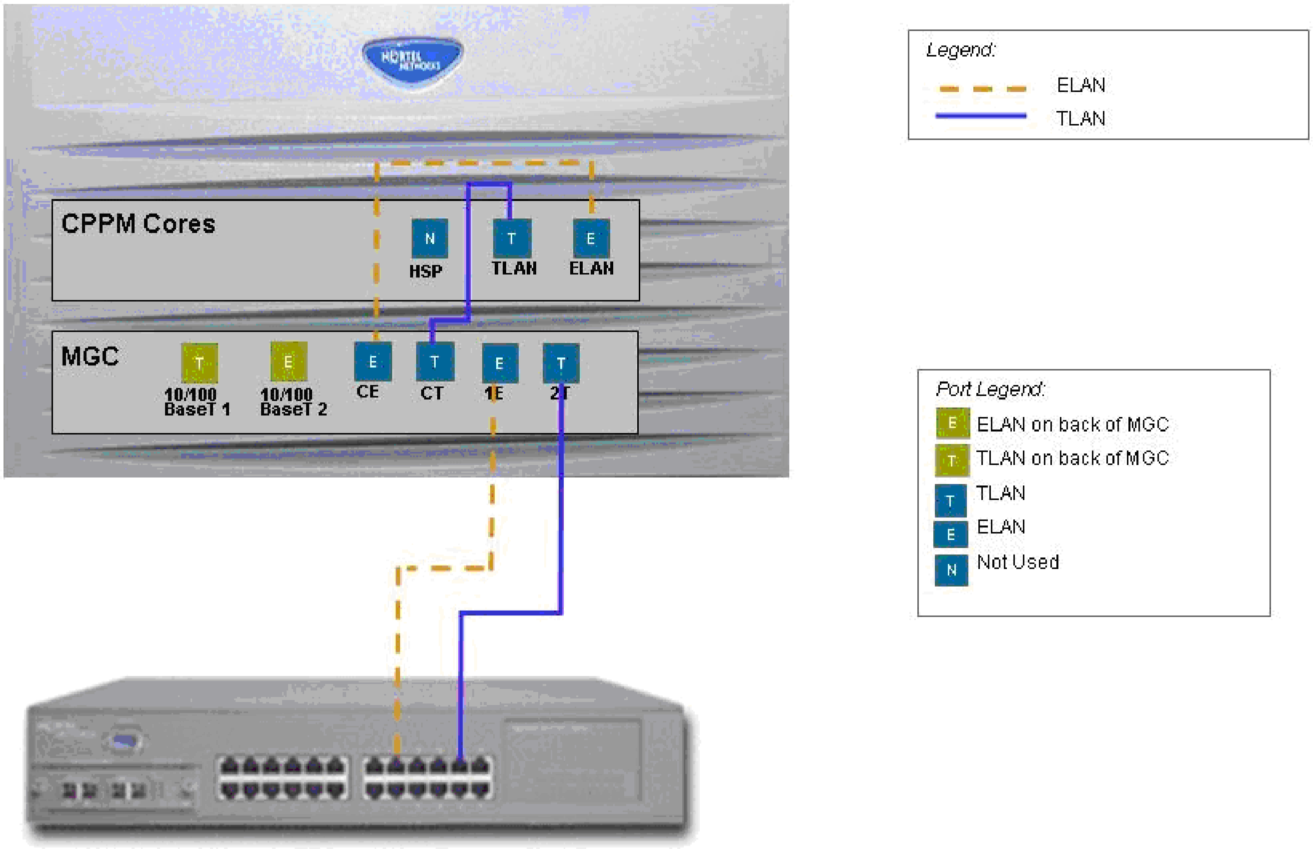


Figure 5: Cabling the CP PM Co-res CS and SS ELAN and TLAN ports by using the MGC

Figure 6: Dual Homed ELAN and TLAN on page 31 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.

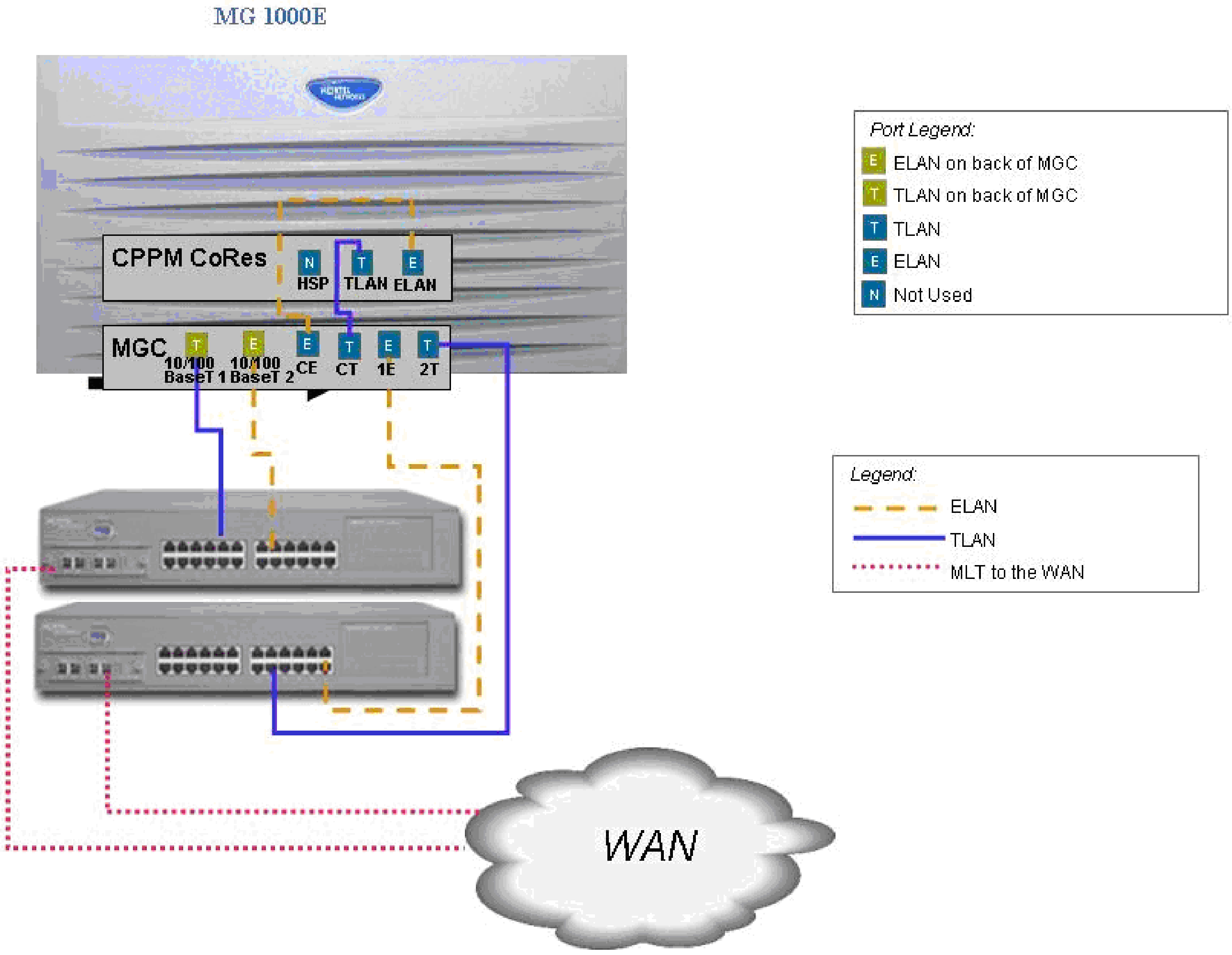


Figure 6: Dual Homed ELAN and TLAN

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 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 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 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 Co-res CS and SS system with distributed Media Gateways. This is a non-GR system with Media Gateways that are in a different subnet than the Co-res CS and SS server.
- CS1000E Co-res CS and SS system where the Telephony Manager (TM) is in a different subnet than the Co-res CS and SS server.

Co-res CS and SS feature package requirements

No new feature packages are introduced for Co-res CS and SS. Table 3: CS 1000E feature package requirements on page 32, Table 4: Branch Office Media Gateway feature package requirements on page 33, and Table 5: SMG feature package requirements on page 33 list the existing CS 1000 Call Server packages that are required for 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 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: Branch Office Media Gateway 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: 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 on page 33 lists the packages that are disabled for 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

Co-res CS and SS deployment configurations

The supported configurations for 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 a Co-res CS and SS system:

- Installing a 2nd TPS (leader and follower) will not give true redundancy for the TPS. If the Co-res system itself fails, then the 2nd TPS has no place to register.
- Installing a 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 exception to this is the NRS.

System capacity

With the Call Server, Signaling Server, and System Management applications sharing the same hardware resources (CPU, memory, disk space), the Co-res CS and SS system capacity can vary for the supported hardware platforms. The following table describes the various Co-res CS and SS system capacities.

Table 7: Co-res CS and SS system capacities

Description	Hardware platform	Notes
ACD Agents (IP agents, IP trunks)	200	
UNIStim telephones	CP MG 128 — 700 CP PM — 1000 CP DC — 1000 COTS2 — 1000	(UNIStim + SipN + Sip3) <= UNIStim telephone limit AND (MSC + Vtrk <= 400)
PD users	CP MG 128 — 700 CP PM — 1000 CP DC — 1000 COTS2 — 1000	
SipLine telephones	CP MG 128 — 400 CP PM — 400 CP DC — 400 COTS2 — 1000	(UNIStim + SipN + Sip3) <= UNIStim telephone limit AND (MSC + Vtrk <= 400)
Vtrks (H323 and/or SIP)	400	
TDM	128 Branch Office / 800 stand alone Co-res CS and SS	

Description	Hardware platform	Notes
PRI Spans	16	
UCM Elements	100	
UCM Active administrators	10	
UCM Supported groups	10	
UCM Configured administrators	50	On each UCM
UCM Concurrent administrators	10	On each UCM
UCM Cconcurrent administrators on same element	5	One or more UCM
Subscriber Manager subscribers	10 000	
Subscriber Manager accounts	17 500	
Media Gateways (IPMG)	5	
Gateway endpoints on NRS	5	
NRE on NRS	20	
OCS TR87 Co-res	CP MG 128 — 700 CP PM — 1000 CP DC — 1000 COTS2 — 1000	
Presence Publisher users	1000	
Media Service Controller (MSC) IPConf sessions	400	
MSC IPMusic sessions	400	
MSC IPRan sessions	400	
MSC IPTone sessions	400	
MSC IPAttn sessions	256	
MSC (total sessions)	400	MSC =(IPConf + IPRan + IPTone + IPMusic + IPAttn) <= 400
Calls per hour (cph)	CP MG 128 — 8000 CP PM — 10 000 CP DC — 15 000 COTS2 — 20 000	Sum of CS + NRS + MSC

Description	Hardware platform	Notes
Media Application Server (MAS)	N/A	Requires a stand-alone MAS platform

An example CP PM based Co-res CS and SS system within the supported line size limit could contain 600 UniSTIM users, 400 SipLine (SipN) 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, Media Gateways, or a higher call rate is required, then a CS 1000E SA system is required.

IP Users = UNIStim + SipN + Sip3

For more information about Co-res CS and SS system capacities, see *Communication Server 1000E Planning and Engineering, NN43041-220*.

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 800 TDM users limit is exceeded. For details see *Communication Server 1000E Planning and Engineering, NN43041-220* 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 7.0 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 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 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 Co-res CS and SS. If upgrading from a CS 1000E CP PM system, all Call Server IP address fields in each Gateway Controller must be updated to reflect the new IP address. See *Linux Platform Base and Applications Installation and Commissioning, NN43001-315* for details.

Chapter 6: Installation and commissioning

Introduction

This chapter contains software installation information. For information on hardware installations, see *Communication Server 1000E Installation and Commissioning, NN43041-310*.

A Co-res CS and SS software 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.

The CP PM, CP MG, CP DC, and COTS2 server hard drives from Nortel ship with the Linux Base Operating System pre-installed.

Pre-installation checklist

The CP MG, CP DC, and COTS2 servers meet the requirements for Co-res CS and SS. No pre-installation steps are necessary beyond installing the server hardware, security dongle, and connecting the server to the network.

The Co-res CS and SS requires a CP PM card with a 40 GB hard drive and 2 GB of memory. The CP PM version 1 hardware (NTDW61 and NTDW99BAE6) must run BIOS Release 18 or later to support Co-res CS and SS. The CP PM version 2 (NTDW99CAE6) meets the requirements for Co-res CS and SS. CP PM version 2 includes an updated hardware design, BIOS, and boot manager.

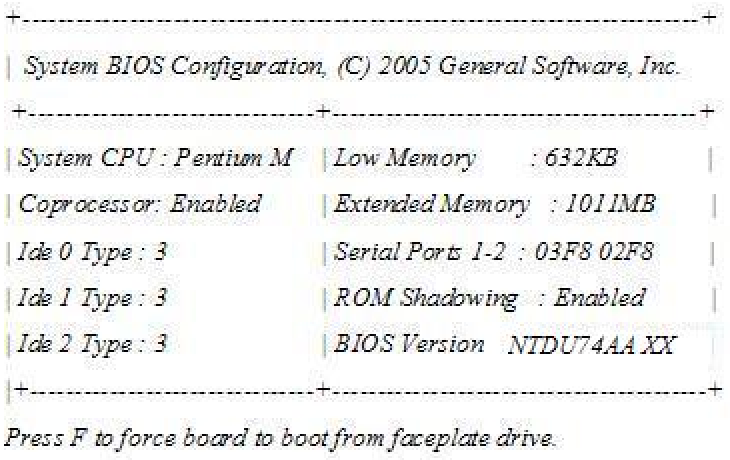
You must perform the following procedures before any installation of a CP PM based Co-res CS and SS to ensure the hardware meets the preceding requirements.

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.

Determining the CP PM BIOS version method 1

1. Power up the CP PM hardware.
2. Observe the CP PM version 1 bootup screen. The BIOS version is shown.



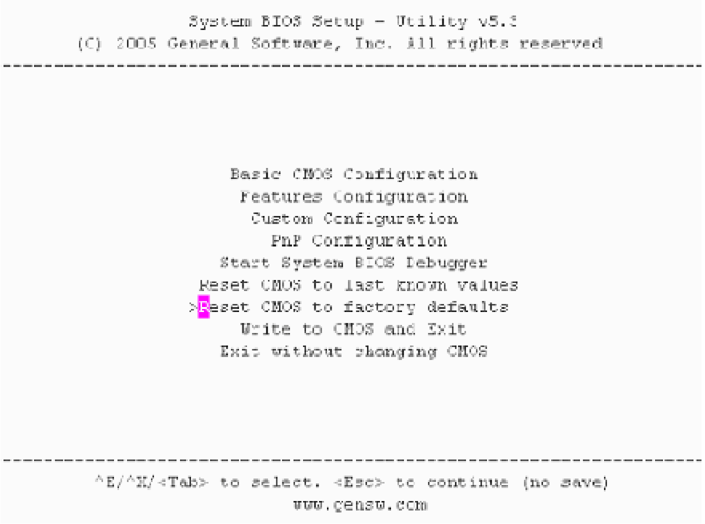
```
+----------------------------------------------------------------------+
| System BIOS Configuration, (C) 2005 General Software, Inc.
+-----------------------------+--------------------------------------+
| System CPU : Pentium M      | Low Memory         : 632KB           |
| Coprocessor: Enabled        | Extended Memory    : 1011MB          |
| Ide 0 Type : 3              | Serial Ports 1-2   : 03F8 02F8       |
| Ide 1 Type : 3              | ROM Shadowing      : Enabled         |
| Ide 2 Type : 3              | BIOS Version    NTDU74AA XX          |
|+----------------------------+--------------------------------------+
Press F to force board to boot from faceplate drive.
```

3. If the CP PM version 1 BIOS version is less than 18, complete Automatically upgrading the CP PM BIOS with the Linux Base installer on page 40.

Automatically upgrading the CP PM BIOS with the Linux Base installer

Perform this procedure for CP PM version 1 cards. CP PM version 2 cards do not require a BIOS update.

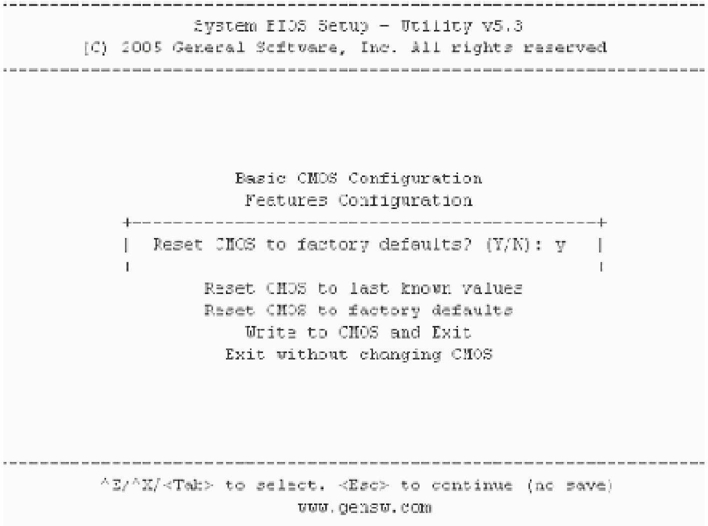
1. Connect to serial port 1 on the CP PM.
2. Insert the Linux Base installation CF card into the faceplate CF slot.
3. Power on the system.
4. During the reboot memory check, quickly press CTRL C to enter the CP PM BIOS.
5. Figure 7: CP PM BIOS setup on page 41 appears. Select Reset CMOS to factory defaults from the menu.



```
                   System BIOS Setup - Utility v5.3
        (C) 2005 General Software, Inc. All rights reserved
----------------------------------------------------------------------




                       Basic CMOS Configuration
                        Features Configuration
                         Custom Configuration
                           PnP Configuration
                      Start System BIOS Debugger
                    Reset CMOS to last known values
                   >Reset CMOS to factory defaults
                        Write to CMOS and Exit
                      Exit without changing CMOS




----------------------------------------------------------------------
         ^E/^X/<Tab> to select. <Esc> to continue (no save)
                            www.gensw.com
```

Figure 7: CP PM BIOS setup

6. Figure 8: CP PM BIOS reset on page 41 appears. Press y to reset CMOS to factory defaults.



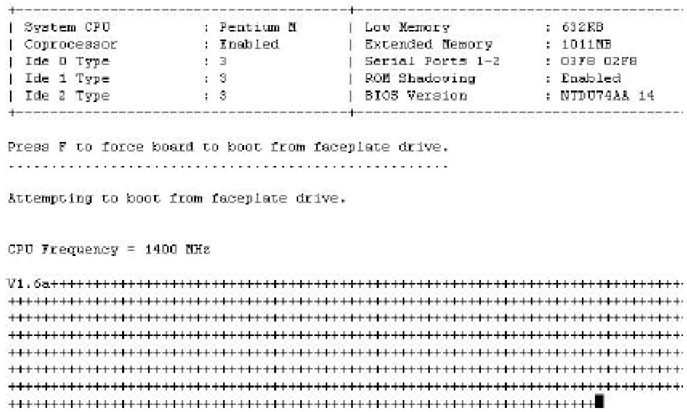
```
----------------------------------------------------------------------
                   System BIOS Setup - Utility v5.3
        (C) 2005 General Software, Inc. All rights reserved
----------------------------------------------------------------------




                       Basic CMOS Configuration
                        Features Configuration
           +----------------------------------------------+
           |  Reset CMOS to factory defaults? (Y/N): y    |
           |                                              |
                    Reset CMOS to last known values
                    Reset CMOS to factory defaults
                        Write to CMOS and Exit
                      Exit without changing CMOS




----------------------------------------------------------------------
         ^E/^X/<Tab> to select. <Esc> to continue (no save)
                            www.gensw.com
```

Figure 8: CP PM BIOS reset

7. Once the reboot and memory check completes, Figure 9: CP PM faceplate drive boot on page 42appears. Press the F key to boot from the Linux Base installation faceplate CF card.

Note:

For CP PM version 2 cards, pressing F enters the boot menu. Select Faceplate RMD, and press Enter to boot from the Linux Base installation faceplate CF card.



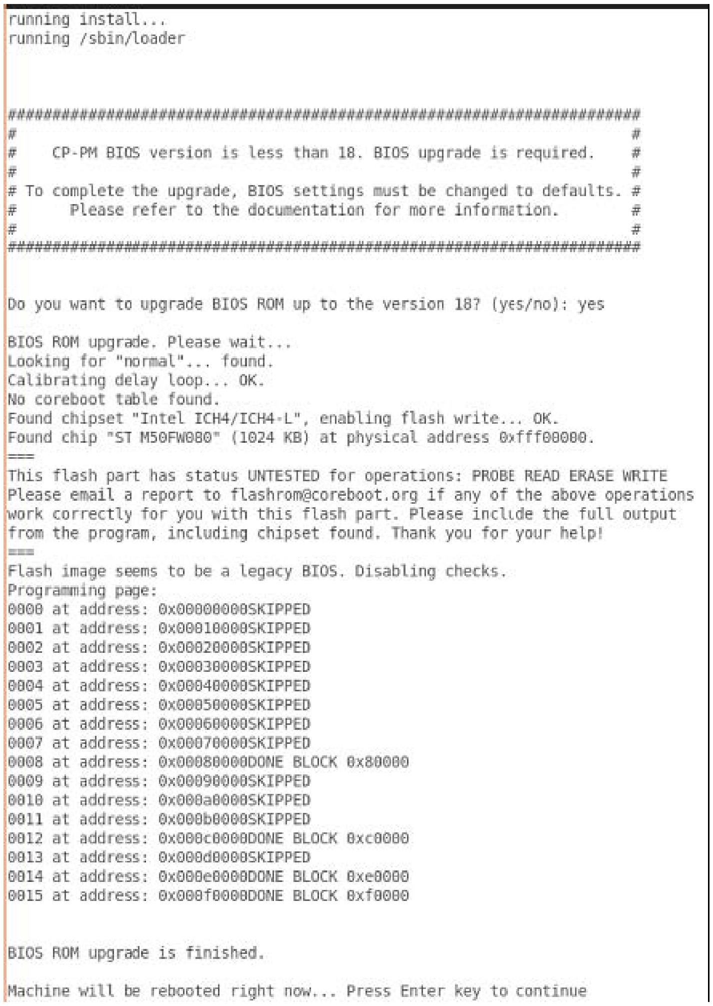
```
+---------------------------------------+---------------------------------------
| System CPU           : Pentium M      | Low Memory             : 632KB
| Coprocessor          : Enabled        | Extended Memory        : 1011MB
| Ide 0 Type           : 3              | Serial Ports 1-2       : 03F8 02F8
| Ide 1 Type           : 3              | ROM Shadowing          : Enabled
| Ide 2 Type           : 3              | BIOS Version           : NTDU74AA 14
+---------------------------------------+---------------------------------------

Press F to force board to boot from faceplate drive.
----------------------------------------------------

Attempting to boot from faceplate drive.


CPU Frequency = 1400 MHz

V1.6a+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++█
```

Figure 9: CP PM faceplate drive boot

8. The welcome screen appears. Press ENTER to direct the input and output to COM1.
9. Figure 10: CP PM BIOS automatic upgrade on page 43 appears if the CP PM version 1 card has a BIOS version less than 18. Press y to proceed with the automatic upgrade.

   ⚠ **Caution:**

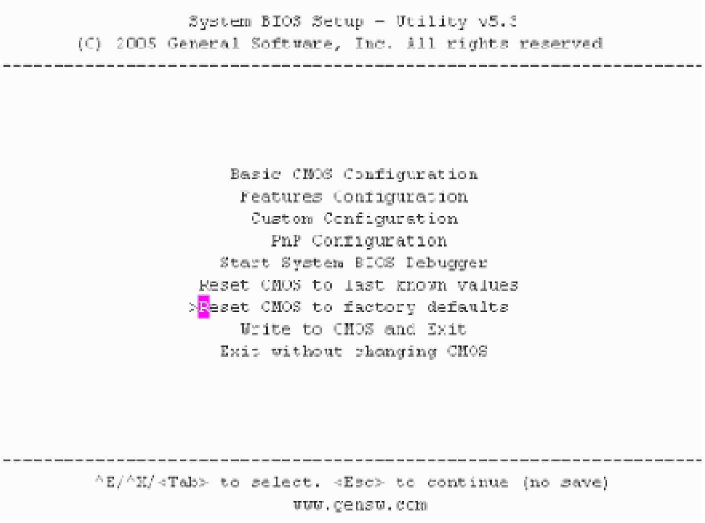
   Do not interrupt the BIOS upgrade process. Damage to equipment may occur.



```
running install...
running /sbin/loader


#######################################################################
#                                                                     #
#    CP-PM BIOS version is less than 18. BIOS upgrade is required.    #
#                                                                     #
# To complete the upgrade, BIOS settings must be changed to defaults. #
#       Please refer to the documentation for more information.       #
#                                                                     #
#######################################################################


Do you want to upgrade BIOS ROM up to the version 18? (yes/no): yes

BIOS ROM upgrade. Please wait...
Looking for "normal"... found.
Calibrating delay loop... OK.
No coreboot table found.
Found chipset "Intel ICH4/ICH4-L", enabling flash write... OK.
Found chip "ST M50FW080" (1024 KB) at physical address 0xfff00000.
===
This flash part has status UNTESTED for operations: PROBE READ ERASE WRITE
Please email a report to flashrom@coreboot.org if any of the above operations
work correctly for you with this flash part. Please include the full output
from the program, including chipset found. Thank you for your help!
===
Flash image seems to be a legacy BIOS. Disabling checks.
Programming page:
0000 at address: 0x00000000SKIPPED
0001 at address: 0x00010000SKIPPED
0002 at address: 0x00020000SKIPPED
0003 at address: 0x00030000SKIPPED
0004 at address: 0x00040000SKIPPED
0005 at address: 0x00050000SKIPPED
0006 at address: 0x00060000SKIPPED
0007 at address: 0x00070000SKIPPED
0008 at address: 0x00080000DONE BLOCK 0x80000
0009 at address: 0x00090000SKIPPED
0010 at address: 0x000a0000SKIPPED
0011 at address: 0x000b0000SKIPPED
0012 at address: 0x000c0000DONE BLOCK 0xc0000
0013 at address: 0x000d0000SKIPPED
0014 at address: 0x000e0000DONE BLOCK 0xe0000
0015 at address: 0x000f0000DONE BLOCK 0xf0000


BIOS ROM upgrade is finished.

Machine will be rebooted right now... Press Enter key to continue
```

Figure 10: CP PM BIOS automatic upgrade

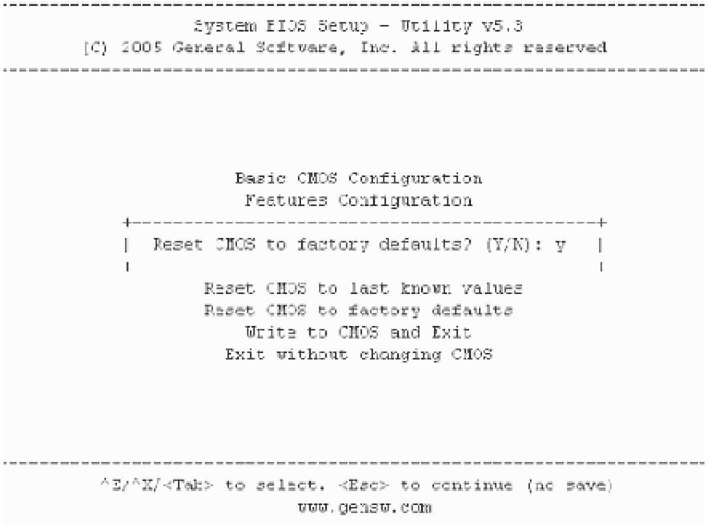
10. Verify that the BIOS upgrade is finished. Press Enter to reboot.
11. During the reboot memory check, quickly press CTRL C to enter the CP PM BIOS.
12. Figure 11: CP PM BIOS setup on page 44 appears. Select Reset CMOS to factory defaults from the menu.



```
                  System BIOS Setup - Utility v5.3
         (C) 2005 General Software, Inc. All rights reserved
----------------------------------------------------------------------



                      Basic CMOS Configuration
                       Features Configuration
                        Custom Configuration
                          PnP Configuration
                     Start System BIOS Debugger
                   Reset CMOS to last known values
                  >Reset CMOS to factory defaults
                       Write to CMOS and Exit
                     Exit without changing CMOS



----------------------------------------------------------------------
        ^E/^X/<Tab> to select. <Esc> to continue (no save)
                            www.gensw.com
```

Figure 11: CP PM BIOS setup

13. Figure 12: CP PM BIOS reset on page 44appears. Press y to reset CMOS to factory defaults.



```
----------------------------------------------------------------------
                  System BIOS Setup - Utility v5.3
         (C) 2005 General Software, Inc. All rights reserved
----------------------------------------------------------------------



                      Basic CMOS Configuration
                       Features Configuration
          +----------------------------------------------+
          |  Reset CMOS to factory defaults? (Y/N): y    |
          |                                              |
                   Reset CMOS to last known values
                   Reset CMOS to factory defaults
                       Write to CMOS and Exit
                     Exit without changing CMOS



----------------------------------------------------------------------
        ^E/^X/<Tab> to select. <Esc> to continue (no save)
                            www.gensw.com
```

Figure 12: 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.

Note:

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

Nortel Linux Base

Server hard drives from Nortel contain a pre-installed Linux Base Operating System. If your hardware contains a pre-installed Linux Base Operating System, you can begin configuration. For more information about configuration, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

Perform the Linux Base installation from the command line interface (CLI) using a bootable RMD applicable for your server hardware. Configure the ELAN, TLAN IP address, gateway, subnet masks, and date and time settings during the Linux Base installation.

For detailed Linux Base installation information, see Nortel Linux base installation on page 71.

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*.

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 Co-res CS and SS (and stand-alone Linux-based CS 1000 servers) using the CS 1000 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 on page 90.

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 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 Co-res CS and SS.

For detailed information, see Application installation using Deployment Manager on page 86.

Call Server Keycode validation and pre-configuration

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

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

Prior to deploying the application software to the Co-res CS and SS, the Deployment Manager performs the Server keycode validation to ensure that the keycode file used matches the software version and the security device on the target server. Table 8: Keycode validation result on page 47 describes the keycode validation results.

Table 8: 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 your 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.

Output message	Description	Action
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 Co-res CS and SS Call Server database is stored in the **backup/single** folder on the RMD. 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 6.0.

Chapter 7: Upgrades

Introduction

This section provides information on upgrading to a CS 1000 Release 7.0 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 on page 55
- upgrade from a CS 1000 Release 6.0 (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 Release 6.0 CP PM Co-res CS and SS (application software version upgrade)

Hardware

The Co-res CS and SS can be deployed to various hardware platforms. For CS 1000 Release 7.0, the Co-res CS and SS supports the following Servers:

- Common Processor Pentium Mobile (CP PM) card
- Common Processor Media Gateway (CP MG) card
- Common Processor Dual Core (CP DC) card
- IBM x3350 and Dell R300 Commercial off-the-shelf (COTS) servers (COTS2)

If you are upgrading an existing CS 1000E system from a CP PII or CP PIV Call Server, you must replace the your existing hardware with a supported Server from the preceding list, and upgrade the software. For more information, see *Communication Server 1000E Hardware Upgrades, NN43041-464*

The Server cards install in Media Gateway IPE slots, the COTS servers install in standard 19 inch racks.

One Gateway Controller is required in each Media Gateway cabinet or chassis. The Gateway Controller can be an MGC card or a CP MG card.

Note:

The CP MG card functions as a Gateway Controller and a Server while occupying only one slot in a Media Gateway. The CP MG card is available with 32 or 128 DSP ports.

For more information about the CP PM, CP DC, CP MG, MGC, and COTS2 hardware, see *Circuit Card Reference, NN43001-311*.

CP PM hard drive and memory upgrades

For information on CP PM memory or hard drive upgrades, see *Circuit Card Reference, NN43001-311*.

- All CP PM cards require a minimum 40 GB hard drive and 2 GB of memory to support Co-res CS and SS.
- When upgrading from CS 1000 Release 5.X, the Call Server requires a 1 GB memory upgrade (for a total of 2 GB memory) and an FMD replacement with a 40 GB hard drive.

Note:

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

Co-res CS and SS application software upgrade (6.0 to 7.0)

This document contains procedures for local system upgrades. For information on performing system upgrades with Deployment Manager (DM), see *Linux Base Platform Base and Applications Installation and Commissioning, NN43001-315*.

For the 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 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 Co-res CS and SS is backed up, including all data for all applications installed on the 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 Co-res CS and SS.

Backing up the CS 1000E Call Server database

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

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

Install the CS 1000E Call Server database on to the 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 Co-res CS and SS. For complete information, see Linux Platform Base and Applications Installation and Commissioning (NN43001-315).

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

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

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

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.

Call Server installation support

Table 9: VxWorks Call Server install program features not available for the Co-res CS and SS on page 52 lists the features the Deployment Manager does not support in the VxWorks Call Server Installation program.

Table 9: VxWorks Call Server install program features not available for the Co-res CS and SS

Feature	CS 1000 Release 7.0 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	--

Feature	CS 1000 Release 7.0 Co-res CS and SS Equivalent command	Notes
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

Feature	CS 1000 Release 7.0 Cores CS and SS Equivalent command	Notes
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*.

Chapter 8: Migration from an SSC-based small system

Supported migration paths

Table 10: Supported migration paths on page 55lists the supported migration paths from an SSC-based system to a Co-res CS and SS based CS 1000E system.

Table 10: Supported migration paths

CS 1000 Release 6.0 or earlier	CS 1000 Release 7.0 System
Option 11C Small System	CS 1000E Co-res CS and SS
CS 1000M Small System Cabinet	CS 1000E Co-res CS and SS
CS 1000M Small System Chassis	CS 1000E Co-res CS and SS
CS 1000S Small System	CS 1000E 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 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). The CF card can be inserted into the CP PM card during software deployment to perform the database conversion. For CP MG, CP DC, or COTS2 servers, you must copy the CF card data onto a USB 2.0 storage device. 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:

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:

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

There is a fundamental difference between the small system, running an SSC, and a 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 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

Backing up the database using LD 43

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.

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.

Archiving the database in LD 143

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
   ```

Once you have completed the backup and archive of the customer database, shut down the system and remove the PCMCIA card with CF card from the slot. You can use the CF card with a CP PM card. For a CP MG, CP DC, or COTS2 server, you must copy the data from the CF card to a USB 2.0 storage device using a PC. You are now ready to install the hardware.

Choosing the cabinet or chassis and slot locations

A Media Gateway performs functions under the control of the CS 1000E Server. Traditionally, this Server was a CP PII or CP PIV in its own call server cabinet or chassis, The Server card for a Co-res CS and SS system sits in one of the Media Gateway IPE slots. Slot location is based on the type of system:

- For Cabinet systems, refer to Cabinet on page 59
- For Chassis systems, refer to Chassis on page 60
- For Communication Server 1000S systems, refer to Communication Server 1000S on page 62

Cabinet

The Server card drives the Media Gateway through the Gateway Controller ELAN interface and therefore only uses the backplane for power. The following rules apply to the preferential placement of the Server card in the Media Gateway:

- The Server card cannot be placed in slot 0 of any Media Gateway. Slot 0 is reserved for the Gateway Controller.

  Note:
  The CP MG card can be placed in slot 0, the CP MG card functions as the Co-res CS and SS, and the Gateway Controller card.

- To allow for ease of cabling, the Server card may be placed in slots 1 through 10. A Signaling Server may be placed in slots 1 through 10 (see Figure 13: CP PM Co-res CS and SS system on page 60) or in another cabinet if necessary.

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

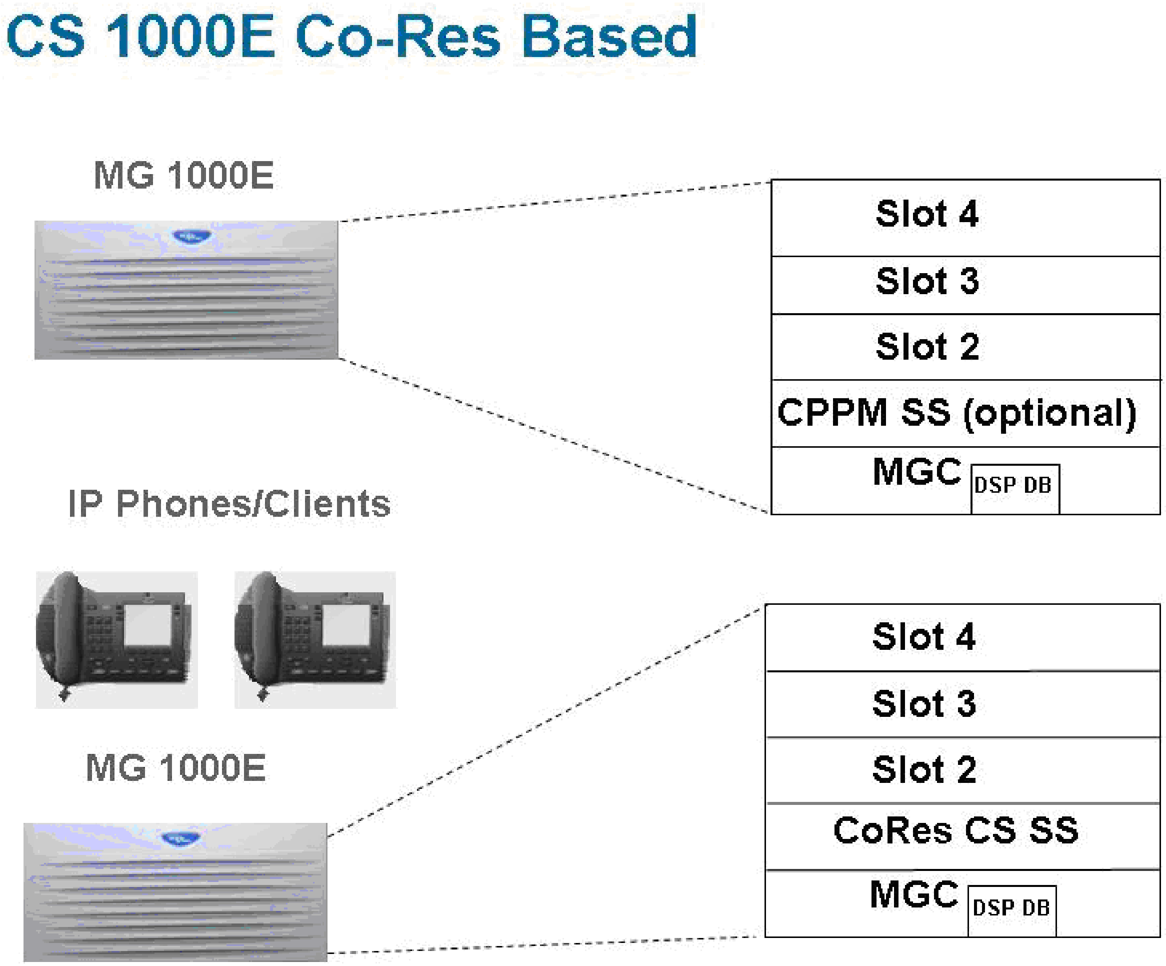


Figure 13: CP PM Co-res CS and SS system

To proceed with the upgrade, proceed to Hardware Upgrade Task Overview on page 63.

Chassis

The Server card drives the Media Gateway through the Gateway Controller ELAN interface and therefore only uses the backplane for power. The following rules apply to the preferential placement of the Server card in the Media Gateway:

- The Server card cannot be placed in slot 0 of any Media Gateway. Slot 0 is reserved for the Gateway Controller.

Note:

The CP MG card can be placed in slot 0, the CP MG card functions as the Co-res CS and SS, and the Gateway Controller card.

- To allow for ease of cabling, the Server 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 Server card installed in slot 4 as this slot was originally allocated for the 48 port DLC only.

Figure 14: Option 11C or Communication Server 1000M Chassis call server on page 62 shows an existing Option 11C or Communication Server 1000M Chassis call server with the SSC card. Once the upgrade is complete, a Co-res CS and SS Chassis system will resemble Figure 15: CP PM Co-res CS and SS system on page 62 with a Gateway Controller in slot 0, and a Server card in the main chassis. The additional Media Gateways contain Gateway Controllers, IPE cards, or another Server card running stand-alone Signaling Server applications.

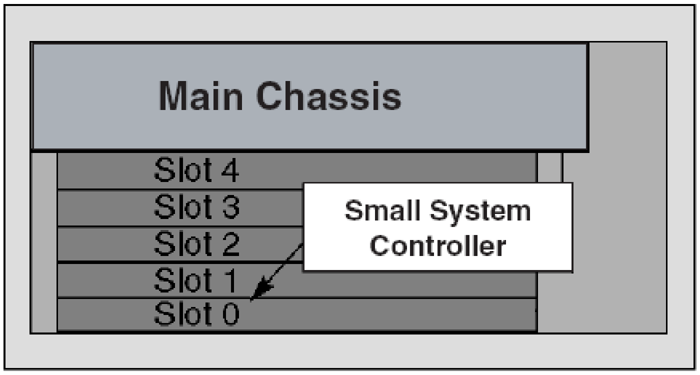


Figure 14: Option 11C or Communication Server 1000M Chassis call server

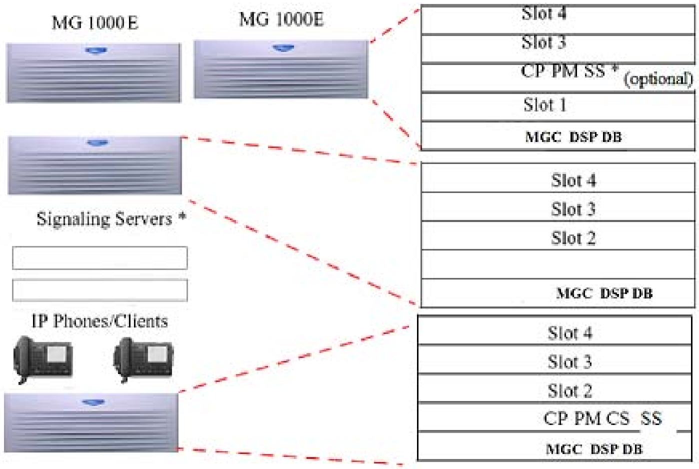


Figure 15: CP PM Co-res CS and SS system

* Signaling Server may be one of the following:

- CP PM Signaling Server
- Commercial off-the-shelf (COTS) Signaling Server

To proceed with the upgrade, proceed to Hardware Upgrade Task Overview on page 63.

Communication Server 1000S

The Server card drives the Media Gateway through the Gateway Controller ELAN interface and therefore only uses the backplane for power. The following rules apply to the preferential placement of the Server card in the Media Gateway:

- The Server card cannot be placed in slot 0 of any Media Gateway. Slot 0 is reserved for the Gateway Controller.

Note:

The CP MG card can be placed in slot 0, the CP MG card functions as the Co-res CS and SS, and the Gateway Controller card.

- To allow for ease of cabling, the Server 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 Server card installed in slot 4 as this slot was originally allocated for the 48 port DLC only.

Figure 16: CS 1000S (NTDU30) call server on page 63 shows an existing CS 1000S Call Server with the SSC card. Once the upgrade is complete, a typical Co-res CS and SS Chassis system will resemble Figure 13: CP PM Co-res CS and SS system on page 60 with a Gateway Controller in slot 0, and a Server card in the Media Gateway. The additional Media Gateways contain Gateway Controllers, IPE cards, or another Server card running stand-alone Signaling Server applications.

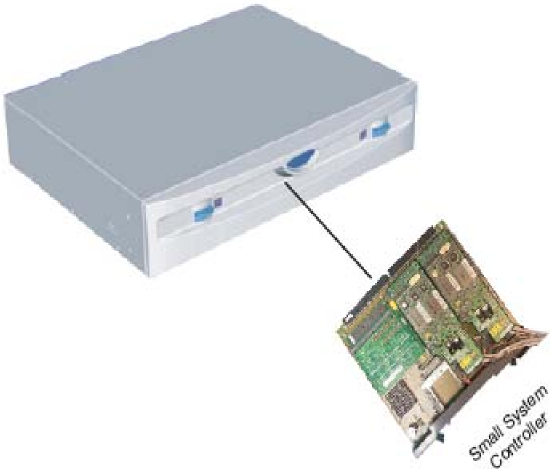


Figure 16: CS 1000S (NTDU30) call server

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 Removing the SSC card on page 64.
- If using an MGC card as the Gateway Controller, install the DSP Daughterboard on the MGC card. See Installing a DSP Daughterboard on page 65
- Install the Gateway Controller card as described in Installing the Gateway Controller card on page 66.
- Install the Server as described in Installing the CP PM or CP DC card on page 67.

- Cable the cards as shown in Cabling the cards on page 69.
- Power up the Media Gateway.
- Enter the ‘mgcsetup’ menu and configure the IP parameters. For details, see *Communication Server 1000E Installation and Commissioning, NN43041-310*.
- Reboot the Gateway Controller

Card installation

The following sections describe the process required to install the Gateway Controller and Server cards.

Removing the SSC card

Removing the SSC card

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

Important:
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.

MGC DSP Daughterboard installation

The MGC card provides two expansion slots to add Digital Signal Processor (DSP) resources with DSP Daughterboards (DSP DB). Three DSP DB capacities are available:

- NTDW62 32-port DSP DB (DB-32)
- NTDW64 96-port DSP DB (DB-96)
- NTDW78 128-port DSP DB (DB-128)

You can configure any combination of the three available DSP DBs on an MGC card. The MGC card supports a maximum of 256 DSP ports (two DB-128). For more information, see *Circuit Card Reference, NN43001-311*.

Important:

Due to historical TN mapping for the Call Server software, even though the DSP channels will occupy Card 0 in the Media Gateways, 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 Media Gateway ONLY if there is a DB-32 installed in daughterboard position #2.

The following procedure describes how to install a DSP Daughterboard on an MGC card. See Figure 17: DSP Daughterboard on page 65.

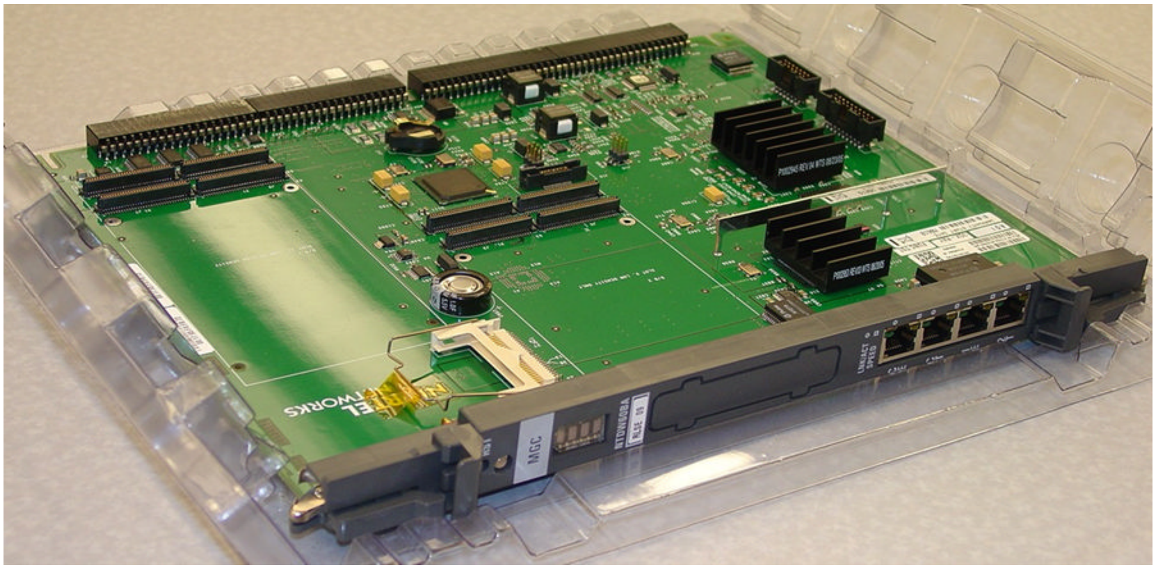


Figure 17: DSP Daughterboard

Installing a DSP Daughterboard

1. Place the MGC on a safe ESD surface.
2. Place the DSP DB in either DB position 1, position 2, or both positions.
3. Ensure the DSP DB are securely attached to the MGC. (using supplied screws).

Gateway Controller installation

You can use an MGC card or a CP MG card as the Gateway Controller for a Co-res CS and SS.

Gateway Controller serial connection

To perform initial configuration of the Gateway Controller you need to connect through the Gateway Controller serial port. You require an NTBK48AA 3-port SDI cable connected to the SDI (RS-232) port on the Chassis

Table 11: Gateway Controller serial port capabilities on page 66 lists the Gateway Controller serial port capabilities.

Table 11: Gateway Controller 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)

Installing the Gateway Controller card

The MGC or CP MG card replaces the existing SSC used in a small system cabinet or chassis.

1. Insert the Gateway Controller into Slot 0 of the cabinet or chassis. The existing 3-port SDI cable (NTBK48AA) is reused for Gateway Controller serial connections. 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.

The CP MG card is a Gateway Controller and a Server on a single card. The preceding procedure connects the CP MG for the Gateway Controller configuration only. For information about the installation and configuration of the Server portion of the CP MG card, see Installing the CP MG card on page 68.

Important:

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.

Server card installation

You can use a CP PM, CP DC, or CP MG card as the Server card in a Co-res CS and SS. Perform the installation procedure applicable for your hardware.

CP PM or CP DC card installation

The following procedure describes how to install the CP PM or CP DC card in a Cabinet or Chassis. The CP PM card may require a CP PM Server Linux Upgrade kit to meet the requirements for a Co-res CS and SS configuration.

Note:

A CP PM card configured for Co-res CS and SS requires 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 CP PM Server Linux Upgrade kit includes the following items:

- 2 GB Compact Flash (CF) with Linux software
- 1 GB DDR SO-DIMM memory
- 40 GB Hard Drive kit, Linux OS preloaded (Optional, provisioned if required)

Note:

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

Installing the CP PM or CP DC card

1. Ensure that the security dongle (the one that comes as part of the software kit) is inserted on the Server card.

   Note:

   This first step is applicable only when the Server card is used as a Call Server.

   Note:

   Remove the retainer clip from the FMD slot when the CP PM card is used as a Signaling Server. The clip must be removed to prevent it from shorting out adjacent cards.

   Note:

   For CP PM cards, ensure switch S5 is in position 2 and a 40GB internal hard disk FMD is installed.
2. Slide the Server card into Slot 1 (or higher) of the cabinet or chassis.
3. Lock the card into the faceplate latches.
4. Attach the 2-port SDI cable (see Figure 18: 2-port SDI cable (NTAK19EC) cable on page 68. The 50-pin Amphenol NTAK19EC connects to the back of the Server card.

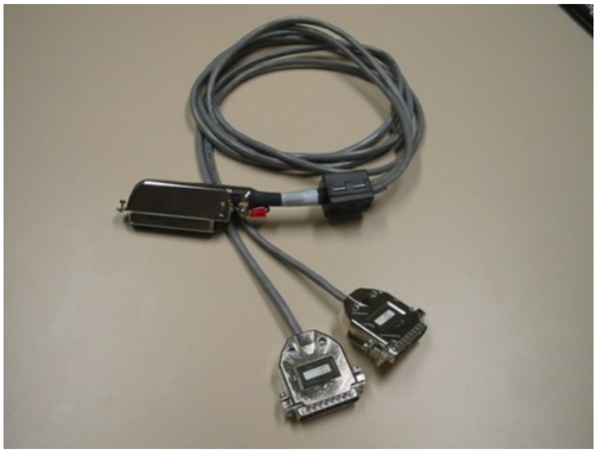


Figure 18: 2-port SDI cable (NTAK19EC) cable

Note:

To connect a maintenance terminal to the Server card, complete the following steps:

- Connect the NTAK19EC cable to the 50 pin MDF connector on the back of the cabinet or chassis.
- 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.

The preceding procedures enable users to upgrade the system one Media Gateway at a time. For each additional Media Gateway, repeat Removing the SSC card on page 64 and Installing the Gateway Controller card on page 66.

CP MG card installation

You install a CP MG card into the Gateway Controller Slot 0 of a Media Gateway. The CP MG card functions as the Gateway Controller and the Server card. Perform the following procedure to install a CP MG card into a Media Gateway cabinet or chassis.

Installing the CP MG card

1. Ensure that the security dongle is inserted on the CP MG card.
2. Insert and slide the CP MG card into Slot 0 of a Media Gateway cabinet or chassis.
3. Lock the card in place with the faceplate latches.

You can now proceed to cabling the CP MG Server.

Cabling the cards

The following sections describe the process required to cable the Gateway Controller and Server cards.

Cabling the Gateway Controller

The existing 3-port SDI cable (NTBK48AA) is reused. It connects to the SDI port on the cabinet or chassis and provides serial connectivity to the Gateway Controller.

MGC Ethernet ports

An MGC features six Ethernet interfaces set to autonegotiate by default: four on the faceplate (see Figure 19: MGC faceplate on page 69), and two on the expansion box connector using the breakout adaptor. The CE and CT ports are reserved for the Server card only. The CE connects to the ELAN port of the Server card, while the CT connects to the TLAN port of the Server card. 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.

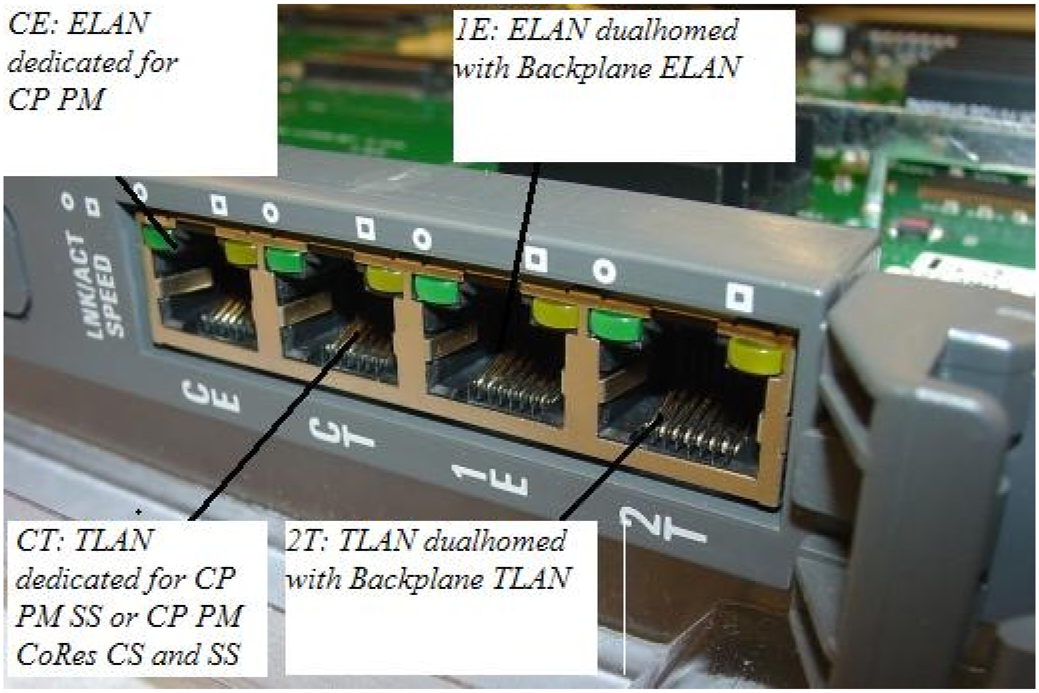

CE: ELAN dedicated for CP PM
1E: ELAN dualhomed with Backplane ELAN
LNK/ACT
SPEED
CE
CT
1E
2T
CT: TLAN dedicated for CP PM SS or CP PM CoRes CS and SS
2T: TLAN dualhomed with Backplane TLAN

Figure 19: MGC faceplate

Cabling the CP PM or CP DC card

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

Connect the ELAN of the CP PM or CP DC card to the CE port of the Gateway Controller or to the VLAN of the external layer 2 switch that is dedicated to ELAN traffic for the system.

CP MG card cabling

The CP MG card is installed in Slot 0 and is uses the 3-port SDI cable for Gateway Controller configuration. Perform the following procedure to cable the CP MG card for Server serial and LAN connections. An NTC325AAE6 serial port adapter kit is required.

Cabling the CP MG Server

1. Connect a Cat5e or Cat6 Ethernet cable to the TTY1 port on the CP MG faceplate.
2. Connect a NTC326AAE6 serial port adapter (9-pin or 25-pin) to the other end of the Ethernet cable.
3. Connect the Ethernet cable with adapter to a serial port on a maintenance terminal.

   Note:

   If you require a longer cable to reach your maintenance terminal, you can attach a standard serial port cable to the adapter for extended cable length.
4. Configure the maintenance terminal for VT-100 emulation, 9600 bps, 8,N,1.
5. Connect the ELAN cable:
   - Connect one end of a shielded Cat5e or Cat6 Ethernet cable to the 1E (ELAN) port on the CP MG faceplate.
   - Connect the other end of the Ethernet cable to the ELAN subnet of the CS 1000E system.
6. Connect the TLAN cable:
   - Connect one end of a shielded Cat5e or Cat6 Ethernet cable to the 2T (TLAN) port on the CP MG faceplate.
   - Connect the other end of the Ethernet cable to the TLAN subnet of the CS 1000E system.

Nortel Linux base installation

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.

The CP MG, CP DC, and COTS2 Servers ship with Linux Base pre-installed. If you are deploying this hardware, you can proceed to configuring and installing Linux applications. For more information, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

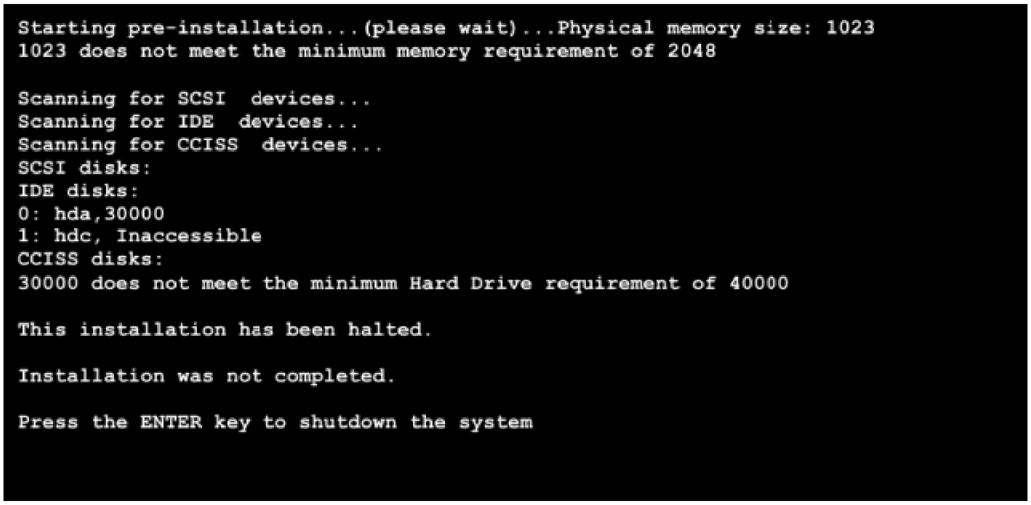
Each Linux server platform requires an installation of the base-level software. You can start the installation from bootable installation media. The process includes the partitioning of hard disk drives, installation of the Linux kernel and the Linux root file system, associated device drivers, base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

CP PM prerequisites

The server must meet the following requirements:

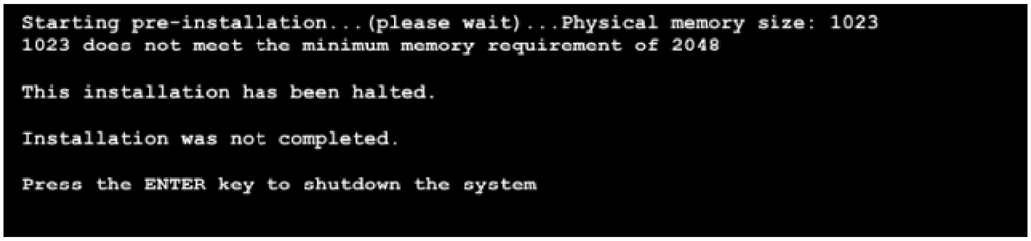
- The hard drive size must be at least 40 GB.
- There must be at least 2 GB of available memory.
- The CP PM version 1 card must run BIOS Release 18 or higher.

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



```
Starting pre-installation...(please wait)...Physical memory size: 1023
1023 does not meet the minimum memory requirement of 2048

Scanning for SCSI  devices...
Scanning for IDE  devices...
Scanning for CCISS  devices...
SCSI disks:
IDE disks:
0: hda,30000
1: hdc, Inaccessible
CCISS disks:
30000 does not meet the minimum Hard Drive requirement of 40000

This installation has been halted.

Installation was not completed.

Press the ENTER key to shutdown the system
```

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



```
Starting pre-installation...(please wait)...Physical memory size: 1023
1023 does not meet the minimum memory requirement of 2048

This installation has been halted.

Installation was not completed.

Press the ENTER key to shutdown the system
```

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:

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:

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:

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:

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:

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.

A USB keyboard and mouse can be used for CP DC server Linux base installation and password recovery.

Note:

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

Note:

If you connect to the IBM x3350 server with a terminal for setup, the server does not function with the serial cable that ships with other COTS platforms. The IBM x3350 server requires an 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 20: NTRX26NPE6 9 pin female to 9 pin female null modem cable on page 74.

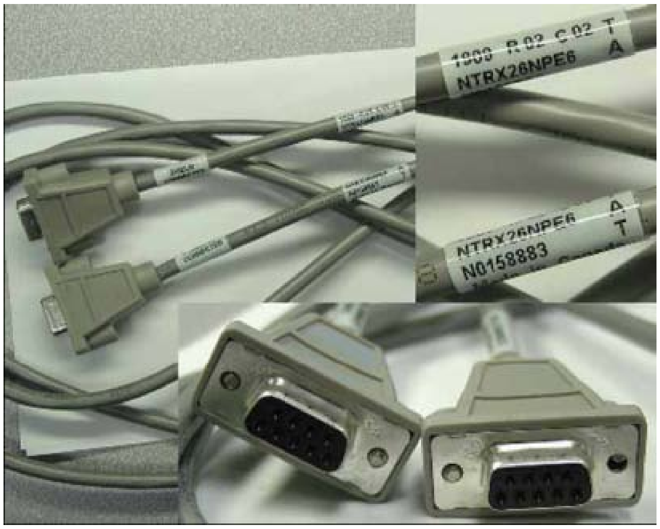


Figure 20: NTRX26NPE6 9 pin female to 9 pin female null modem cable

Installing the Linux base on a CP PM server

Important:

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*.

Important:

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

Warning:

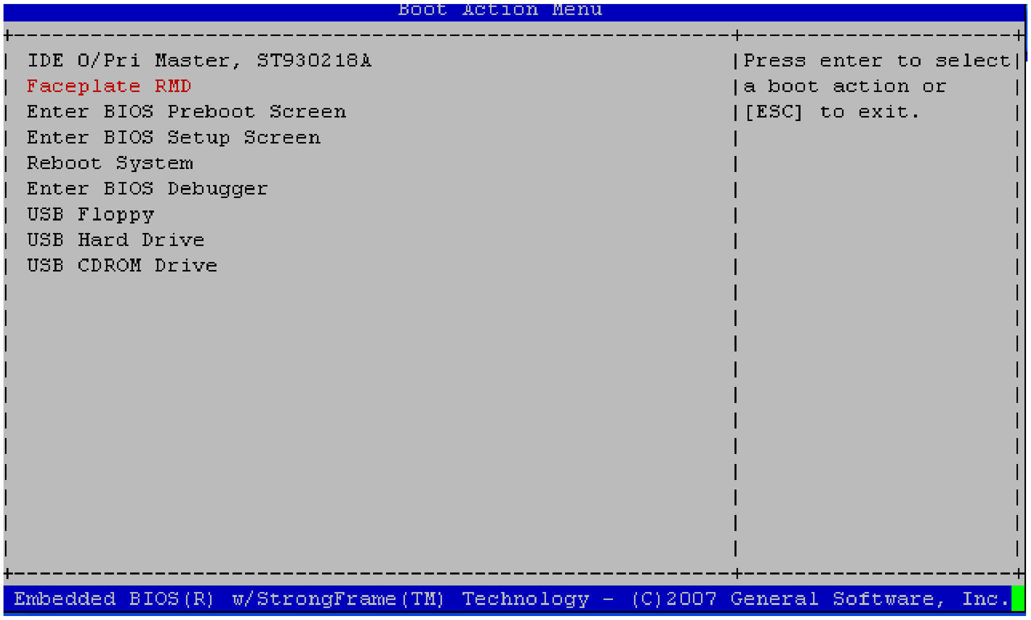
If you are installing Linux base on a CP PM card and the CP PM card is currently running Signaling Server software from VxWorks, you must either press the faceplate reset button or reseat the card before you begin the Linux base installation. Failure to do so results in a watchdog reset during installation. 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.

1. Connect to the CP PM server using the serial console.
2. Insert the Linux base compact flash installation media into the CP PM faceplate CF card slot.
3. Power on the server. Immediately press `F` when prompted on the boot screen.

Note:

CP PM version 1 cards attempt to directly boot from the CF card. CP PM version 2 cards enter the boot menu.

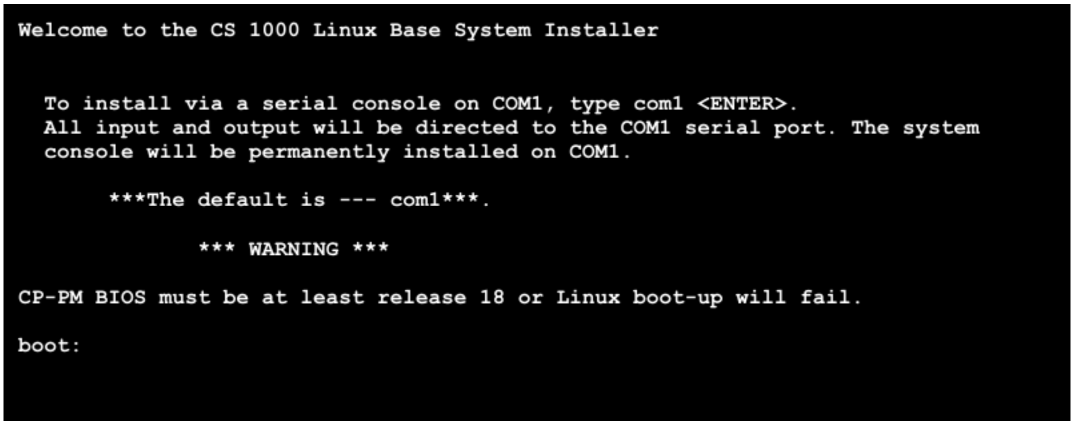
4. For CP PM version 2 cards, Select Faceplate RMD from the boot menu and press `Enter` to boot from the CF card, see Figure 21: CP PM version 2 boot menu on page 75.



```
                          Boot Action Menu
+---------------------------------------------------------+------------------+
| IDE 0/Pri Master, ST930218A                             |Press enter to select|
| Faceplate RMD                                           |a boot action or  |
| Enter BIOS Preboot Screen                               |[ESC] to exit.    |
| Enter BIOS Setup Screen                                 |                  |
| Reboot System                                           |                  |
| Enter BIOS Debugger                                     |                  |
| USB Floppy                                              |                  |
| USB Hard Drive                                          |                  |
| USB CDROM Drive                                         |                  |
|                                                         |                  |
+---------------------------------------------------------+------------------+
Embedded BIOS(R) w/StrongFrame(TM) Technology - (C)2007 General Software, Inc.
```

Figure 21: CP PM version 2 boot menu

When the server boots from the CF card, the CS 1000 Linux Base System Installer window appears as shown in Figure 22: CS 1000 Linux base system installer (CP PM server) on page 75.



```
Welcome to the CS 1000 Linux Base System Installer


  To install via a serial console on COM1, type com1 <ENTER>.
  All input and output will be directed to the COM1 serial port. The system
  console will be permanently installed on COM1.

       ***The default is --- com1***.

              *** WARNING ***

CP-PM BIOS must be at least release 18 or Linux boot-up will fail.

boot:
```

Figure 22: CS 1000 Linux base system installer (CP PM server)

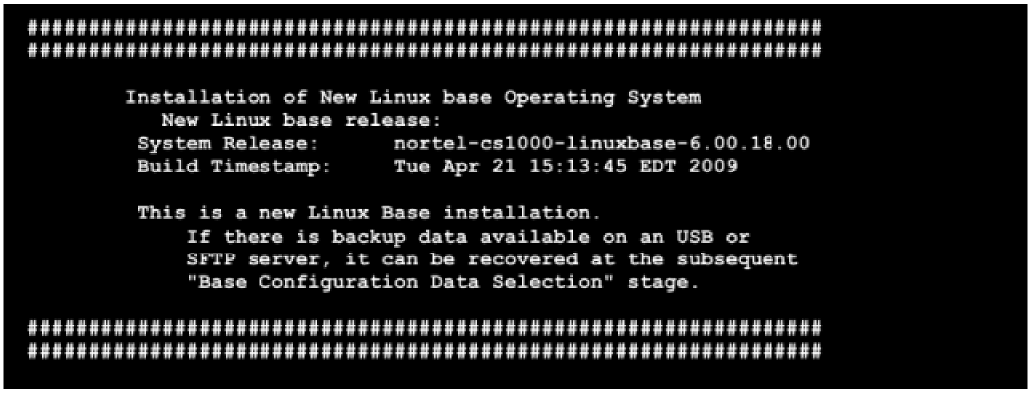
5. Type `com 1` to install using a serial console on COM1.

Important:

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 23: CS 1000 Linux base system installer confirmation window on page 76.

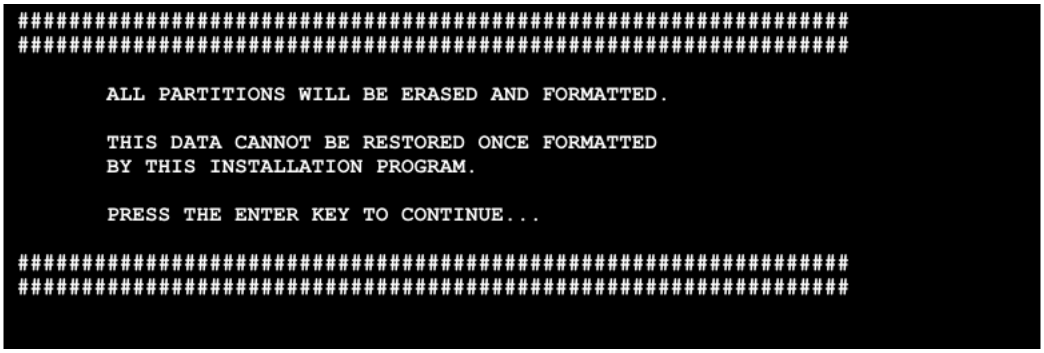


```
#################################################################
#################################################################

        Installation of New Linux base Operating System
           New Linux base release:
         System Release:      nortel-cs1000-linuxbase-6.00.18.00
         Build Timestamp:     Tue Apr 21 15:13:45 EDT 2009

         This is a new Linux Base installation.
             If there is backup data available on an USB or
             SFTP server, it can be recovered at the subsequent
             "Base Configuration Data Selection" stage.

#################################################################
#################################################################
```

Figure 23: CS 1000 Linux base system installer confirmation window

6. Type `Y` and press `Enter` .

   The Format all partitions screen appears, as shown in Figure 24: Format all partitions window on page 76.

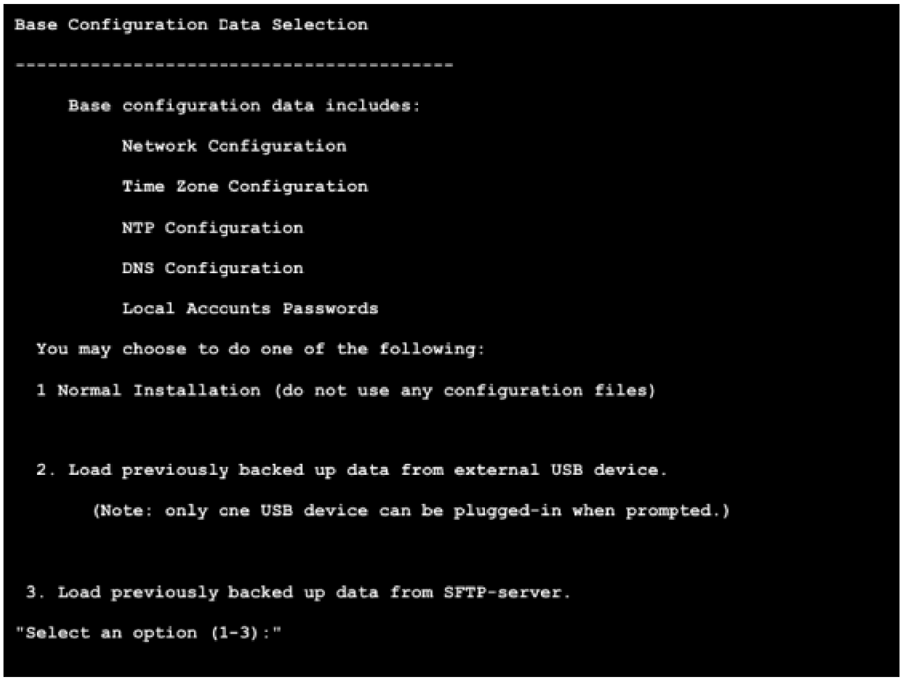


```
#################################################################
#################################################################

       ALL PARTITIONS WILL BE ERASED AND FORMATTED.

       THIS DATA CANNOT BE RESTORED ONCE FORMATTED
       BY THIS INSTALLATION PROGRAM.

       PRESS THE ENTER KEY TO CONTINUE...

#################################################################
#################################################################
```

Figure 24: Format all partitions window

7. Press `Enter` to continue.

   The Base Configuration Data Selection screen appears, as shown in Figure 25: Base Configuration Data Selection window on page 77.



```
Base Configuration Data Selection
-----------------------------------------
     Base configuration data includes:
          Network Configuration
          Time Zone Configuration
          NTP Configuration
          DNS Configuration
          Local Accounts Passwords
  You may choose to do one of the following:
  1 Normal Installation (do not use any configuration files)


  2. Load previously backed up data from external USB device.
       (Note: only one USB device can be plugged-in when prompted.)


 3. Load previously backed up data from SFTP-server.
"Select an option (1-3):"
```

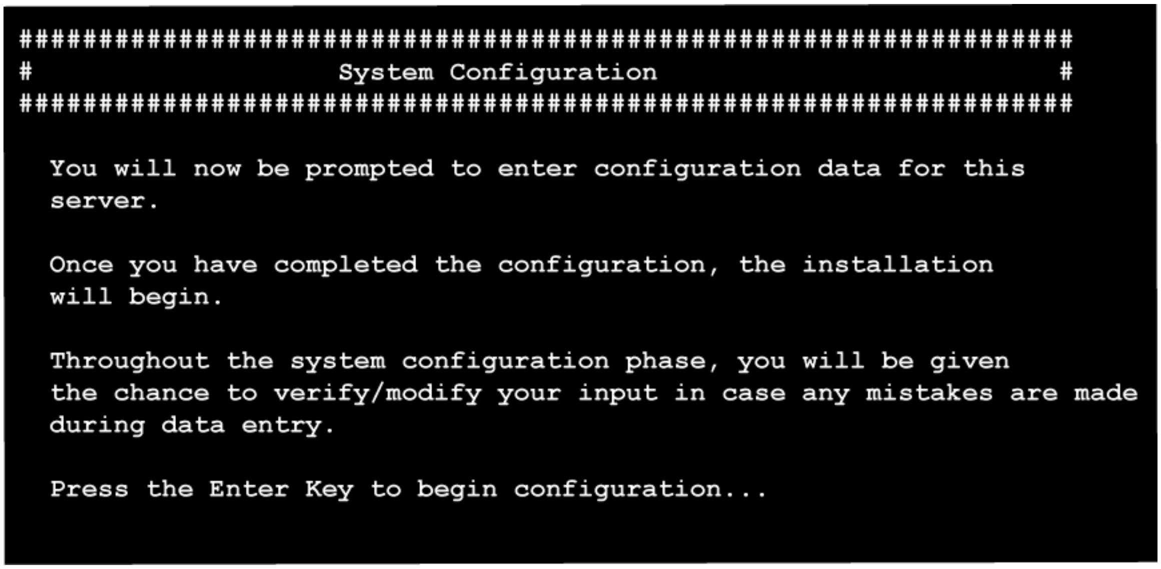
Figure 25: Base Configuration Data Selection window

8. Type `1` and press `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.

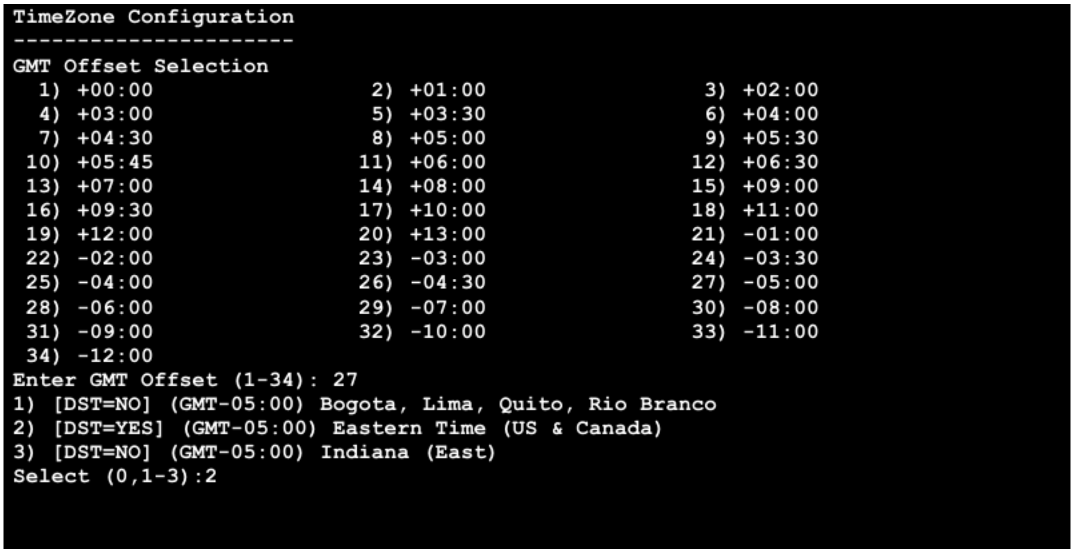
   The System configuration window appears, as shown in Figure 26: System configuration window on page 78.



```
####################################################################
#                    System Configuration                          #
####################################################################

  You will now be prompted to enter configuration data for this
  server.

  Once you have completed the configuration, the installation
  will begin.

  Throughout the system configuration phase, you will be given
  the chance to verify/modify your input in case any mistakes are made
  during data entry.

  Press the Enter Key to begin configuration...
```

Figure 26: System configuration window

9. Press `Enter` to continue. The TimeZone Configuration screen appears, as shown inFigure 27: TimeZone Configuration window on page 78 .



```
TimeZone Configuration
----------------------
GMT Offset Selection
  1) +00:00                 2) +01:00                 3) +02:00
  4) +03:00                 5) +03:30                 6) +04:00
  7) +04:30                 8) +05:00                 9) +05:30
 10) +05:45                11) +06:00                12) +06:30
 13) +07:00                14) +08:00                15) +09:00
 16) +09:30                17) +10:00                18) +11:00
 19) +12:00                20) +13:00                21) -01:00
 22) -02:00                23) -03:00                24) -03:30
 25) -04:00                26) -04:30                27) -05:00
 28) -06:00                29) -07:00                30) -08:00
 31) -09:00                32) -10:00                33) -11:00
 34) -12:00
Enter GMT Offset (1-34): 27
1) [DST=NO] (GMT-05:00) Bogota, Lima, Quito, Rio Branco
2) [DST=YES] (GMT-05:00) Eastern Time (US & Canada)
3) [DST=NO] (GMT-05:00) Indiana (East)
Select (0,1-3):2
```

Figure 27: TimeZone Configuration window

10. 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 on page 78.

    Table 12: GMT offset timezones

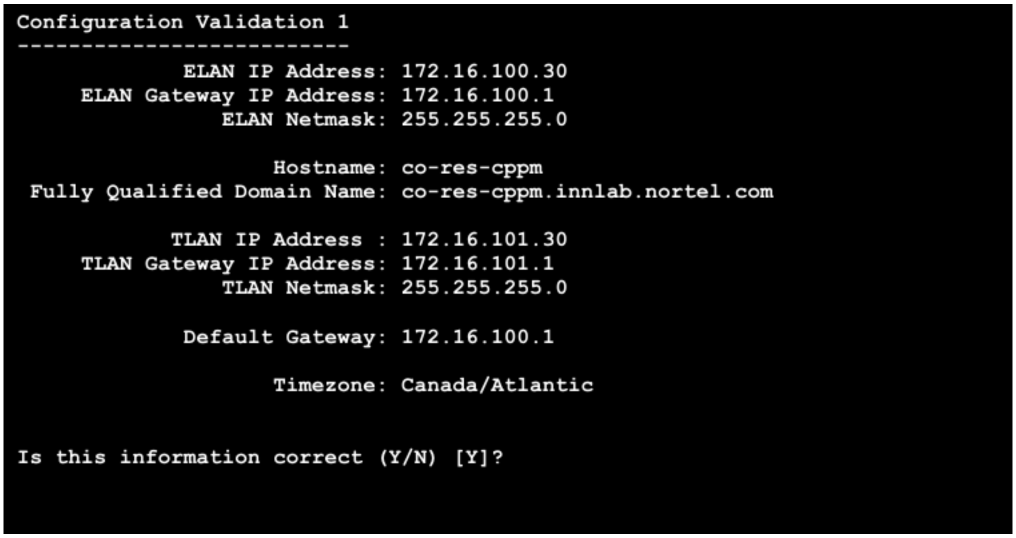
Name	Description	Relative to GMT
GMT	Greenwich Mean Time	GMT

Name	Description	Relative to 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

Name	Description	Relative to GMT
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

11. 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 28: Configuration Validation 1 window on page 80.



```
Configuration Validation 1
--------------------------
             ELAN IP Address: 172.16.100.30
     ELAN Gateway IP Address: 172.16.100.1
                ELAN Netmask: 255.255.255.0

                    Hostname: co-res-cppm
 Fully Qualified Domain Name: co-res-cppm.innlab.nortel.com

            TLAN IP Address : 172.16.101.30
     TLAN Gateway IP Address: 172.16.101.1
                TLAN Netmask: 255.255.255.0

             Default Gateway: 172.16.100.1

                    Timezone: Canada/Atlantic


Is this information correct (Y/N) [Y]?
```

Figure 28: Configuration Validation 1 window

12. Review the configuration information, type `Y` to confirm the data, and press `Enter`.

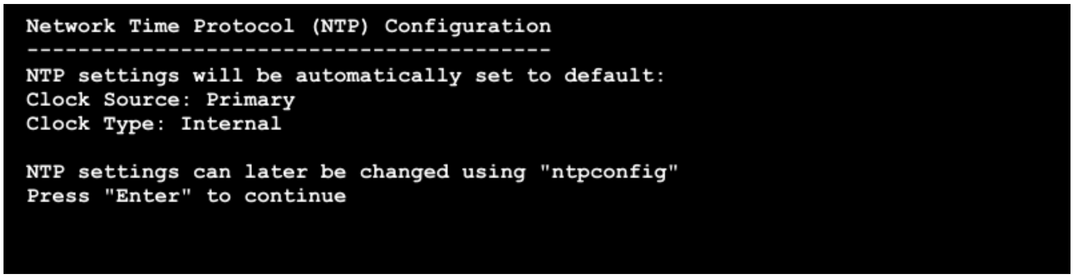
    OR

    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 29: Network Time Protocol (NTP) Configuration window on page 81 .

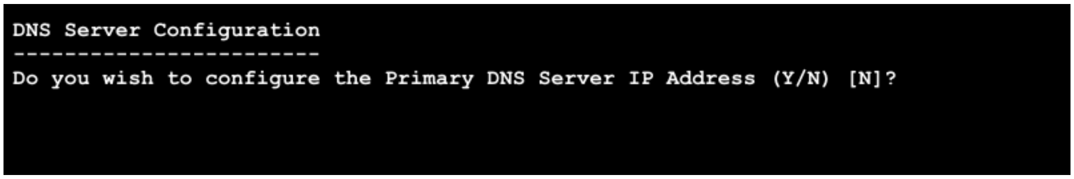


```
Network Time Protocol (NTP) Configuration
-----------------------------------------
NTP settings will be automatically set to default:
Clock Source: Primary
Clock Type: Internal

NTP settings can later be changed using "ntpconfig"
Press "Enter" to continue
```

Figure 29: Network Time Protocol (NTP) Configuration window

13. Press `Enter`.

    The DNS Server Configuration screen appears, as shown in Figure 30: DNS Server Configuration window on page 81.



```
DNS Server Configuration
------------------------
Do you wish to configure the Primary DNS Server IP Address (Y/N) [N]?
```

Figure 30: DNS Server Configuration window

14. Type `Y` and press `Enter` to configure the Primary DNS server IP address.

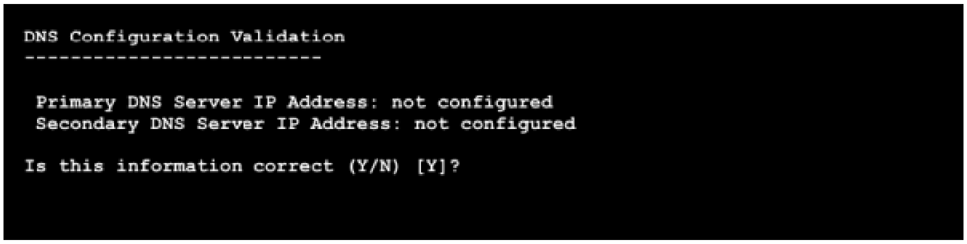
    OR

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

    Note:
    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:
    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 31: Configuration Validation window on page 81 .



```
DNS Configuration Validation
-------------------------

 Primary DNS Server IP Address: not configured
 Secondary DNS Server IP Address: not configured

Is this information correct (Y/N) [Y]?
```

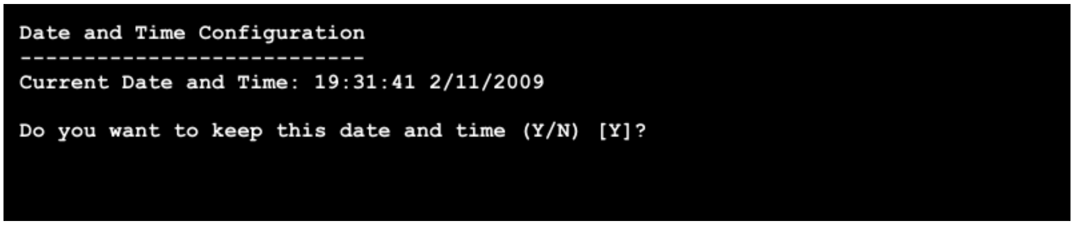
Figure 31: Configuration Validation window

15. 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 32: Date and Time Configuration window on page 82.



```
Date and Time Configuration
---------------------------
Current Date and Time: 19:31:41 2/11/2009

Do you want to keep this date and time (Y/N) [Y]?
```

Figure 32: Date and Time Configuration window

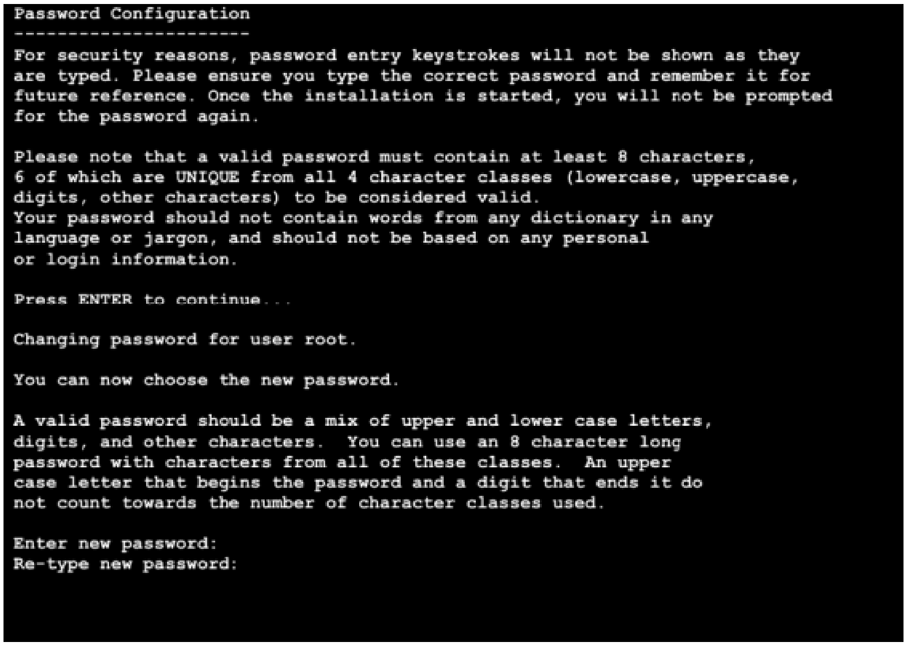
16. Type `Y` and press `Enter` to confirm the date and time.

    OR

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

    > **Important:**
    > 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 33: root Password Configuration window on page 83.

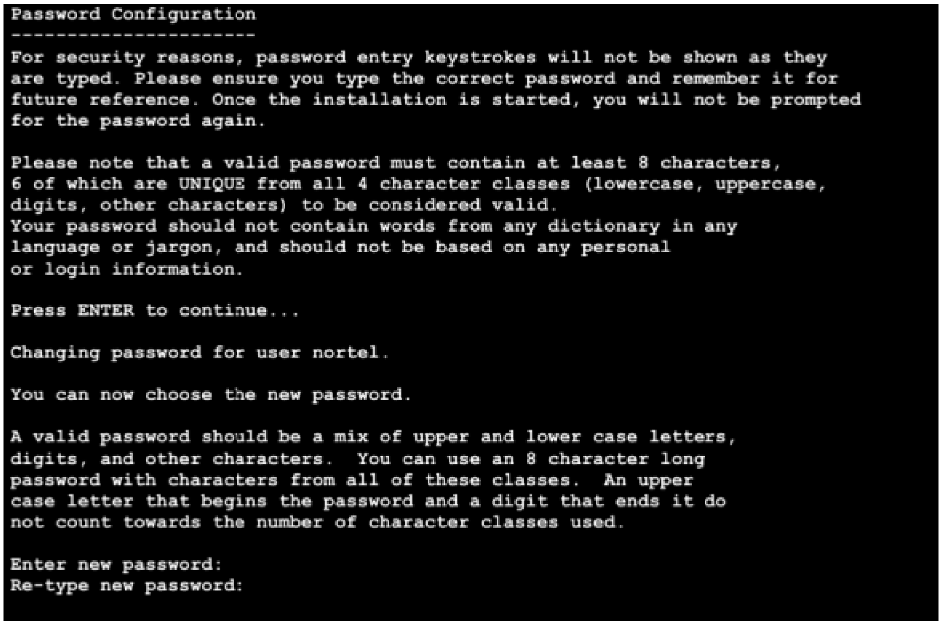


```
Password Configuration
----------------------
For security reasons, password entry keystrokes will not be shown as they
are typed. Please ensure you type the correct password and remember it for
future reference. Once the installation is started, you will not be prompted
for the password again.

Please note that a valid password must contain at least 8 characters,
6 of which are UNIQUE from all 4 character classes (lowercase, uppercase,
digits, other characters) to be considered valid.
Your password should not contain words from any dictionary in any
language or jargon, and should not be based on any personal
or login information.

Press ENTER to continue...

Changing password for user root.

You can now choose the new password.

A valid password should be a mix of upper and lower case letters,
digits, and other characters.  You can use an 8 character long
password with characters from all of these classes.  An upper
case letter that begins the password and a digit that ends it do
not count towards the number of character classes used.

Enter new password:
Re-type new password:
```

Figure 33: root Password Configuration window

17. Enter a value for the root password.
18. Reenter the value for the root password and press `Enter`.

    The nortel Password Configuration screen appears, as shown in Figure 34: nortel Password Configuration window on page 83.

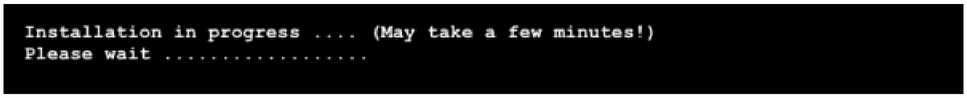


```
Password Configuration
----------------------
For security reasons, password entry keystrokes will not be shown as they
are typed. Please ensure you type the correct password and remember it for
future reference. Once the installation is started, you will not be prompted
for the password again.

Please note that a valid password must contain at least 8 characters,
6 of which are UNIQUE from all 4 character classes (lowercase, uppercase,
digits, other characters) to be considered valid.
Your password should not contain words from any dictionary in any
language or jargon, and should not be based on any personal
or login information.

Press ENTER to continue...

Changing password for user nortel.

You can now choose the new password.

A valid password should be a mix of upper and lower case letters,
digits, and other characters.  You can use an 8 character long
password with characters from all of these classes.  An upper
case letter that begins the password and a digit that ends it do
not count towards the number of character classes used.

Enter new password:
Re-type new password:
```

Figure 34: nortel Password Configuration window

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

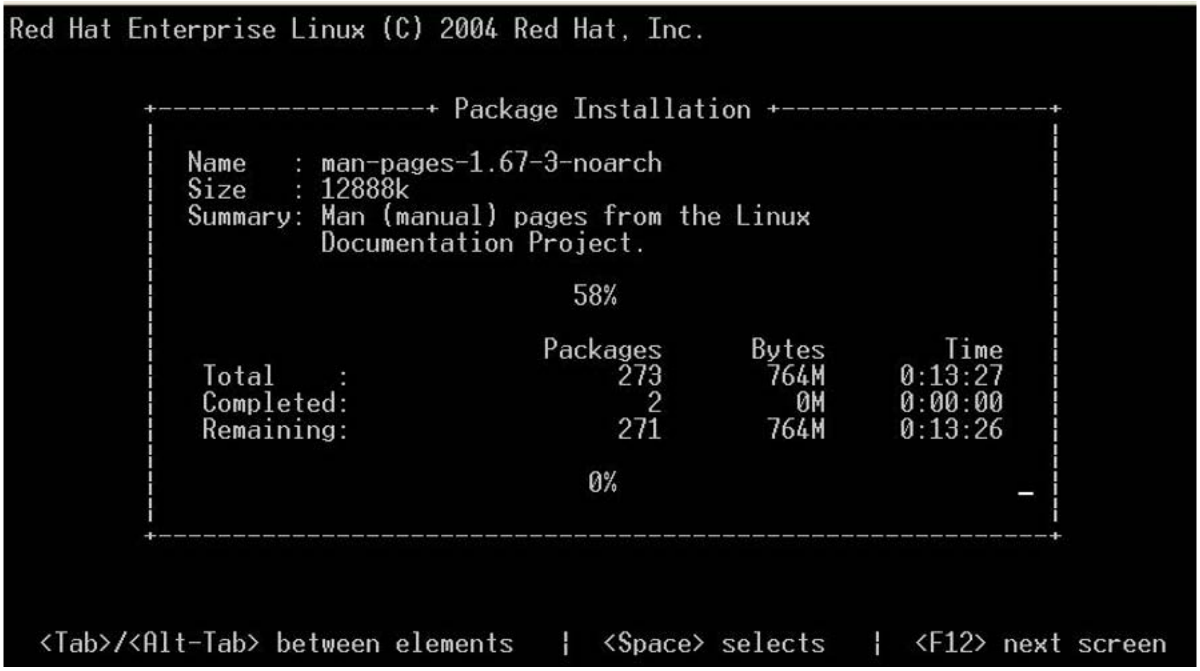
    A pre-installation status screen appears as shown in Figure 35: Pre-installation status window on page 84.



```
Installation in progress .... (May take a few minutes!)
Please wait .................
```

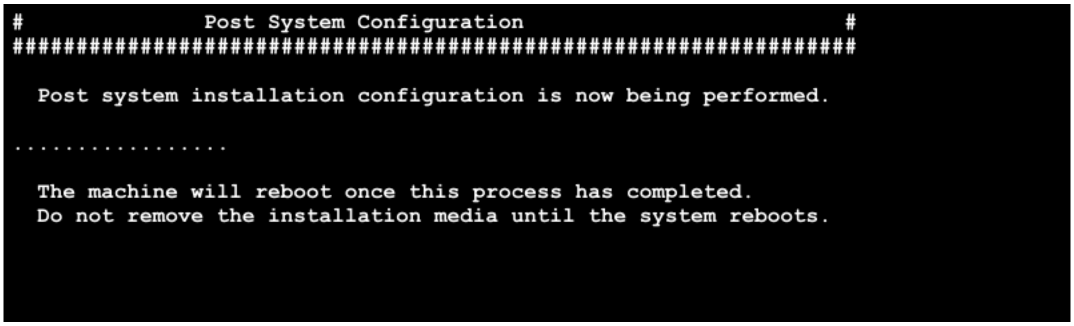
Figure 35: Pre-installation status window

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 36: Package Installation window on page 85, Figure 37: Post System Configuration window on page 85, and Figure 38: Status of Linux Hardening items window on page 85.



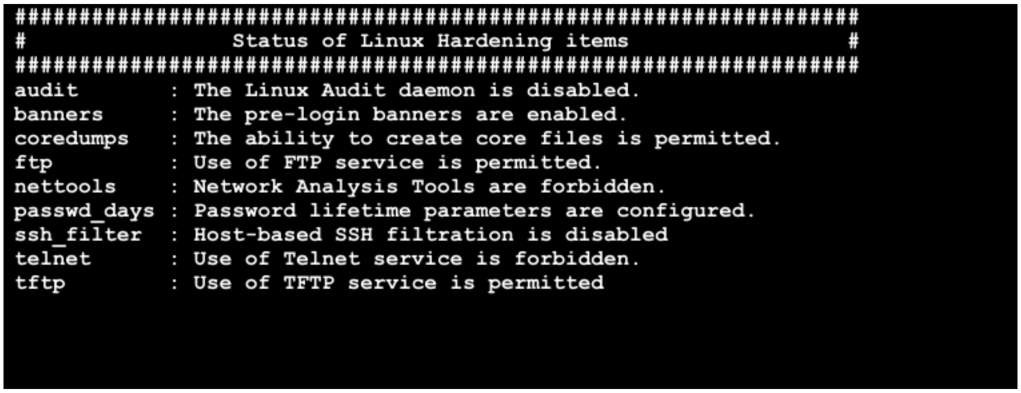
```
Red Hat Enterprise Linux (C) 2004 Red Hat, Inc.

         +-------------------+ Package Installation +-------------------+
         |                                                              |
         |  Name    : man-pages-1.67-3-noarch                           |
         |  Size    : 12888k                                            |
         |  Summary: Man (manual) pages from the Linux                  |
         |           Documentation Project.                             |
         |                                                              |
         |                         58%                                  |
         |                                                              |
         |                       Packages      Bytes       Time         |
         |   Total     :              273       764M     0:13:27        |
         |   Completed:                 2         0M     0:00:00        |
         |   Remaining:               271       764M     0:13:26        |
         |                                                              |
         |                          0%                                  |
         |                                                              |
         +--------------------------------------------------------------+


  <Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

Figure 36: Package Installation window



```
#               Post System Configuration                           #
#####################################################################

  Post system installation configuration is now being performed.

.................

  The machine will reboot once this process has completed.
  Do not remove the installation media until the system reboots.
```

Figure 37: Post System Configuration window



```
#####################################################################
#                 Status of Linux Hardening items                   #
#####################################################################
audit        : The Linux Audit daemon is disabled.
banners      : The pre-login banners are enabled.
coredumps    : The ability to create core files is permitted.
ftp          : Use of FTP service is permitted.
nettools     : Network Analysis Tools are forbidden.
passwd_days  : Password lifetime parameters are configured.
ssh_filter   : Host-based SSH filtration is disabled
telnet       : Use of Telnet service is forbidden.
tftp         : Use of TFTP service is permitted
```

Figure 38: Status of Linux Hardening items window

The CP PM Card now has the Nortel Linux Base installed. You must complete the procedures in Application installation using Deployment Manager on page 86to deploy the Call Server and Signaling Server Applications to this server using the UCM Deployment Manager.

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*.

Logging on to UCM

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**.

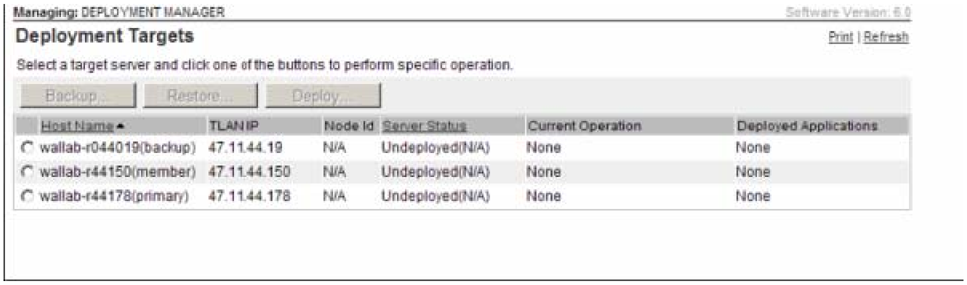
   The default navigation Web page for UCM appears.

Access the centralized software Deployment Manager

Accessing the centralized software Deployment Manager

1. Log on to UCM. See Logging on to UCM on page 87.
2. In the navigation pane, click Network, CS 1000 Servers, Software Deployment.

   The Deployment Manager screen appears, as shown in Figure 39: Deployment Manager window on page 88.



Managing: DEPLOYMENT MANAGER

Software Version: 6.0

Deployment Targets

Print | Refresh

Select a target server and click one of the buttons to perform specific operation.

	Host Name ▲	TLAN IP	Node Id	Server Status	Current Operation	Deployed Applications
○	wallab-r044019(backup)	47.11.44.19	N/A	Undeployed(N/A)	None	None
○	wallab-r44150(member)	47.11.44.150	N/A	Undeployed(N/A)	None	None
○	wallab-r44178(primary)	47.11.44.178	N/A	Undeployed(N/A)	None	None

Figure 39: Deployment Manager window

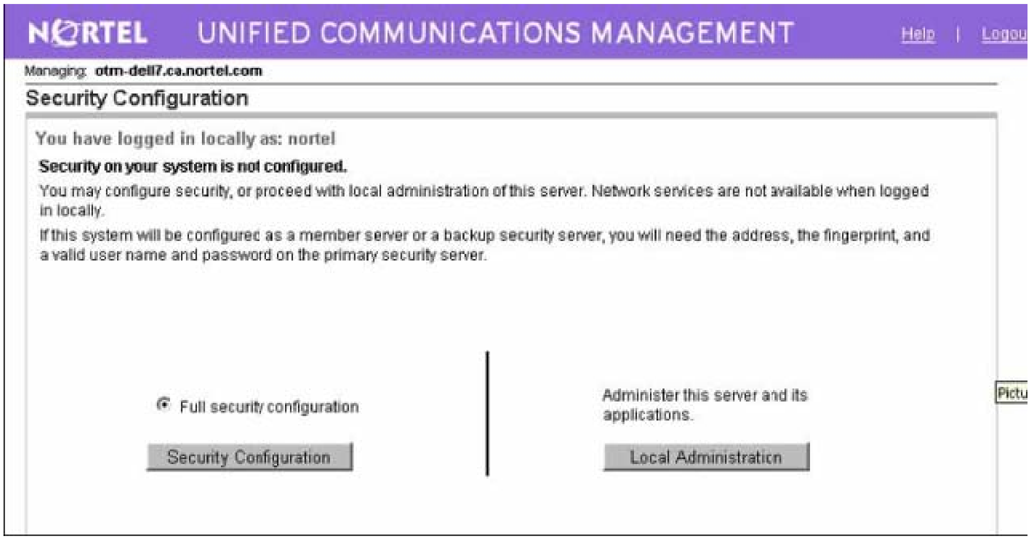
Access the Local Deployment Manager

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

1. Log on to the linux base server using the nortel user ID and password.

   The Security Configuration screen appears, as shown in Figure 40: Security Configuration window on page 89.



Managing: otm-dell7.ca.nortel.com

Security Configuration

You have logged in locally as: nortel

Security on your system is not configured.

You may configure security, or proceed with local administration of this server. Network services are not available when logged in locally.

If this system will be configured as a member server or a backup security server, you will need the address, the fingerprint, and a valid user name and password on the primary security server.

● Full security configuration

Security Configuration

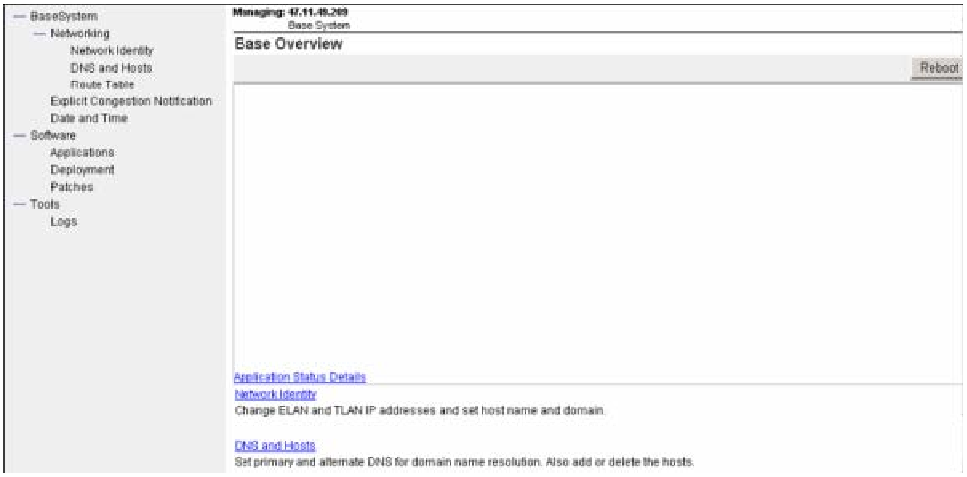
Administer this server and its applications.

Local Administration

Figure 40: Security Configuration window

2. Click Local Administration.

   The Base Manager screen appears, as shown in Figure 41: Base Manager window on page 89.



Managing: 47.11.49.209
Base System

Base Overview

Application Status Details

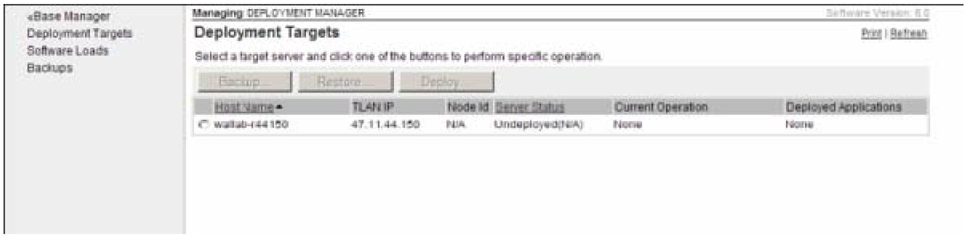
Network Identity
Change ELAN and TLAN IP addresses and set host name and domain.

DNS and Hosts
Set primary and alternate DNS for domain name resolution. Also add or delete the hosts.

Figure 41: Base Manager window

3. In the navigation pane click Applications Deployment Manager.

   The Deployment Manager screen appears, as shown in Figure 42: Deployment Manager window on page 90.



Deployment Targets

Select a target server and click one of the buttons to perform specific operation.

Host Name ▲	TLAN IP	Node Id	Server Status	Current Operation	Deployed Applications
○ wallab-r44150	47.11.44.150	N/A	Undeployed(N/A)	None	None

Figure 42: Deployment Manager window

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.

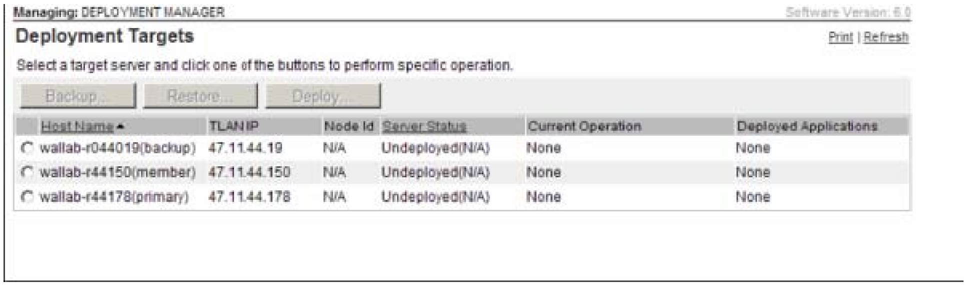
Centralized deployment requires that the application software load be loaded only once to the primary Security Server's hard drive. The primary Security Server can then deploy the software applications to other servers in the same security domain.

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

Adding a new software load to the Deployment Manager

1. In the navigation pane, click Software Deployment.

   The Deployment Manager screen appears, as shown in Figure 43: Deployment Manager window on page 91.



Deployment Targets

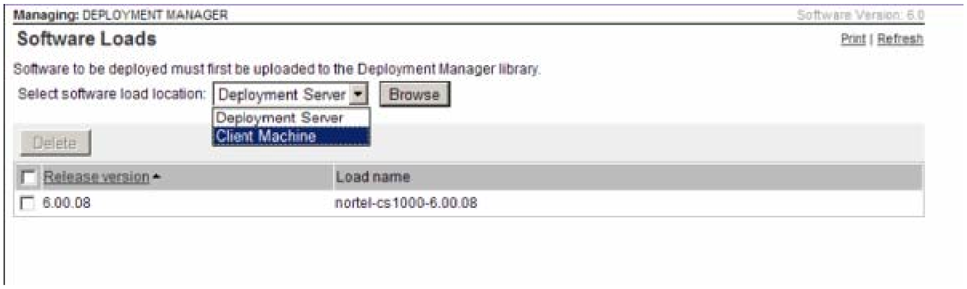
Select a target server and click one of the buttons to perform specific operation.

	Host Name ▲	TLAN IP	Node Id	Server Status	Current Operation	Deployed Applications
○	wallab-r044019(backup)	47.11.44.19	N/A	Undeployed(N/A)	None	None
○	wallab-r44150(member)	47.11.44.150	N/A	Undeployed(N/A)	None	None
○	wallab-r44178(primary)	47.11.44.178	N/A	Undeployed(N/A)	None	None

Figure 43: Deployment Manager window

2. In the navigation pane, click Software Loads.

   The Software Loads page appears, as shown in Figure 44: Software Loads window on page 91.



Software Loads

Software to be deployed must first be uploaded to the Deployment Manager library.

Select software load location: Deployment Server

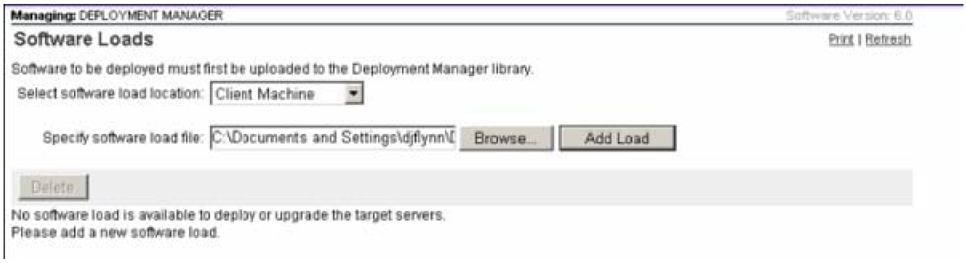
□ Release version ▲	Load name
□ 6.00.08	nortel-cs1000-6.00.08

Figure 44: 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 45: Software Loads file selection window on page 91.



Software Loads

Software to be deployed must first be uploaded to the Deployment Manager library.

Select software load location: Client Machine

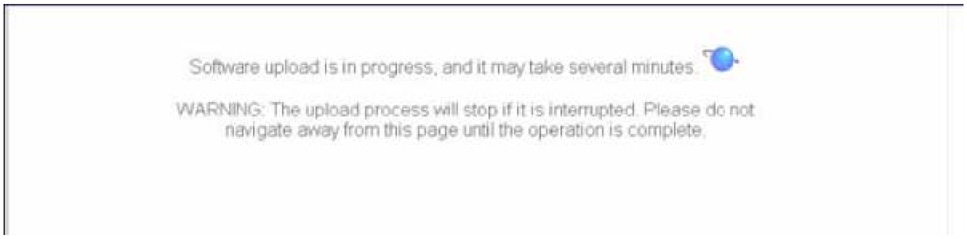
Specify software load file: C:\Documents and Settings\djflynn\[

No software load is available to deploy or upgrade the target servers.
Please add a new software load.

Figure 45: Software Loads file selection window

5. Click Add Load.

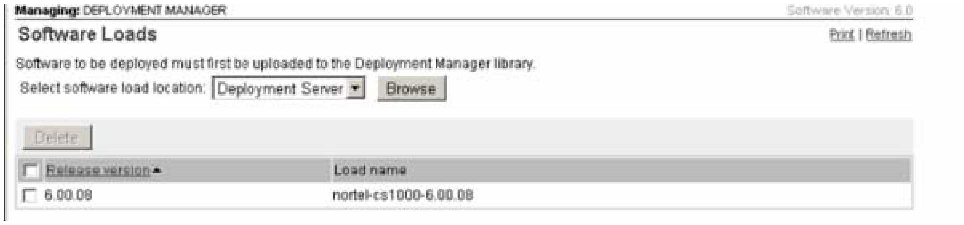
   An upload progress screen appears, as shown in Figure 46: Software upload progress window on page 92When the upload is complete the software load appears, as shown in Figure 44: Software Loads window on page 91.



Software upload is in progress, and it may take several minutes.

WARNING: The upload process will stop if it is interrupted. Please do not navigate away from this page until the operation is complete.

Figure 46: Software upload progress window



Managing: DEPLOYMENT MANAGER

Software Version: 6.0

Software Loads

Print | Refresh

Software to be deployed must first be uploaded to the Deployment Manager library.

Select software load location: Deployment Server

□ Release version	Load name
□ 6.00.08	nortel-cs1000-6.00.08

Figure 47: Software Loads window

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.

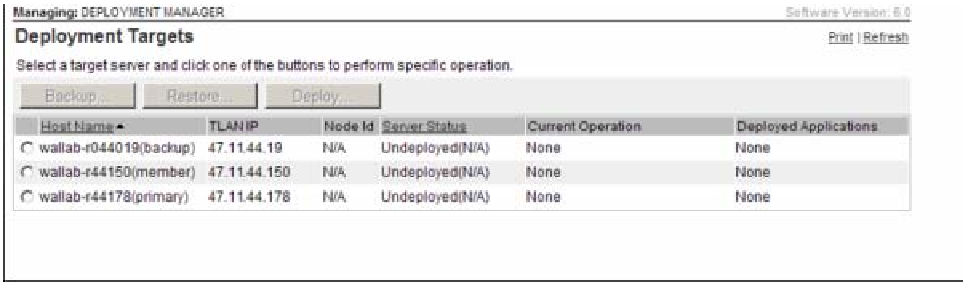
Note:

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.

Deleting a software load from the Deployment Manager

1. In the navigation pane, click Network, CS 1000 Servers, Software Deployment.

   The Deployment Manager screen appears, as shown in Figure 48: Deployment Manager window on page 92.



Managing: DEPLOYMENT MANAGER

Software Version: 6.0

Deployment Targets

Print | Refresh

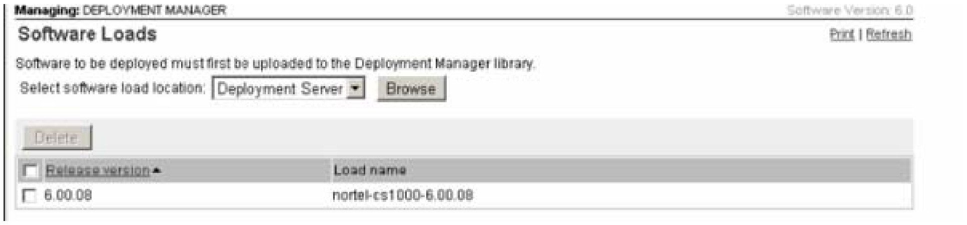
Select a target server and click one of the buttons to perform specific operation.

Host Name	TLAN IP	Node Id	Server Status	Current Operation	Deployed Applications
○ wallab-r044019(backup)	47.11.44.19	N/A	Undeployed(N/A)	None	None
○ wallab-r44150(member)	47.11.44.150	N/A	Undeployed(N/A)	None	None
○ wallab-r44178(primary)	47.11.44.178	N/A	Undeployed(N/A)	None	None

Figure 48: Deployment Manager window

2. In the navigation pane, click Software Loads.

The Software Loads page appears, as shown in Figure 49: Software Loads window on page 93.



Managing: DEPLOYMENT MANAGER

Software Version: 6.0

Software Loads

Print | Refresh

Software to be deployed must first be uploaded to the Deployment Manager library.

Select software load location: Deployment Server ▾ Browse

Delete

□ Release version ▴	Load name
□ 6.00.08	nortel-cs1000-6.00.08

Figure 49: Software Loads window

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

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 Server

Prerequisites

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

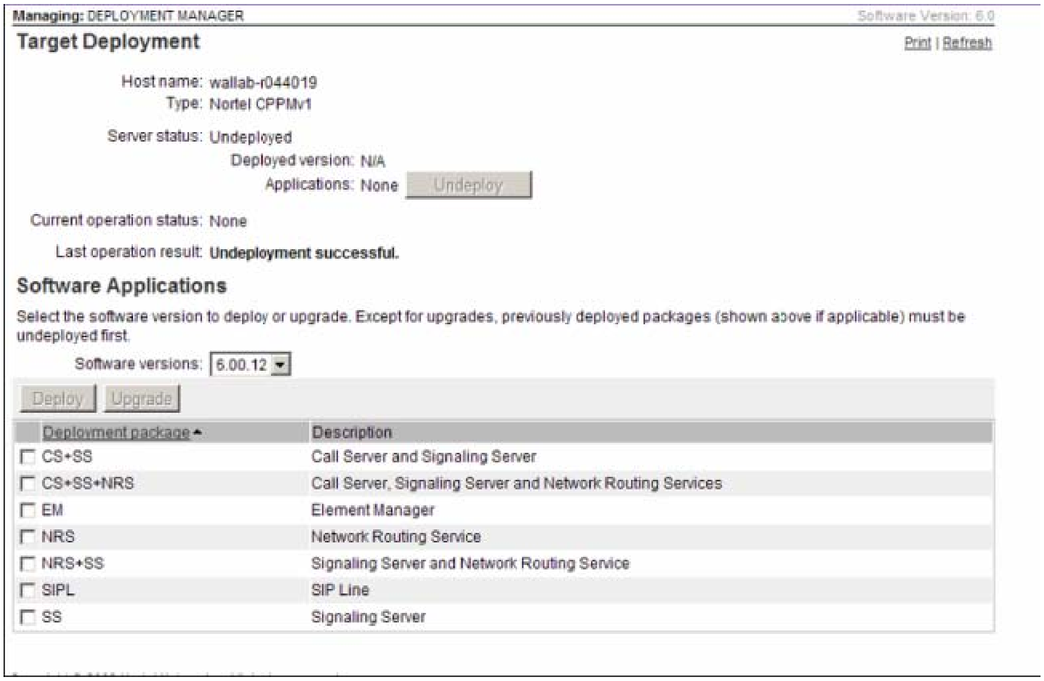
Deploying application software to a Server

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 50: Target deployment and available software applications on page 94.



Target Deployment

Host name: wallab-r044019
Type: Nortel CPPMv1

Server status: Undeployed
Deployed version: N/A
Applications: None

Current operation status: None

Last operation result: **Undeployment successful.**

Software Applications

Select the software version to deploy or upgrade. Except for upgrades, previously deployed packages (shown above if applicable) must be undeployed first.

Software versions: 6.00.12

Deployment package ▲	Description
□ CS+SS	Call Server and Signaling Server
□ CS+SS+NRS	Call Server, Signaling Server and Network Routing Services
□ EM	Element Manager
□ NRS	Network Routing Service
□ NRS+SS	Signaling Server and Network Routing Service
□ SIPL	SIP Line
□ SS	Signaling Server

Figure 50: 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.

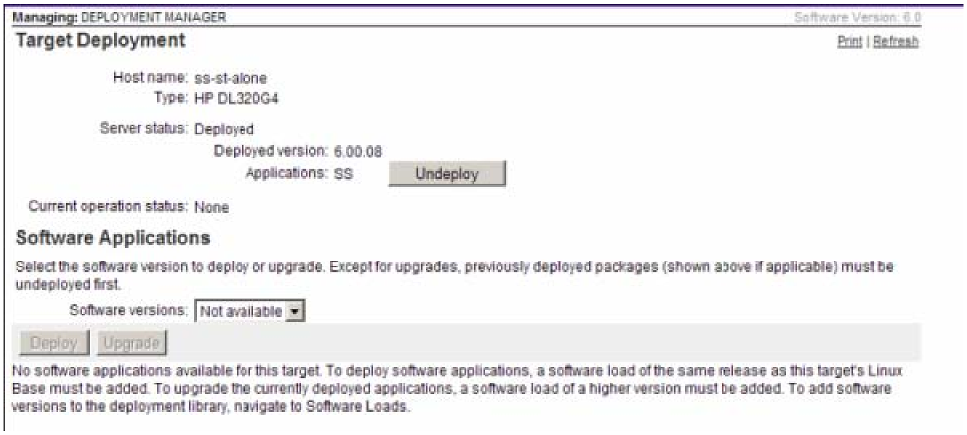
   Note:

   Deployment packages are platform dependant; the platform of the target server influences which deployment packages are available..

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 Application installation using Deployment Manager on page 86.
7. Click **Deploy**.

   Important:

   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 51: Target Deployment window on page 95.



Target Deployment

Host name: ss-st-alone
Type: HP DL320G4

Server status: Deployed
Deployed version: 6.00.08
Applications: SS

Current operation status: None

Software Applications

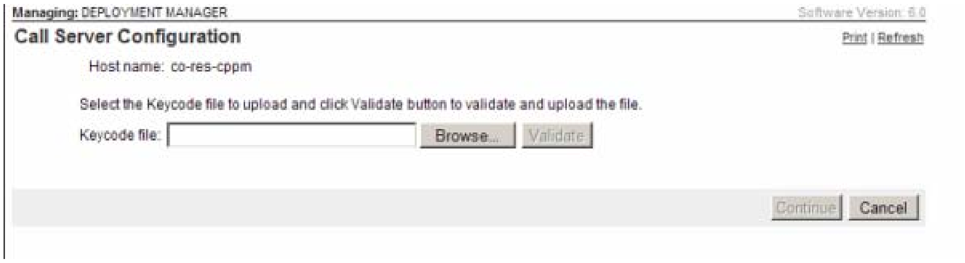
Select the software version to deploy or upgrade. Except for upgrades, previously deployed packages (shown above if applicable) must be undeployed first.

Software versions: Not available

No software applications available for this target. To deploy software applications, a software load of the same release as this target's Linux Base must be added. To upgrade the currently deployed applications, a software load of a higher version must be added. To add software versions to the deployment library, navigate to Software Loads.

Figure 51: 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 52: Call Server Configuration window on page 95.



Call Server Configuration

Host name: co-res-cppm

Select the Keycode file to upload and click Validate button to validate and upload the file.

Keycode file:

Figure 52: Call Server Configuration window

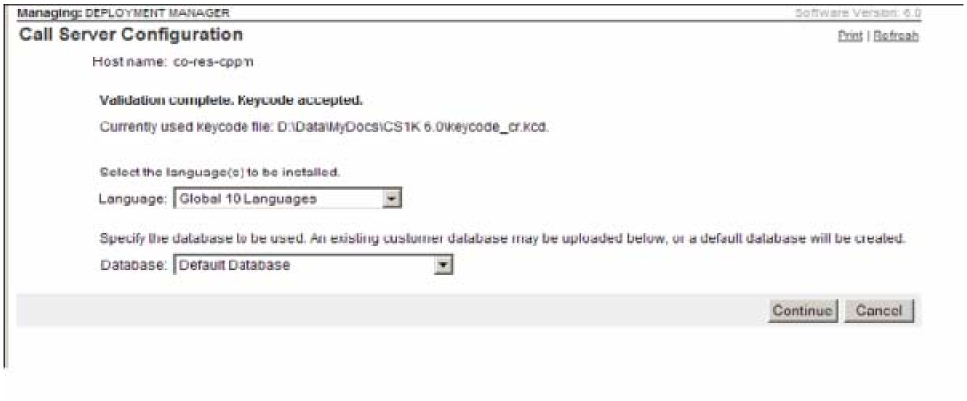
9. In the Keycode file box, type the path and filename for the keycode file.

   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 53: Call Server Configuration language and database selection window on page 96.



Managing: DEPLOYMENT MANAGER

Software Version: 6.0

Call Server Configuration

Host name: co-res-cppm

Validation complete. Keycode accepted.

Currently used keycode file: D:\Data\MyDocs\CS1K 6.0\keycode_cr.kcd.

Select the language(s) to be installed.

Language: Global 10 Languages

Specify the database to be used. An existing customer database may be uploaded below, or a default database will be created.

Database: Default Database

Figure 53: 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 RMD, proceed to step 25.

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

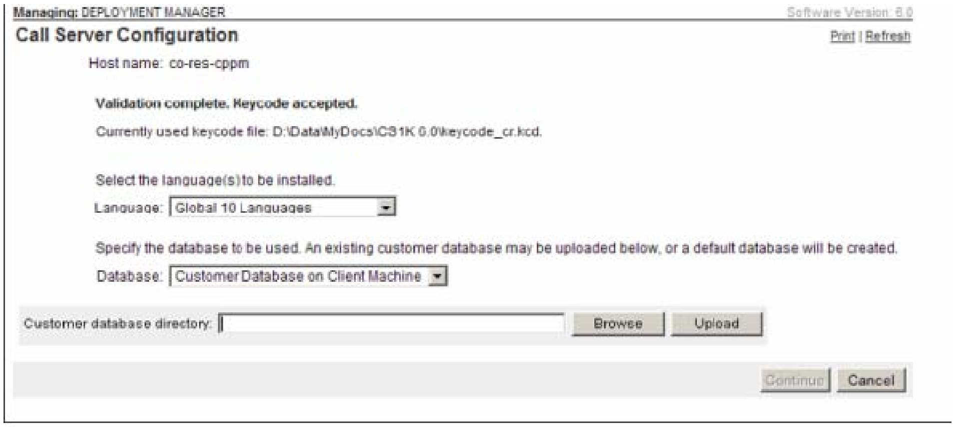
    Note:

    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 54: Call Server Configuration customer database directory window on page 97.



Managing: DEPLOYMENT MANAGER

Software Version: 6.0

Call Server Configuration

Host name: co-res-cppm

Validation complete. Keycode accepted.

Currently used keycode file: D:\Data\MyDocs\CS1K 6.0\keycode_cr.kcd.

Select the language(s) to be installed.

Language: Global 10 Languages

Specify the database to be used. An existing customer database may be uploaded below, or a default database will be created.

Database: Customer Database on Client Machine

Customer database directory:

Figure 54: Call Server Configuration customer database directory window

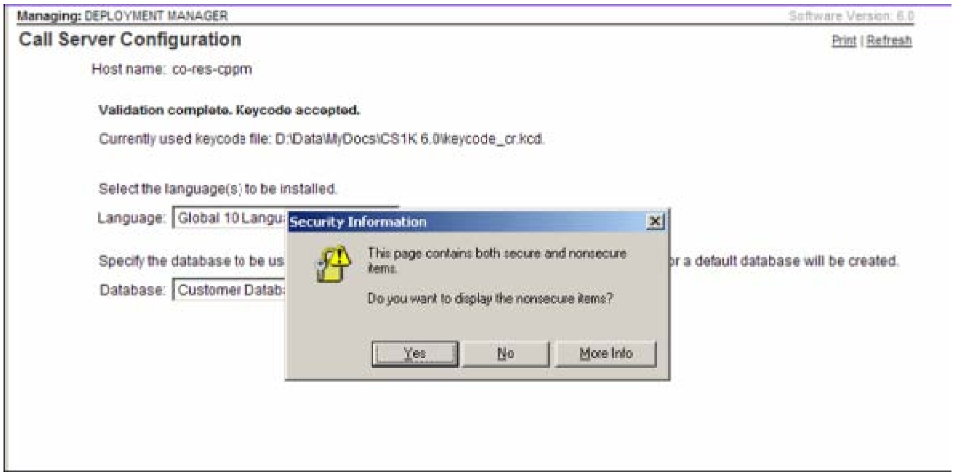
16. In the **Customer database directory** box, type a value for the customer database directory.

    OR

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

17. Click **Upload**.

    The Security Information screen appears, as shown in Figure 55: Security Information window on page 97.



Managing: DEPLOYMENT MANAGER

Software Version: 6.0

Call Server Configuration

Host name: co-res-cppm

Validation complete. Keycode accepted.

Currently used keycode file: D:\Data\MyDocs\CS1K 6.0\keycode_cr.kcd.

Select the language(s) to be installed.

Language: Global 10 Langu

Specify the database to be us ... r a default database will be created.

Database: Customer Datab

Security Information

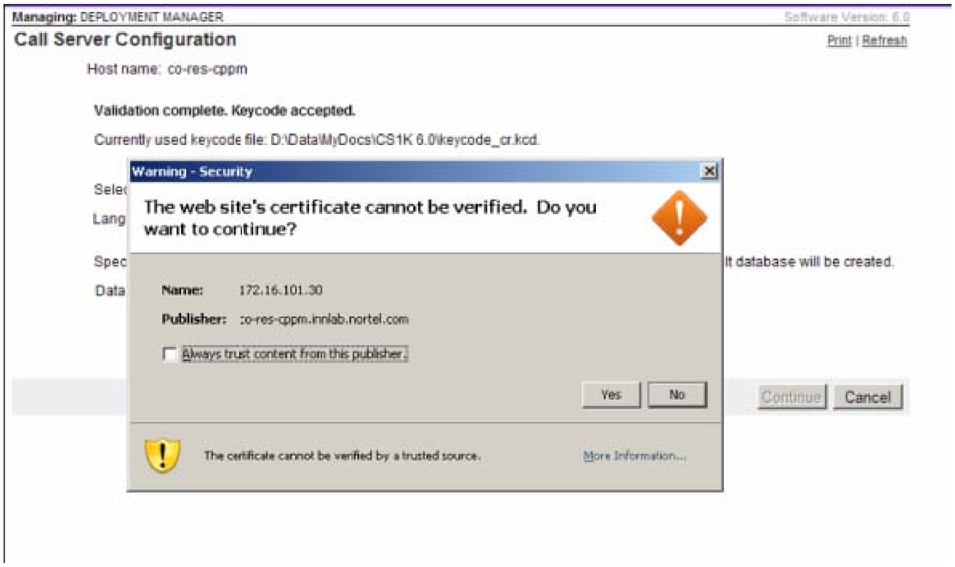
This page contains both secure and nonsecure items.

Do you want to display the nonsecure items?

Figure 55: Security Information window

18. Click **Yes**.

    The Security warning 1 screen appears, as shown in Figure 56: Security warning 1 window on page 98.



Managing: DEPLOYMENT MANAGER

Software Version: 6.0

Call Server Configuration

Host name: co-res-cppm

Validation complete. Keycode accepted.

Currently used keycode file: D:\Data\MyDocs\CS1K 6.0\keycode_cr.kcd.

Warning - Security

The web site's certificate cannot be verified. Do you want to continue?

Name: 172.16.101.30

Publisher: co-res-cppm.innlab.nortel.com

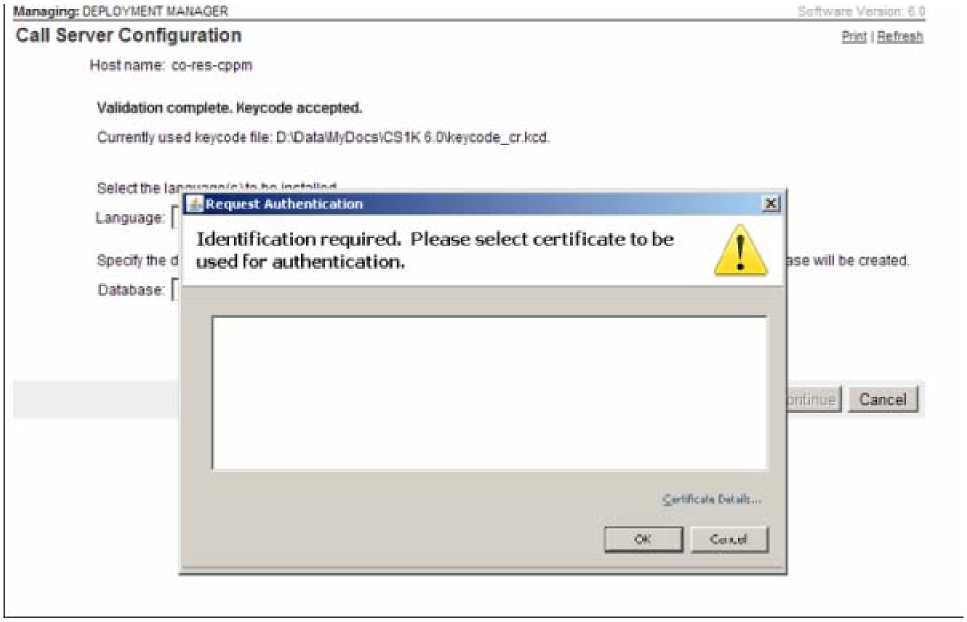
□ Always trust content from this publisher.

The certificate cannot be verified by a trusted source.

Figure 56: Security warning 1 window

19. Click **Yes**.

    The Request Authentication screen appears, as shown in Figure 57: Request Authentication window on page 98.



Managing: DEPLOYMENT MANAGER

Software Version: 6.0

Call Server Configuration

Host name: co-res-cppm

Validation complete. Keycode accepted.

Currently used keycode file: D:\Data\MyDocs\CS1K 6.0\keycode_cr.kcd.

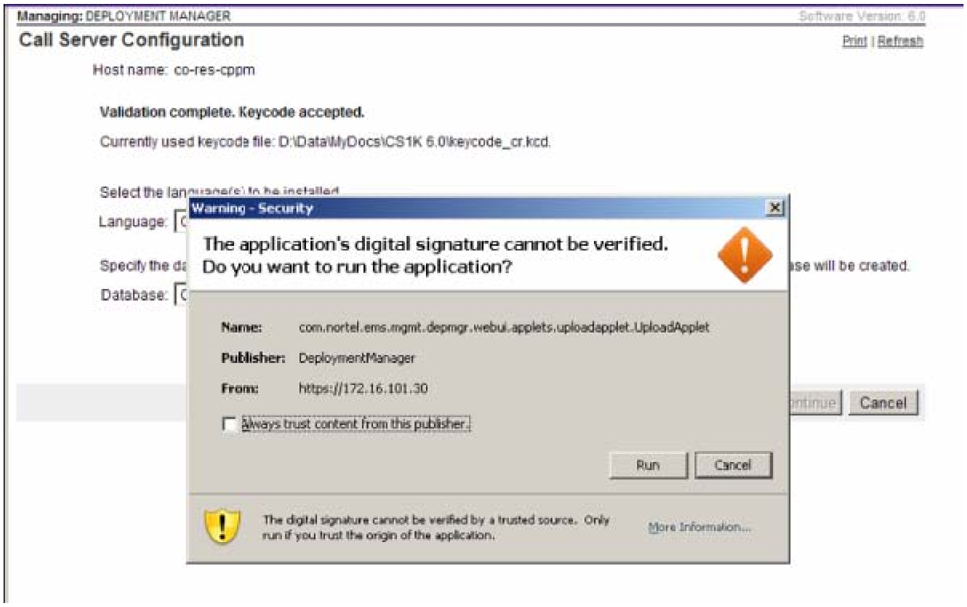
Request Authentication

Identification required. Please select certificate to be used for authentication.

Figure 57: Request Authentication window

20. Click **OK**.

    The Security warning 2 screen appears, as shown in Figure 58: Security warning 2 window on page 99.



Managing: DEPLOYMENT MANAGER

Software Version: 6.0

Call Server Configuration

Print | Refresh

Host name: co-res-cppm

Validation complete. Keycode accepted.

Currently used keycode file: D:\Data\MyDocs\CS1K 6.0\keycode_cr.kcd

Select the languages(s) to be installed

Language: C

Specify the da ...se will be created.

Database: C

Warning - Security

The application's digital signature cannot be verified.
Do you want to run the application?

Name: com.nortel.ems.mgmt.depmgr.webui.applets.uploadapplet.UploadApplet

Publisher: DeploymentManager

From: https://172.16.101.30

☐ Always trust content from this publisher.

Run | Cancel

The digital signature cannot be verified by a trusted source. Only run if you trust the origin of the application.

More Information...

ntinue | Cancel

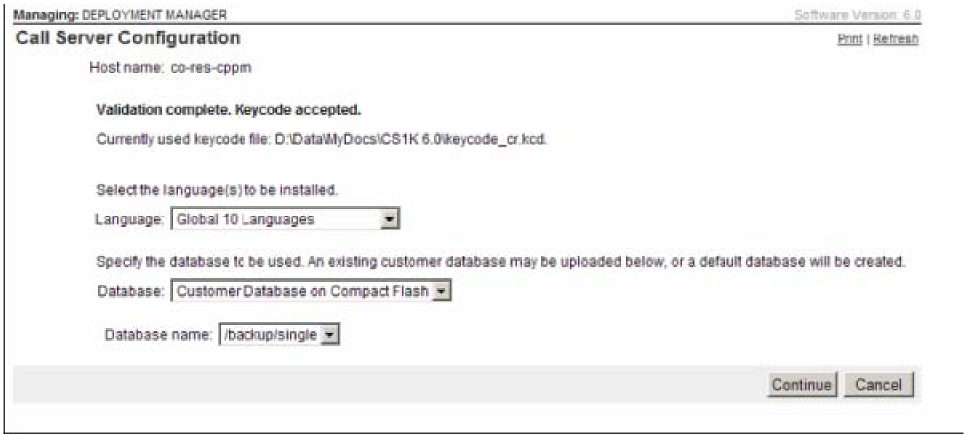
Figure 58: Security warning 2 window

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 59: Call Server Configuration database name window on page 99.



Managing: DEPLOYMENT MANAGER

Software Version: 6.0

Call Server Configuration

Print | Refresh

Host name: co-res-cppm

Validation complete. Keycode accepted.

Currently used keycode file: D:\Data\MyDocs\CS1K 6.0\keycode_cr.kcd

Select the language(s) to be installed.

Language: Global 10 Languages

Specify the database tc be used. An existing customer database may be uploaded below, or a default database will be created.

Database: Customer Database on Compact Flash

Database name: /backup/single

Continue | Cancel

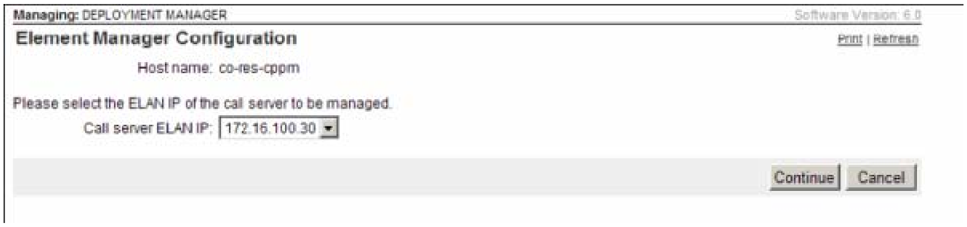
Figure 59: Call Server Configuration database name window

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 60: Element Manager Configuration window on page 100.



Managing: DEPLOYMENT MANAGER

Software Version: 6.0

Element Manager Configuration

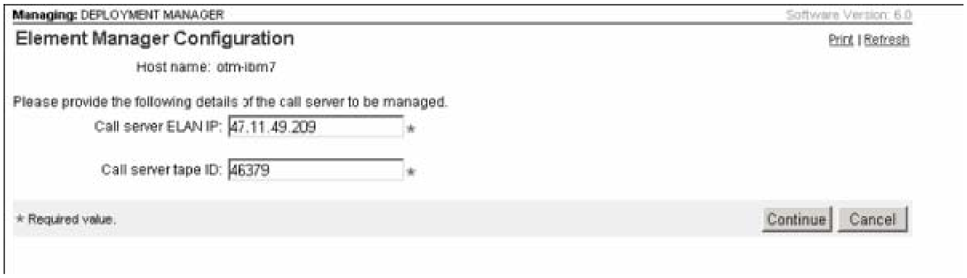
Host name: co-res-cppm

Please select the ELAN IP of the call server to be managed.

Call server ELAN IP: 172.16.100.30

Figure 60: 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 61: Element Manager Configuration window on page 100



Managing: DEPLOYMENT MANAGER

Software Version: 6.0

Element Manager Configuration

Host name: otm-ibm7

Please provide the following details of the call server to be managed.

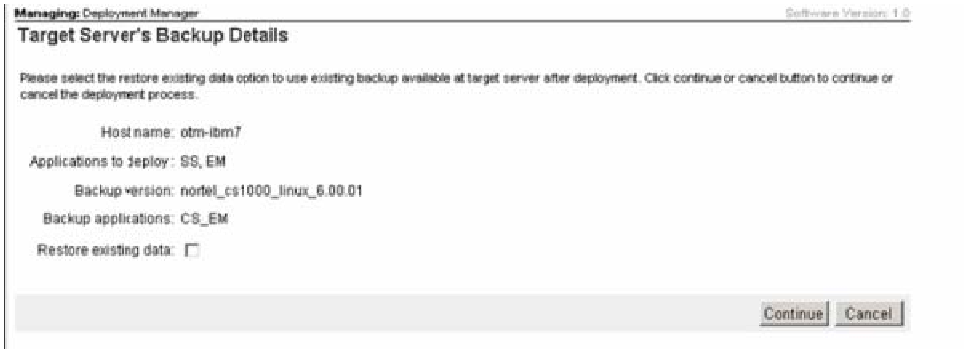
Call server ELAN IP: 47.11.49.209 *

Call server tape ID: 46379 *

* Required value.

Figure 61: 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 62: Target Servers Backup Details window on page 101.



Managing: Deployment Manager | Software Version: 1.0

Target Server's Backup Details

Please select the restore existing data option to use existing backup available at target server after deployment. Click continue or cancel button to continue or cancel the deployment process.

Host name: otm-ibm7

Applications to deploy : SS, EM

Backup version: nortel_cs1000_linux_6.00.01

Backup applications: CS_EM

Restore existing data: □

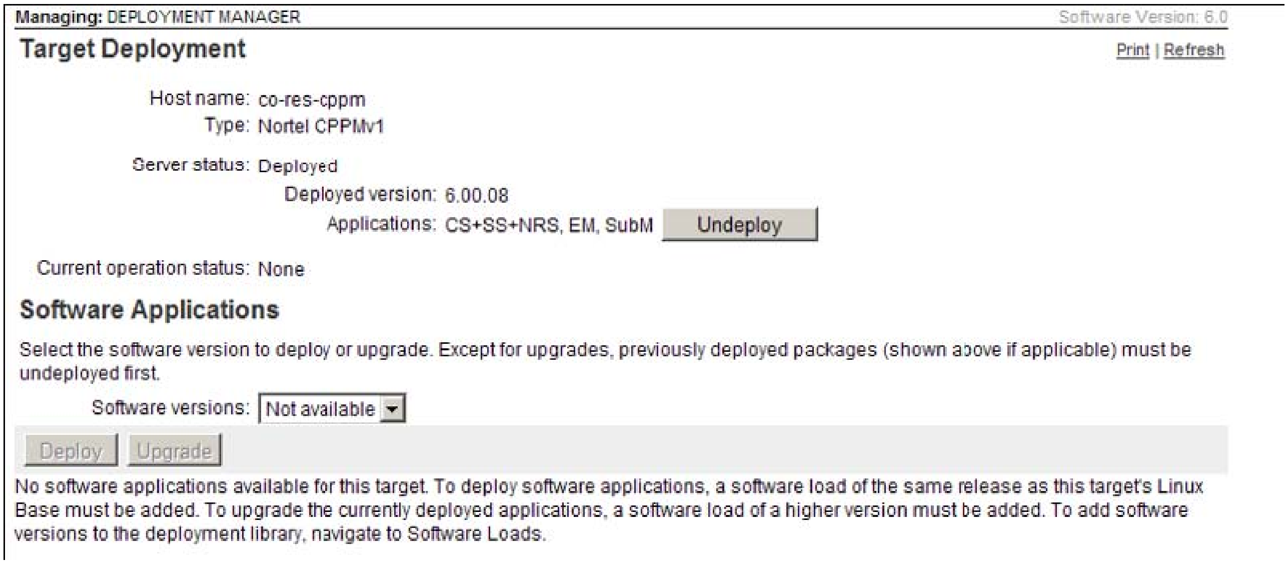
Figure 62: Target Servers Backup Details window

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 63: Target Deployment window on page 101. The screen displays the server deployment status and deployed packages.



Managing: DEPLOYMENT MANAGER | Software Version: 6.0

Target Deployment

Host name: co-res-cppm

Type: Nortel CPPMv1

Server status: Deployed

Deployed version: 6.00.08

Applications: CS+SS+NRS, EM, SubM

Current operation status: None

Software Applications

Select the software version to deploy or upgrade. Except for upgrades, previously deployed packages (shown above if applicable) must be undeployed first.

Software versions: Not available

No software applications available for this target. To deploy software applications, a software load of the same release as this target's Linux Base must be added. To upgrade the currently deployed applications, a software load of a higher version must be added. To add software versions to the deployment library, navigate to Software Loads.

Figure 63: Target Deployment window

Chapter 9: Patching

Patching the 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 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.

Patching Call Server binary patches

1. Ensure the patch file is in the /var/opt/nortel/cs/fs/u/patch directory.
2. Connect to the Co-res CS and SS remotely (ssh) or locally (serial port).
3. Log on to theCo-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>
```

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:

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

Chapter 10: 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 Gateway Controller remote TTY ports. Support is unavailable for CCBR backup and restore on the Server card serial port.
- Support exists for Xmodem sx and rx commands on the Gateway Controller 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.

Chapter 11: Configuration management

OAM User Interface

While support exists for most of the existing CS 1000E Call Server and Signaling Server application user commands for 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 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 Co-res CS and SS
- Co-res CS and SS restart
- Geographic Redundancy Survivable Media Gateway Configuration
- Serial port configuration
- Co-res CS and SS software version
- Co-res CS and SS configuration/database backup and restore
- Media Gateway Centralized Software Upgrade
- 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 Co-res CS and SS

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 on page 110 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 64: CP PM Co-res CS and SS access mechanisms on page 110 provides the supported access mechanisms to the CP PM Co-res CS and SS.

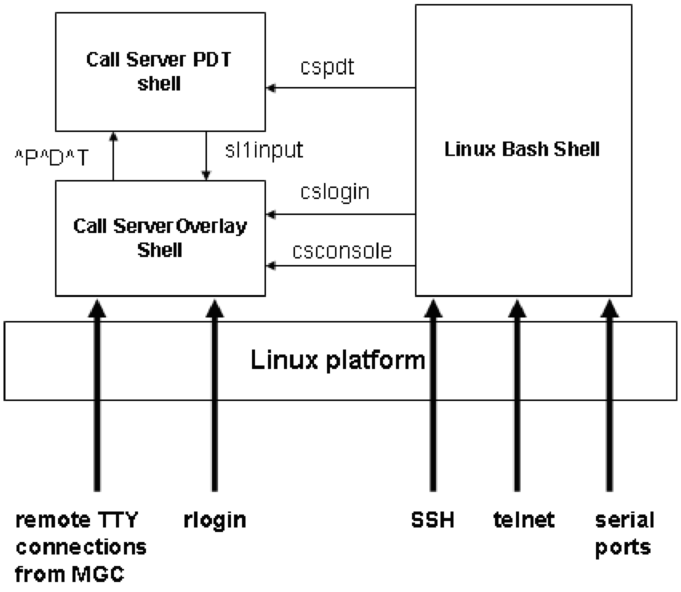


Figure 64: CP PM Co-res CS and SS access mechanisms

Serial ports on Server

After connecting to the serial ports on the Server 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 on page 110.

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 on page 110.

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 the Gateway Controller

The Co-res CS and SS supports remote TTY connections. You can configure serial ports of the Gateway Controller 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 7.0, the serial port is shared with other applications, therefore the output for the Call Server console port is redirected to **/var/log/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.

Connecting the Call Server using cslogin

1. Connect to the Co-res CS and SS remotely (ssh) or locally (serial port).
2. Log on to Co-res CS and SS.
3. Issue the `cslogin`command from Linux Bash Shell;

```
[nortel@ccName_cppm ~]$ cslogin
OVL111 000 IDLE
Logi admin2
PASS
```

Connecting the Call Server using csconsole

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

Connecting the Call Server using cspdt

1. Connect to the Co-res CS and SS remotely (ssh) or locally (serial port)
2. Log on to 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>
```

IP Management for Co-res CS and SS

For 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 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 on page 113 and Table 15: Overlay 137 commands on page 114 lists the Overlay 117 and 137 commands that do not apply to 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)

Command	Description
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 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 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 7.0.

NTP configuration

The Network Time Protocol (NTP) feature is supported on the 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 on page 115 lists the Call Server Overlay 117 NTP commands that are no longer supported for the 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

Command	Description
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 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 on page 116 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 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 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 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 on page 117 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 Co-res CS and SS

The Xmodem protocol is supported on 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 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

Accessing Call Server file system from Call Server PDT shell

1. Connect to the Co-res CS and SS remotely (ssh) or locally (serial port) .
2. Log on to 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>
```

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).

Co-res CS and SS restart

Table 19: Restart Commands on page 118 lists the restart commands supported on the 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 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 CP PM INI button warmstarts the Call Server. All other Linux applications are not affected. The push button event is logged to the 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.

The INI button is not available on all Server hardware. To warmstart a Co-res CS and SS without an INI button, use the CLI command appstart cs restart.

Reset button

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

Reset Reason

Table 20: Co-res CS and SS reset reasons on page 120 lists the reset reasons and the corresponding code stored in the cppmRestart.dat.

Table 20: 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 and later 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 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 Co-res CS and SS.

Upgrading a CS 1000 Release 5.5 or 5.0 GR N-way system to CS 1000 Release 7.0 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
BITL	8	Data Bit Length
STOP	1	Number of Stops
PARY	NONE	Parity Type
FLOW	NO	Flow Control
BCST	<cr>	

Displaying Co-res CS and SS software version

Perform the following procedure to display the Co-res CS and SS software version.

Displaying Co-res CS and SS software version

1. Connect to the Co-res CS and SS remotely (ssh) or locally (serial port).
2. Log on to 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 7.00.19
base           7.00.19
Snmp-Daemon-TrapLib 7.00.19
NTAFS  7.00.19
nortel-Radius    7.00.19
Jboss-Quantum    7.00.19
cnd    7.00.19
lhmonitor      7.00.19
kcv  7.00.19
pcap       7.00.19
cppmUtil       7.00.19
oam-logging       7.00.19
dmWeb       7.00.19
baseWeb      7.00.19
ipsec      7.00.19
tap     7.00.19
ISECSH      7.00.19
ipsec      7.00.19
ipsec      7.00.19
Application configuration: CS+SS+NRS_EM
Packages:
CS+SS+NRS
EM
NRS
CS
LTPS
Configuration version:  7.00.19

cs       7.00
dbcom    7.00.19
cslogin    7.00.19
sigServerShare   7.00.19
csv 7.00.19
tps   7.00.19
vtrk   7.00.19
pd     7.00.19
sps 7.00.19
ncs     7.00.19
gk      7.00.19
nrsm    7.00.19
nrsmWebService   7.00.19
emWeb_6-0        7.00.19
csmWeb           7.00.19
bcc_6-0          7.00.19
csoneksvrmgr     7.00.19
ftrpkg           7.00.19
cs1000WebService_6-0  7.00.19
```

Displaying Call Server Software Version using Overlay 22 iss command

Perform the following procedure to display the Call Server software version from Overlay 22.

Displaying Call Server software version using Overlay 22 iss command

1. Connect to the Co-res CS and SS remotely (ssh) or locally (serial port).
2. Log on to 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` and `iss` commands

```
[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
```

Displaying the Call Server software version from PDT

Perform the following procedure to display the Call Server software version from the PDT.

Displaying the Call Server Software version from PDT

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

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 Co-res CS and SS.

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

For CP MG, CP DC and COTS2, only USB 2.0 removable storage devices are supported.

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

Backing up Call Server data to RMD

1. Connect to the Co-res CS and SS remotely (ssh) or locally (serial port).
2. Log on to 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/ccbr.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/backup/single"
Database backup Complete!
TEMU207 Backup process to local Removable Media Device ended successfully.
.
EDD000
```

Backing up Call Server data to USB

Note:

The N0220961 USB memory stick is supported for Communication Server 1000 Release 7.0. Not all USB memory sticks are supported.

Backing up Call Server data to USB

1. Connect to the Co-res CS and SS remotely (ssh) or locally (serial port).
2. Log on to 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/ccbr.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/backup/single"
Database backup Complete!
TEMU207 Backup process to local Removable Media Device ended successfully.
.
EDD000
```

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

Restoring Call Server data from RMD

1. Connect to the Co-res CS and SS remotely (ssh) or locally (serial port).
2. Log on to 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/cf2/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
```

Restoring Call Server data from USB

Note:

The N0220961 USB memory stick is supported for Communication Server 1000 Release 7.0. Not all USB memory sticks are supported.

Restoring Call Server data from USB

1. Connect to the Co-res CS and SS remotely (ssh) or locally (serial port).
2. Log on to 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/usb/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
```

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, 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 Co-res CS and SS supports the existing Centralized Media Gateway software upgrade feature for upgrading the loadware on the Gateway Controller. The option to select the sequential or simultaneous upgrade method is no longer available during the Co-res CS and SS installation. The default setting for Centralized Software Upgrade is enabled and sequential upon completion of the 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:

If you add additional Media Gateways to the system after you enable the Centralized Software Upgrade feature, the Co-res CS and SS automatically downloads the current Gateway Controller loadware to the newly added Media Gateways.

Note:

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 Co-res CS and SS installation or upgrade.

Server card location (loop and shelf) configuration

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

On the Co-res CS and SS, the Server card location configuration can only be performed using the Overlay 117 CHG LCL commands. Unlike a VxWorks-based Call Server, the 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 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 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 on page 130lists 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). 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.

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 on page 131 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 (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

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

Table 24: Overlay 117 Shell and Transfer commands on page 133 lists the shell and transfer commands supported for 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 Co-res CS and SS but it will enable secure shells on all the Gateway Controllers and Voice Gateway Media Cards that are registered to the 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 Co-res CS and SS but it will disable secure shells all the Gateway Controllers and Voice Gateway Media Cards that are registered to the Co-res CS and SS Call Server.
STAT SHELLS SECURE	Shows whether secure shell access is enabled or disabled on all the Gateway Controllers and Voice Gateway Media Cards that are registered to the 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 Co-res CS and SS but it will enable secure transfers on all the Gateway Controllers and Voice Gateway Media Cards that are registered to the 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 Co-res CS and SS but it will disable secure transfers all the Gateway Controllers and Voice Gateway Media Cards that are registered to the Co-res CS and SS Call Server.
STAT TRANSFERS SECURE	Shows whether secure transfer is enabled or disabled on all the Gateway Controllers and Voice Gateway Media Cards that are registered to the 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

Command	Description
	insecure shell settings on the Co-res CS and SS but it will enable insecure shells on all the Gateway Controllers and Voice Gateway Media Cards that are registered to the 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 Co-res CS and SS but it will disable insecure shells all the Gateway Controllers and Voice Gateway Media Cards that are registered to the Co-res CS and SS Call Server.
STAT SHELLS INSECURE	Shows whether insecure shell access is enabled or disabled on all the Gateway Controllers and Voice Gateway Media Cards that are registered to the 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 Co-res CS and SS but it will enable insecure transfers on all the Gateway Controllers and Voice Gateway Media Cards that are registered to the 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 Co-res Server but it will disable insecure transfers all the Gateway Controllers and Voice Gateway Media Cards that are registered to the Co-res CS and SS Call Server.
STAT TRANSFERS INSECURE	Shows whether insecure transfer is enabled or disabled on all the Gateway Controllers and Voice Gateway Media Cards that are registered to the Co-res CS and SS Call Server.

SSH Commands

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 on page 135 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		Activate the ssh key for the specified cabinet or all or the cabinets
SSH KEY ACTIVATE CABINET		
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		Activate the ssh key for the active core
SSH KEY ACTIVATE ACTIVE		
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

Command		Description
SSH KEY SHOW INACTIVE		Display the ssh key finger prints for the inactive core

Accessing RMD and USB from Call Server PDT shell

1. Connect to the Co-res CS and SS remotely (ssh) or locally (serial port).
2. Log in to Co-res CS and SS 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
```

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*.

Chapter 12: Maintenance

Power up and power down procedures

The existing Call Server power up and power down procedure is supported for 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 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.

Viewing the Call Server report log using rpt

1. Connect to the Co-res CS and SS remotely (ssh) or locally (serial port).
2. Log on to 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 Newest File Name "/var/
opt/nortel/cs/fs/e/rpt/LOG00000.RPT"
File being viewed    : "/var/opt/nortel/cs/fs/e/rpt/LOG00000.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
```

Call Server csconsole log

On startup the Call Server application is run as a background process on the 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.

Chapter 13: System messages

Co-res CS and SS system messages

The following lists system messages for 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:**

Chapter 14: 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 systems, Nortel provides technical assistance in resolving system problems. Table 26: Customer Technical Services (CTS) on page 141 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
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

Location	Contact
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 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 on page 142 and Table 28: Technical services non-emergency classifications on page 143 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.

Class	Degree of failure	Symptoms
		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.
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 on page 144 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) ________________________________

Seriousness of request (see Table 27: Technical service emergency classifications on page 142 and Table 28: Technical services non-emergency classifications on page 143) ________________________________

Description of assistance required ________________________________

____

____