Nortel Communication Server 1000

Linux Platform Base and Applications Installation and Commissioning

Release: 6.0
Document Revision: 03.13

www.nortel.com

NN43001-315

Nortel Communication Server 1000
Release: 6.0
Publication: NN43001-315
Document release date: 23 March 2010

Contents

New in this Release

The following sections detail what's new in *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315) for Release 6.0.

Features

See the following sections for information about feature changes.

CP PM Co-resident Call Server and Signaling Server

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

Commercial off-the-shelf hardware platform types

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

- Dell R300
- IBM x3350

Linux security hardening

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

Patching Manager

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

Note: Patching Manager does not patch VxWorks components, including VxELL.

Base Manager

The Base Manager provides access to a subset of Linux base CLI configuration commands at the UCM GUI. Click on an Element to access the base manager interface. For more information about Base Manager, see "Base Manager" (page 149).

Deployment Manager

The Deployment Manager is introduced in CS1000 Release 6.0 UCM Common Services. Use Deployment Manager to deploy software applications from a central location. Every Linux server that is installed on the network is learned by UCM Common Services where the Deployment Manager is running. The Deployment Manager picks up these servers and initiates a remote software deployment from within UCM Common Services. The Service Cluster management interface adds servers to a cluster from the list of servers that UCM has learned. Before you add the servers to a Cluster, the Deployment Manager feature deploys the necessary software application to each Linux server. Centralized software deployment is the Nortel recommended solution for deployment but local deployment remains an option. Deployment Manager provides the following benefits:

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

For more information about Deployment Manager, see "Application installation using Deployment Manager" (page 99).

Other changes

See the following sections for information about changes that are not feature-related.

Revision history

March 22, 2010	Standard 03.13. This document is up-issued to update password policy information in the section "User accounts and access control" (page 29)
March 03, 2010	Standard 03.12. This document is up-issued to update the section User accounts and access control.
February 15, 2010	Standard 03.11. This document is up-issued to update the section Install Nortel Linux base on a CP PM or COTS server.
February 09, 2010	Standard 03.10. This document is up-issued to update the section Install Nortel Linux base on a CP PM or COTS server.
December 02, 2009	Standard 03.09. This document is up-issued to add a warning in procedure 15, in the section Nortel Linux base installation.
July 09, 2009	Standard 03.08. This document is up-issued to include revised information for "Disaster recovery" (page 83).
July 02, 2009	Standard 03.07. This document is up-issued to support Communications Server 1000 Release 6.0.
June 23, 2009	Standard 03.06. This document is up-issued to support Communications Server 1000 Release 6.0.
June 18, 2009	Standard 03.05. This document is up-issued to support Communications Server 1000 Release 6.0.
May 29, 2009	Standard 03.04. This document is up-issued to support Communications Server 1000 Release 6.0.
May 15, 2009	Standard 03.03. This document is up-issued to support Communications Server 1000 Release 6.0.
May 11, 2009	Standard 03.02. This document is up-issued to support Communications Server 1000 Release 6.0.
April 20, 2009	Standard 03.01. This document is up-issued to support Communications Server 1000 Release 6.0.

May 01, 2008	Standard 02.08. This document is up-issued to update information in the Upgrading Nortel Linux base procedures.
April 18, 2008	Standard 02.07. This document is up-issued to add information to the procedure Installing the Primary Security Service and Network Routing Service and added UCM Upgrade Procedures 5.00 GA to 5.50.12 to Task Flow chapter.
April 15, 2008	Standard 02.06. This document is up-issued to add lab trial information.
February 22, 2008	Standard 02.05. This document is up-issued to include references to host configuration scripts found in *Unified Communications Management Fundamentals* (NN43001-116).
February 4, 2008	Standard 02.04. This document is up-issued to support changes in technical content, including the addition of task flow diagrams for the installation and upgrade of the Linux base and applications.
January 15, 2008	Standard 02.03. This document is up-issued for changes in technical content. New screen captures have been included and an installation and upgrade task flow section has been added.
December 19, 2007	Standard 02.02. This document is up-issued for changes in technical content.
December 7, 2007	Standard 02.01. This document is up-issued to support Nortel Communication Server 1000 Release 5.5. This document contains new information on CLI commands, an upgrade procedure, firewall ports, and alarms. Screen captures for the Linux base installation procedure are updated.
November 27, 2007	Standard 01.04. This document is up-issued for changes in technical content.
September 10, 2007	Standard 01.03. This document is up-issued to address changes in technical content for Release 5.0.

June 20, 2007	Standard 01.02. This document is up-issued to remove the Nortel Networks Confidential statement.
May 30, 2007	Standard 01.01. This document is issued to support Nortel Communication Server 1000 Release 5.0.

How to get help

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

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site: www.nortel.com/support

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

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

Getting help over the telephone from a Nortel Solutions Center

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

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

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

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

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

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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

Introduction

Linux Platform Base and Applications Installation and Commissioning (NN43001-315) describes the features of Nortel Linux base and details about the installation and configuration of Nortel Linux base on commercial off-the-shelf (COTS) servers. This document also provides installation instructions for Nortel Linux applications.

Linux base applications installation and commissioning task flow

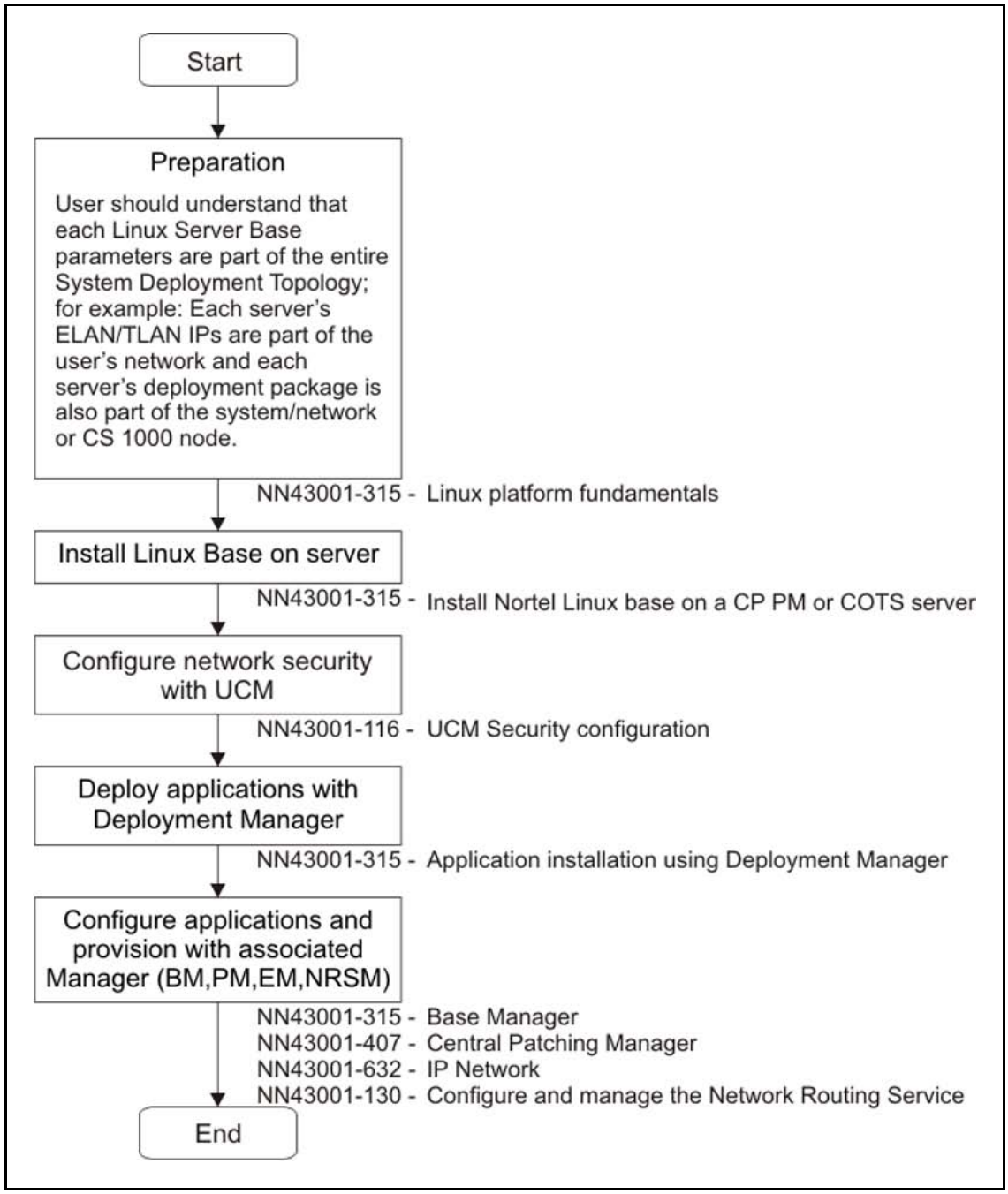
Figure 1 "Linux base applications installation and commissioning task flow" (page 16)provides a high-level task flow for the installation and commissioning of Linux base and applications on a COTS or CP PM server. The task flow depicts the recommended sequence of events and provides a reference to the relevant NTP for each event. Each NTP reference also includes a reference to the section of the NTP that contains the information you need to perform the task.

Each box in the task flow represents a stage in the Linux base installation and commissioning process. The stages are as follows:

- Preparation
- Linux base and base applications installation
- Unified Communications Management (UCM) security configuration
- Application deployment using Deployment Manager (DM)
- Configuration and provisioning using Base Manager (BM), Patching Manager (PM), Element Manager (EM), and Network Routing Service Manager (NRSM)

As this NTP progresses to each of the stages, the task flow is presented again and the current stage is highlighted to indicate to overall progress and to identify the NTP(s) you need to complete the tasks.

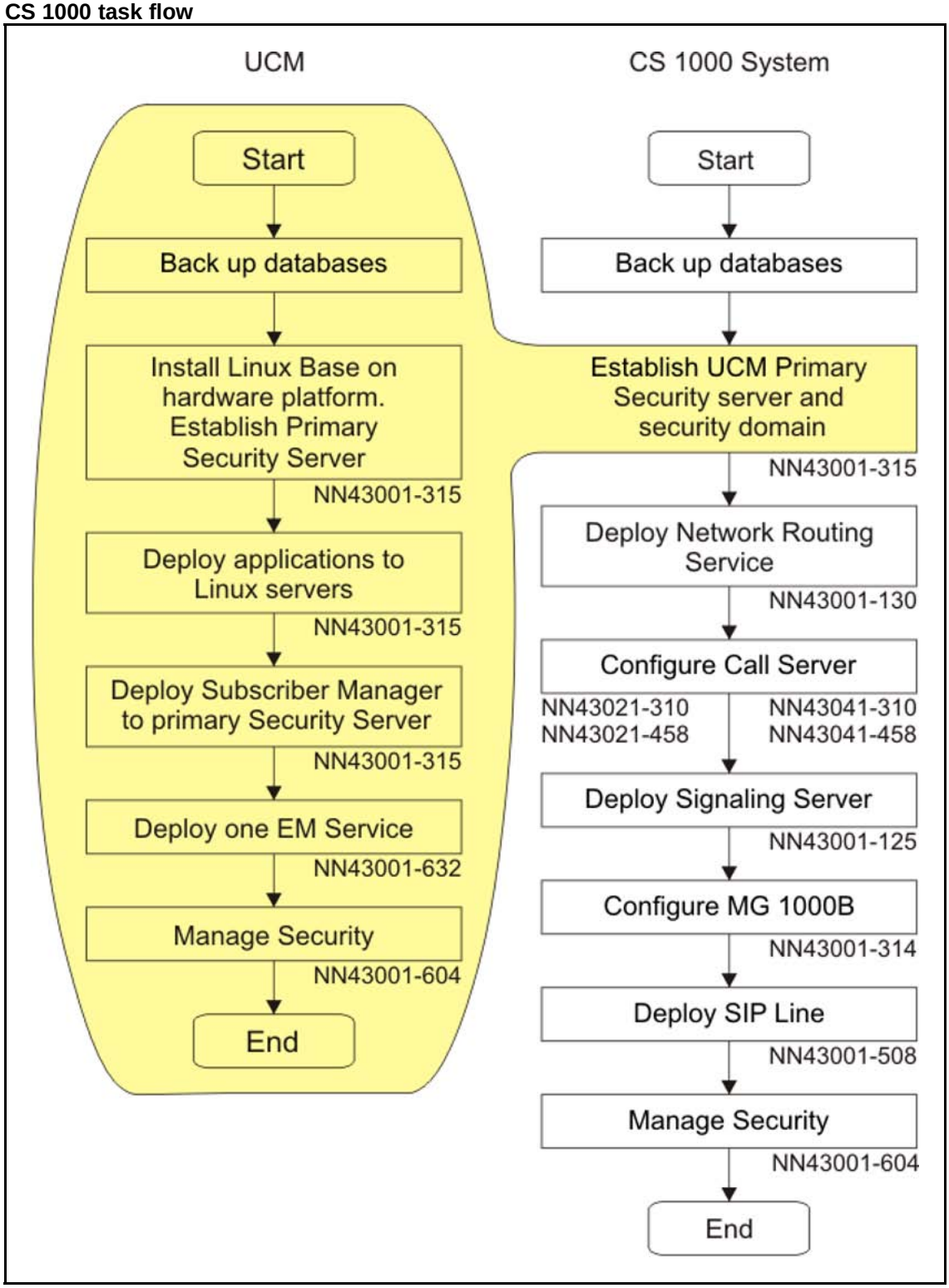
Figure 1
Linux base applications installation and commissioning task flow



CS 1000 task flow

Figure 2 "CS 1000 task flow" (page 18) provides a high-level task flow for the installation or upgrade of a CS 1000 system. The task flow indicates the recommended sequence of events to follow when configuring a system and provides the NTP number that contains the detailed procedures required for the task.

Figure 2
CS 1000 task flow



For more information refer to the following NTPs, which are referenced in the task flow diagram:

- *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315)
- *Element Manager System Reference - Administration* (NN43001-632)
- *Security Management Fundamentals* (NN43001-604)

Note: For the purposes of this diagram, Linux patching is considered to be part of the Configure Call Server box in the CS 1000 task flow. For more information about Linux patching, see *Patching Fundamentals* (NN43001-407)

Subject

Linux Platform Base and Applications Installation and Commissioning describes the installation and configuration of Nortel Linux base on COTS and CP PM servers, and the deployment of Nortel applications.

This document describes the upgrade and configuration of Nortel Linux base on the Dell R300, HP DL320 G4, IBM x306m, and IBM x3350 COTS servers, and the Nortel CP PM server.

To view licensing information, see " Passthrough end user license agreement" (page 191).

Linux base overview

The Communication Server 1000 (CS 1000) Linux base system provides a Linux server platform for applications on a commercial off-the-shelf (COTS) Pentium server. The platform supports Session Initiation Protocol Network Redirect Server (SIP NRS), Unified Communications Management (UCM), traditional Signaling Server applications, SIP Line Gateway Applications, and the co-resident deployment of the Call Server and Signaling Server applications.

Note: Co-resident deployment of the Call Server and Signaling Server applications is available only on the Nortel CP PM server.

Nortel Linux base is supported on the Dell R300, HP DL320 G4, IBM x306m, and IBM x3350 COTS servers, and the Nortel CP PM server.

Key features

Linux base provides features and enhancements in the following areas:

- Linux operating system and distribution
- Firewall

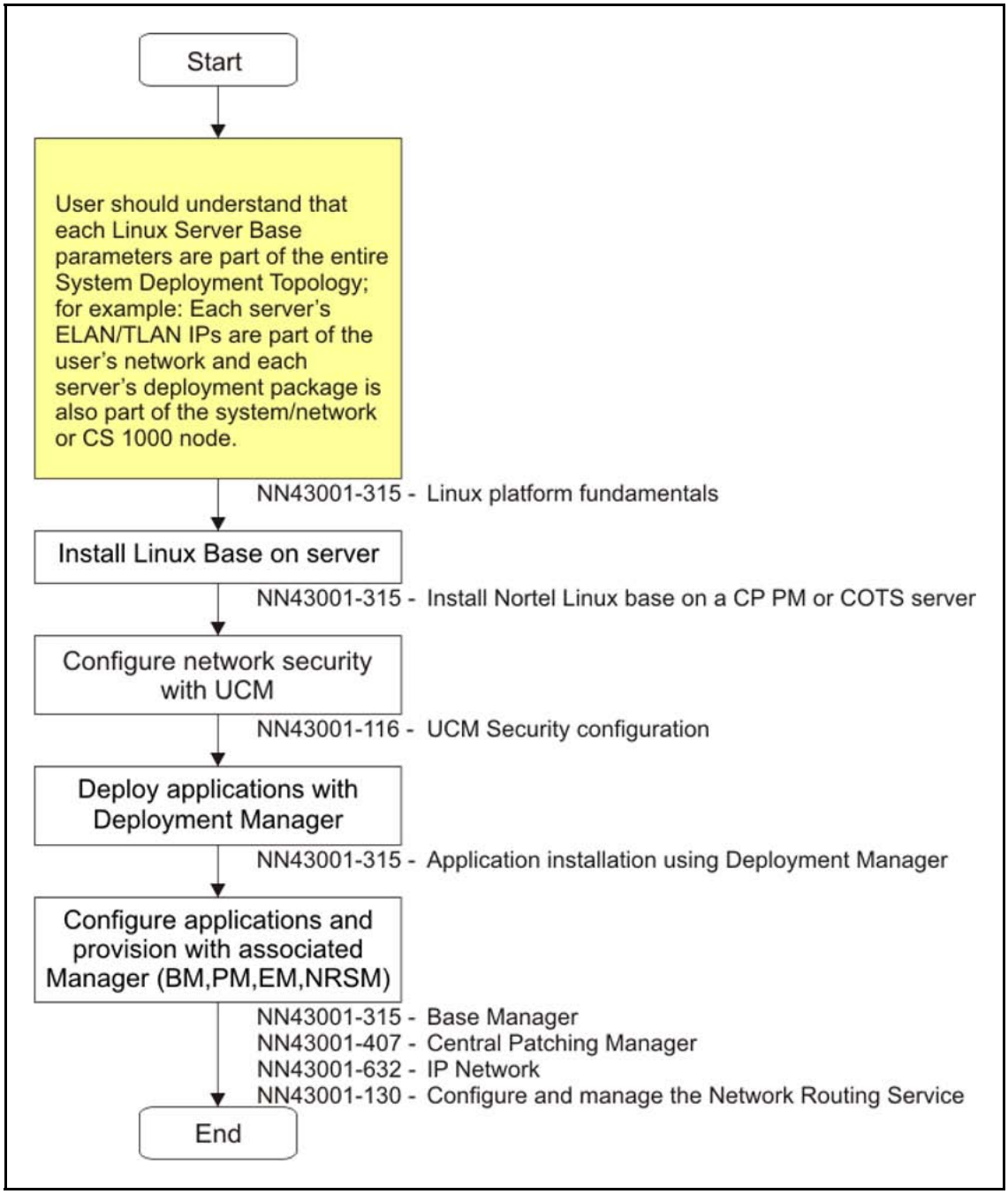
- Software reliability
- Linux security hardening
- Patching
- User accounts and access control
- Software installation and delivery
- System upgrades
- Debugging
- Logging
- Disaster recovery
- Network Time Protocol (NTP)

Linux platform fundamentals

Preparation workflow stage

Prepare to install and configure Linux base and applications by becoming familiar with the information and concepts in “Linux platform fundamentals” (page 21) This chapter contains information in the following areas:

Figure 3
Linux base applications installation and commissioning task flow (Preparation stage)



provides basic information and concepts necessary to successfully install and configure the Linux base and applications.

Linux Operating System and Distribution

The selected distribution is Red Hat Linux 5. This distribution is built on a 2.6.18 kernel, and supports many Open Source Development Lab (OSDL) Carrier Grade Linux (CGL) features.

Red Hat Linux 5 (update 1) supports Linux kernel version 2.6.18 and the following applications:

- Unified Communications Management (UCM)
- Nortel Simple Network Management Protocol (SNMP)
- Deployment Manager (DM)
- Signaling Server (SS)
- Network Routing Service (NRS)
- Call Server (CS)
- Session Initiation Protocol Line (SIPL)
- Element Manager (EM)
- Subscriber Manager (SubM)

Co-resident Call Server and Signaling Server

The Nortel Communication Server 1000 (CS 1000) Linux base Co-resident (CoRes) Server can run the Call Server software, the Signaling Server software, and the System Management software on the same hardware platform. The CoRes server runs on the Common Processor Pentium Mobile (CP PM) hardware platform; it is not available on the commercial off -the-shelf (COTS) platforms.

The Signaling Server software on the CoRes server refers to a suite of CS 1000 software applications which includes:

- Line Telephony Proxy Server (LTPS)
- Virtual Trunk (VTRK) includes H.323 Gateway or SIP Gateway
- NRS includes SIP Proxy Server (SPS), SIP Redirect Server (SRS), H323 Gatekeeper (GK) , Network Connect Server (NCS), NRS Manager (NRS-M)
- Personal Directory (PD) includes RL, CL, and Unicode Name Directory
- UCM Common Services
  - Security Server
  - Element Manager (EM), including Cluster Manager/IP Telephony node
  - Deployment Manager

— Base Manager

— Patching Manager

— Subscriber Manager

You need not deploy all the preceding software applications on the CoRes server. For example, you can install and configure a CoRes Server to run only the Call Server, LTPS, VTRK, UCM Security Server, and EM software. However, the CoRes server must have the Call Server and at least one Signaling Server application installed. A stand alone Call Server is not supported on the CP PM based CoRes system.

Note: A CP PM or COTS server running Signaling Server and/or UCM applications in the absence of a Call Server is not referred to as a CoRes server.

Upgrade paths

The following upgrade paths are supported for CP PM Co-res CS and SS:

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

  Note: If upgrading from a non-CP PM-based CS 1000E Call Server both software and hardware upgrade are required.

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

  Note: If upgrading from non-CP PM-based CS 1000E Signaling Server, both software and hardware upgrade are required.

- CS 1000 Release 5.5 or earlier Option 11C Call Server to CS 1000 Release 6.0 CP PM Co-res CS and SS
- CS 1000 Release 4.5 or earlier CS 1000M Call Server (cabinet/chassis) to CS 1000 Release 6.0 CP PM Co-res CS and SS
- CS 1000 Release 4.5 or earlier CS 1000S Call Server to CS 1000 Release 6.0 CP PM Co-res CS and SS

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

For more information about the Nortel CS 1000 CoRes server, see *CP PM Co-resident Call Server and Signaling Server Fundamentals* (NN43001-509).

Server security configuration

A Linux base server can be assigned one of three security roles: Primary, Backup, or Member.

A network requires one primary security server. The backup security service is optional. One backup security server and one or more member servers can exist for each UCM security domain.

The primary security server must be configured; it provides basic security features such as user administration including password changes, the ability to configure different authorization levels, and the enforcement of security policies.

The backup security server is an optional server that you can configure to perform authentication and authorization when the primary security server is unavailable.

For a more details about UCM configuration of primary, backup, and member servers, see *Unified Communications Management* (NN43001-116). For more information about security management, see *Security Management Fundamentals* (NN43001-604).

Network and firewall

All applications operate behind a network firewall. The firewall starts on system boot, which invokes the Linux iptables facility to load the firewall configuration.

Each Linux server supports at least two Ethernet ports; one for ELAN subnet connectivity and another for TLAN subnet connectivity. By default, the TLAN is open to the network, while the ELAN is reachable only within the subnet. The Linux application selects the Ethernet port to use. The firewall protects both ports. For a list of Linux base open firewall ports see Table 1 "Linux base open firewall ports" (page 26). For a definition of ELAN and TLAN see “Network configuration” (page 273).

Use the command line interface (CLI) command **`basefirewallconfig`** to configure the network firewall. For a list of Nortel Linux base CLI commands see “ Nortel Linux base CLI commands” (page 265).

Table 1
Linux base open firewall ports

Protocol	Port number or range
TCP	22
UDP	22
UDP	53 (to configured DNS servers only)
UDP	123
UDP	500
UDP	514
TCP	2100
UDP	33434—33524

Note: The port numbers in Table 1 "Linux base open firewall ports" (page 26) apply only to the Linux base. Linux applications can require different ports. For a list of ports opened for the application, see the appropriate application document.

Software reliability

Software monitoring

MONIT is an open source package used to monitor the important daemon services automatically initiated at startup. If a malfunction occurs, MONIT provides actions such as alert, start, stop, and restart.

The following system parameters are monitored: memory, CPU, and device space usage. If a parameter exceeds a warning threshold a message appears and an SNMP trap is generated. Table 2 "Warning and Critical thresholds" (page 26) shows the warning and critical thresholds.

Table 2
Warning and Critical thresholds

System Resource	Warning Clear	Warning Set	Critical Clear	Critical Set
Memory usage	—	—	90%	95%
CPU usage	—	—	90%	95%
/boot (/dev/sda1) Size: 100 MB. Critical.	70%	75%	80%	85%
admin (/dev/sda2) Size: 4 GB.	80%	85%	85%	90%

System Resource	Warning Clear	Warning Set	Critical Clear	Critical Set
/ (/dev/sda6) Size: 4 GB.	80%	85%	85%	90%
/opt (/dev/sda7) Size: 8 GB. Not critical.	80%	85%	90%	95%
/home (/dev/sda8) Size: 4 GB. Not critical.	80%	85%	90%	95%
/tmp (/dev/sda9) Size: 20 GB. Critical.	80%	85%	85%	90%
/var (/dev/sda10) Size: 30 GB. Critical.	80%	85%	85%	90%

Figure 4 "Critical Set alarm example" (page 27)shows an example of a Critical Set alarm. Figure 5 "Critical Clear alarm example" (page 27)shows an example of a Critical Clear alarm message.

Note: If critical alarms persist, contact your Nortel technical support.

Figure 4
Critical Set alarm example

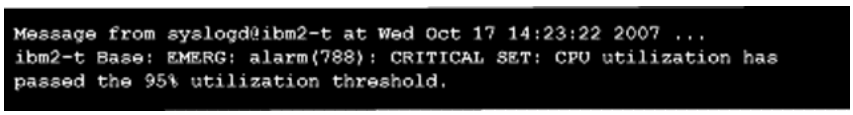
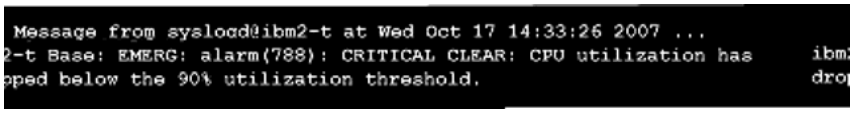


Figure 5
Critical Clear alarm example



Hardware watchdog

The COTS and CP PM servers offer a hardware watchdog. The watchdog timer is programmed during the server startup and requires continuous resets from a daemon running in Linux. The watchdog timer duration is 5 minutes.

> ***Note:*** The CP PM server can retrieve the reason for the last restart of the server, including hardware watchdog time outs. For more information about the hardware watchdog on the Linux base CP PM server, see *CP PM Co-resident Call Server and Signaling Server Fundamentals* (NN43001-509).

The server restarts if the watchdog timer is not reset within the allotted time. The operating system and applications are reloaded from disk and started after the server reset occurs. The following conditions can trigger the watchdog:

- The software daemon, which notifies hardware watchdog, fails to respond.
- A hardware or software problem causes the system to freeze.

Linux security hardening

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

Basic hardening

Basic Linux security hardening includes all hardening items that do not affect the performance of Nortel applications. Basic hardening items are on by default and they are not configurable.

Enhanced hardening

Enhanced hardening items include all hardening items that can affect the performance of Nortel applications, or hardening items that require configuration. Enhanced hardening items that do not affect Nortel applications performance are on by default, enhanced hardening items that affect performance are turned off by default.

For details about Nortel Linux security hardening, see *Security Management Fundamentals* (NN43001-604).

Patching

Nortel Linux base uses Patching Manager to perform patching tasks. You can use Patching Manager on the primary security server to remotely deploy patches from a central location to other Linux servers in the same security domain using the Central Patching Manager. You can also install patches locally. You can access Local patching from the Base Manager of each element, using the Local Patching Manager.

For more information about Nortel Linux patching, see *Patching Fundamentals* (NN43001-407).

Centralized authentication

UCM provides a centralized, GUI-based interface for individual account administration for the CS 1000 network. When a user logs on to a Linux server CLI they receive a prompt for user name and password. First, the user name and password are authenticated locally. If authentication fails, the user name and password is encrypted and sent to the centralized UCM security server via the RADIUS protocol for verification. UCM acts as a RADIUS server to provide authentication for RADIUS clients. If the user is defined in the UCM database then access is granted to the proper Linux shell with the roles defined in the UCM database. For more information about UCM role creation, see *Unified Communications Management* (NN43001-116).

User accounts and access control

User accounts and access control methods are managed by native Linux user account management (root and nortel) and tools such as RADIUS and PAM for the UCM managed accounts.

Linux base includes the following accounts:

- root (as Linux default)

  Note 1: Nortel does not recommend logging on using the root account unless you are explicitly directed to do so. All base maintenance and debug actions must be performed using the nortel account.

  Note 2: You can log on directly as root through the COM1 console, or through a keyboard and video monitor (KVM).

WARNING
Do not change your KVM terminal. If you switch the KVM terminal, logon can fail if you log on directly as root.

WARNING
If you log on to the COM1 port, make sure you turn off **Caps Lock** before you log on.

- nortel: The user account for the basic Linux base operations as well as for base manager. For a list of CLI commands that can be invoked by nortel, see " Nortel Linux base CLI commands" (page 265).
- System UCM accounts: These accounts are governed by UCM policies; for information about UCM password policies, see *Unified Communications Management Common Services Fundamentals* (NN4300-116).

Note 1: If you log on and your account remains inactive for 15 minutes, you are automatically logged out.

Note 2: System Linux base accounts that make three successive incorrect logon attempts are locked for up to 1 hour.
System UCM accounts making successive incorrect logons will be locked based on the policy settings defined in UCM.

Passwords

The following regulations govern the use of passwords:

Password Policy

- root account: The password for the ROOT account will expire after three months but the Root account will not expire.

  Note: A warning that the password will expire is given by the system during the last seven days prior it expiring when logging into the server. After the password for the account has expired, the password must be changed then next time the account is used to log into the server.

- nortel account: The password for the NORTEL account never expires, but Nortel recommends that you change the password regularly, based on a schedule that meets your security requirements.
- System UCM accounts: System UCM accounts making successive incorrect logons will be locked based on the policy settings defined in UCM. For information about UCM password policies, see *Unified Communications Management Common Services Fundamentals* (NN4300-116).

A new password must differ from the previous three passwords. This applies to root, nortel, and system UCM accounts.

Password creation guidelines

Passwords must meet the following criteria:

- Passwords must contain both uppercase letters, lowercase letters, numeric characters, and special characters.
- In addition to letters, passwords must use digits (0 to 9) and special characters (@#$%^&*()_+|~-=\‘{}[]:";’&;<>?,./).
- The password must contain at least eight alphanumeric characters.
- The password cannot be a word in the English language as defined in the Linux Pluggable Authentication Module (PAM) module.
- Passwords cannot use discernible character patterns such as abcdef or 123123.
- Passwords cannot use the backward spelling of a word.
- Passwords cannot be an English language word (as defined in the Linux PAM module) preceded or followed by a digit. For example, 1secret or secret1.
- You can change your password by using the **`passwd`** CLI command.

Changing Nortel Linux base passwords

You can change Nortel Linux base passwords for the root or nortel accounts if they are forgotten or lost. Use the following procedure to change the Nortel Linux base passwords for the root or nortel accounts.

Prerequisites

- Ensure you have physical access to the system.
- Ensure you have access to the serial COM port of the Linux server.
- Ensure you have the Linux base installation media (DVD for COTS servers, compact flash for CP PM servers).

Changing the Nortel Linux base root or nortel password

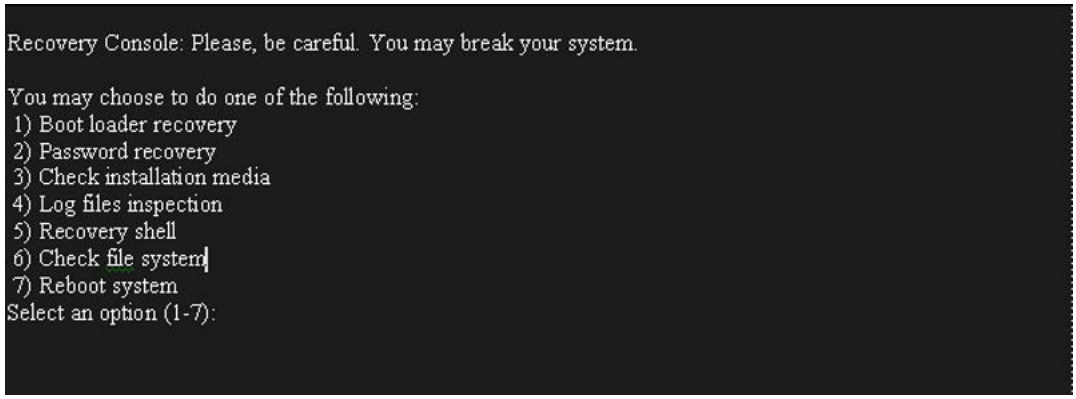
Step	Action
1	Insert the Linux base installation media.
2	Restart the system.
3	If you connect to the server through the COM1 console, type **recovery-com1** in the CS 1000 Linux base system installer screen and press **Enter**. **OR**

If you connect to the server using a keyboard and video monitor (kvm) type **recovery-kvm** in the CS 1000 Linux base system installer screen and press **Enter**.

Note: If you connect to the IBM x3350 server with a terminal for setup, the server does not function with the serial cable that was previously shipped with the ISP 1100 or other COTS platforms. The IBM x3350 server requires the new NTRX26NPE6 9 pin female to 9 pin female null modem cable. The NTRX26NPE6 9 pin female to 9 pin female null modem cable is displayed in Figure 219 "NTRX26NPE6 9 pin female to 9 pin female null modem cable" (page 250).

The Recovery Console menu appears, as shown in Figure 6 "Recovery Console window" (page 32).

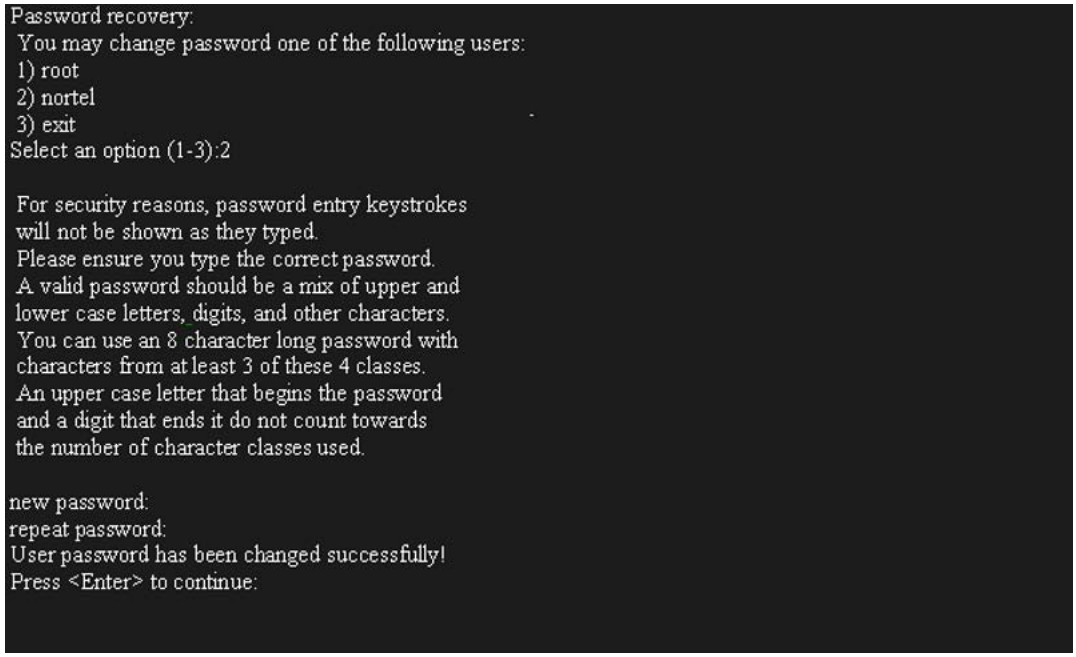
Figure 6
Recovery Console window



4 Select option 2 for password recovery and press **Enter**.

The Password recovery screen appears, as shown in Figure 7 "Password recovery window" (page 33).

Figure 7
Password recovery window



5 Type the option number for the password that you want to change, and press **Enter**.

6 Enter the new password. For password creation guidelines, see "Password creation guidelines" (page 31).

7 Re-enter the new password.

8 Press **Enter**.

--End--

Logging

The CS 1000 logging infrastructure is a collection of log files that are created and archived across multiple elements that make up a CS 1000 solution, including the Linux base. The logs provide various levels of information about specific events that occur during different operational states of the CS 1000 solution. The collected information consolidated in the various logs includes information related to the status of software and hardware, such as user administrative activity, security events, operational messages, and software debug messages.

The collected information has a variety of uses and applies to many aspects of system management. The users of this log information typically include network operations, security administrators, software developers, network engineers and customer support.

For more detailed information on Linux base logs and logs for applications that run on the Linux base, see *System Management Reference* (NN43001-600).

SNMP

Linux base supports standard server type Management Information Base (MIB) II MIBs. For information about the configuration of SNMP on Linux base see *Communication Server 1000 Fault Management — SNMP* (NN43001-719).

Disaster recovery

Hardware faults can occur that require disaster recovery. Recovery occurs in two steps. First, restore the Linux base (including operating system and base applications), and then restore the Nortel applications. For disaster recovery details and procedures, see “Disaster recovery” (page 83).

Install Nortel Linux base on a CP PM or COTS server

Nortel Communication Server 1000 (CS 1000) Linux base introduces a two-stage installation procedure. The operating system and base applications are installed, then the Nortel applications. This section provides the procedure for installing the Linux base.

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

The Linux server supports two network interfaces, TLAN and ELAN. The configuration and utilization of two network interfaces is based on network topology and application deployment.

For a definition of the Embedded Local Area Network (ELAN) and the Telephony Local Area Network (TLAN) see “Network configuration” (page 273).

Nortel Linux base can be pre-loaded on CP PM cards shipped new from the factory. Use “Configuration for a CP PM card pre-loaded with Nortel Linux base” (page 56) to make the necessary configuration changes.

For information about installation times for Nortel Linux base, see “Installation times” (page 259).

WARNING

If you access the Linux server through a Terminal Server connected to the COM port, it is possible that garbled characters (such as uuuuuu) can appear during a system restart (for example, during the installation or upgrade procedure). This appearance can make the system seem to hang.

You can resolve the problem by re-establishing the COM1 connection from the client PC or work station to the Linux server.

Do not manually restart the system during the upgrade or installation. This can result in hard drive corruption, and forces you to reinstall the system.

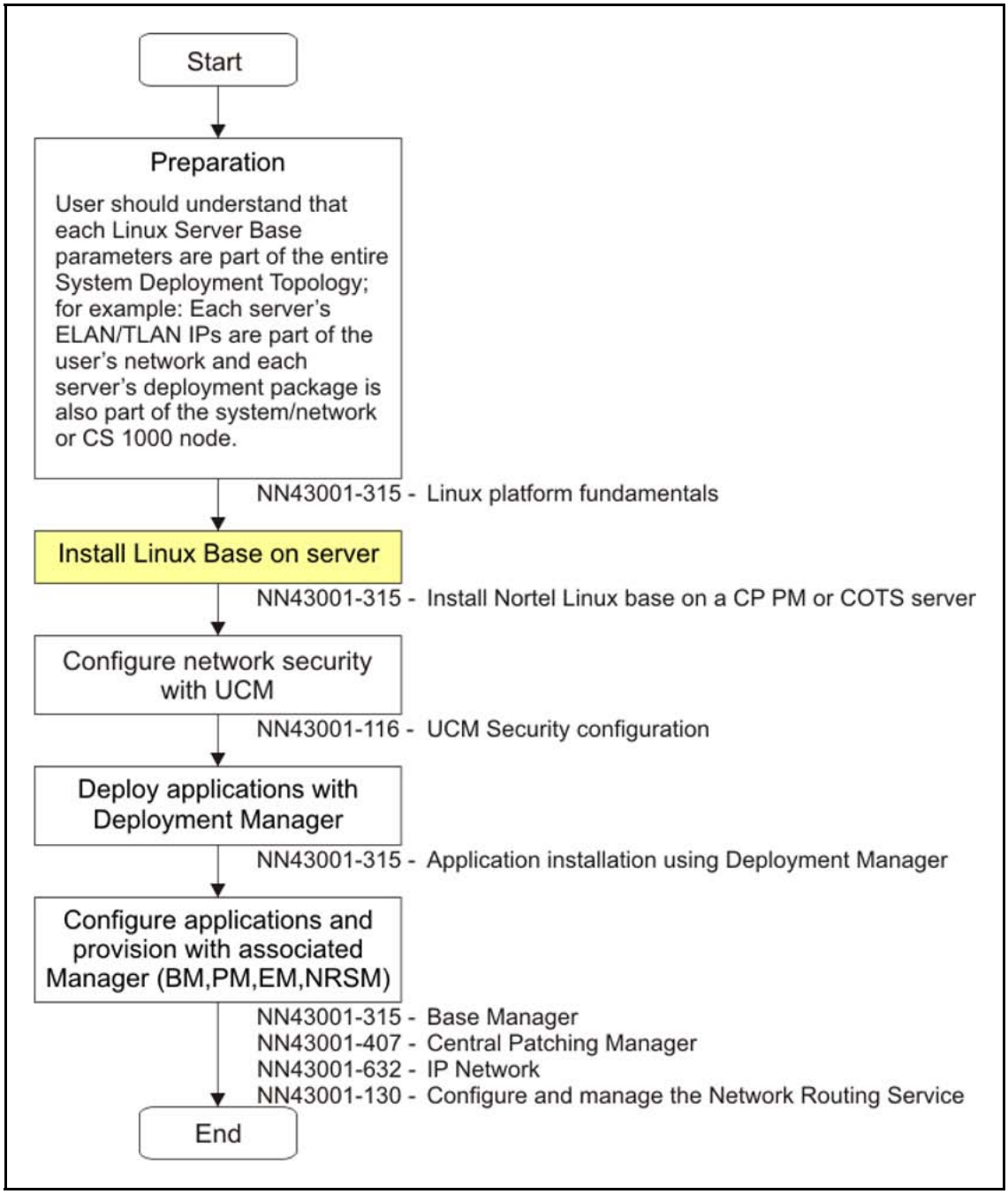
Installation workflow stage

"Install Nortel Linux base on a CP PM or COTS server" (page 35)provides information, prerequisites, and procedures for installing Linux base and base applications on a COTS or CP PM server. Figure 8 "Installation workflow stage" (page 37) shows the position of the installation stage in the overall workflow.

This chapter provides information and procedures in the following areas:

- "Prerequisites" (page 37)
- "Nortel Linux base installation" (page 41)
- "Configuration for a CP PM card pre-loaded with Nortel Linux base" (page 56)

Figure 8
Installation workflow stage



Prerequisites

The server must meet the following requirements:

- The hard drive size must be at least 40 GB.

If you are installing Linux base on a VxWorks CP PM Signaling Server, use the command **diskSizeShow** to check the hard drive size. For information about upgrading the CP PM hard drive, see procedure *Replacing the hard drive on a Nortel CP PM Signaling Server* in *Circuit Card Reference* (NN43001-311).

- There must be at least 2 GB of available memory.

  If you are installing Linux base on a VxWorks CP PM Signaling Server, use the command **memSizeShow** to check the memory size. For information about upgrading the memory capacity of a CP PM Signaling Server, see procedure *Upgrading the CP PM memory*. in *Circuit Card Reference* (NN43001-311)

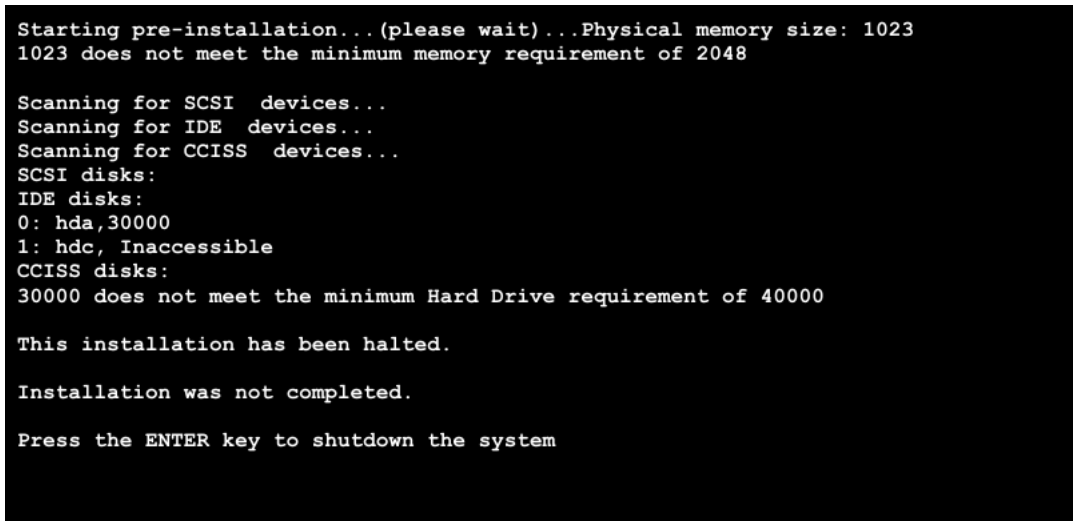
- If you are installing Linux base on a CP PM server, the BIOS must be Release 18 or higher.

  To determine the BIOS release value for a CP PM server, use Procedure 35 “Determining CP PM BIOS Method 1 ” (page 198) or Procedure 36 “Determining CP PM BIOS Method 2” (page 199).

  If you need to upgrade the BIOS for a CP PM server, use Procedure 37 “Upgrading the CP PM BIOS” (page 199).

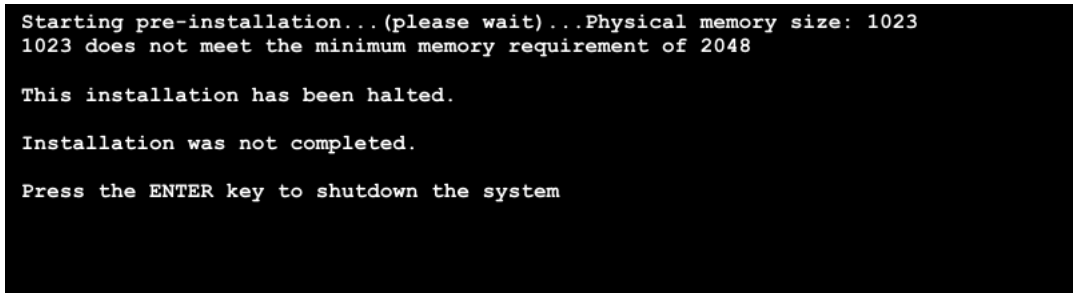
If the hard drive is less than 40 GB, the following screen appears:

Figure 9
Insufficient hard drive capacity



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

Figure 10
Insufficient memory size



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. For more information about hard drive, memory, and BIOS requirements for the COTS and CP PM platforms, see “Hardware platforms” (page 193).

If you are configuring Linux base on a CP PM server for co-resident Call Server and Signaling Server applications, the CP PM BIOS must be Release 18 or higher.

If you are configuring Linux base on a CP PM server, the compact flash card used for installation must have a capacity of at least 2 Gb. For details about creating a compact flash removable media device, see Procedure 38 “Creating a CF RMD for Linux base installation on a CP PM server” (page 203).

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

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

    Note 1: A Fully Qualified Domain Name (FQDN) consists of a host name and a domain name, and includes a top-level domain name. Using kwei.ca.nortel.com as an example, kwei is the host name, ca.nortel.com is the domain name, and .com is the top-level domain name. The FQDN must contain at least three fields separated by dots. The host name cannot contain dots.

    Note 2: If you are using a DNS server to resolve the FQDN to an IP address, ensure that prior to the installation of the Linux server that you can resolve the FQDN to the expected IP

address. For example, attempt to ping the FQDN from a PC that uses the external DNS server, and it should resolve to the expected IP address.

— TLAN IP address

— TLAN gateway IP address

— TLAN netmask

— Timezone

— IP address of the Primary Domain Name Service (DNS) server

— Default system gateway associated with the network interface (ELAN or TLAN)

Note 1: The choice of ELAN or TLAN as the default gateway NIC can be influenced by the applications that you are going to deploy on the server and by network topology. For a definition of ELAN and TLAN see “Network configuration” (page 273).

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

Note 3: The CLI command **`routeconfig`** can be used to add routing entries. The choice of routing entries will depend upon the network topology and application deployment. For a list of Nortel Linux base CLI commands see “ Nortel Linux base CLI commands” (page 265).

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.

Additional equipment

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

- **PC**

  you can use a PC for the following installation tasks:

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

— Configure UCM primary, backup, and member servers.

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

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

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

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

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

  Note 2: If you connect to the IBM x3350 server with a terminal for setup, the server does not function with the serial cable that was previously shipped with the ISP 1100 or other COTS platforms. The IBM x3350 server requires the new NTRX26NPE6 9 pin female to 9 pin female null modem cable. The NTRX26NPE6 9 pin female to 9 pin female null modem cable is displayed in Figure 219 "NTRX26NPE6 9 pin female to 9 pin female null modem cable" (page 250).

Nortel Linux base installation

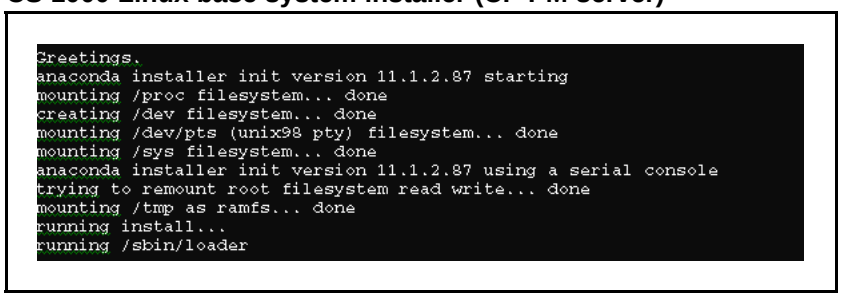
Installing the Linux base on a CP PM or COTS server

ATTENTION
This procedure documents the installation of Nortel Linux base on a CP PM or COTS 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 the chapter “Upgrade Nortel Linux base ” (page 59).

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

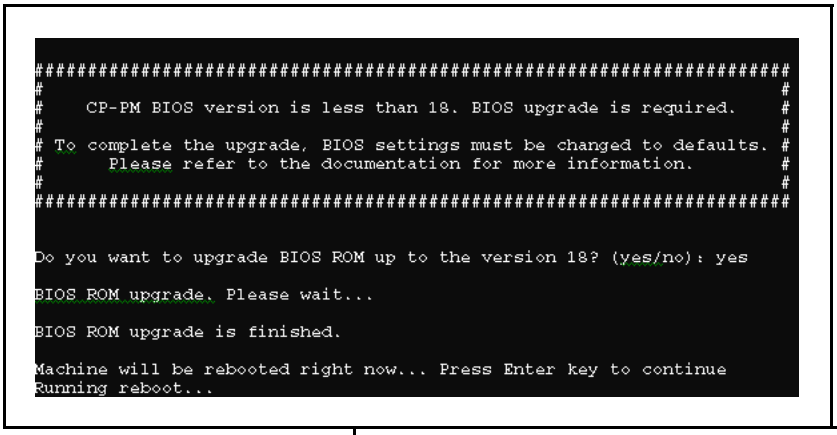
Step	Action
1	Connect to the CP PM server using the serial console, or to a COTS server using the serial console or keyboard and video monitor (kvm). ***Note:*** If you connect to the IBM x3350 server with a terminal for setup, the server does not function with the serial cable that was previously shipped with the ISP 1100 or other COTS platforms. The IBM x3350 server requires the new NTRX26NPE6 9 pin female to 9 pin female null modem cable. The NTRX26NPE6 9 pin female to 9 pin female null modem cable is displayed in Figure 219 "NTRX26NPE6 9 pin female to 9 pin female null modem cable" (page 250).
2	Insert the Linux base installation media. For CP PM servers, insert the compact flash installation media. For COTS servers, insert the DVD installation media. **WARNING** The Linux Base DVD should only be inserted in the DVD drive during the Linux Base installation on a COTS server (this does not apply to CP PM servers). Normally the DVD auto-ejects after the Linux base installation is complete. If the Linux base DVD is accidentally left in the DVD drive after installation and a system restart occurs, the system will boot into the installation program. This can be interpreted as a hung system. If this occurs, eject the DVD and restart the system. ***Note:*** For CP PM servers, reseat the CP PM card to ensure a successful restart.
3	On the CP PM server, press F when the system prompts you. The following text is displayed after pressing F

Figure 11
CS 1000 Linux base system installer (CP PM server)



4	The following output appears. Note this will only be displayed if the card BIOS version is below 18. Type **Yes** at the BIOS upgrade prompt.

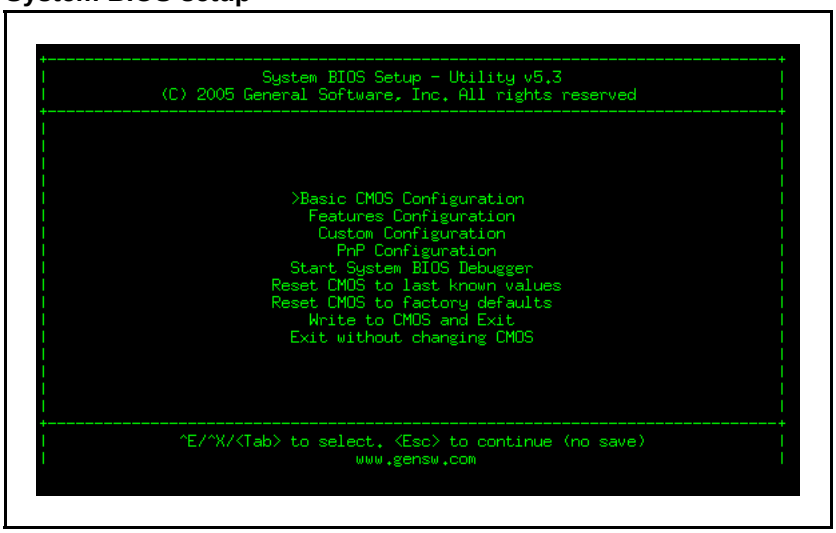
Figure 12
CP PM BIOS upgrade



ATTENTION
Before proceeding, note that a reboot is required once the BIOS upgrade completes. Be prepared to press Ctrl-C when the card starts booting and you see the message **Hit ^C if you want to run SETUP**.

5 After the BIOS upgrade completes, press Ctrl-C during reboot and the following appears.

Figure 13
System BIOS setup



6 Choose **Reset CMOS to factory defaults** and hit **Enter**.

7 Restart the server.

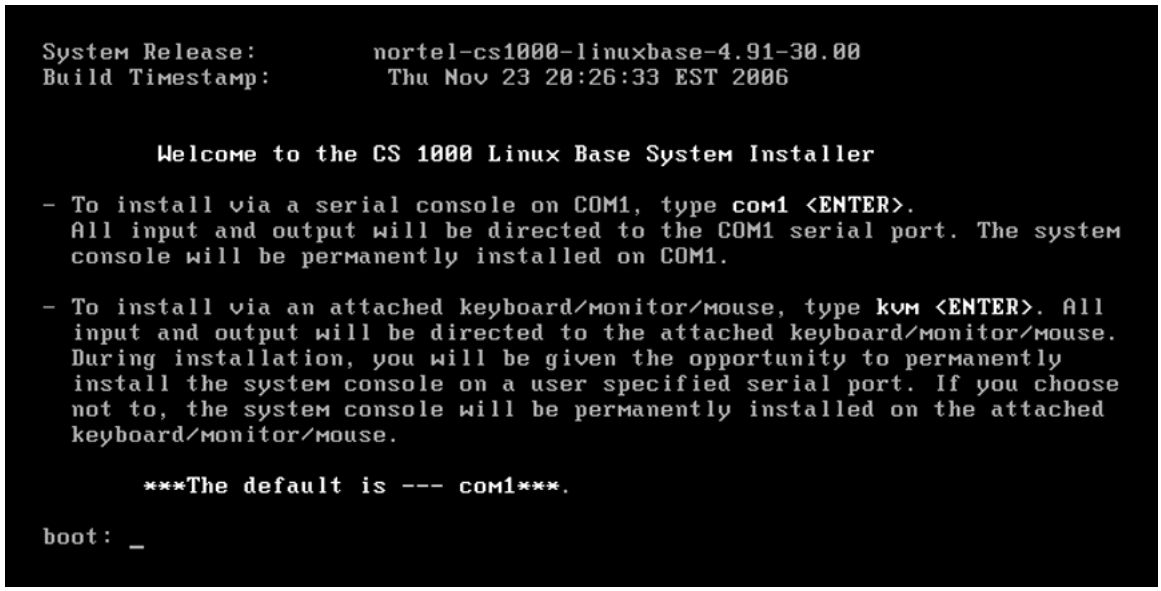
Note: For CP PM servers, reseat the CP PM card to ensure a successful restart.

When the server boots up, the CS 1000 Linux Base System Installer window appears. For CP PM servers, the CS 1000 Linux Base System Installer window appears as shown in Figure

14 "CS 1000 Linux base system installer (CP PM server)" (page 44). For COTS servers, the CS 1000 Linux Base System Installer window appears as shown in Figure 15 "CS 1000 Linux base system installer (Applies to COTS Server only)" (page 44).

Figure 14
CS 1000 Linux base system installer (CP PM server)

Figure 15
CS 1000 Linux base system installer (Applies to COTS Server only)



8 Type **com1** or press **Enter** to install using a serial console on COM1.

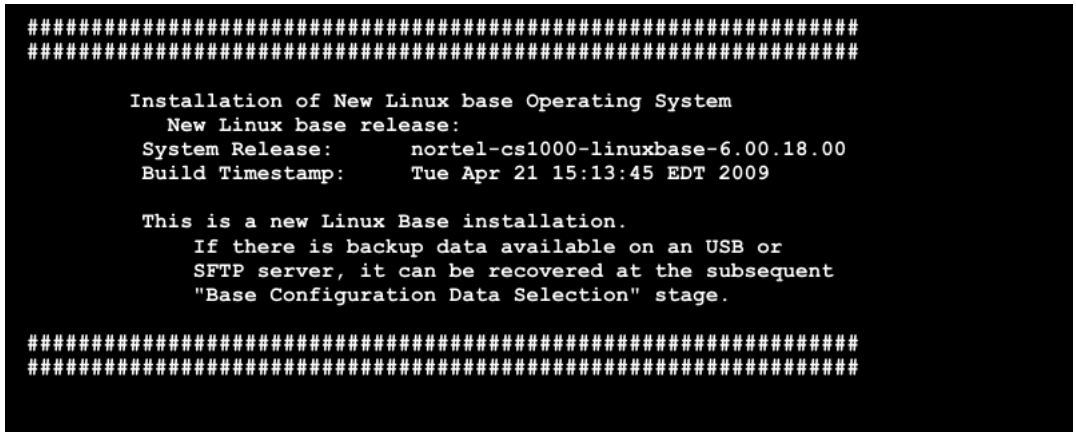
OR

Type **kvm** to install using an attached keyboard and video monitor.

WARNING
If you log on to the COM1 port, make sure that **Caps Lock** is turned off before you log on.

The CS 1000 Linux base system installer confirmation screen appears, as shown in Figure 16 "CS 1000 Linux base system installer confirmation window" (page 45).

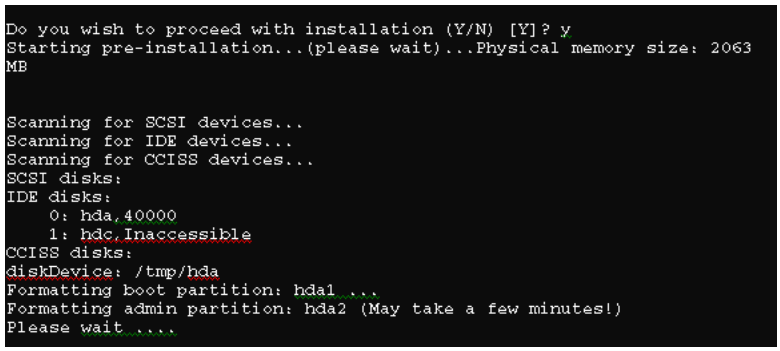
Figure 16
CS 1000 Linux base system installer confirmation window



9 Type **Y** and press **Enter**. .

The Format all partitions screen appears, as shown in Figure 17 "Format all partitions window" (page 45).

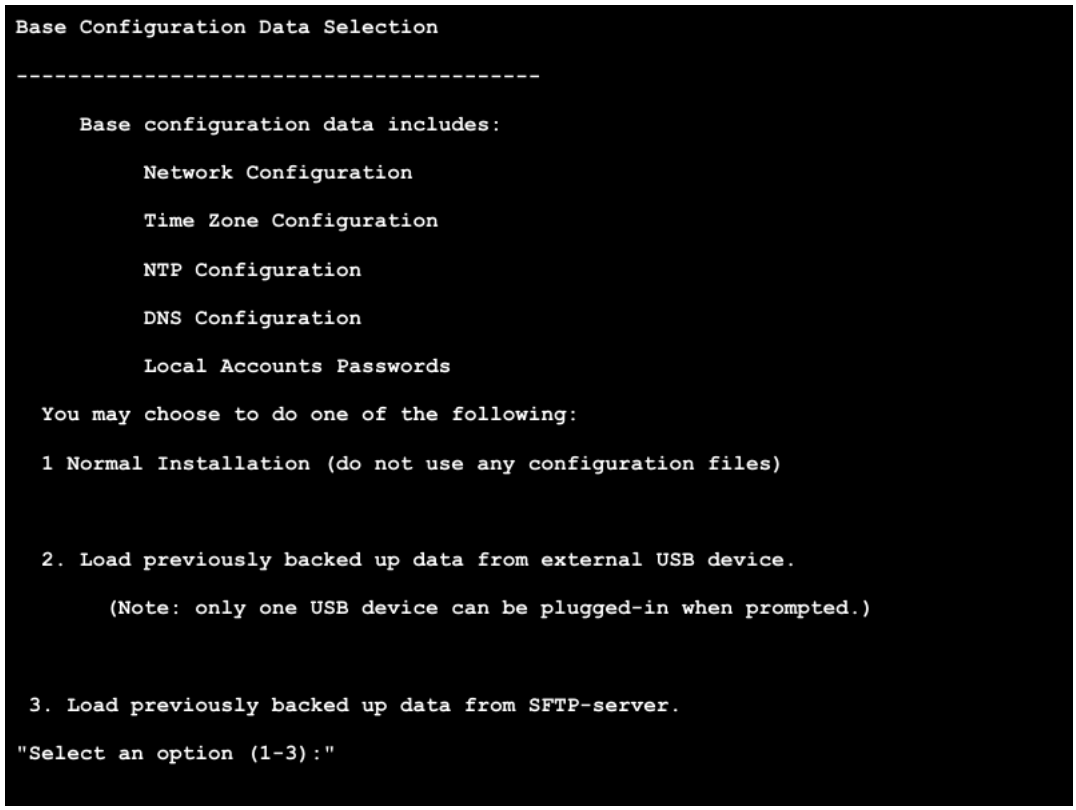
Figure 17
Format all partitions window



10 Press **Enter** to continue.

The Base Configuration Data Selection screen appears, as shown in Figure 18 "Base Configuration Data Selection window" (page 46).

Figure 18
Base Configuration Data Selection window

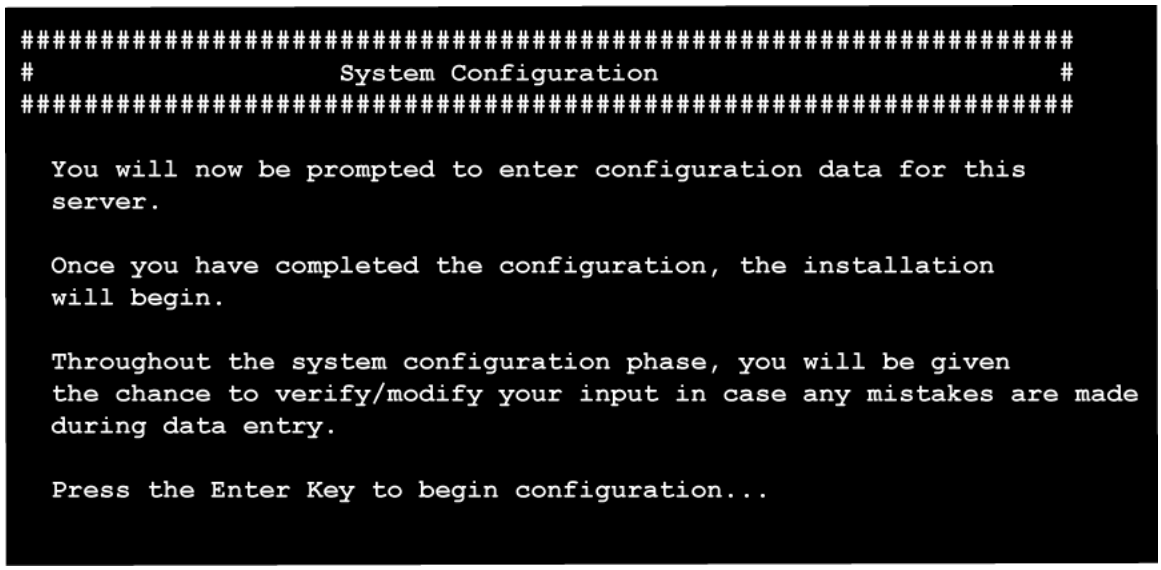


11 Type **1** and press **Enter**.

Note: If you select option 2 or 3, the remainder of the process is the same as the upgrade procedure. Proceed to step 20 in “Upgrading Nortel Linux base ” (page 65).

The System configuration window appears, as shown in Figure 19 "System configuration window" (page 47).

Figure 19
System configuration window



12 . Press **Enter** to continue.

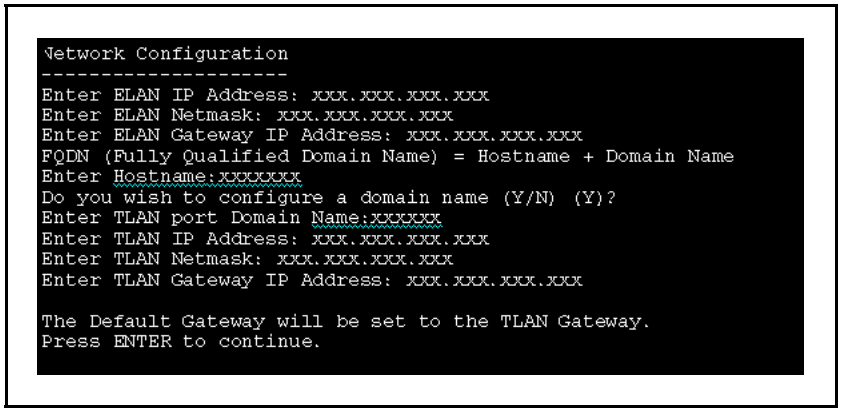
13 If you are installing Linux base on a COTS server using a KVM, the System Console Redirection screen appears, as shown in Figure 20 "System Console Redirection window (Applies to COTS Server only)" (page 47). Type the option number corresponding to your choice for redirection.

Figure 20
System Console Redirection window (Applies to COTS Server only)

14 Press **Enter**.

The Network Configuration screen appears, as shown in Figure 21 "Network configuration" (page 48)

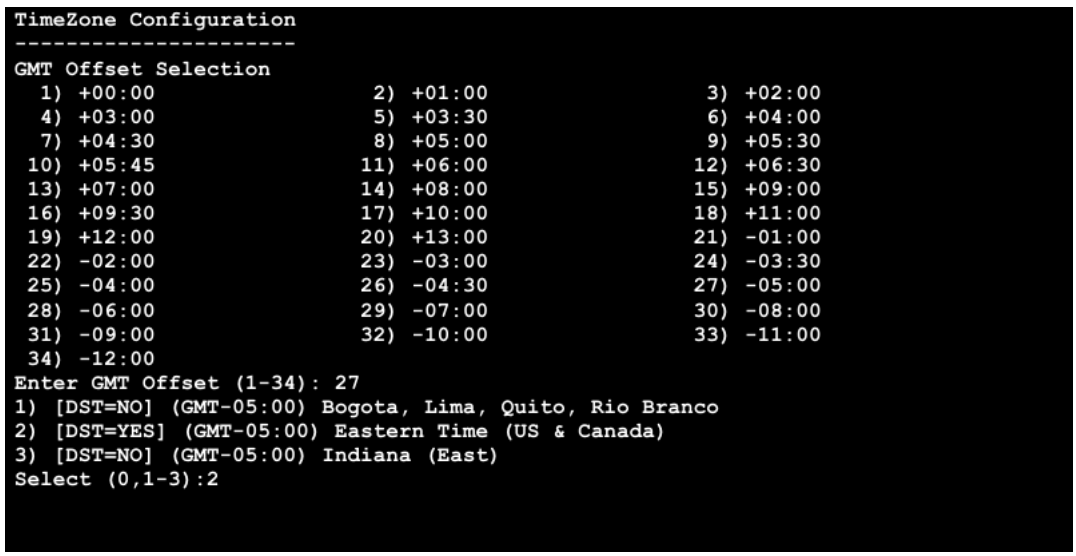
Figure 21
Network configuration



15 Press **Enter**.

The TimeZone Configuration screen appears, as shown in Figure 22 "TimeZone Configuration window" (page 48).

Figure 22
TimeZone Configuration window



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

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

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 3 "Time zone offsets" (page 49).

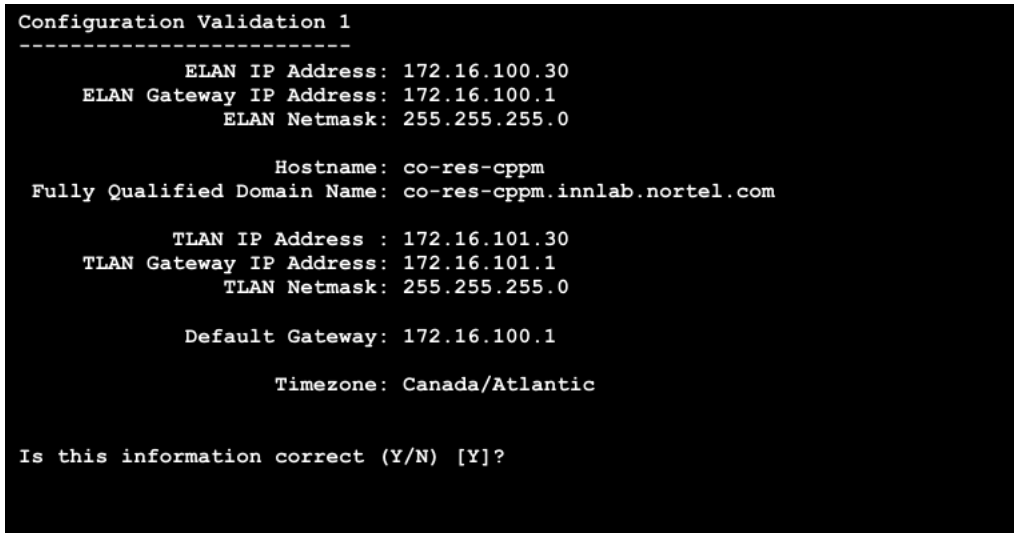
Table 3
Time zone offsets

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

Name	Description	Relative to GMT
AGT	Argentina Standard Time	GMT-3:00
BET	Brazil Eastern Time	GMT-3:00
CAT	Central African Time	GMT-1:00

The Configuration Validation 1 screen appears, as shown in Figure 23 "Configuration Validation 1 window" (page 50).

Figure 23
Configuration Validation 1 window



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

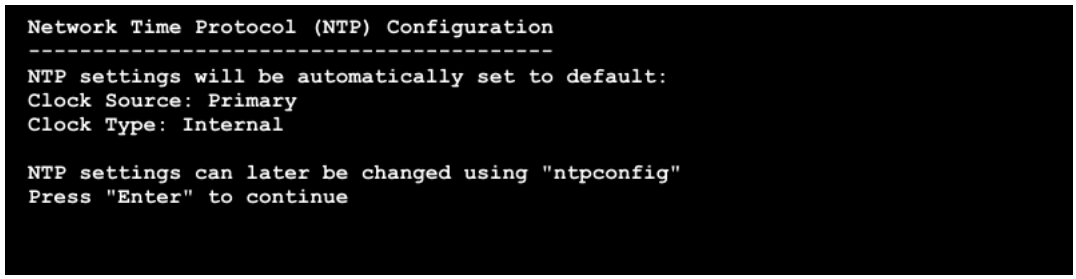
OR

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 24 "Network Time Protocol (NTP) Configuration window" (page 51).

Figure 24
Network Time Protocol (NTP) Configuration window

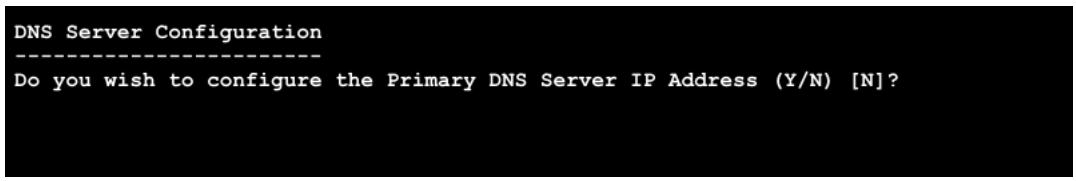


19 Press **Enter**.

Note: NTP settings can be changed after the installation is complete. To change NTP settings, use the procedures in the "Date and time" (page 170) section of “Base Manager” (page 149). You can also configure NTP settings using the CLI command **`ntpconfig`**.

The DNS Server Configuration screen appears, as shown in Figure 25 "DNS Server Configuration window" (page 51).

Figure 25
DNS Server Configuration window



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

OR

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

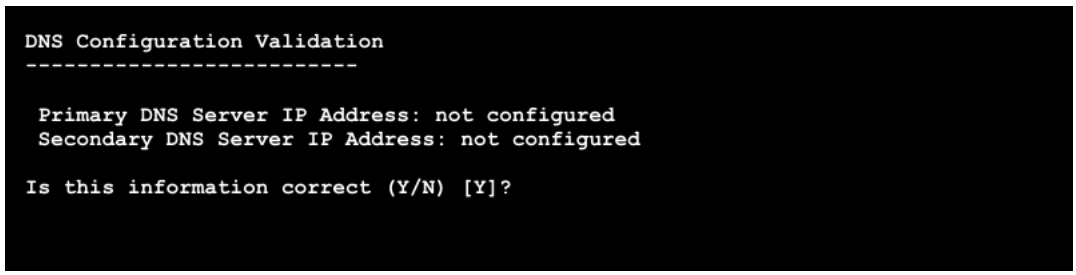
Note 1: In this example we do not configure the Primary DNS server IP address. If you choose **Y** you receive a prompt to provide the Primary DNS server IP address.

Note 2: You can use Base Manager to modify the static lookup table for host names; for details, see Procedure 19 “Adding a host” (page 160) and Procedure 20 “Deleting a host” (page 163). The CLI command **`hostconfig`** can also be used to modify the static lookup table for host names. For a list of Nortel Linux base CLI commands see “ Nortel Linux base CLI commands” (page 265).

The DNS Configuration Validation screen appears, as shown in Figure 26 "DNS Configuration Validation window" (page 52).

WARNING
Do not program DNS IP addresses when no active DNS server is present on the network. If later DNS IP addresses need to be added please refer *Troubleshooting Guide for Distributors* (NN43001-730)on "dnsconfig " command to configure IP addresses.

Figure 26
DNS Configuration Validation window



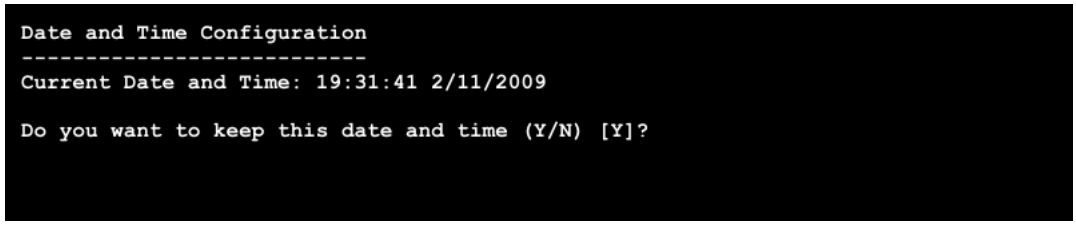
21 Type **Y** and press **Enter** to confirm the configuration.

OR

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

The Date and Time Configuration screen appears, as shown in .

Figure 27
Date and Time Configuration window



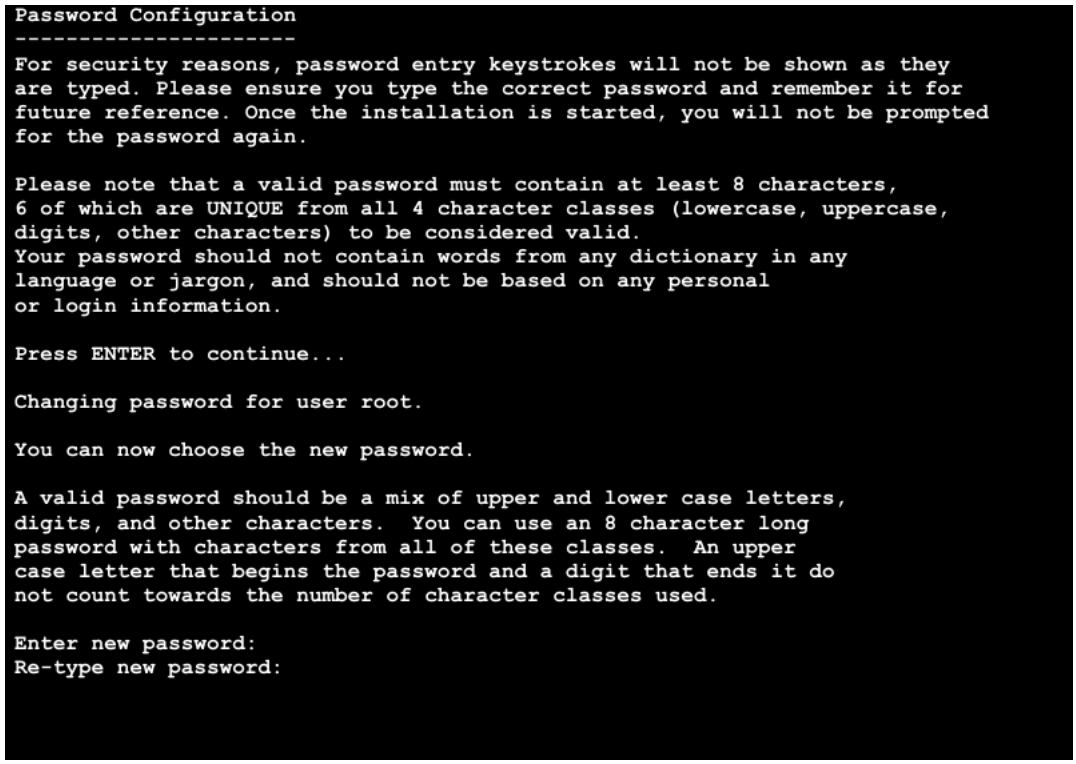
22 Type **Y** and press **Enter** to confirm the date and time.

OR

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

The root Password Configuration screen appears, as shown in Figure 28 "root Password Configuration window" (page 53).

Figure 28
root Password Configuration window



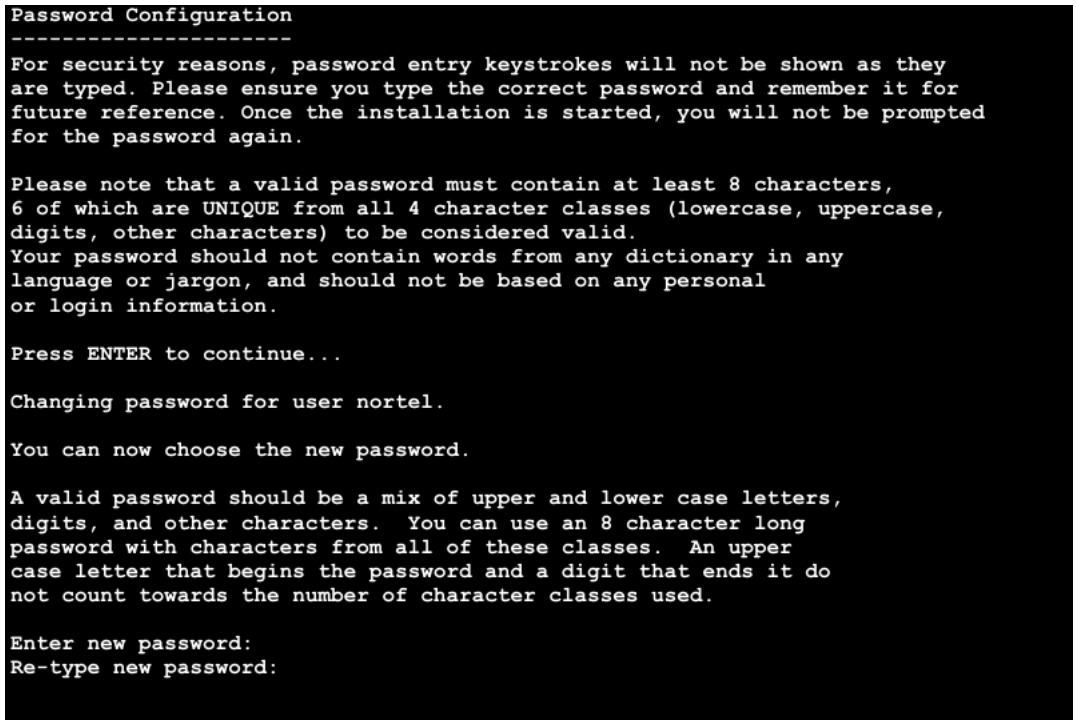
23 Enter a value for the root password.

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

> ***Note:*** For information about the creation and use of passwords, see “Passwords” (page 30).

The nortel Password Configuration screen appears, as shown in .

Figure 29
nortel Password Configuration window



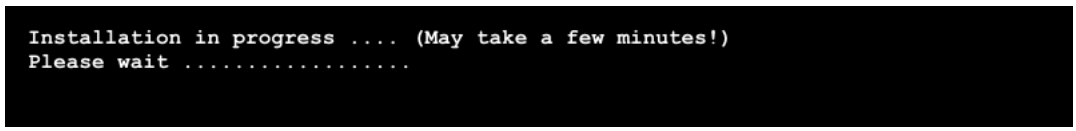
25 Enter a value for the nortel password.

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

Note: For information about the creation and use of passwords, see "Passwords" (page 30).

A pre-installation status screen appears, as shown in Figure 30 "Pre-installation status window" (page 54).

Figure 30
Pre-installation status window



After several minutes elapse, the Package Installation screen, Post System Configuration screen, and Status of Linux Hardening items screens appear, as shown in Figure 31 "Package Installation window" (page 55), Figure 32 "Post System Configuration (CP PM) window" (page 55) for a CP PM server or Figure 33 "Post System Configuration (COTS) window" (page 55) for a COTS server, and Figure 34 "Status of Linux Hardening items window" (page 56).

Figure 31
Package Installation window

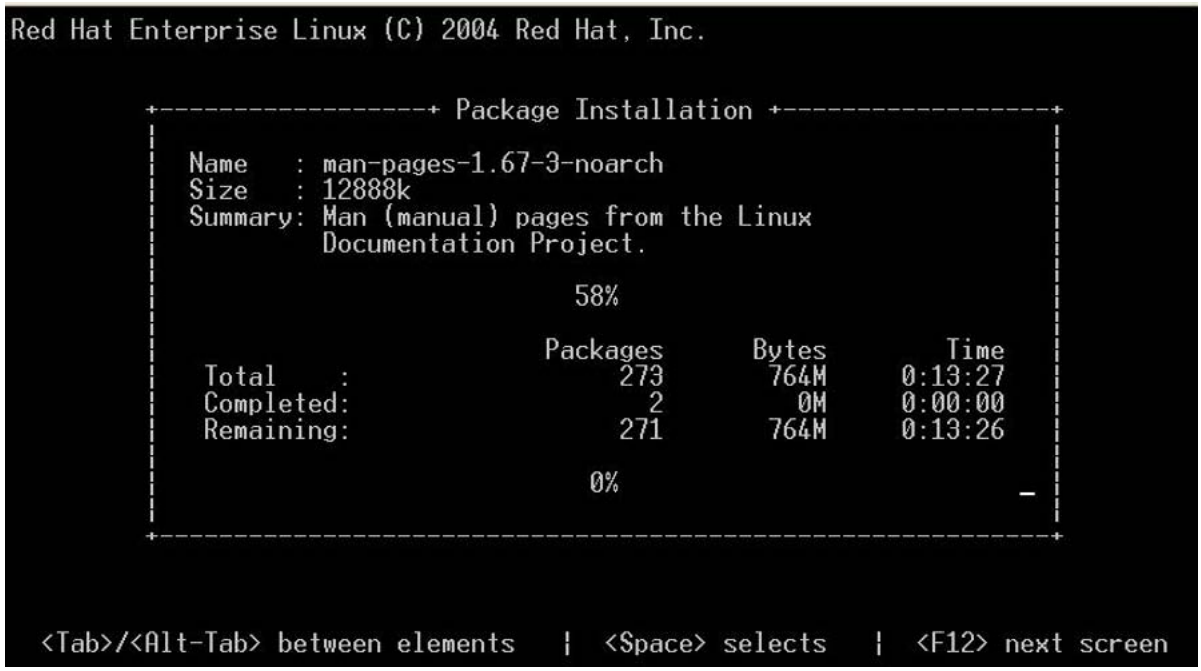


Figure 32
Post System Configuration (CP PM) window

Figure 33
Post System Configuration (COTS) window

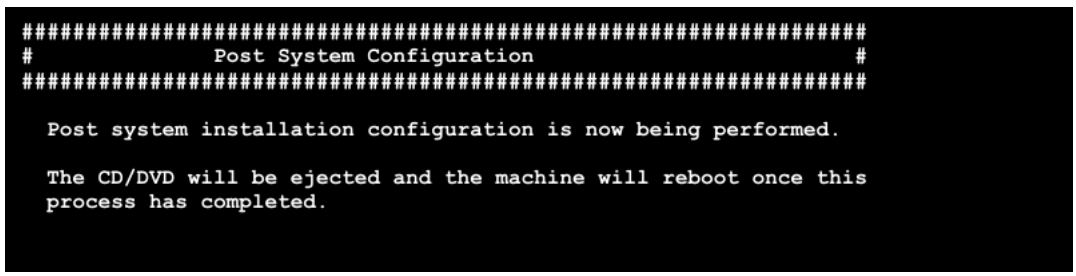
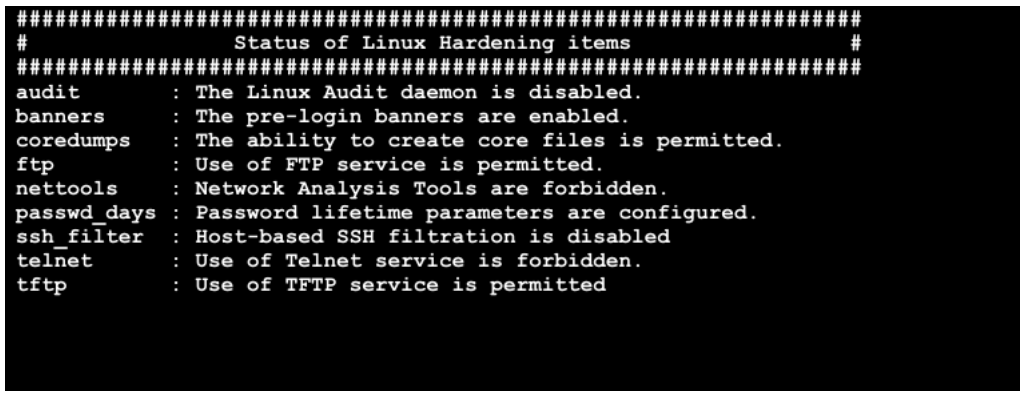


Figure 34
Status of Linux Hardening items window



WARNING
For COTS servers, make sure that the installation DVD ejects. If the installation DVD does not eject automatically, eject the DVD manually.

--End--

After the server boots up you can proceed with UCM security configuration, then application deployment and patching. For information about UCM security configuration, see *Unified Communications Management* (NN43001-116). For information about application deployment, see "Deploy application software to a COTS or CP PM server" (page 116). For information about patching, see *Patching Fundamentals* (NN43001-407).

Configuration for a CP PM card pre-loaded with Nortel Linux base

The Nortel Linux Base image can be pre-loaded on new CP PM cards shipped from the factory; this saves the Linux base installation time. The pre-loaded CP PM card is shipped with some default settings pre-set, such as:

- The default password for both the root and nortel user accounts is nortel12_Nortel
- The default IP address for the ELAN interface is 192.168.1.3
- The default IP address for the TLAN interface is 192.168.1.2
- The default hostname is: localhost

Pre-configuration requires you to start the commissioning of the server by connecting the client PC COM port to the EIA232 com port on the CP-PM server, in order to configure customer-assigned IP addresses, the FQDN, and other customer settings such as DNS server or time and date.

Use Procedure 1 “Configuring a pre-loaded CP PM card” (page 57) to prepare the CP PM card for installation.

Procedure 1
Configuring a pre-loaded CP PM card

Step	Action
1	Connect the management PC to the server using the CP-PM EIA232 COM port.
2	Logon as nortel using the default password.
3	Issue the **passwd** CLI command.
4	Change the nortel password. For information about changing passwords, see “Passwords” (page 30).
5	Logon as root by using **su-** and the default password.
6	Issue the **passwd** CLI command.
7	Change the root password. For information about changing passwords, see “Passwords” (page 30).
8	Logon as nortel by issuing the **exit** CLI command. ***Note:*** Issue the **exit** CLI command while you are logged on as root. **OR** Logon as nortel by logging on to the COM1 port as nortel and using the newly created password.
9	Issue the CLI command **baseparamsconfig**.  **WARNING** Do not change the FQDN of the primary or backup security server when you use the baseparamsconfig command.
10	Make appropriate changes to base parameters, such as FQDN or IP settings.
11	Type **Y** to save the base parameters changes. The system restarts.

12 Connect the ELAN and TLAN interfaces to the data network.

--End--

After the server boots up the work flow for commissioning the server is the same as the work flow that follows a fresh installation; you can proceed with UCM security configuration, then application deployment. For information about UCM security configuration, see *Unified Communications Management* (NN43001-116). For information about application deployment, see “Deploy application software to a COTS or CP PM server” (page 116).

Upgrade Nortel Linux base

This chapter documents the process of upgrading Nortel Linux base.

WARNING
If you perform a system upgrade from a 5.x system to 6.0, the hard drive is formatted and all data is lost. To preserve the data, perform a backup to an external source before you attempt an upgrade. If you are upgrading a CoRes Linux server, perform an LD 43 EDD, before you begin the upgrade. If you are performing an interim upgrade (within Release 6.0) refer to the information found in "Install Nortel Linux base on a CP PM or COTS server" (page 35).

WARNING
The information in this chapter does not apply to upgrades within release 5.x. For information about upgrading from a 5.x release to a higher 5.x version, consult the appropriate version of *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315)

The Linux platform supports upgrades for the delivery of new interim releases within Release 6.0, and upgrades from Release 5.x to Release 6.0. The installation or reinstallation provides the option to preserve the customer installation parameters for upgrade purposes. You can upgrade the complete platform including the operating system and Linux base applications.

WARNING
Linux base and applications upgrade causes the loss of keycodes for CoRes installations and for installations of Sunscriber Manager. You must create a copy of the keycodes before you perform the upgrade procedure.

Nortel Linux base uses the CLI command **`upgrade`** to upgrade the base installation. System upgrade redeploys Linux base and applications and reloads the software. Insert the Linux base installation media and invoke the **`upgrade`** command. You can choose to back up the data to a USB

device, to an SFTP server, or type **q** to exit the upgrade operation. For more information about SFTP data back up, see "Network configuration for Secure File Transfer Protocol (SFTP) data backup" (page 273)When you reinstall Linux base you can use the data stored in the USB device or the SFTP server.

Release 6.0 Linux base backs up the following data during the Linux upgrade process. The backed up data is restorable when the applications are reinstalled:

- UCM
- SNMP
- DM
- SS
- NRS
- CS
- SIPL
- EM
- SubM
- Intrasystem Signaling Security Solution (ISSS)
- Patches
- Route and host configuration information (if this information was changed using the **`routeconfig`** or **`hostconfig`** commands)
- Linux security hardening settings

Release 5.x Linux base backs up the following data during the Linux upgrade process. The backed up data is restorable when the applications are reinstalled:

- Enterprise Common Manager (ECM)
- NRS
- SubM (Release 5.5 only)

Note: You must logon in a systemadmin role to run the installation or upgrade process.

WARNING

If you access the Linux server through a Terminal Server connected to the COM port, it is possible that garbled characters (such as uuuuuu) can appear during a system restart (for example, during the installation or upgrade procedure). This appearance can make the system seem to hang.

You can resolve the problem by re-establishing the COM1 connection from the client PC or work station to the Linux server.

Do not manually restart the system during the upgrade or installation. This can result in hard drive corruption, and forces you to reinstall the system.

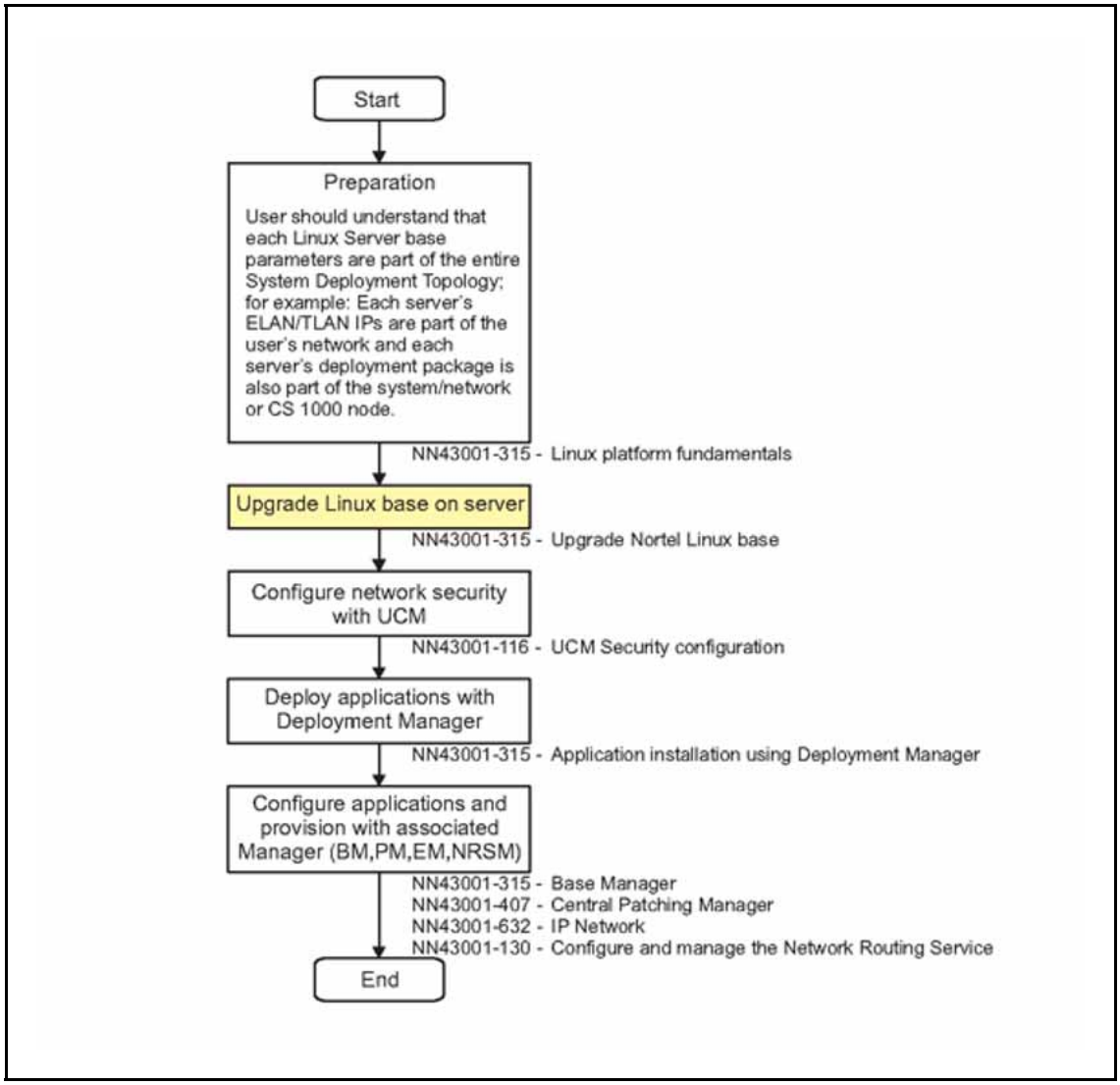
Upgrade workflow stage

"Upgrade Nortel Linux base " (page 59) provides information, prerequisites, and procedures for upgrading Nortel Linux base on a COTS or CP PM server.Figure 35 "Upgrade workflow stage" (page 62) shows the position of the upgrade stage in the overall workflow.

This chapter provides information and procedures in the following areas:

- "Prerequisites to upgrade Nortel Linux base" (page 62)
- "Nortel Linux base upgrade" (page 64)

Figure 35
Upgrade workflow stage



Prerequisites to upgrade Nortel Linux base

- Before you perform the upgrade you must gather the following information:
  - ELAN IP address
  - ELAN gateway IP address
  - ELAN netmask
  - The host name associated with the TLAN
  - The domain name

Note 1: A Fully Qualified Domain Name (FQDN) consists of a host name and a domain name, and includes a top-level domain name. Using kwei.ca.nortel.com as an example, kwei is the host name, ca.nortel.com is the domain name, and .com is the top-level domain name. The FQDN must contain at least three fields separated by dots. The host name cannot contain dots.

Note 2: If you are using a DNS server to resolve the FQDN to an IP address, ensure that prior to the installation of the Linux server that you can resolve the FQDN to the expected IP address. For example, attempt to ping the FQDN from a PC that uses the external DNS server, and it should resolve to the expected IP address.

— TLAN IP address

— TLAN gateway IP address

— TLAN netmask

— Time zone

— IP address of Network Time Protocol (NTP) Server

— 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. Figure 203 "HP DL320 G4 rear view" (page 235) shows the ELAN and TLAN network interfaces for the HP DL320 G4 server. It shows the ELAN and TLAN network interfaces for the IBM x306m server. For a definition of ELAN and TLAN see “Network configuration” (page 273).

- To upgrade Nortel Linux base from Release 5.x to Release 6.0, you must login using the nortel user account and invoke the **`upgrade`** command You must provide the root password to invoke the **`upgrade`** command.
- To upgrade Nortel Linux base within Release 6.0, you must login as any user belonging to the systemadmin group and invoke the **`upgrade`** command. For example, both nortel and admin belong to the systemadmin group; therefore either can be used to login, additionally any other UCM user with systemadmin permissions can be used.
- You must have a user role in the systemadmin group to perform the upgrade procedure. “Centralized authentication” (page 29) provides an

overview of UCM roles and role creation. For a more detailed of UCM roles, see *Unified Communications Management* (NN43001-116).

- You must have a higher version of Nortel Linux base.

You can change the base parameters after the upgrade is complete using the CLI command **baseparamsconfig**. A change in the base parameters can impact other application components. For example, if the current server is the Primary UCM security server and the FQDN changes it is necessary to reinstall the applications.

The CLI command **baseparamsconfig** is an umbrella command that you can use to configure parameters for network settings, Network Time Protocol settings, date and time settings, and DNS settings. These parameters can also be configured individually by using the CLI commands **networkconfig**, **ntpconfig**, **datetimeconfig**, and **dnsconfig**. For a list of Nortel Linux base CLI commands see " Nortel Linux base CLI commands" (page 265).

WARNING
Do not change the FQDN of the primary or backup security server when you use the baseparamsconfig or networkconfig commands.

Use the CLI command **routeconfig** 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 " Nortel Linux base CLI commands" (page 265).

Nortel Linux base upgrade

Use the following procedure to upgrade Nortel Linux base. Nortel Linux base consists of the operating system and the base applications.

The time required to perform backup, installation, deployment and patching is approximately 3 to 4 hours. For more information about upgrade times, see "Installation times" (page 259).

Note 1: In this procedure system data refers to Linux base data, base application data, and Nortel application data.

Note 2: It is not required to attach a keyboard and video monitor (KVM) to view output. A console-based installation can also provide output. If KVM is used, not all application update information is displayed; some information points to COM1 only. You do not see the entire upgrade status using KVM.

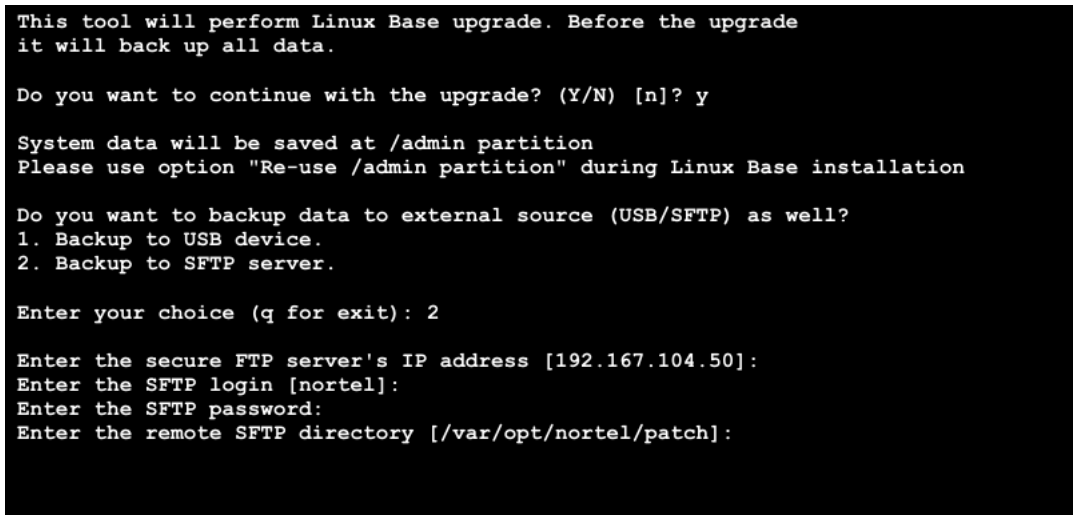
Note 3: If you connect to the IBM x3350 server with a terminal for setup, the server does not function with the serial cable that was

previously shipped with the ISP 1100 or other COTS platforms. The IBM x3350 server requires the new NTRX26NPE6 9 pin female to 9 pin female null modem cable. The NTRX26NPE6 9 pin female to 9 pin female null modem cable is displayed in Figure 219 "NTRX26NPE6 9 pin female to 9 pin female null modem cable" (page 250).

Upgrading Nortel Linux base

Step	Action
1	Log on to the server using the nortel account.
2	At the command prompt, type **upgrade**. The System data backup screen appears, as shown in Figure 36 "System data backup window" (page 65).

Figure 36
System data backup window



3	The system data is saved at the /admin partition; you also have an option to save the system data to an external source. Type **Y** and press **Enter** to save the system data to an external source. **OR** Type **N** and press **Enter** to proceed without saving the system data to an external source. ***Note 1:*** In this example, the system data is saved to an external SFTP server. System data backup to a USB device will produce different screens. ***Note 2:*** If a USB device is used, this process formats the device prior to backup if the existing file system is not FAT32. If the USB device contains information that you want to preserve, copy it elsewhere before you perform the backup or

use a different USB device. You must install the USB device before you issue the upgrade command.

4 Type the number corresponding to the type of external storage that you want to select.

5 In the **secure FTP server's IP address** line, type a value for secure FTP server IP address.

6 In the **SFTP login** line, enter a value for SFTP login.

7 In the **SFTP password** line, enter a value for SFTP password.

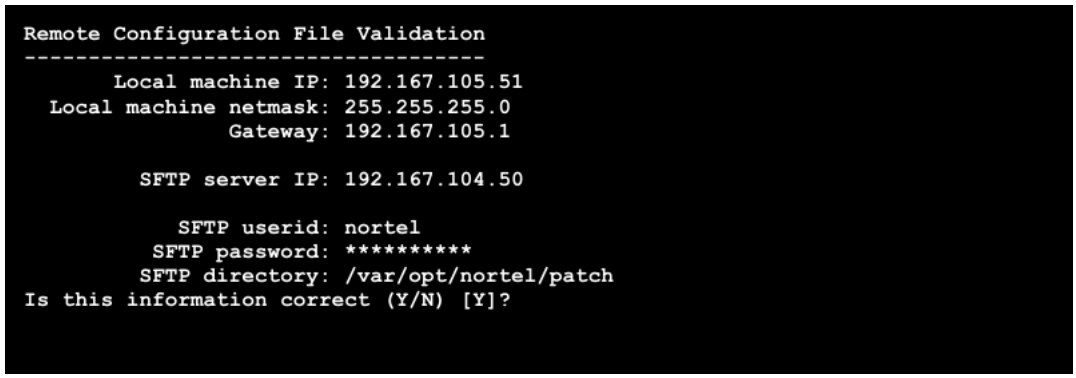
8 In the **remote SFTP directory** line, enter a value for remote SFTP directory.

Note: If you perform SFTP as the nortel user (non-jailed) then an example of an absolute sftp path is:
/var/opt/nortel/patch.
If you perform SFTP as any other user (jailed) then an example of an absolute sftp path is:
/patch (assuming that the user is part of the patchadmin group). For users other than nortel (jailed), the directories available using SFTP depend on what group(s) they belong to.

9 Press **Enter**.

The Remote Configuration File Validation screen appears, as shown in .

Figure 37
Remote Configuration File Validation window



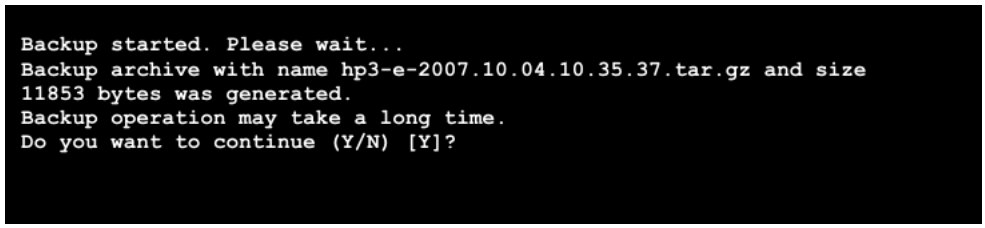
10 Type **Y** to confirm the Remote Configuration File information, and press **Enter**.

OR

Type **N** to reject the Remote Configuration File information and enter different values.

The backup archive name generates, as shown in Figure 38 "Backup data window 2" (page 67).

Figure 38
Backup data window 2



11 Type **Y** to continue.

OR

Type **N** to cancel the backup operation.

12 If you are upgrading a COTS server, insert the DVD installation media.

OR

If you are upgrading a CP PM server, insert the Compact Flash (CF) installation media.

13 Press **Enter** to restart a COTS server.

OR

When prompted, press **F** to restart the CP PM server from the faceplate. If you miss this step, you must allow the server to boot up and then reissue the upgrade command.

After the server restarts, the CS 1000 Linux base system installer screen appears. If you are upgrading a COTS server, the CS 1000 Linux base system installer screen appears as shown in Figure 39 "CS 1000 Linux base system installer (COTS server)" (page 68). If you are upgrading a CP PM server, the CS 1000 Linux base system installer screen appears as shown in Figure 40 "CS 1000 Linux base system installer (CP PM server)" (page 68).

Figure 39
CS 1000 Linux base system installer (COTS server)

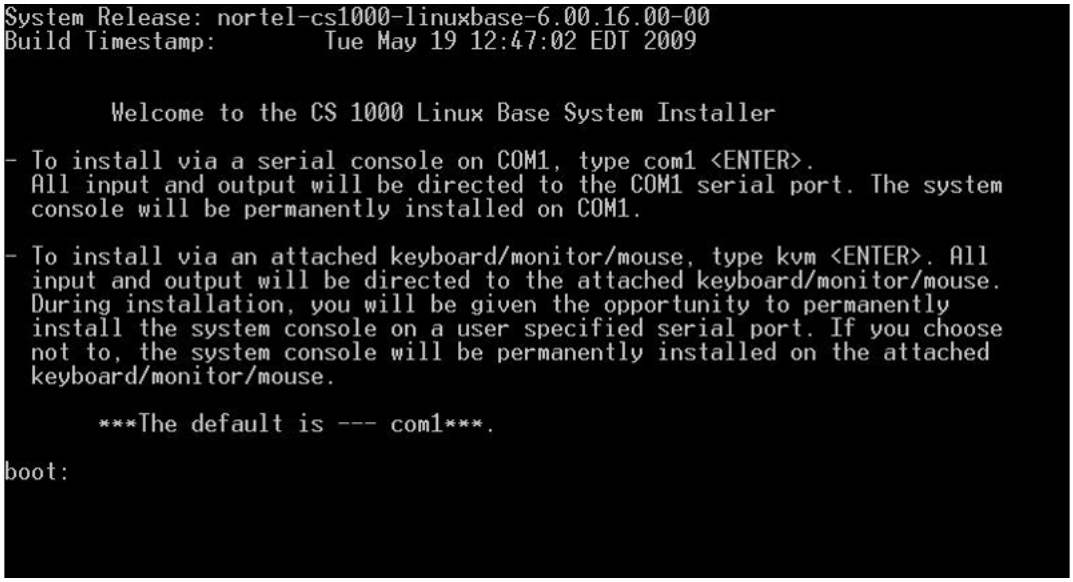


Figure 40
CS 1000 Linux base system installer (CP PM server)

Note:

14 Type **COM1** or press **Enter** to install using a serial console on COM1.

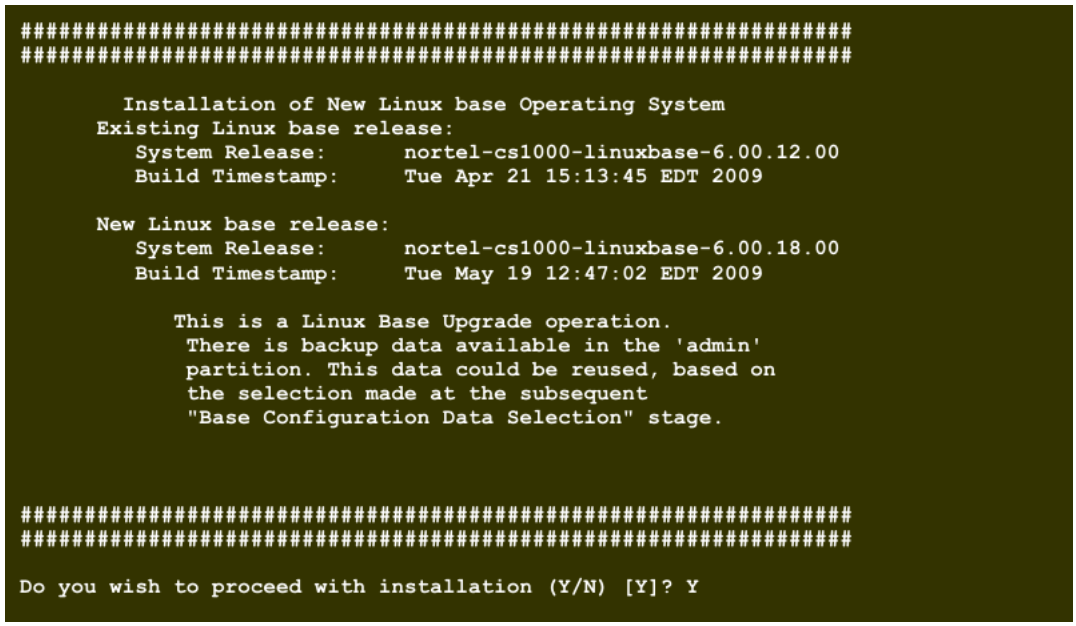
OR

Type **kvm** to install using an attached keyboard and video monitor.

WARNING
If you log on to the COM1 port, ensure that **Caps Lock** is turned off before you log on.

The CS 1000 Linux base system installer confirmation screen appears, as shown in Figure 41 "CS 1000 Linux base system installer confirmation window" (page 69).

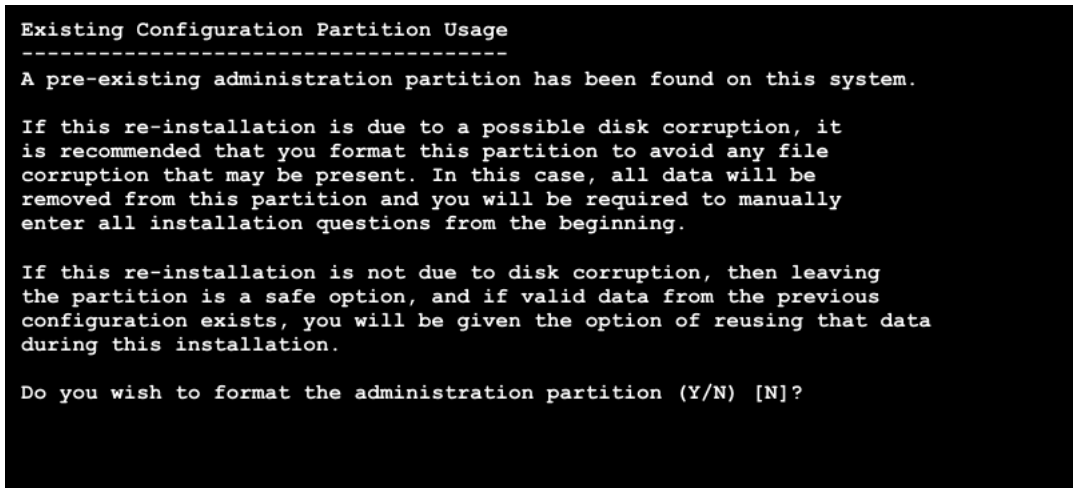
Figure 41
CS 1000 Linux base system installer confirmation window



15 Type **Y** to accept the new installation and press **Enter** to continue.

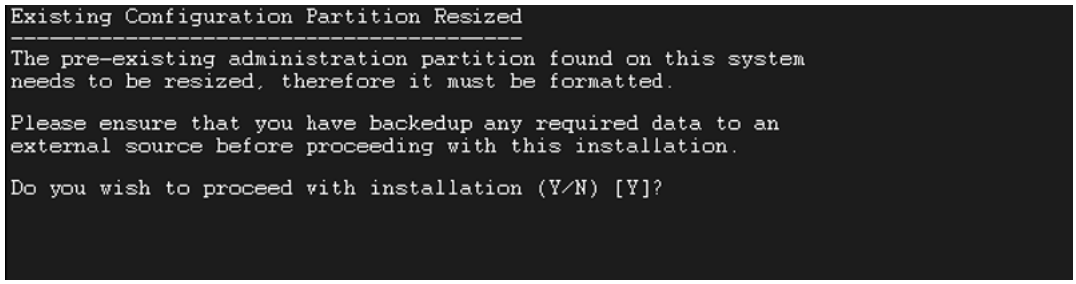
For upgrades within Release 6.0, the Existing Configuration Partition Usage window appears, as shown in Figure 42 "Existing Configuration Partition Usage window" (page 70).

Figure 42
Existing Configuration Partition Usage window



For upgrades from release 5.x to 6.0, the Existing Configuration Partition Resized screen appears, as show in .

Figure 43
Existing Configuration Partition Resized window



16 . Type **Y** to format the partition.

OR

Type **N** to maintain the partition.

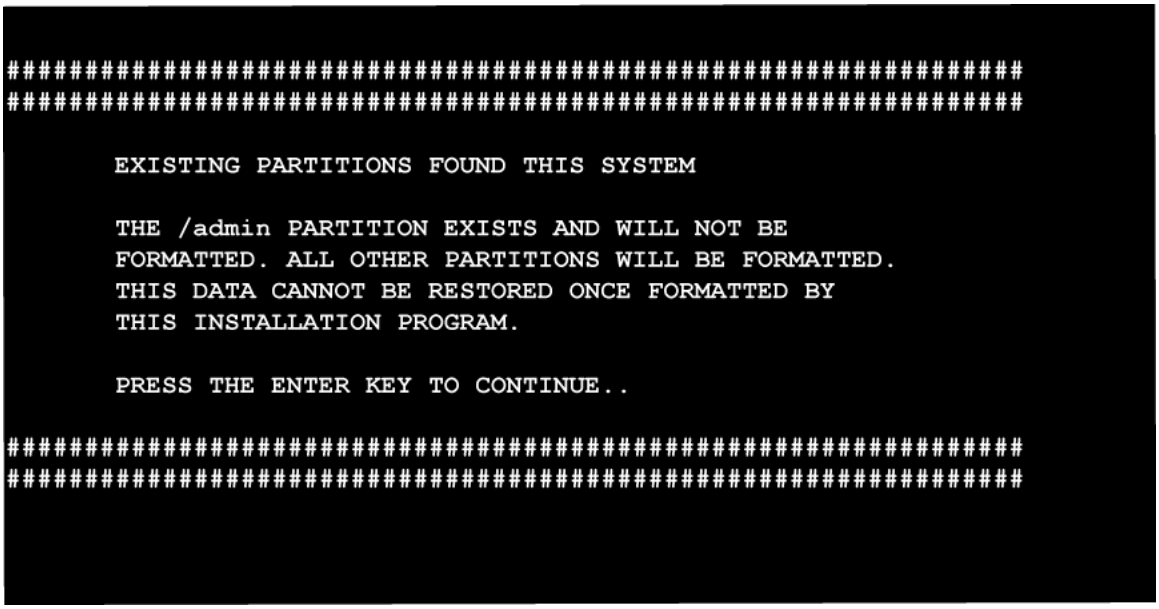
Note 1: Upgrades within Release 6.0 should not format the partition unless an existing external system data backup is used. Releases 5.0 or 5.5 upgrading to 6.0 must format the administration partition because there is a requirement to resize the administration partition.

Note 2: If this reinstallation is due to possible disk corruption, Nortel recommends that you format this partition. If this reinstallation is not due to disk corruption, leaving this partition is a safe option.

17 Press **Enter**

The Existing Partitions screen appears as shown in Figure 44 "Existing Partitions window" (page 71).

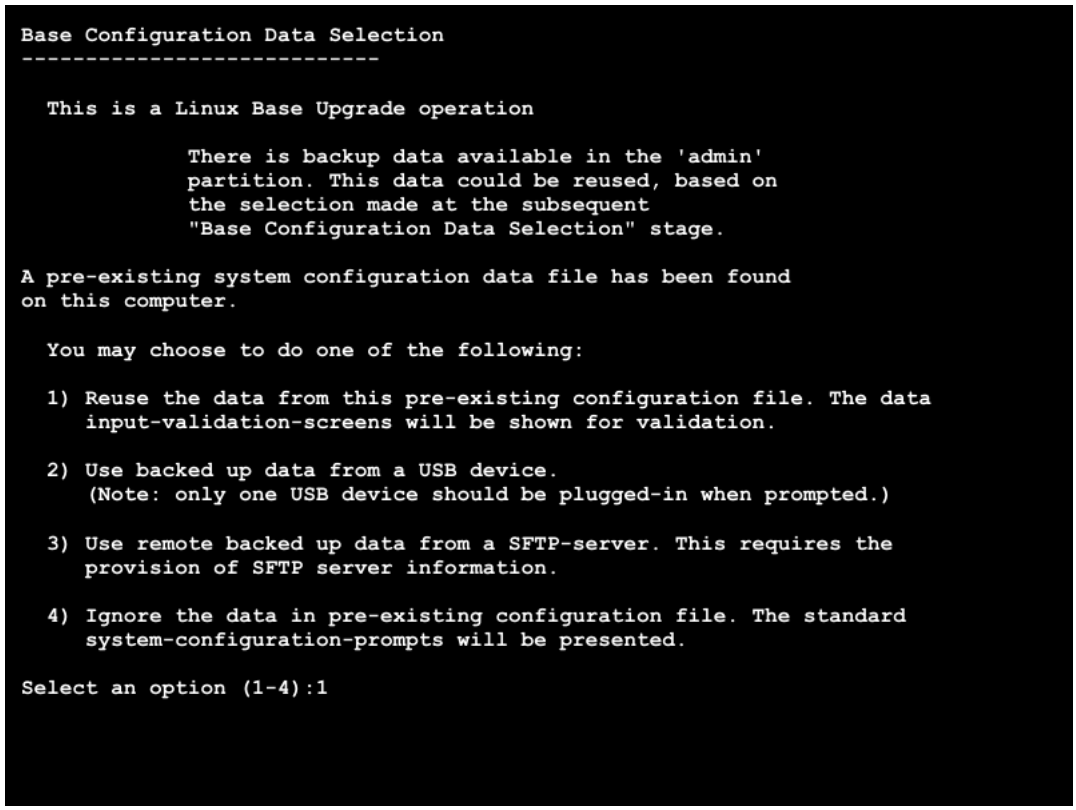
Figure 44
Existing Partitions window



18 Press **Enter** to continue.

The Base Configuration Data Selection screen appears, as shown in Figure 45 "Base Configuration Data Selection window" (page 72).

Figure 45
Base Configuration Data Selection window



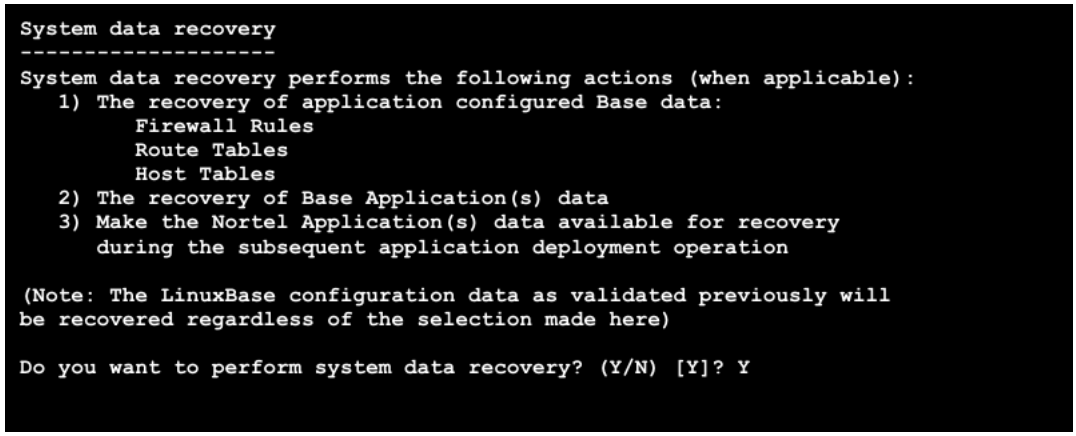
Note: If you chose to format the /admin partition in step 16, option 1 in Figure 45 "Base Configuration Data Selection window" (page 72) does not appear.

19 Type **1** to reuse the data from the previous configuration and press **Enter**.

Note: Typically, you would only use options 2 or 3 if the data in the pre-existing configuration file is corrupt. Option 4 discards any backup data and performs the equivalent of a new installation.

The System data recovery screen appears, as shown in Figure 46 "System data recovery window" (page 73).

Figure 46
System data recovery window



20 Type **Y** to recover system wide data.

OR

Type **N** to reject the system wide data.

Note: Nortel strongly recommends that you recover system wide data.

ATTENTION

If you do not receive a time zone conversion error, the Network Configuration Validation screen appears, as shown in Figure 47 "Network Configuration Validation window" (page 74). Proceed to step 25.

If you encounter a time zone conversion error, the System data recovery screen displays an error message, as shown in Figure 48 "System data recovery (time zone conversion error) window" (page 74). Proceed to step 21.

.

Figure 47
Network Configuration Validation window

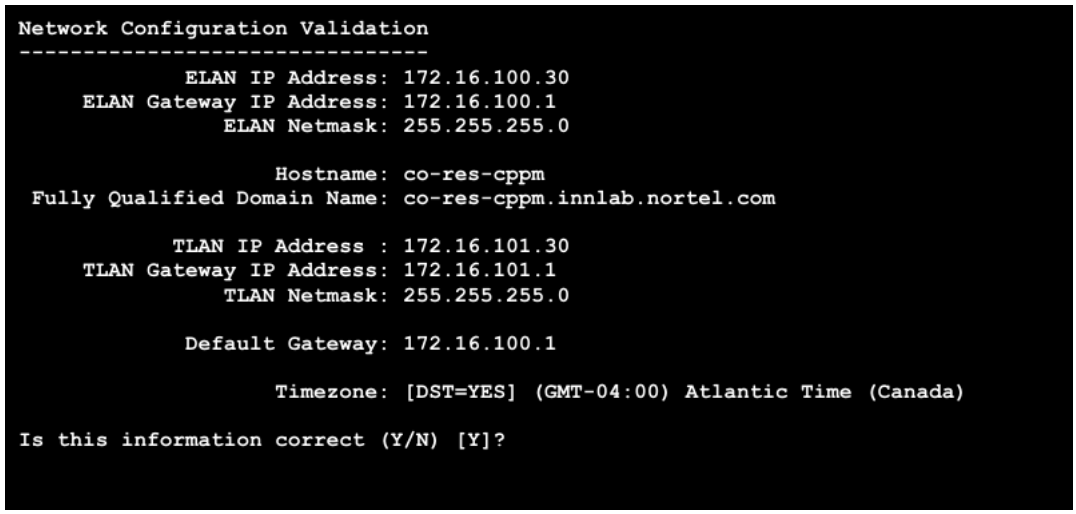
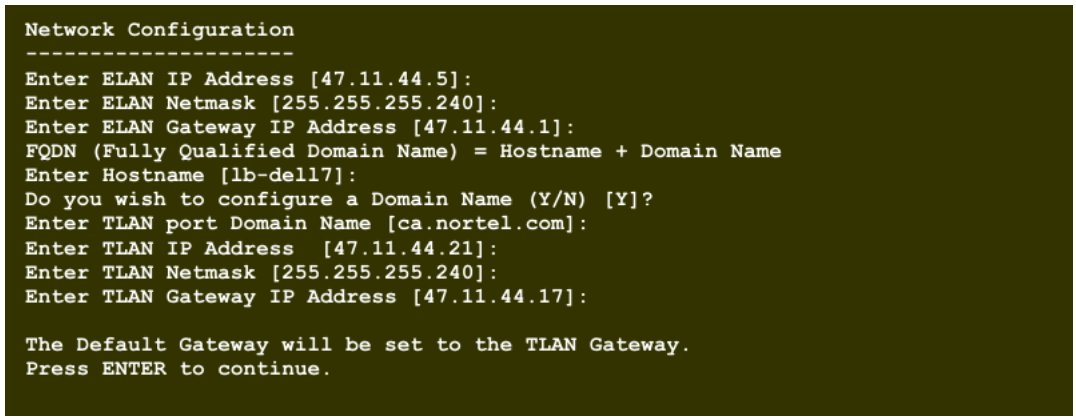


Figure 48
System data recovery (time zone conversion error) window

21 Press **Enter**.

The Network Configuration screen appears, as shown in Figure 49 "Network Configuration window" (page 75).

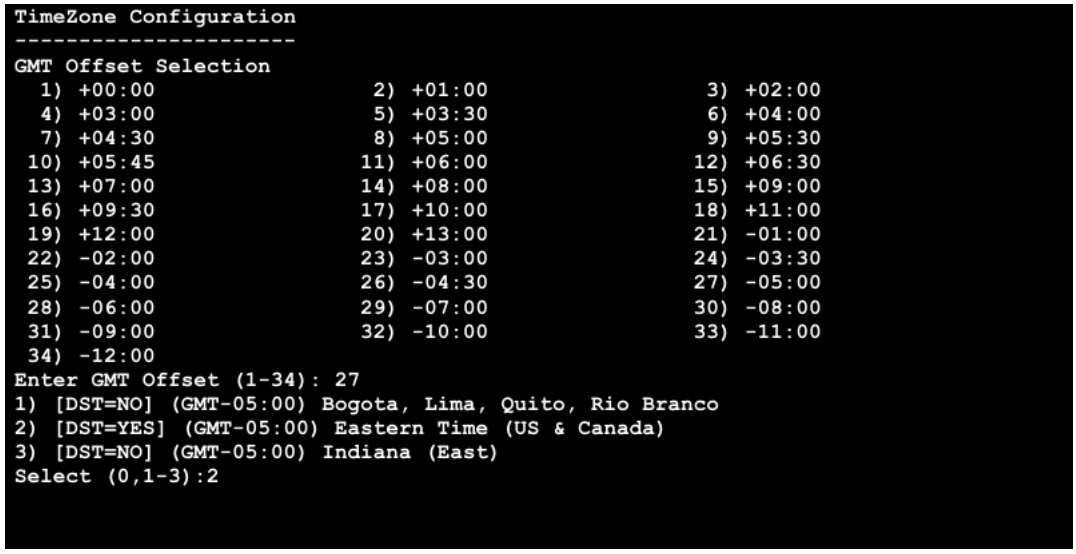
Figure 49
Network Configuration window



22 Press **Enter** to confirm the configuration values.

The TimeZone Configuration screen appears, as shown in Figure 50 "TimeZone Configuration window" (page 75).

Figure 50
TimeZone Configuration window



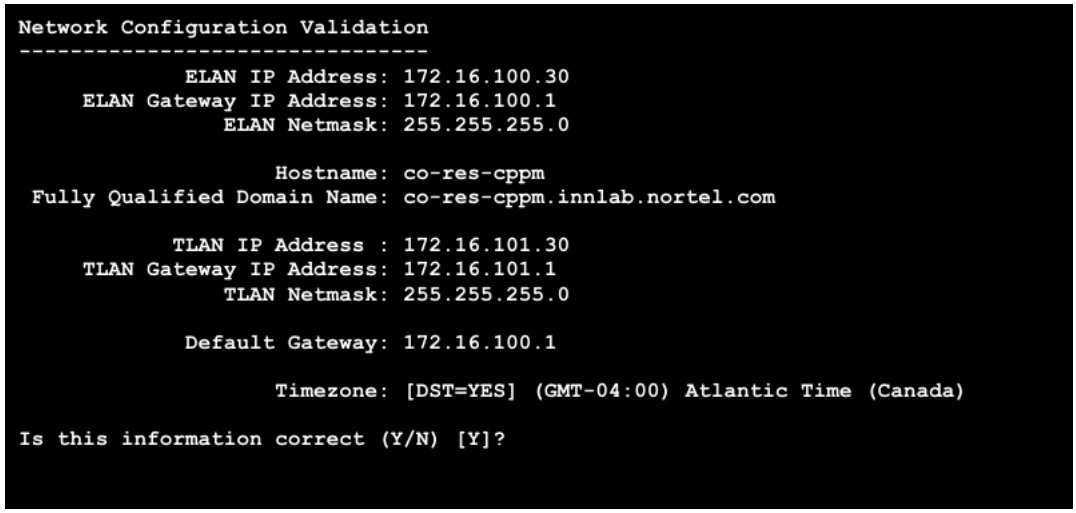
23 Type the number corresponding to the GMT offset you want to choose.

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

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 3 "Time zone offsets" (page 49).

The Network Configuration Validation screen appears, as shown in Figure 51 "Network Configuration Validation window" (page 76).

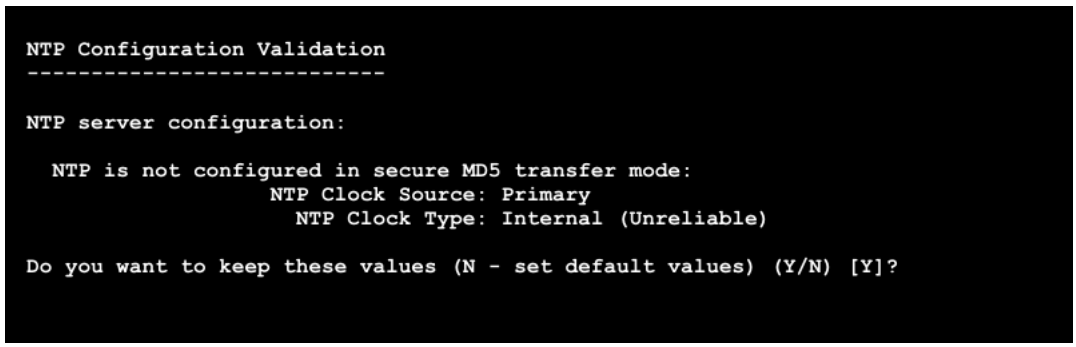
Figure 51
Network Configuration Validation window



25 Type **Y** to confirm the configuration information.

The NTP Configuration Validation screen appears, as shown in Figure 52 "NTP Configuration Validation window" (page 76).

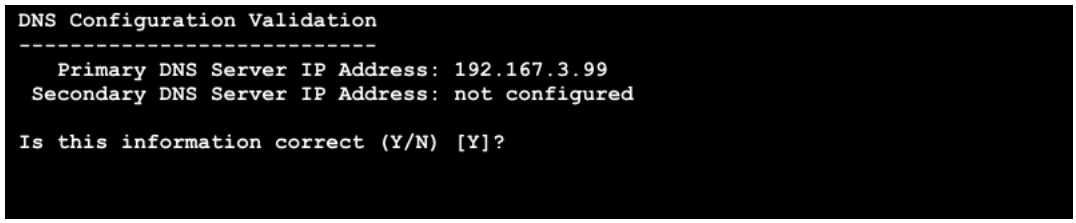
Figure 52
NTP Configuration Validation window



26 Type **Y** to confirm the configuration information.

The DNS Configuration Validation screen appears, as shown in Figure 53 "DNS Configuration Validation window" (page 77).

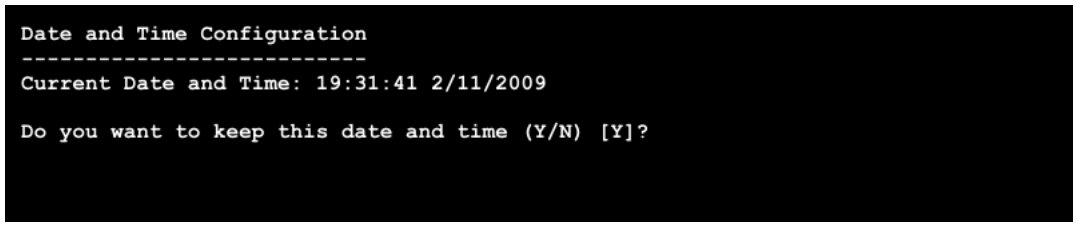
Figure 53
DNS Configuration Validation window



27 Type **Y** to confirm the configuration information.

The Date and Time Configuration screen appears, as shown inFigure 54 "Date and Time Configuration window" (page 77) .

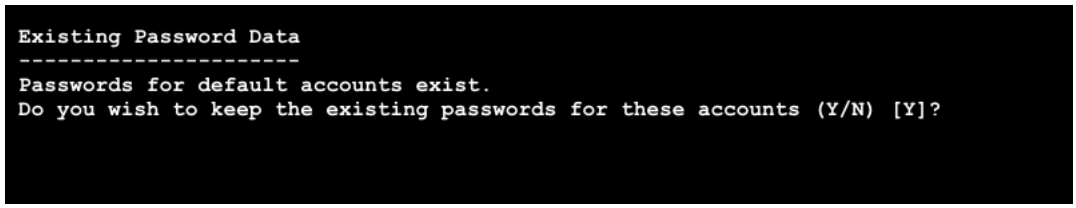
Figure 54
Date and Time Configuration window



28 Type **Y** to keep the date and time.

The Existing Password Data screen appears, as shown in Figure 55 "Existing Password Data window" (page 77).

Figure 55
Existing Password Data window



29 Type **Y** to keep the existing passwords for the default accounts.

OR

Type **N** to enter new passwords for the default accounts.

The CS 1000 Linux Base System pre-installation screen appears, as shown in Figure 56 "CS 1000 Linux Base System pre-installation window" (page 78).

Figure 56
CS 1000 Linux Base System pre-installation window

The Installation in progress screen appears, followed by the Installation complete screen, as shown in Figure 57 "Installation in progress window" (page 78)and Figure 58 "Installation complete window" (page 78)

Figure 57
Installation in progress window

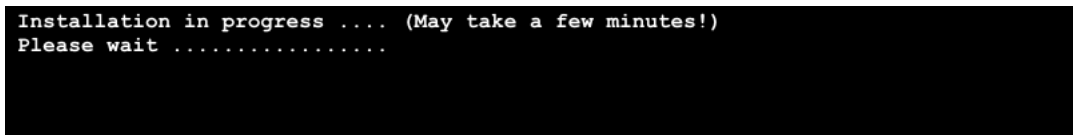
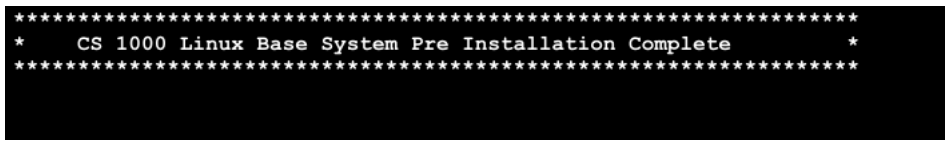


Figure 58
Installation complete window



After several minutes elapse, the Package Installation screen, Post System Configuration screen, and Status of Linux Hardening items screens appear, as shown in Figure 59 "Package Installation window" (page 79), Figure 60 "Post System Configuration window" (page 79), and Figure 61 "Status of Linux Hardening items window" (page 80).

Note: If you are using a KVM to perform the upgrade these screens do not appear, but the time interval to the next step remains the same

Figure 59
Package Installation window

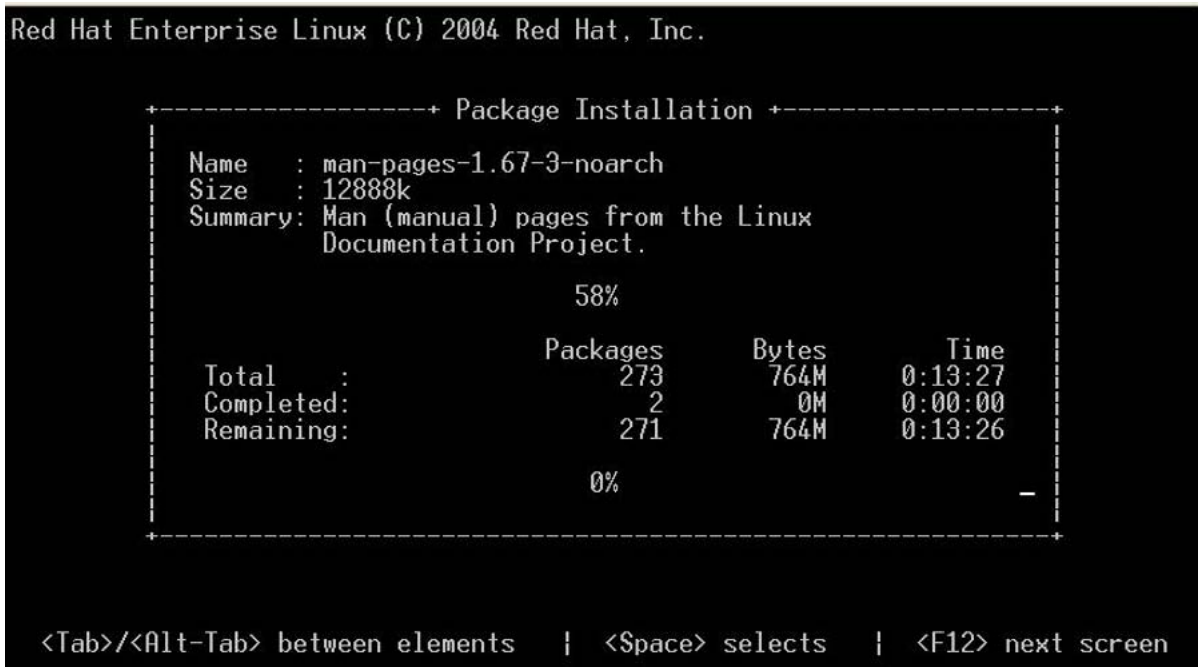
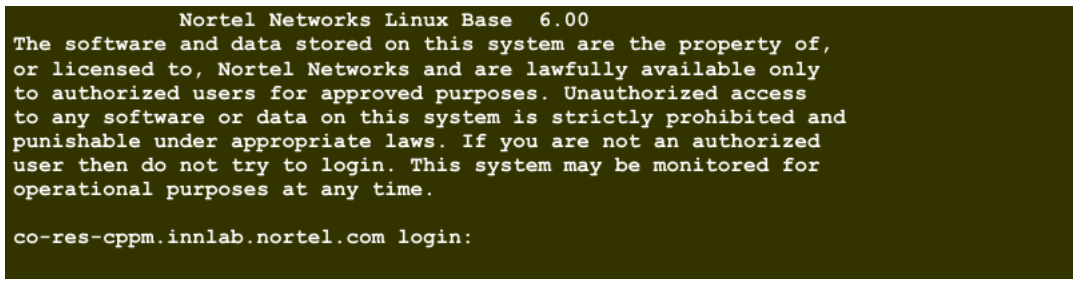


Figure 60
Post System Configuration window

Note: COTS servers automatically eject the DVD when ready; do not remove the DVD until the server opens the drive bay

Figure 61
Status of Linux Hardening items window

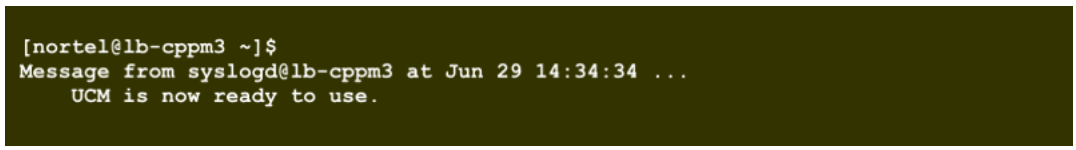
30 After the server restarts, the following screen appears:



At the prompt, log on using the nortel account.

After several minutes the UCM confirmation screen appears, as shown in Figure 62 "UCM confirmation window" (page 80).

Figure 62
UCM confirmation window



Note: You must wait approximately 10 minutes after the server restarts to perform UCM tasks; you cannot perform UCM tasks until UCM recognizes the server. For other servers in the domain, you must wait to see UCM display the target release before you take any action. Monitor the deployment targets screen in Deployment Manager and refresh the screen until the target release appears. For more information about Deployment Manager, see “Application installation using Deployment Manager” (page 99).

31 Log on to UCM using an admin role. For information about logging on to UCM, see Procedure 2 “Logging on to UCM” (page 105).

32 Remove the installation media; CF for a CP PM server, or DVD for a COTS server.

WARNING
For COTS servers, make sure that the installation DVD ejects. If the installation DVD does not eject automatically, eject the DVD manually.

33 If the server is the primary security server, add the appropriate software load. To add a software load, see Procedure 4 “Adding a new software load to the Deployment Manager from the client machine” (page 109).

34 Deploy the software to the target server. To deploy software applications, see Procedure 7 “Deploying application software to a COTS or CP PM server” (page 116).

Note 1: Use the **Upgrade** option in the deployment procedure; the previous deployment is displayed at the top of the screen. .

Note 2: You can upgrade the application software after you complete a Linux base upgrade. For information about upgrading applications after performing a Linux base upgrade, see Procedure 10 “Upgrading application software after a Linux base upgrade” (page 132).

35 Deploy any necessary Linux base or base application patches. For more information about patching, see *Patching Fundamentals* (NN43001-407).

When application deployment and patching are finished the upgrade is complete.

--End--

Disaster recovery

"Disaster recovery" (page 83) provides information, prerequisites, and procedures for Nortel Linux system disaster recovery on a COTS or CP PM server.

This chapter contains information and procedures in the following area:

- "Disaster recovery for a Linux base system on a COTS or CP PM server" (page 84)

Disaster recovery fundamentals

A system backup and restore option supports the base disaster recovery.

During a system backup, information for the following applications (if installed) is backed up and is restorable when the applications are reinstalled:

Note: The list of Base and Nortel applications backed up is composed of applications successfully installed prior to the backup. This list contains common applications; your installation can only contain a subset of the applications listed here.

- Base configuration data
- UCM

  UCM backs up the following data:

  — Data pertaining to Element Registry

  — Certificate Authority (if the server is the primary UCM server); certificates and jboss keystore.

  — User and Emergency accounts. If Subscriber Manager is installed, subscriber accounts are also backed up.

  — Configuration files

  — SSH keys
- SNMP

- DM
- SS
- NRS
- CS
  - Data from the last EDD is backed up.
- SIPL
- EM
- SubM
- Intrasystem Signaling Security Solution (ISSS)

Backup data does not back up Nortel logs; however, UCM backs up security logs.

Application-configured system data

You can configure values for routes using Procedure 21 “Adding a route entry” (page 165). You can add or delete host records using Editing DNS IP addresses, host records, and firewall rules using the CLI commands **`routeconfig`**, **`hostconfig`**, and **`basefirewallconfig`**. These values are application-configured system data. Application-configured system data is backed up as part of the system data backup. For more information about Nortel Linux base CLI commands, see “ Nortel Linux base CLI commands” (page 265).

Disaster recovery for a Linux base system on a COTS or CP PM server

Prerequisites

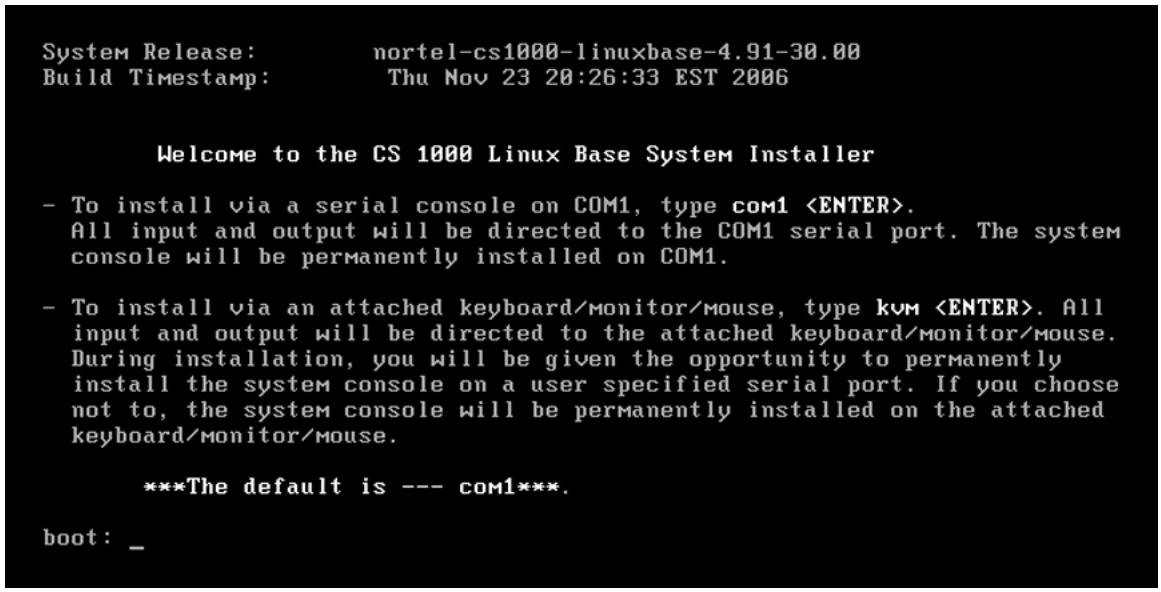
- You must have a system backup file stored on a USB device or SFTP server. Use Procedure 12 “Backing up system data including application data” (page 142) to perform a system back up to an external SFTP or USB source.

Performing disaster recovery for a Nortel Linux server

Step	Action
1	Connect to the CP PM server using the serial console, or to a COTS server using the serial console or keyboard and video monitor (kvm). ***Note:*** If you connect to the IBM x3350 server with a terminal for setup, the server does not function with the serial cable that was previously shipped with the ISP 1100 or other COTS platforms. The IBM x3350 server requires the new NTRX26NPE6 9 pin female to 9 pin female null modem cable. The NTRX26NPE6 9 pin female to 9 pin female null modem cable is displayed in Figure 219 "NTRX26NPE6 9 pin female to 9 pin female null modem cable" (page 250).
2	Insert the Linux base installation media. For CP PM servers, insert the compact flash installation media. For COTS servers, insert the DVD installation media.  **WARNING** The Linux Base DVD should only be inserted in the DVD drive during the Linux Base installation on a COTS server (this does not apply to CP PM servers). Normally the DVD auto-ejects after the Linux base installation is complete. If the Linux base DVD is accidentally left in the DVD drive after installation and a system restart occurs, the system will boot into the installation program. This can be interpreted as a hung system. If this occurs, eject the DVD and restart the system.
3	Restart the server. ***Note:*** For CP PM servers, reseat the CP PM card to ensure a successful restart. When the server boots up, the CS 1000 Linux Base System Installer window appears. For CP PM servers, the CS 1000 Linux Base System Installer window appears as shown in Figure 63 "CS 1000 Linux base system installer (CP PM server)" (page 86). For COTS servers, the CS 1000 Linux Base System Installer window appears as shown in Figure 64 "CS 1000 Linux base system installer (COTS server)" (page 86).

Figure 63
CS 1000 Linux base system installer (CP PM server)

Figure 64
CS 1000 Linux base system installer (COTS server)



4 Type **com1** or press **Enter** to install using a serial console on COM1.

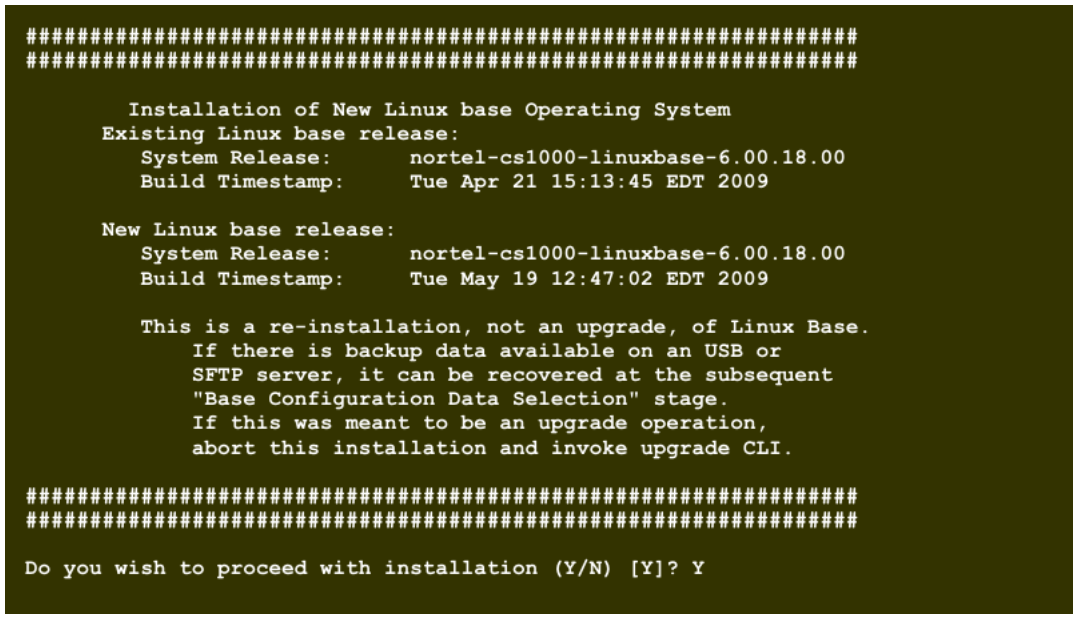
OR

Type **kvm** to install using an attached keyboard and video monitor.

WARNING
If you log on to the COM1 port, make sure that **Caps Lock** is turned off before you log on.

The CS 1000 Linux base system installer confirmation screen appears, as shown in Figure 65 "CS 1000 Linux base system installer confirmation window" (page 87).

Figure 65
CS 1000 Linux base system installer confirmation window



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

From this point forward the disaster recovery procedure uses steps in the upgrade procedure.

6 If you are performing disaster recovery with a new hard drive, or if the /admin partition has been reformatted, proceed to step 6 of "Installing the Linux base on a CP PM or COTS server" (page 41).

OR

If the data stored in the /admin partition is not corrupt and you trust the contents, proceed to step 15 of “Upgrading Nortel Linux base ” (page 65).

> ***Note:*** If you are performing disaster recovery with a new hard drive, or if the /admin partition has been reformatted, you must select option 2 (USB) or option 3 (SFTP) as the data source in step 7 of “Installing the Linux base on a CP PM or COTS server” (page 41).If the data stored in the /admin partition is not corrupt, you must select option 1 (/admin partition), option 2 (USB), or option 3 (SFTP) as the data source in step 19 of “Upgrading Nortel Linux base ” (page 65).

Proceed with the remaining upgrade steps to complete the recovery.

> ***Note:*** The disaster recovery process is not complete until you perform application deployment and patch deployment. The upgrade procedure provides directions for completing both of these tasks.

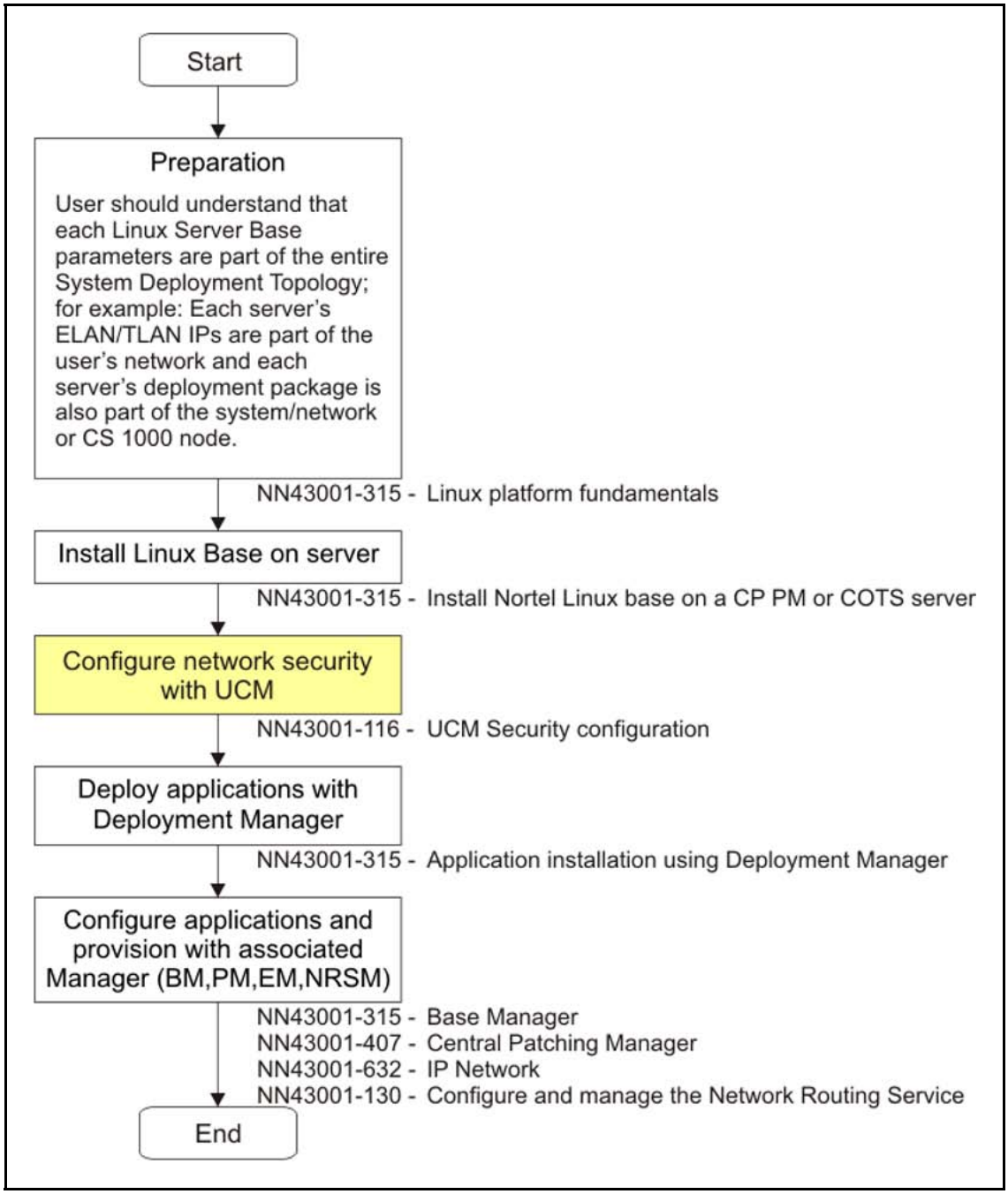
--End--

UCM overview

UCM network security configuration workflow stage

"UCM overview" (page 89) contains information and references you need to perform Unified Communications Management (UCM) security configuration . Figure 66 "UCM network security configuration workflow stage" (page 90) shows the position of UCM network security configuration in the overall workflow.

Figure 66
UCM network security configuration workflow stage



UCM overview

UCM is a collection of system management tools. UCM provides a consistent methodology and interface to perform system management tasks. System management tools are Web-based system management solutions supported by the UCM framework.

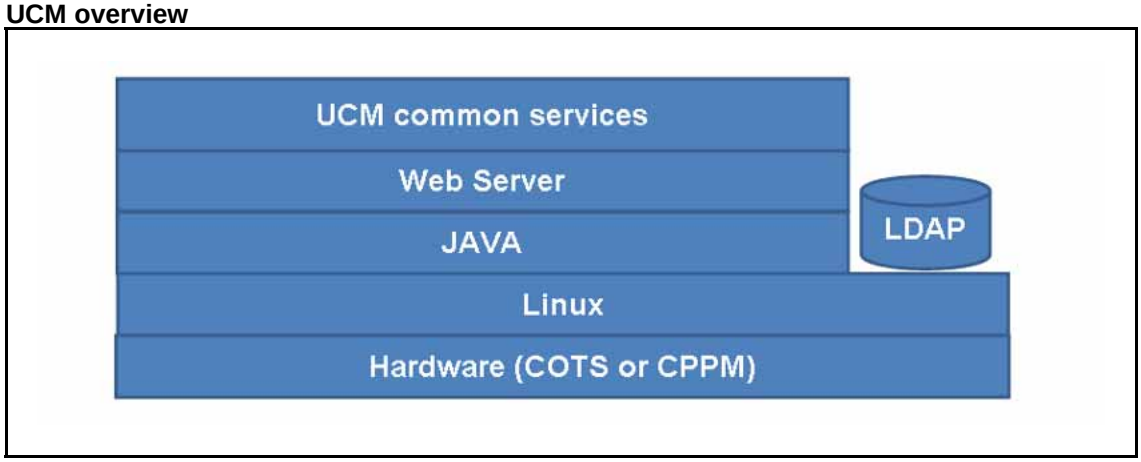
Installed on every Nortel Linux base operating system is a Web server with extended security features that forms the basis for UCM and provides the following key features:

- Central element registry for all elements
- Authorization and authentication functionality
- Single sign on across application and hardware platforms
- PKI management
- RADIUS support
- External authentication support

Note: Support terminals not connected to the DNS domain must modify their local host files to gain initial access to UCM. For more information about managing local host files, see the section *SSO using FQDN without DNS infrastructure in the logon and logoff options* in *Unified Communications Management* (NN43001-116).

Figure 67 "UCM overview" (page 91) shows UCM on a Nortel Linux base system.

Figure 67
UCM overview

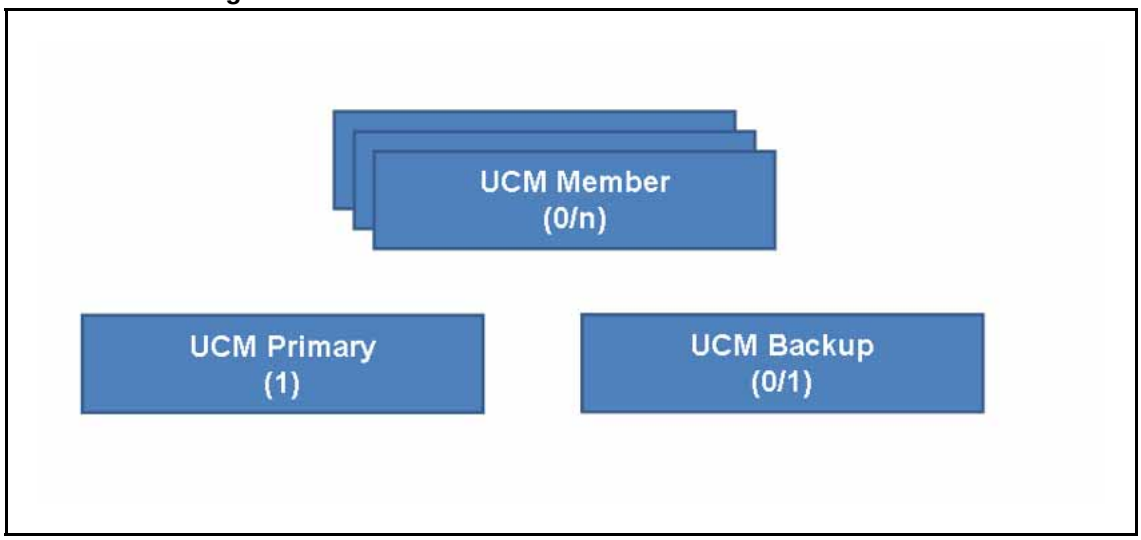


You can configure UCM in one of the following ways:

- Primary security server
- Backup security server
- Member security server

Every security domain must have one primary security server. The security domain can have one or no backup servers; additional servers are member servers.

Figure 68
UCM server configurations



UCM framework is installed and run on all CS 1000 Linux platforms (CP PM and COTS). Management applications are packaged as Web Archive (WAR) files and load into the UCM framework.

CS 1000 management applications are auto-deployed, other applications are deployed as required.

- Auto-deployed to the UCM server
  - Base Manager: Provides local Web management for Linux base.
  - Deployment Manager: Enables application installations and upgrades. Deployment Manager is centrally accessible from the Primary security server or locally on the target server.
  - Patching Manager: Provides Web-based patch delivery. Patching Manager is centrally accessible from the primary security server or locally on the target server.
  - IPSec Manager: Provides centralized Web-based IPSec management.
  - SNMP: Provides centralized Web-based fault management.
- User deployed

— Element Manager: Provides traditional CS 1000 Web-based management, including Call Server overlay support.

— Network Routing Service Manager

— Subscriber Manager

— Signaling Server (virtual trunks, Terminal Proxy Server)

— SIP Line

Figure 69 "UCM application deployment" (page 93) shows application deployment on UCM servers.

Figure 69
UCM application deployment

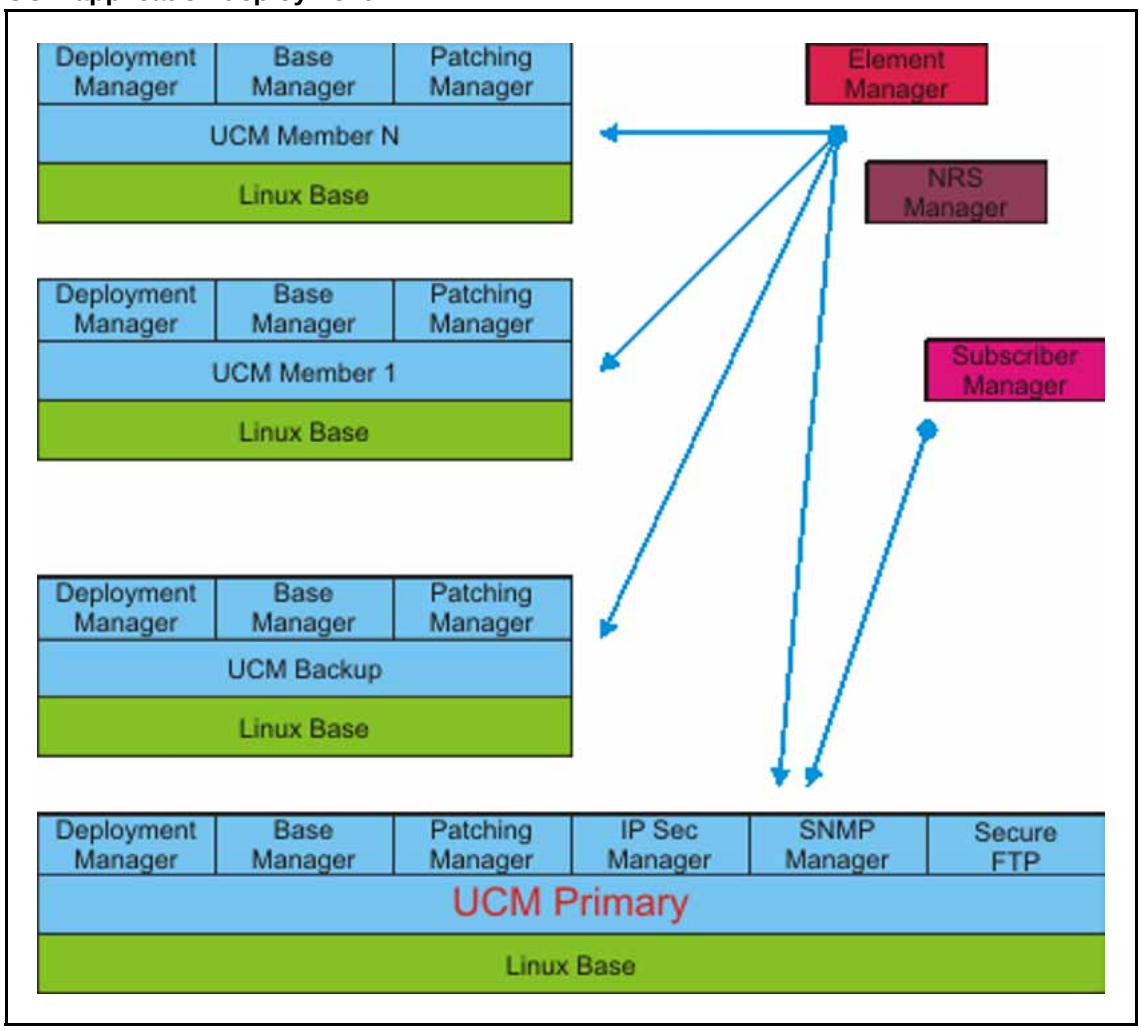
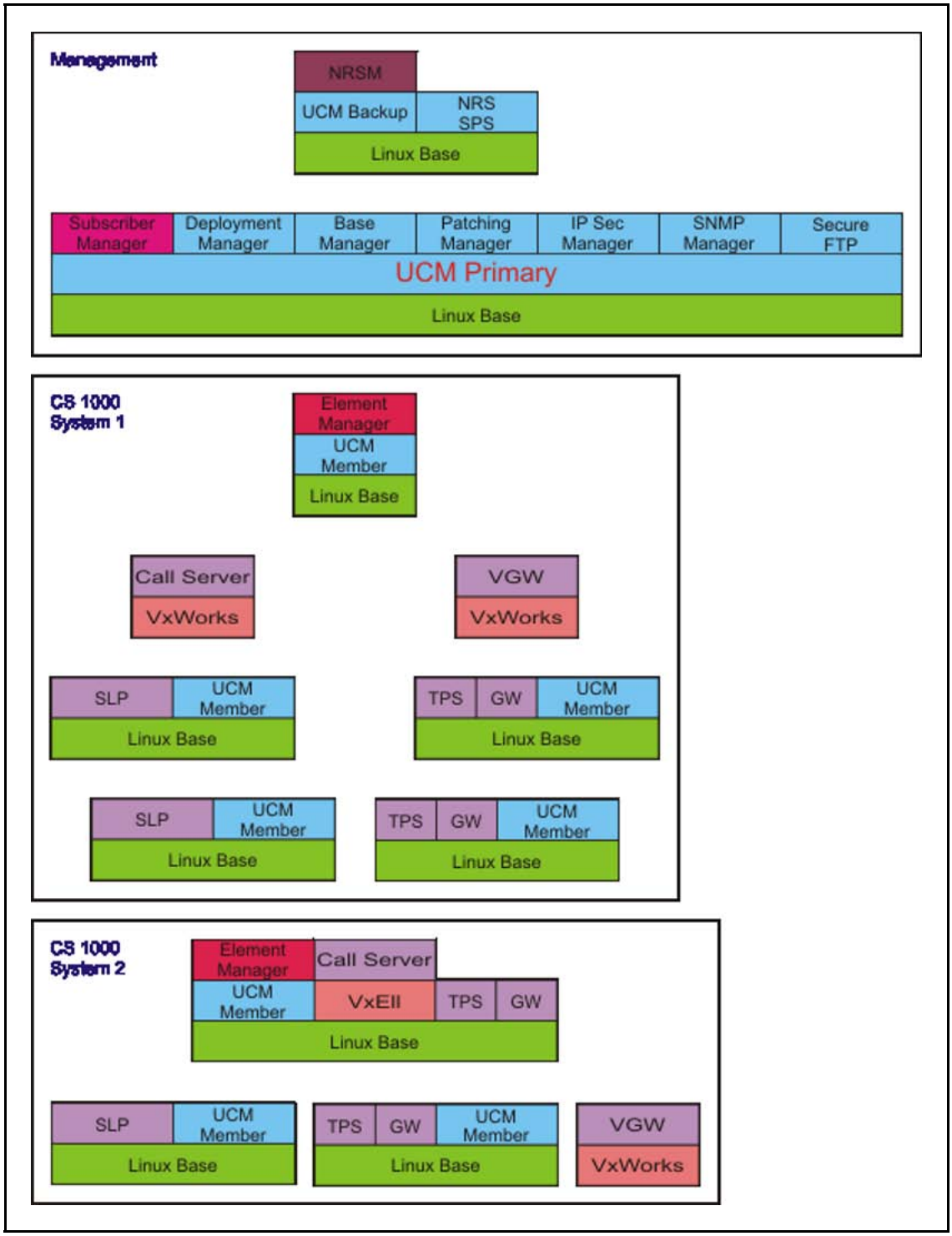


Figure 70 "Physical deployment of UCM" (page 95) provides an example of system management components deployed in a typical installation. Network and engineering analysis determines the location of the UCM primary and backup servers. Typically EM is deployed physically close to the Call Server it manages.

Figure 70
Physical deployment of UCM



The UCM Graphical User Interface (GUI) is shown in Figure 71 "UCM graphical view" (page 96).

Figure 71
UCM graphical view

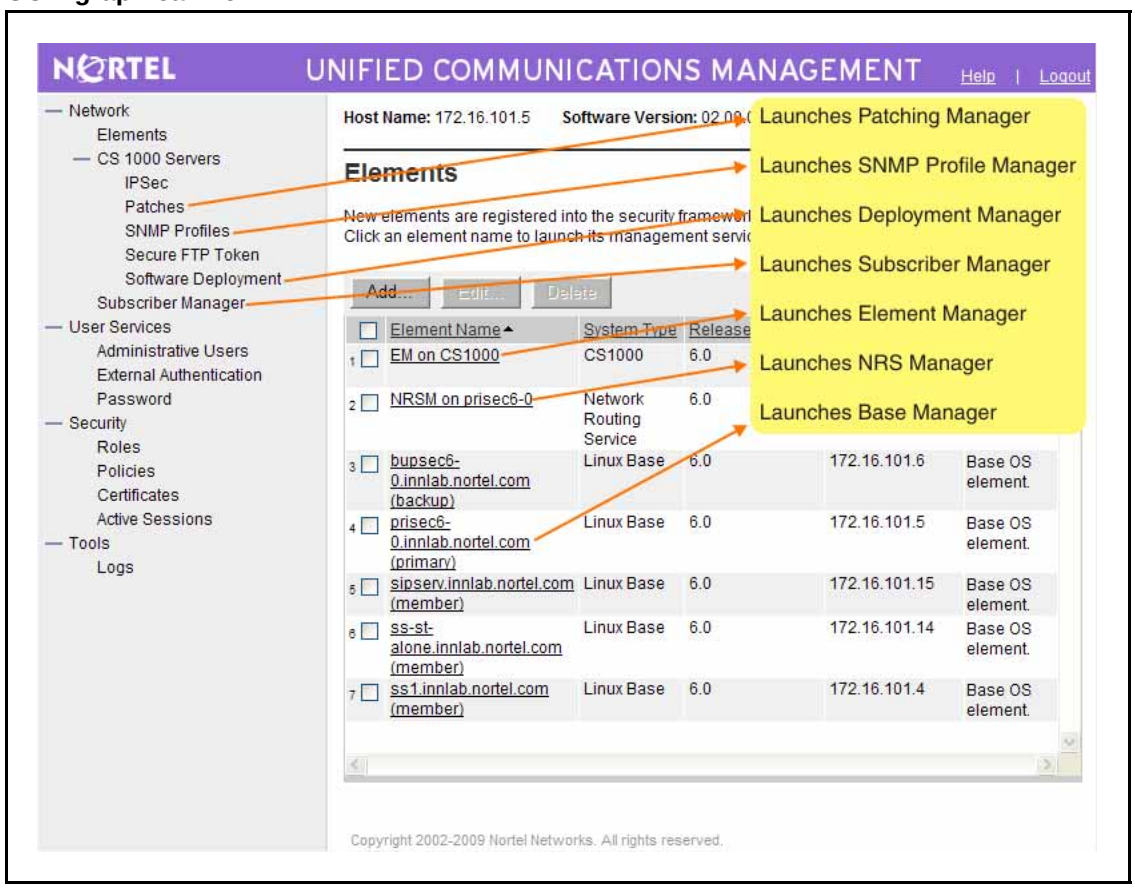
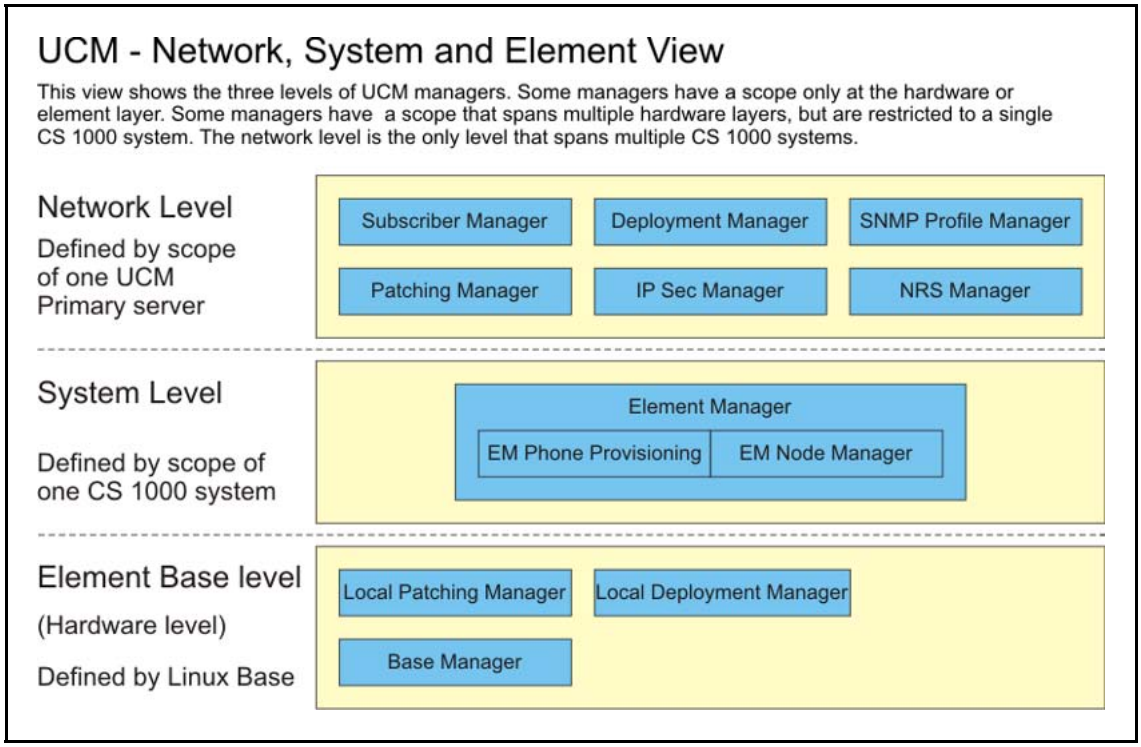


Figure 72 "UCM management levels" (page 97) illustrates the three levels of UCM management.

Figure 72
UCM management levels



For detailed information about the components, features, and benefits of Unified Communications Management, see *Unified Communications Management* (NN43001-116).

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.

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 major base applications:

- Unified Communications Management (Jboss-Quantum)
- Base Manager (BM)
- Unified Communications Management (UCM)
- Nortel Simple Network Management Protocol (SNMP)
- Deployment Manager

- Patching Manager (PM)
- ISECSH

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

The choice of deployment package is limited by the type of server you are using, and whether the server will be a primary security server. Table 4 "Valid deployment package and server combinations" (page 100) shows the valid deployment packages for each type of server.

Table 4
Valid deployment package and server combinations

Deployment package	COTS server (primary security server)	COTS server (member or backup security server)	CP PM server (primary security server)	CP PM server (member or backup security server)
SS	YES	YES	YES	YES
NRS	YES	YES	YES	YES
SS + NRS	YES	YES	YES	YES
CS + SS + EM	NO	NO	YES	YES
CS + SS + NRS + EM	NO	NO	YES	YES
SIPL	YES	YES	YES	YES
EM	YES	YES	YES	YES
SubM	YES	NO	YES	NO

Note 1: Table 4 "Valid deployment package and server combinations" (page 100) shows which deployment packages you can deploy on the various types of servers, based on hardware platform type or UCM

security server role. However, a deployment package may not be suitable for a server even if it is deployable. Network topology and system capacity influence the choice of a deployment package for a server. For example, a large system may not function efficiently if you deploy SS, SS + NRS, NRS, or SIPL to the primary or backup security server.For information about system planning and engineering that pertains to the above deployment considerations, see *Planning the Network-Wide Upgrade* (NN43001-406) and *Communication Server 1000E Planning and Engineering (Conceptual)* (NN43041-220).

Note 2: It is possible to deploy more than one EM pointing to a Call Server using Deployment Manager, but the EM Phone provisioning application (Phones) does not support this. For more information about deploying EM, see *Element Manager System Reference - Administration* (NN43001-632).

Deployment package selection begins by choosing a deployment package from the following list:

- SS
- NRS
- SS + NRS
- CS + SS + EM
- CS + SS + NRS + EM
- SIPL
- EM
- SubM

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:

Supported deployment configurations

- SubM
- EM
- SS
- SS and EM
- NRS
- SS and NRS

- SS + NRS and EM
- SS, EM, and SubM
- CS + SS + EM
- CS + SS + NRS + EM
- SIPL
- CS + SS + NRS, EM, and SubM

You can encounter errors during application deployment. For a list of deployment errors, error descriptions, and user actions, see "Deployment errors" (page 275).

Centralized deployment has the following limitations:

- You can only deploy predetermined application deployment packages. Once you choose a deployment package you can only choose additional packages that are compatible with the previous selection.
- You can only upgrade the deployed applications; you cannot change the configuration using the upgrade procedure.
- Deployment of VxWorks servers is not supported.
- Application deployment for each server in the security domain is done individually. However, you can perform up to 3 deployments at the same time.
- Each application must be configured individually after deployment.
- There can be a temporary connection loss during deployment. UCM requires a J-Boss restart to register new plug-ins.
- A maximum number of 3 software loads can reside on the server simultaneously.
- IP connectivity is required to preform central deployment.

Deployment Manager access is controlled by Unified Communications Management (UCM); you must be granted Allow access to deployment manager permission for the element of type Software Deployment (or All elements of type: Deployment Manager). To deploy or restore applications on a Linux server, you must have system administrator privileges for that particular Linux base element (or All elements of type: Linux Base). To perform application backup on a Linux server, you must have system administrator or backup administrator privileges for that particular Linux base element (or All elements of type: Linux Base).

For more information about user roles in UCM, see *Unified Communications Management Fundamentals* (NN43001-116).

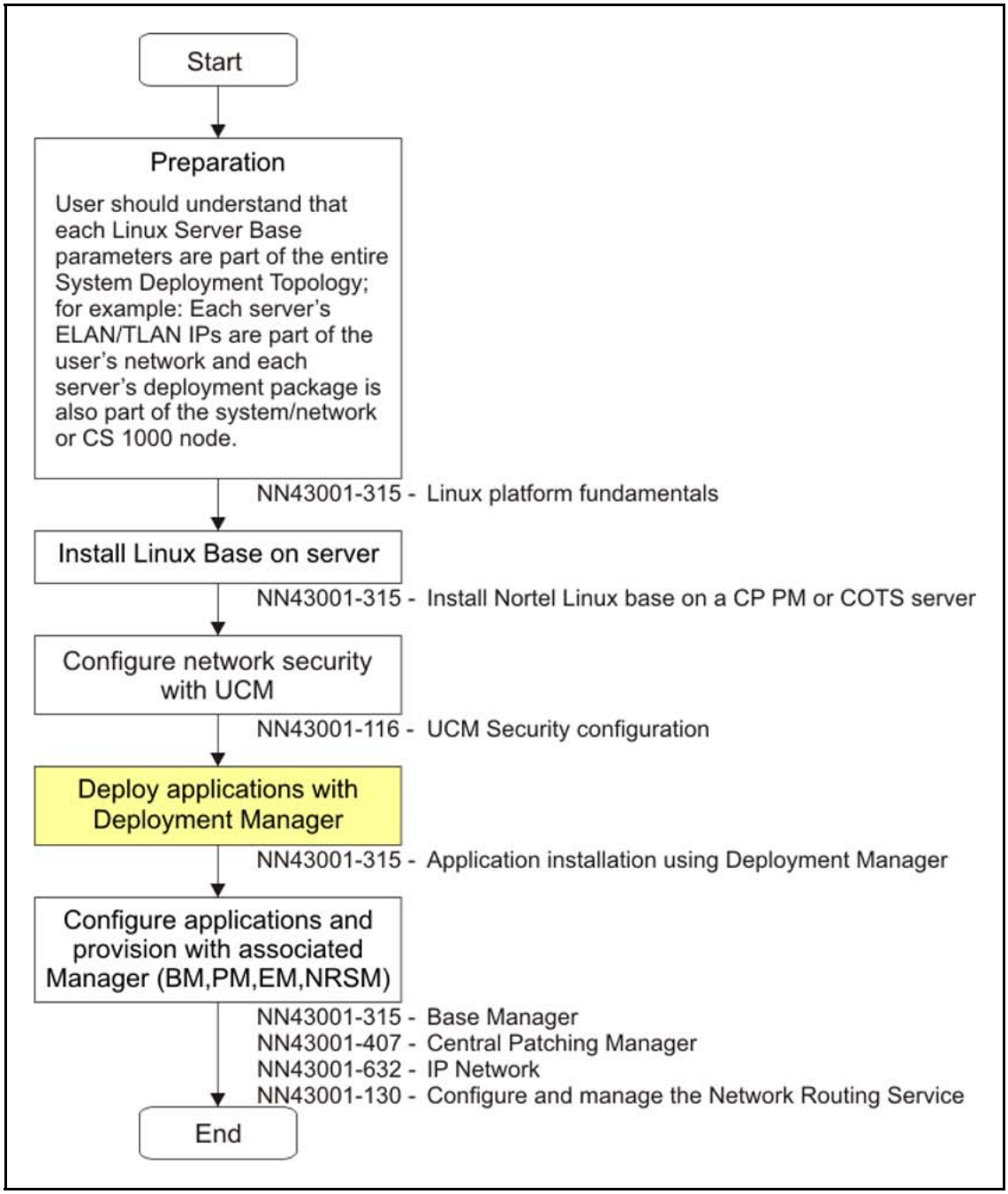
Application installation workflow stage

"Application installation using Deployment Manager" (page 99) contains information, references, and procedures you need to perform application deployment using Local or Central Deployment Manager. Figure 73 "Application installation using Deployment Manager" (page 104) shows the position of application installation in the overall workflow.

This chapter provides application deployment information in the following areas:

- "Access Unified Communications Management" (page 104)
- "Access the centralized software Deployment Manager" (page 105)
- "Access the Local Deployment Manager" (page 106)
- "Software loads" (page 108)
- "Software deployment" (page 116)
- "Application software undeployment" (page 127)
- "Application software upgrades" (page 130)
- "System data backup including application data" (page 142)
- "Restore system data including application data" (page 145)
- "System data backup management" (page 147)

Figure 73
Application installation using Deployment Manager



Access Unified Communications Management

You must access UCM to perform application deployment using Centralized Deployment Manager.

Procedure 2
Logging on to UCM

Step	Action
1	Open the Web browser.
2	Enter one of the following in the Address bar, and then press **Enter**: • FQDN for the UCM server (preferred). • Unified Communications Management (UCM) framework IP address—After you enter the UCM framework IP address, a Web page appears stating that you must access Unified Communications Management 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 user ID.
5	In the **Password** field, enter your password.
6	Click **Log In**. The default navigation Web page for UCM appears.

--End--

Access the centralized software Deployment Manager

Use Procedure 3 “Accessing the centralized software Deployment Manager” (page 105) to deploy software applications from a central server.

Note: The server must be part of the security domain before you can perform central deployment. For a more details about UCM configuration of primary, backup, and member servers, see *Unified Communications Management* (NN43001-116). For more information about security management, see *Security Management Fundamentals* (NN43001-604).

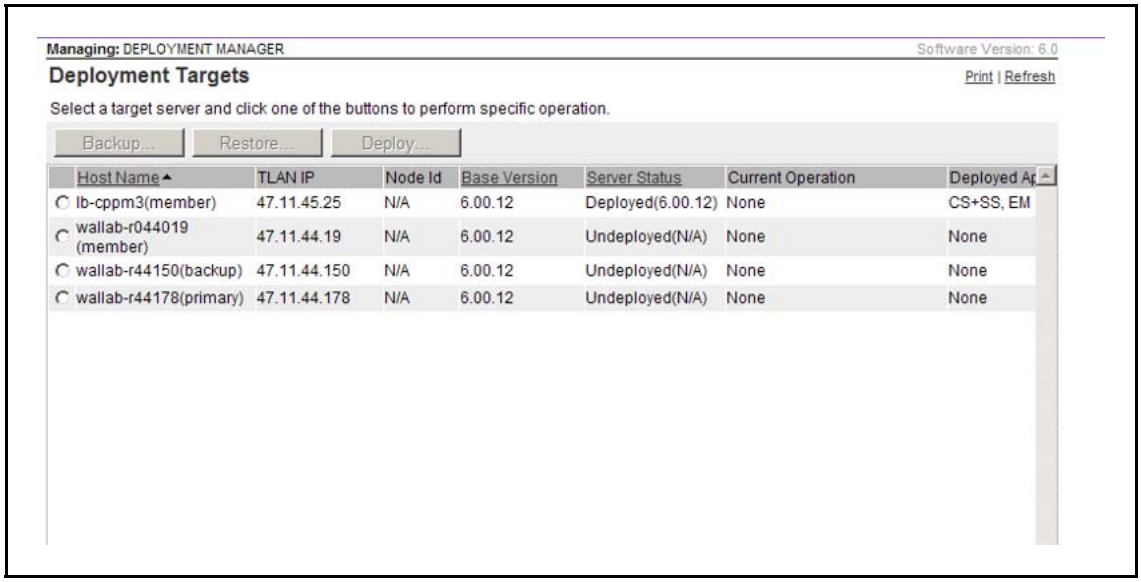
Procedure 3
Accessing the centralized software Deployment Manager

Step	Action
1	Log on to UCM. See Procedure 2 “Logging on to UCM” (page 105).

2 In the navigation pane, click **Network**, **CS 1000 Services**, **Software Deployment**.

The Deployment Manager screen appears, as shown in Figure 74 "Deployment Manager window" (page 106).

Figure 74
Deployment Manager window



--End--

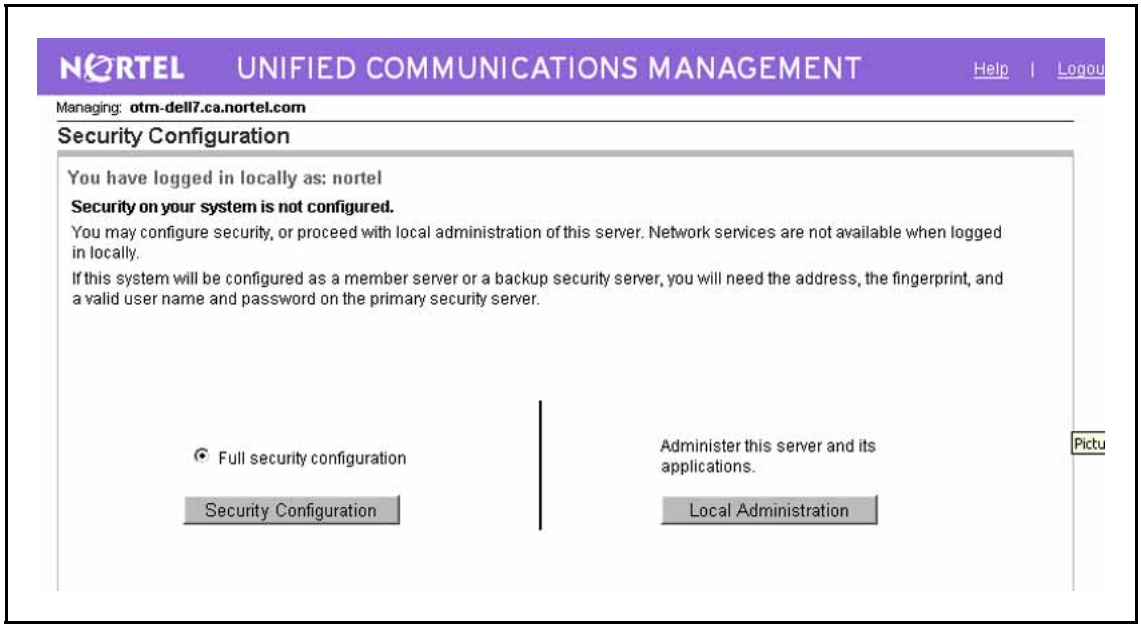
Access the Local Deployment Manager

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 join the security domain, local deployment information is recognized by the Central Deployment Manager. For information about joining the security domain, see *Unified Communications Management* (NN43001-116).

Accessing the Local Deployment Manager

Step	Action
1	Log on to the server using the nortel user ID and password. The Security Configuration screen appears, as shown in Figure 75 "Security Configuration window" (page 107).

Figure 75
Security Configuration window



2 Click **Local Administration**.

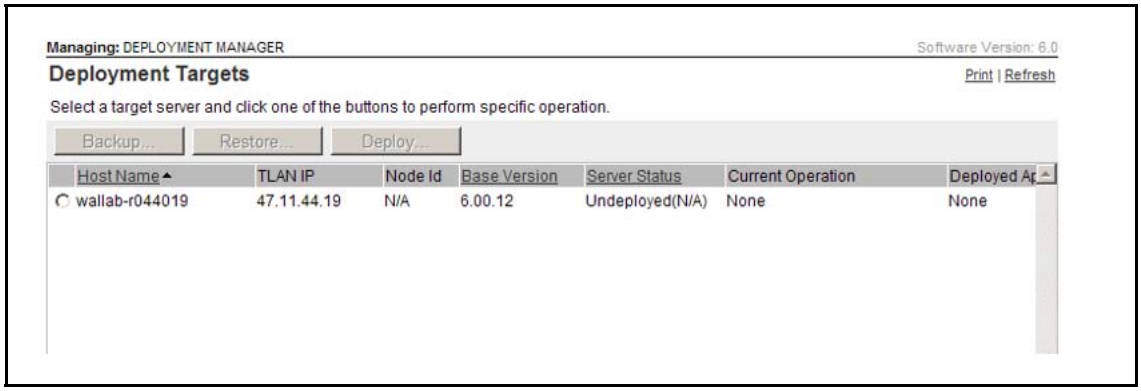
The Base Manager screen appears, as shown in Figure 76 "Base Manager window" (page 107).

Figure 76
Base Manager window

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

The Deployment Manager screen appears, as shown in Figure 77 "Deployment Manager window" (page 108).

Figure 77
Deployment Manager window



--End--

Software loads

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

- 6xx 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.

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.

This section provides procedures for 2 methods of adding a software load.

- Procedure 4 “Adding a new software load to the Deployment Manager from the client machine” (page 109)
- Procedure 5 “Adding a new software load to the Deployment Manager from a deployment server” (page 112)

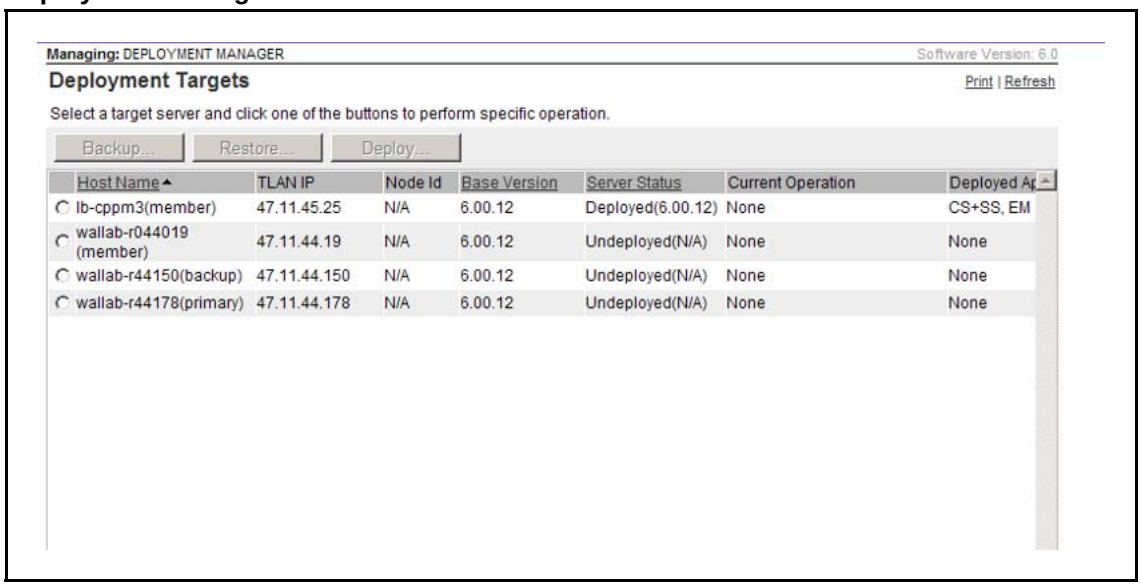
Software loads added from the client machine

Use Procedure 4 “Adding a new software load to the Deployment Manager from the client machine” (page 109) to add a software load from the client machine.

Procedure 4
Adding a new software load to the Deployment Manager from the client machine

Step	Action
1	In the navigation pane, click **Network**, **CS 1000 Services**, **Software Deployment**. The Deployment Manager screen appears, as shown in Figure 78 "Deployment Manager window" (page 109).

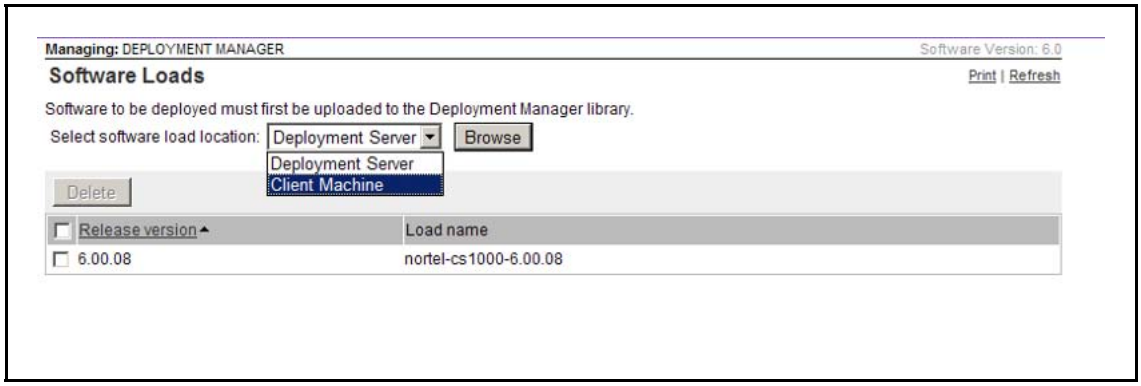
Figure 78
Deployment Manager window



2	In the navigation pane, click **Software Loads**.

The Software Loads page appears, as shown in Figure 79 "Software Loads window" (page 110).

Figure 79
Software Loads window

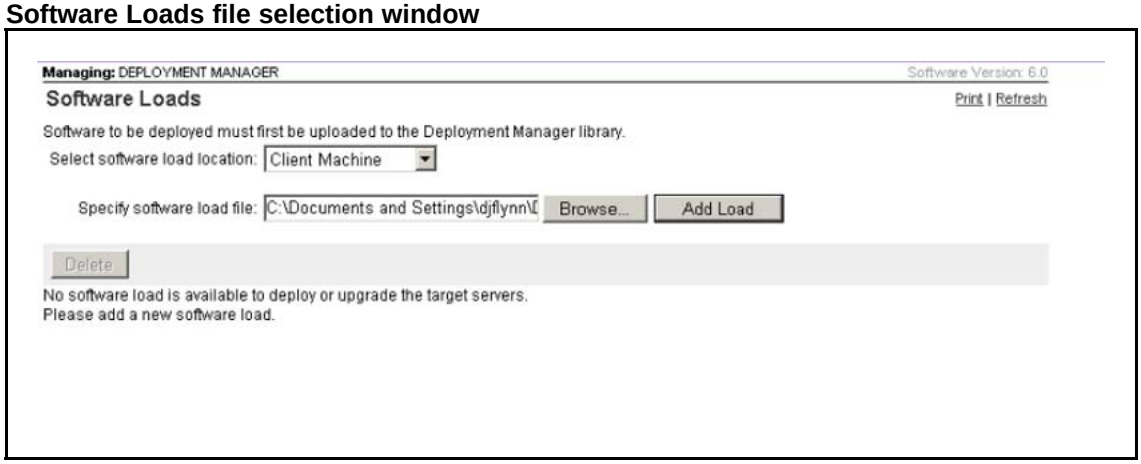


3 In the Select software load location list, select **Client Machine**.

4 In the **Specify software load file** field, click **Browse** to browse to the location of the software load file.

The **Add Load** button activates, as shown in Figure 80 "Software Loads file selection window" (page 110).

Figure 80
Software Loads file selection window



5 Click **Add Load**.

An upload progress screen appears, as shown in Figure 81 "Software upload progress window" (page 111). When the upload is complete the software load appears, as shown in Figure 82 "Software Loads window" (page 111).

Figure 81
Software upload progress window

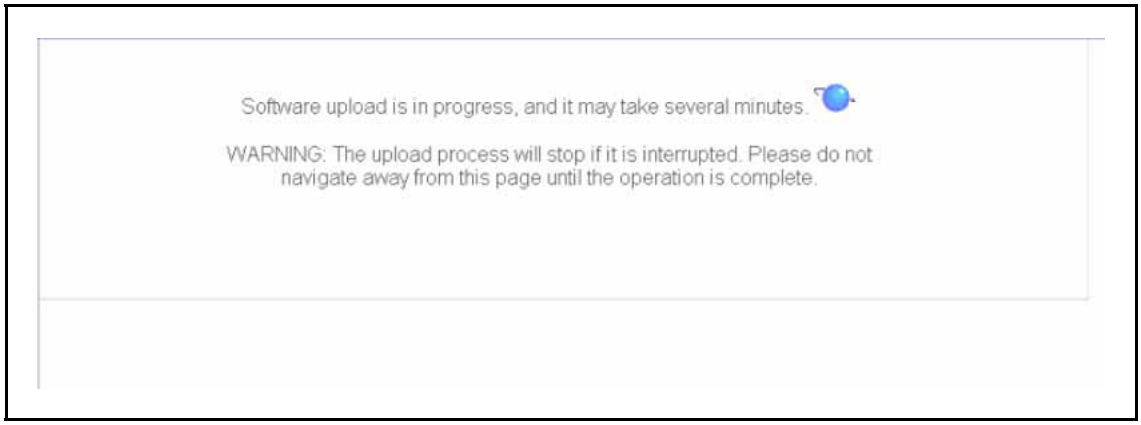


Figure 82
Software Loads window

--End--

Software loads added from a deployment server

Use Procedure 5 “Adding a new software load to the Deployment Manager from a deployment server” (page 112) to add a software load from a deployment server.

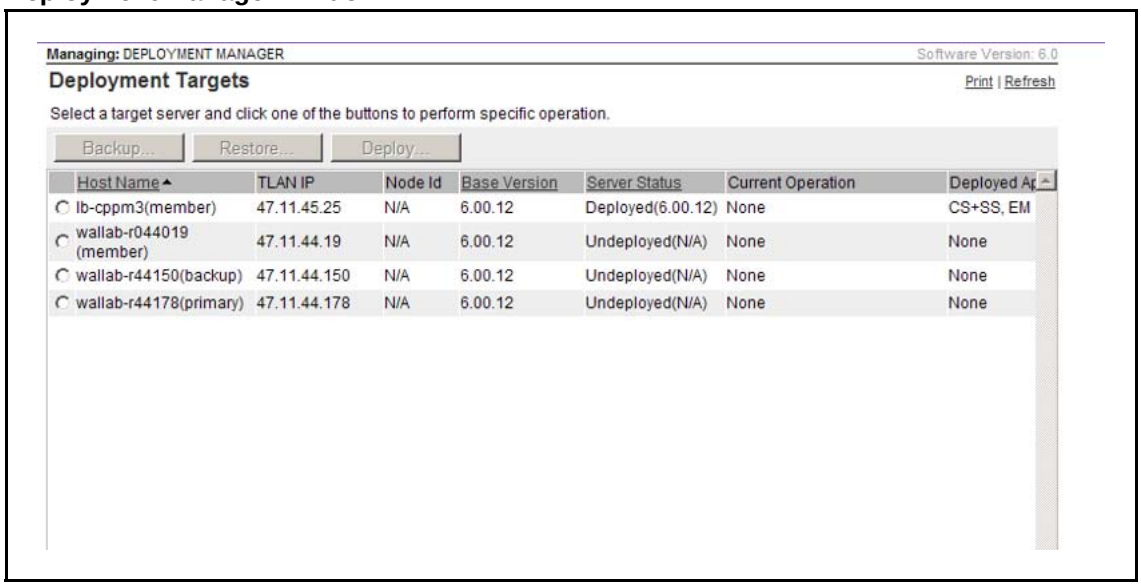
Prerequisites

- You must have the correct software media (CD/DVD/CF/USB).

Procedure 5
Adding a new software load to the Deployment Manager from a deployment server

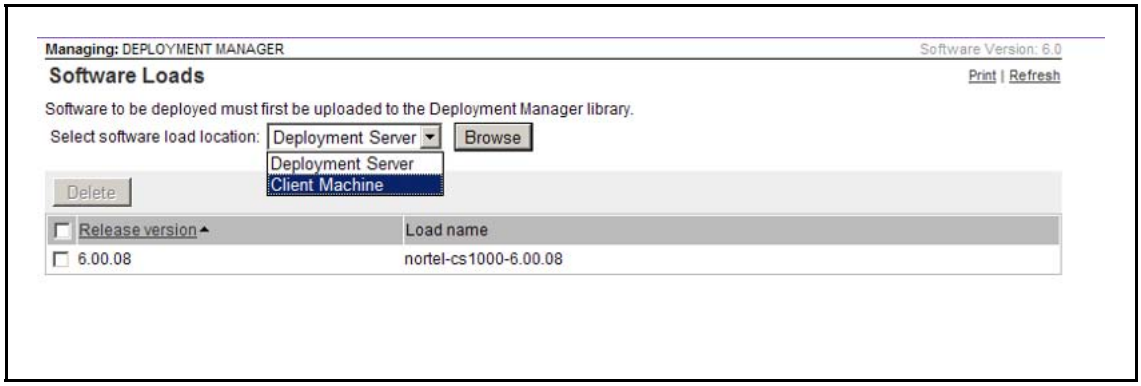
Step	Action
1	In the navigation pane, click **Network**, **CS 1000 Services**, **Software Deployment**. The Deployment Manager screen appears, as shown in Figure 83 "Deployment Manager window" (page 112).

Figure 83
Deployment Manager window



2	In the navigation pane, click **Software Loads**. The Software Loads page appears, as shown in Figure 84 "Software Loads window" (page 112).

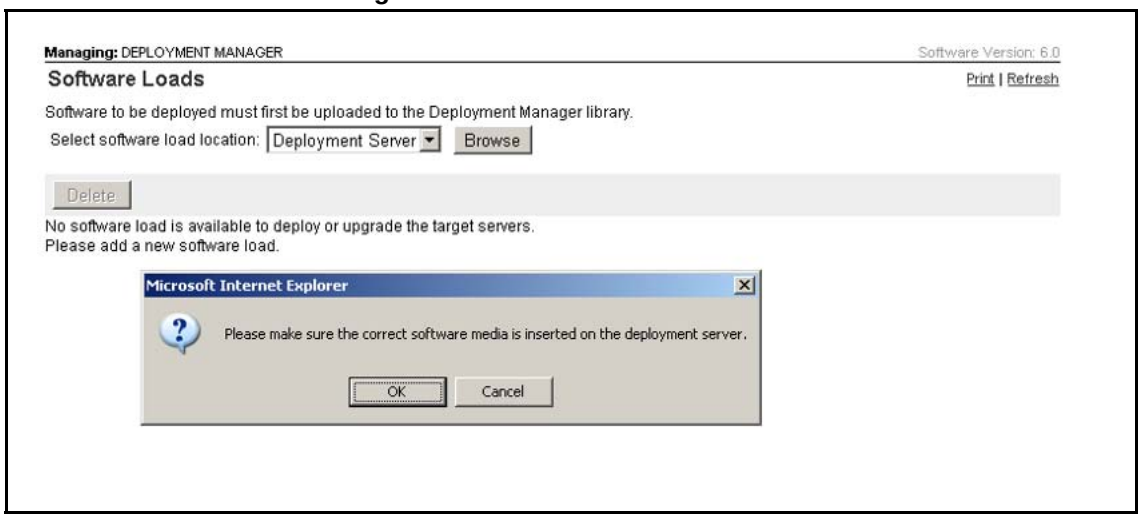
Figure 84
Software Loads window



3	In the Select software load location list, select **Deployment Server**.

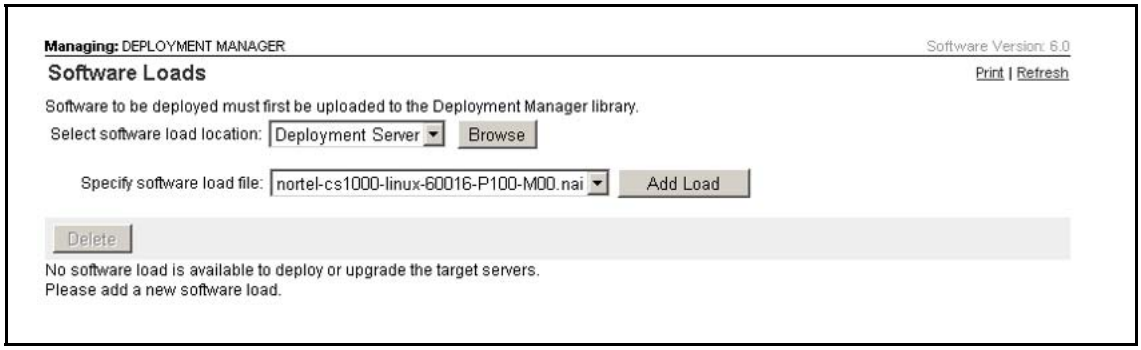
A warning screen appears, as shown in Figure 85 "Software loads media warning window" (page 113).

Figure 85
Software loads media warning window



4 Click **OK**.

The Specify software load file field appears in the Software Loads screen, as shown in the following figure:



5 In the Specify software load file list, select a value for the software load file.

6 Click **Add Load**.

An upload progress screen appears, as shown in Figure 86 "Software upload progress window" (page 114). When the upload is complete the software load appears, as shown in Figure 87 "Software Loads window" (page 114).

Figure 86
Software upload progress window

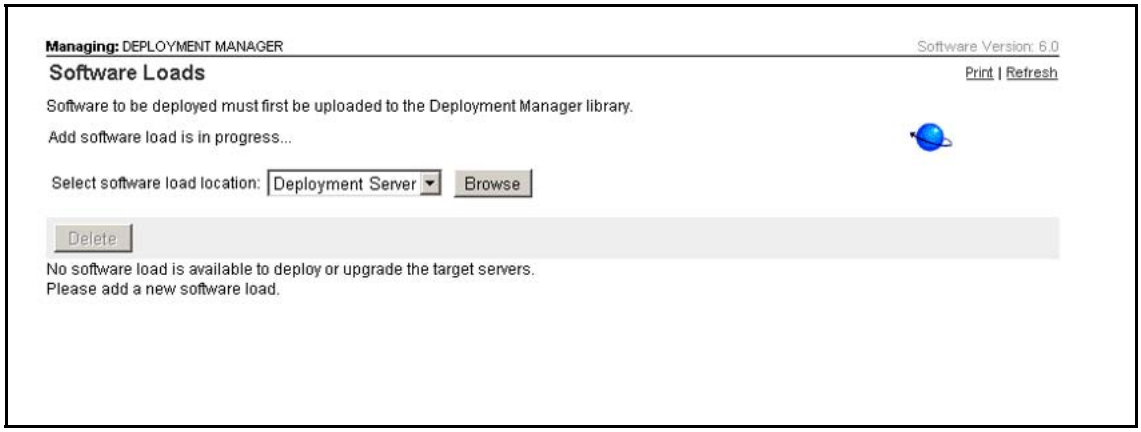
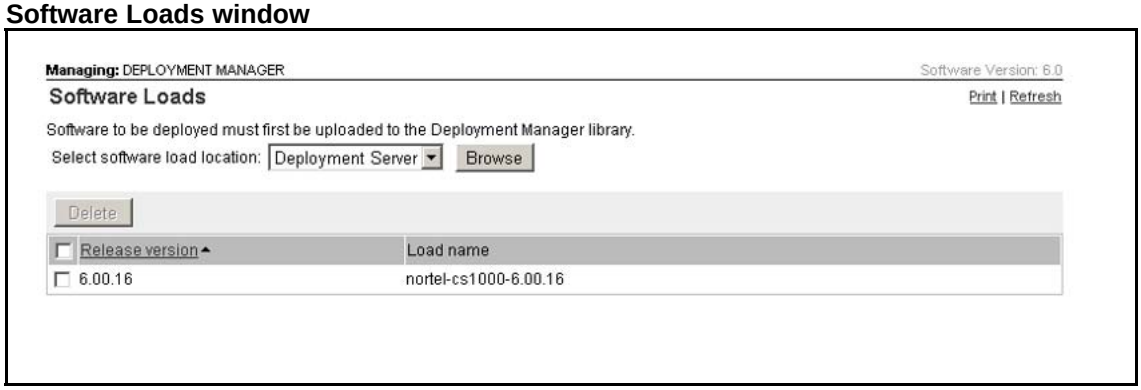


Figure 87
Software Loads window



--End--

Delete a software load from the Deployment Manager

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

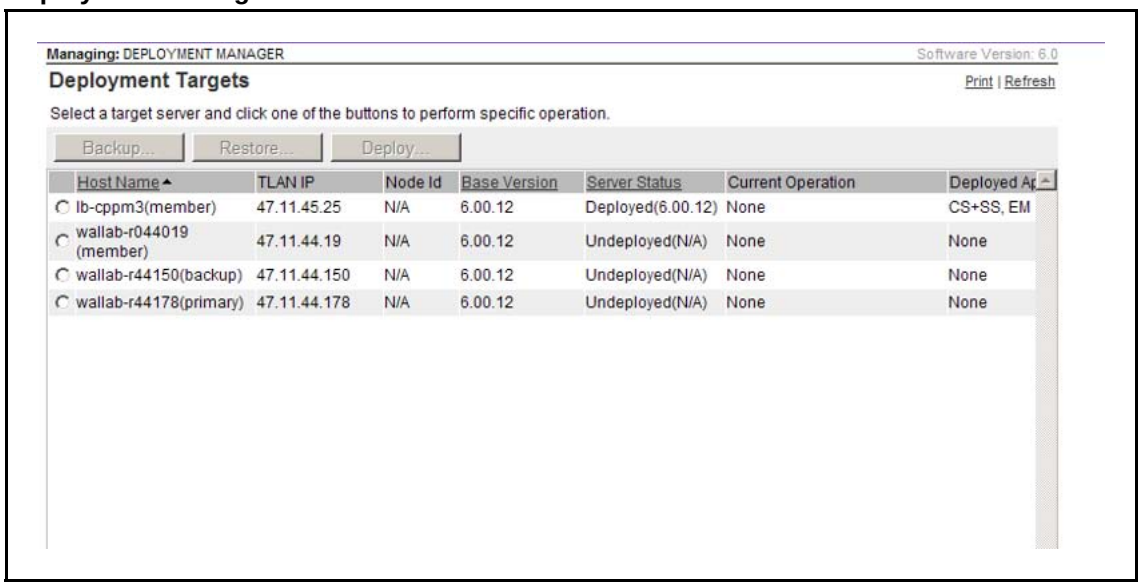
Note: Nortel recommends that before the server joins the UCM security domain, you delete software loads added in a local deployment scenario. Software loads added during local deployment are not visible from Deployment Manager after the server joins the UCM security domain.

Procedure 6
Deleting a software load from the Deployment Manager

Step	Action
1	In the navigation pane, click **Network**, **CS 1000 Services**, **Software Deployment**.

The Deployment Manager screen appears, as shown in Figure 88 "Deployment Manager window" (page 115).

Figure 88
Deployment Manager window



2 In the navigation pane, click **Software Loads**.

The Software Loads page appears, as shown in Figure 89 "Software Loads window" (page 115).

Figure 89
Software Loads window

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

4 Click **Delete**.

--End--

Software deployment

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

Deploy application software to a COTS or CP PM server

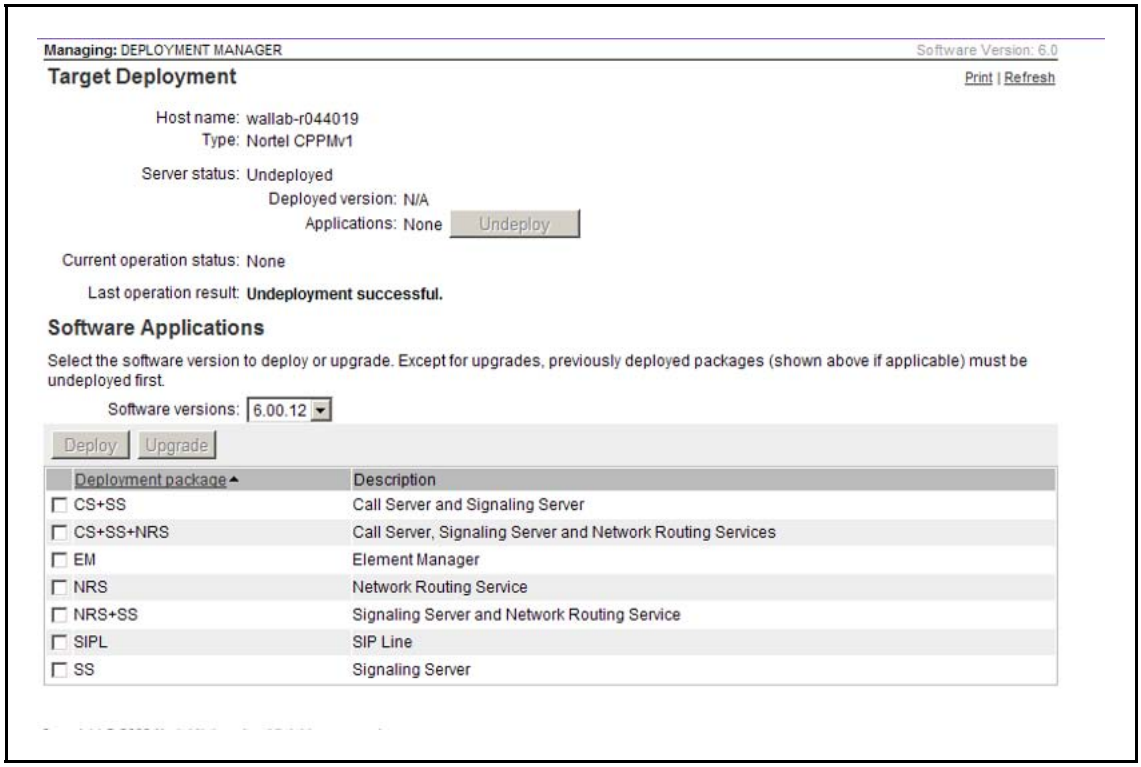
Prerequisites

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

Procedure 7
Deploying application software to a COTS or CP PM server

Step	Action
1	On the UCM Login page, enter the User ID and Password.
2	Click **Log In**.
3	In the navigation pane, click **Network**, **CS 1000 Services**, **Software Deployment**, **Deployment Targets**.
4	Select the target for deployment. ***Note:*** The target server must have a status of **Undeployed**.
5	Click **Deploy**. Target information and available software applications are displayed, as shown in Figure 90 "Target Deployment and Software Applications window" (page 117).

Figure 90
Target Deployment and Software Applications window



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

7 Select a deployment package to deploy.

WARNING
EM is not part of the SS deployment package; EM must be selected in addition to SS if it is required. For additional information about system planning, see *Planning the Network-wide Upgrade* (NN43001-406).

Note: Deployment packages are platform dependant; the platform of the target server influences which deployment packages are available. For more information on deployment packages see Table 4 "Valid deployment package and server combinations" (page 100).

8 Select any additional deployment packages that you want to deploy. Only deployment packages that are valid in combination with the previously selected deployment package are available for selection. For a list of supported deployment package configurations, see "Supported deployment package configurations" (page 101) .

9 Click **Deploy**.

ATTENTION

If you chose a deployment package that includes Call Server and Element Manager, proceed to steps 10. If you chose a package that does not include Call Server but does include Element Manager, proceed to step 29. If you did not choose a deployment package that includes Call Server or Element Manager the deployment completes and the deployed packages are displayed in the Target Deployment screen, as shown in Figure 91 "Target Deployment window" (page 118).

In the Target Deployment screen you can click the **deployment summary** link to display a summary screen, as shown in Figure 92 "Deployment Summary window" (page 119).

Figure 91
Target Deployment window

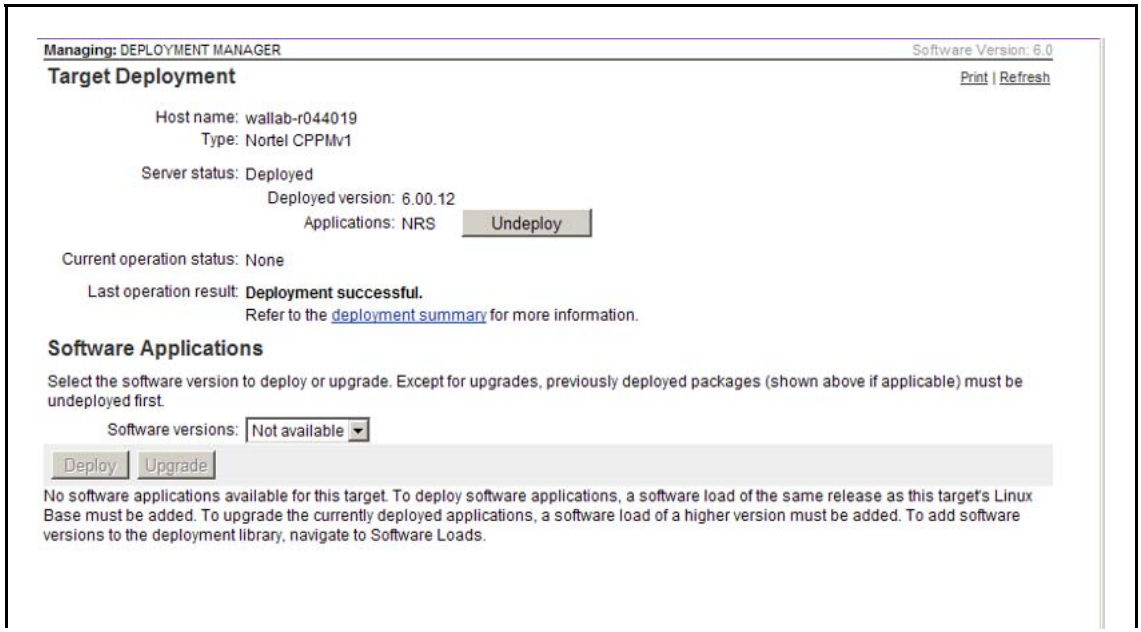
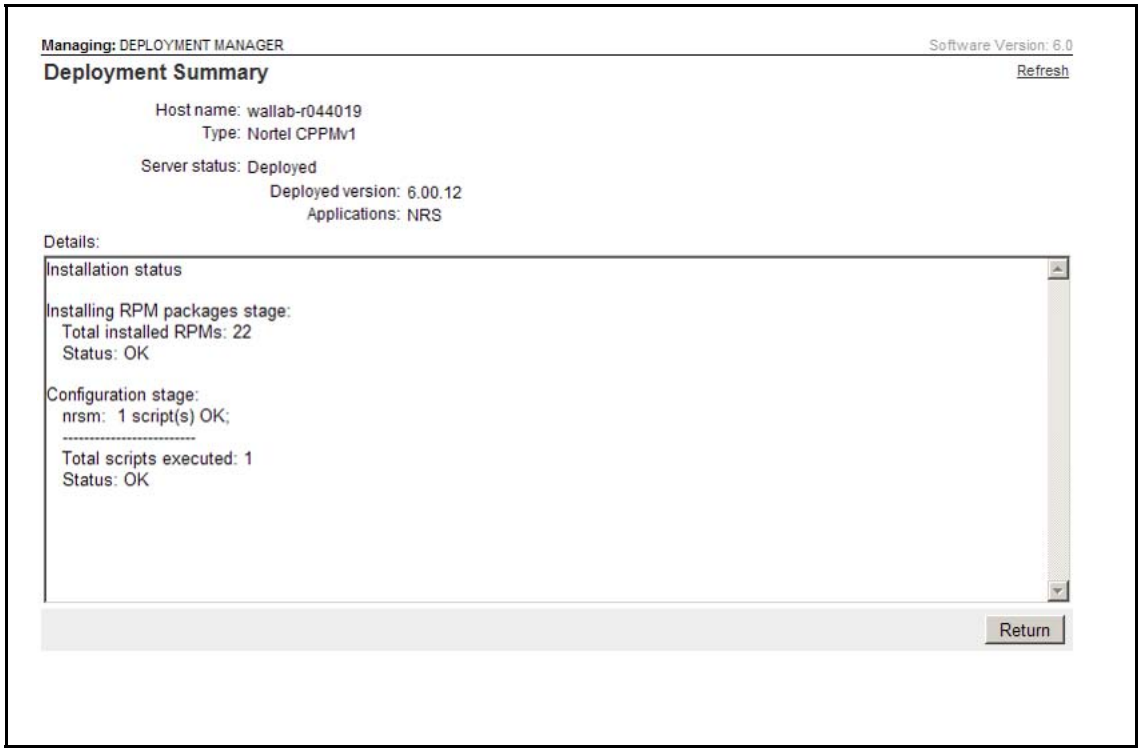


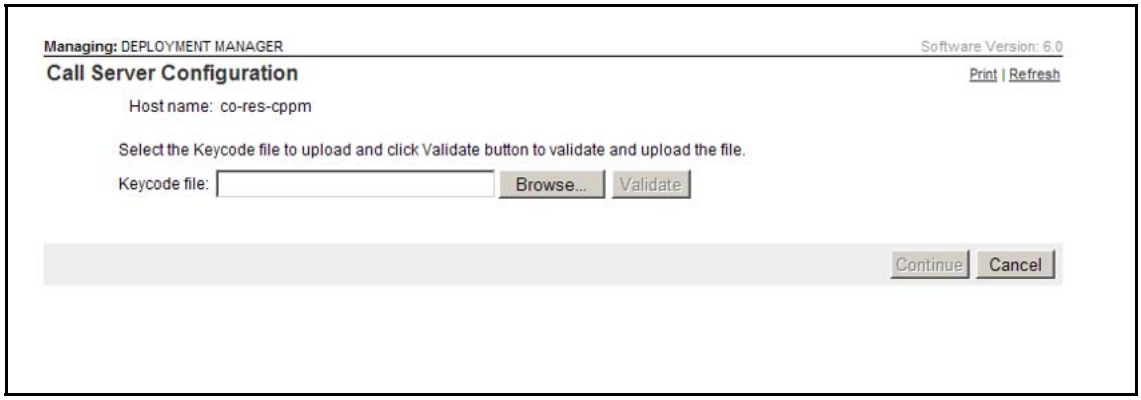
Figure 92
Deployment Summary window



.

10 If you choose a package that includes Call Server, the Call Server Configuration screen appears, as shown in Figure 93 "Call Server Configuration window" (page 119). For details on pre-configuring the Call Server, see Call server keycode validation and preconfiguration

Figure 93
Call Server Configuration window

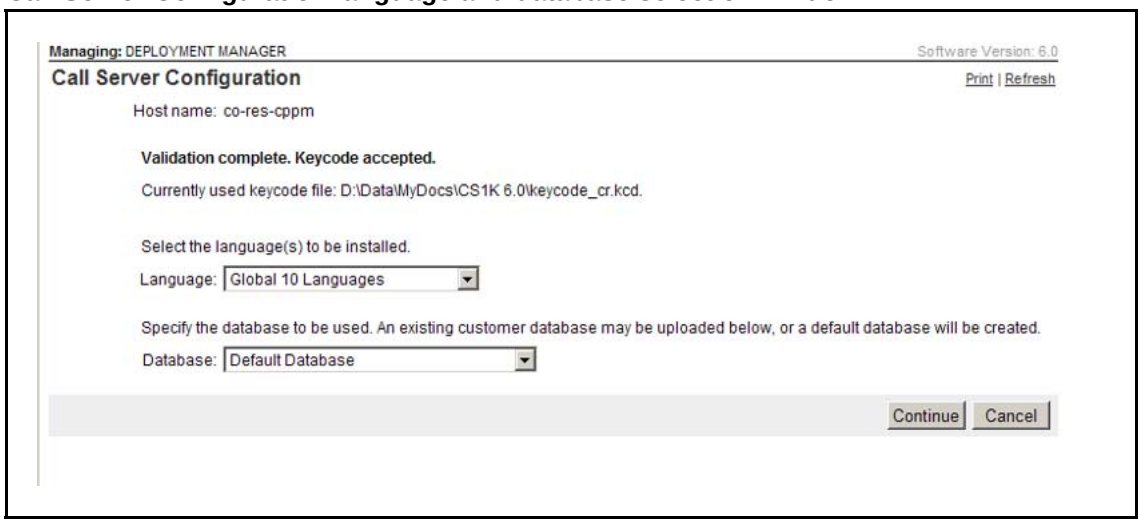


11 In the **Keycode file** box, click **Browse** to browse for the keycode file.

12 Click **Validate** to validate the file selection.

After the keycode file validates successfully, language and database options are displayed, as shown in Figure 94 "Call Server Configuration language and database selection window" (page 120).

Figure 94
Call Server Configuration language and database selection window



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

14 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 compact flash, proceed to step 25.

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

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

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

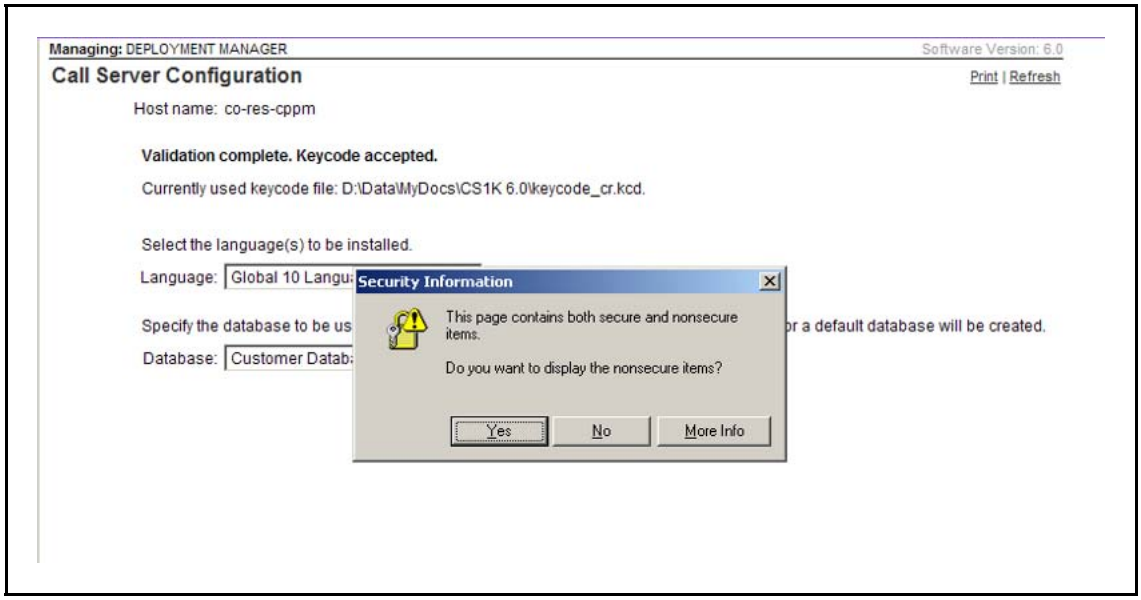
16 Click **Continue**.

Proceed to step 29.

17 In the **Database** list, select **Customer Database on Client Machine**.

The Security Information screen appears, as shown in Figure 95 "Security Information window" (page 121).

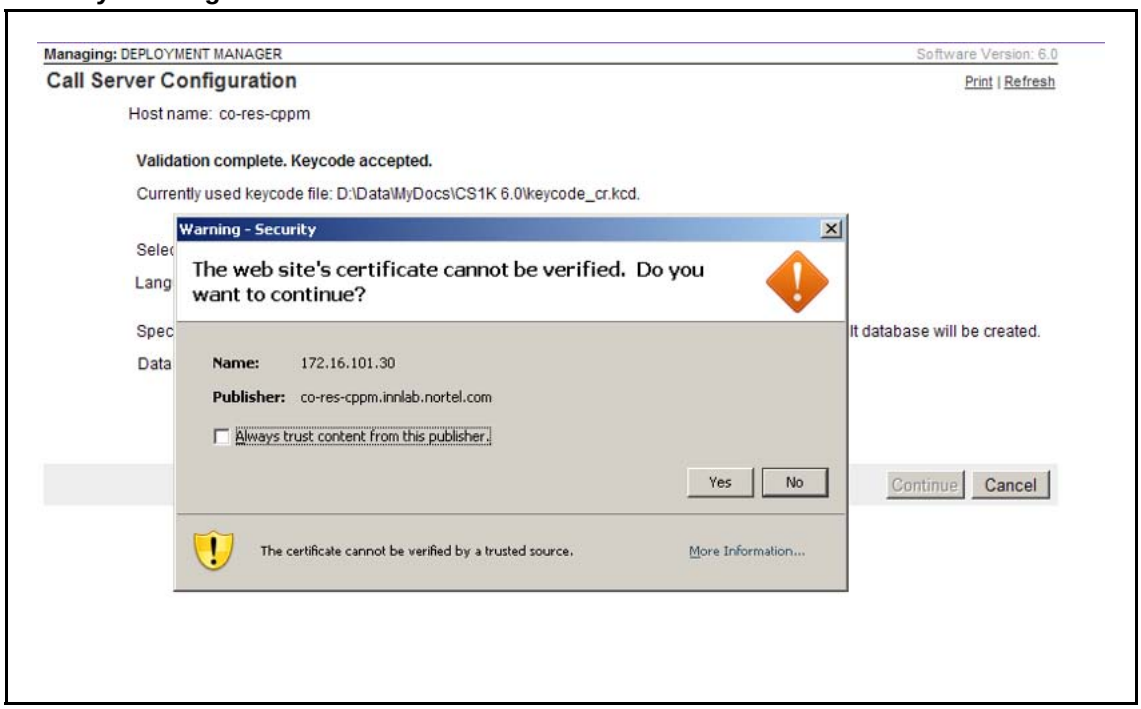
Figure 95
Security Information window



18 Click **Yes**.

The Security warning 1 screen appears, as shown in Figure 96 "Security warning 1 window" (page 121).

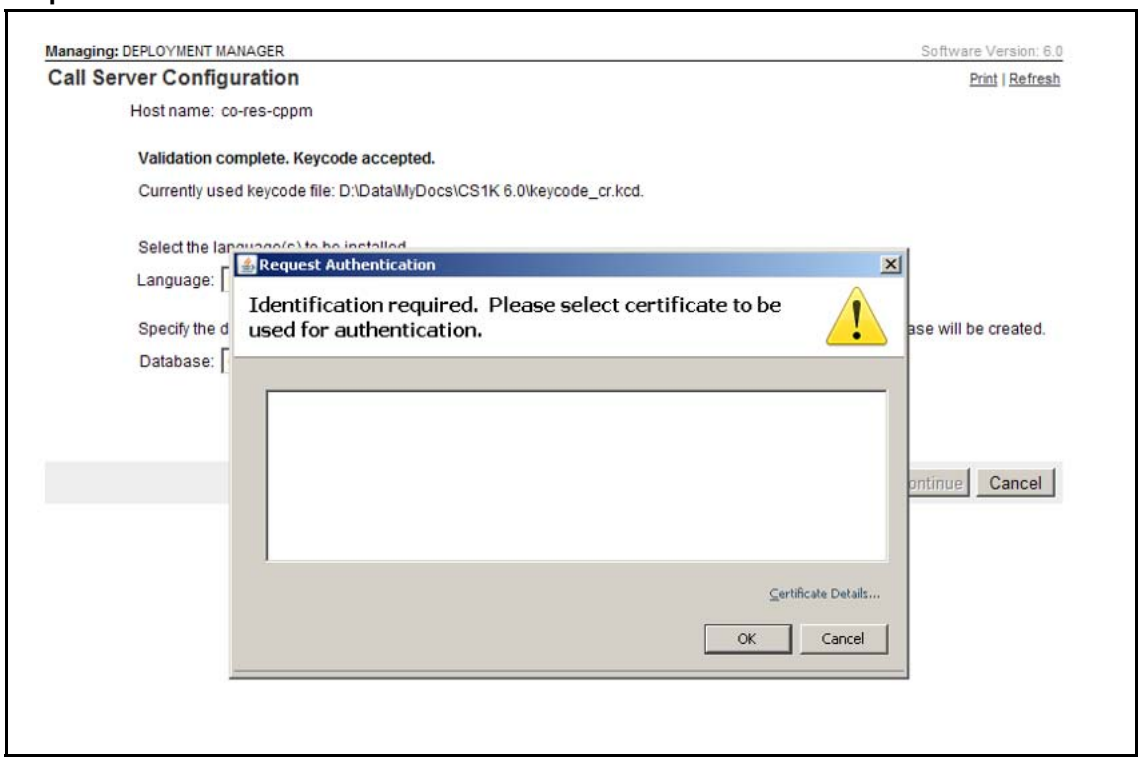
Figure 96
Security warning 1 window



19 Click **Yes**.

The Request Authentication screen appears, as shown in Figure 97 "Request Authentication window" (page 122).

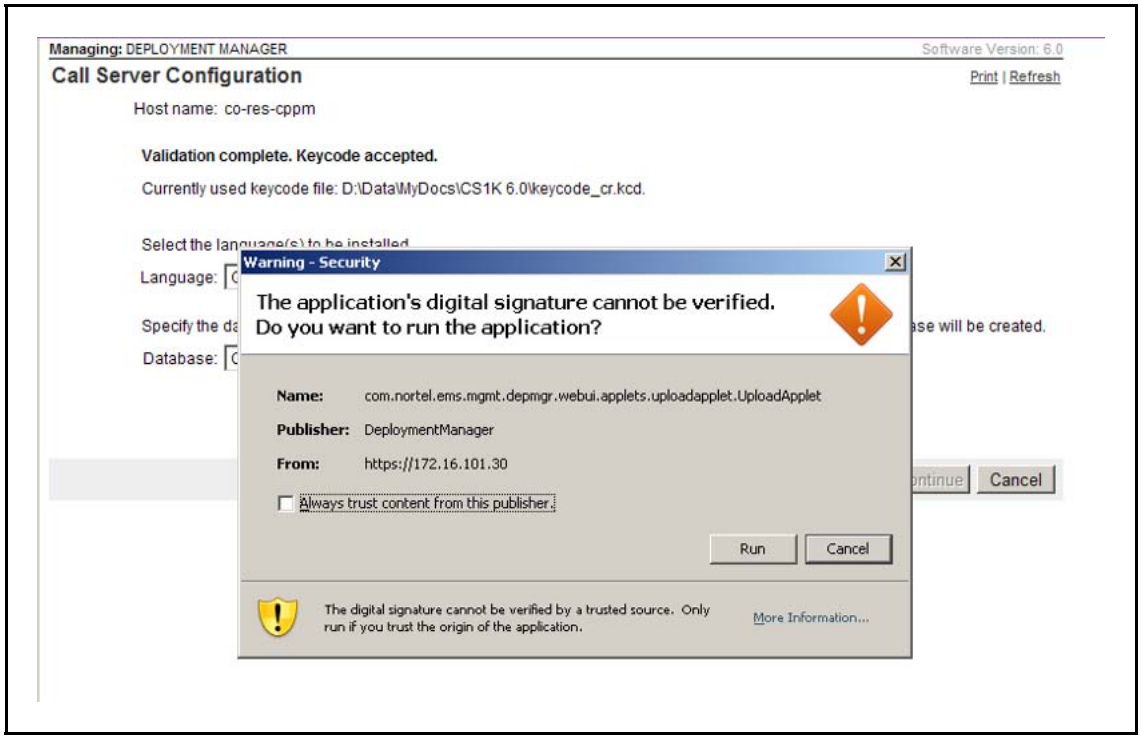
Figure 97
Request Authentication window



20 Click **OK**.

The Security warning 2 screen appears, as shown in Figure 98 "Security warning 2 window" (page 123).

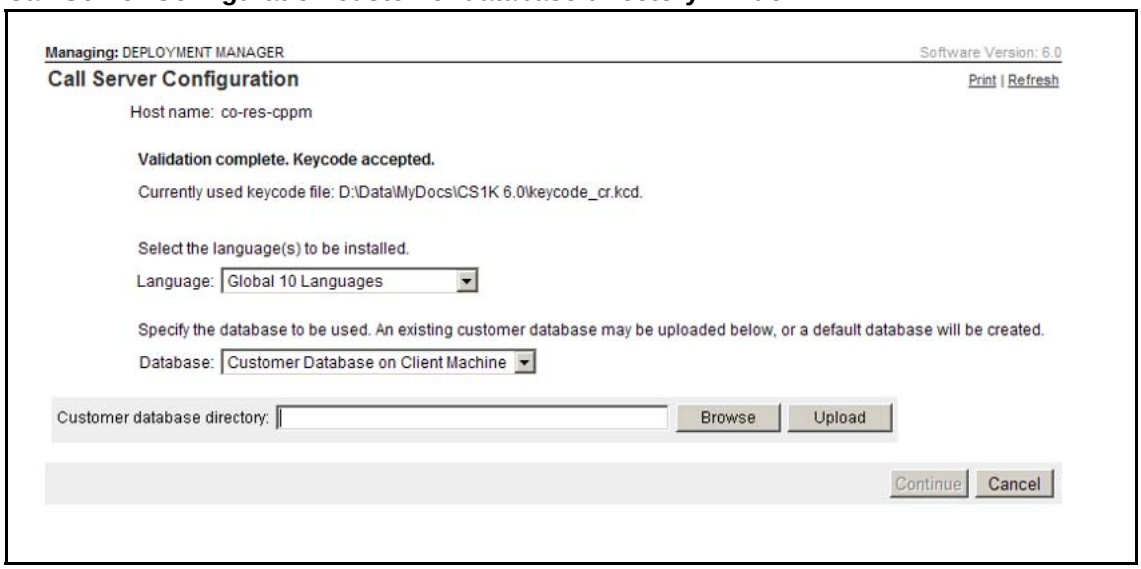
Figure 98
Security warning 2 window



21 Click **Run**.

The **Customer database directory** field appears, as shown in Figure 99 "Call Server Configuration customer database directory window" (page 123).

Figure 99
Call Server Configuration customer database directory window



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

OR

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

23 Click **Upload**.

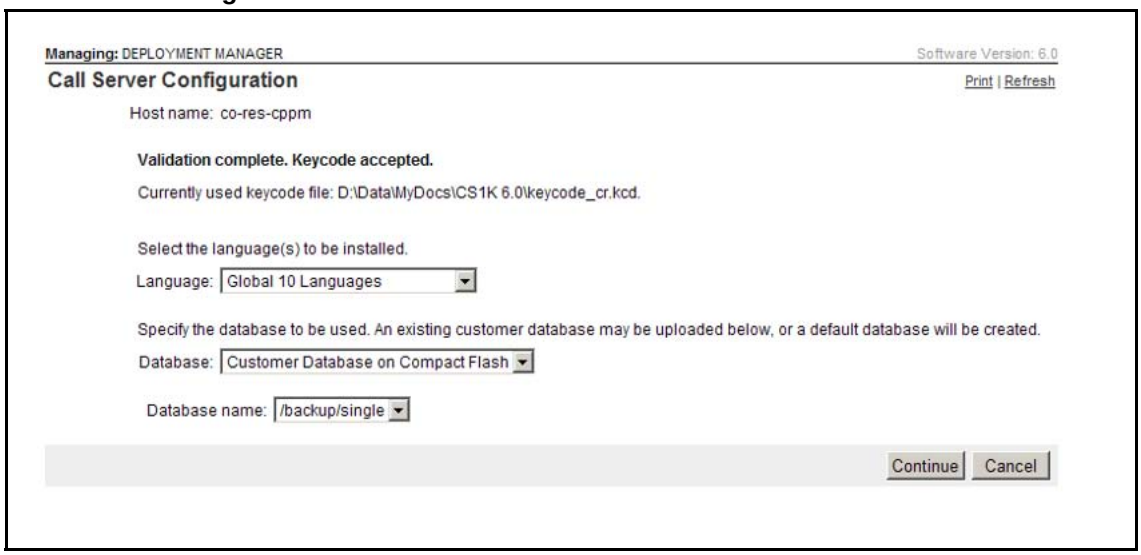
24 Click **Continue**.

Proceed to step 29.

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

The **Database name** list appears, as shown in Figure 100 "Call Server Configuration database name window" (page 124).

Figure 100
Call Server Configuration database name window



26 Click **Continue**.

Proceed to step 29.

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

28 Click **Continue**.

Proceed to step 29.

29 If you chose a 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 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 35.

30 If you chose a package that includes Element Manager , the Element Manager Configuration screen appears, as shown in Figure 101 "Element Manager Configuration window" (page 125).

Note: If you log on locally, or if there are no Call Servers in the security domain, the Element Manager Configuration screen appears as shown in Figure 102 "Element Manager Configuration window" (page 125).

Figure 101
Element Manager Configuration window

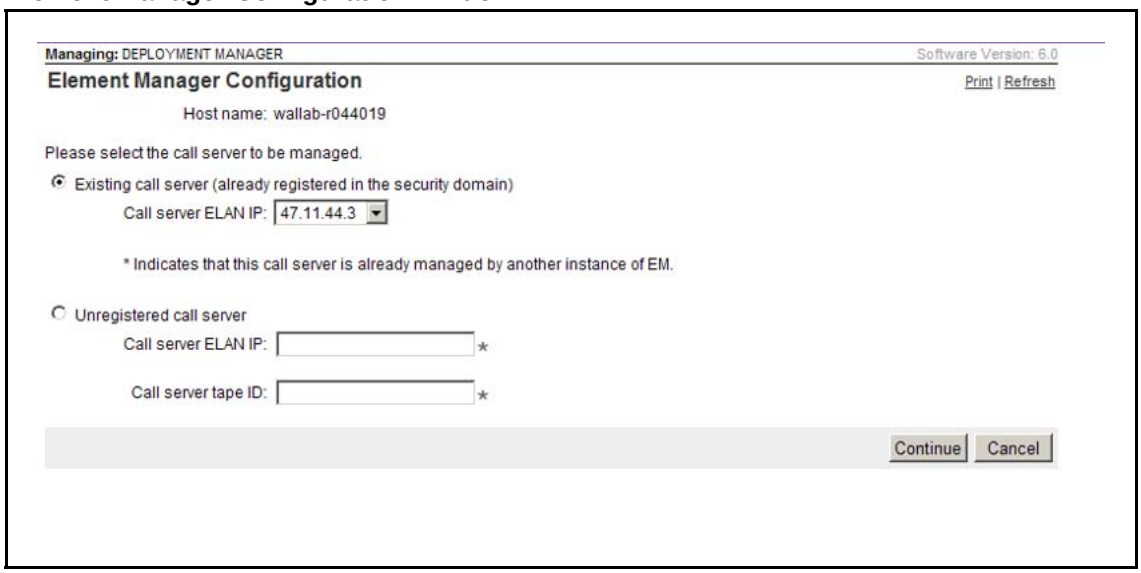
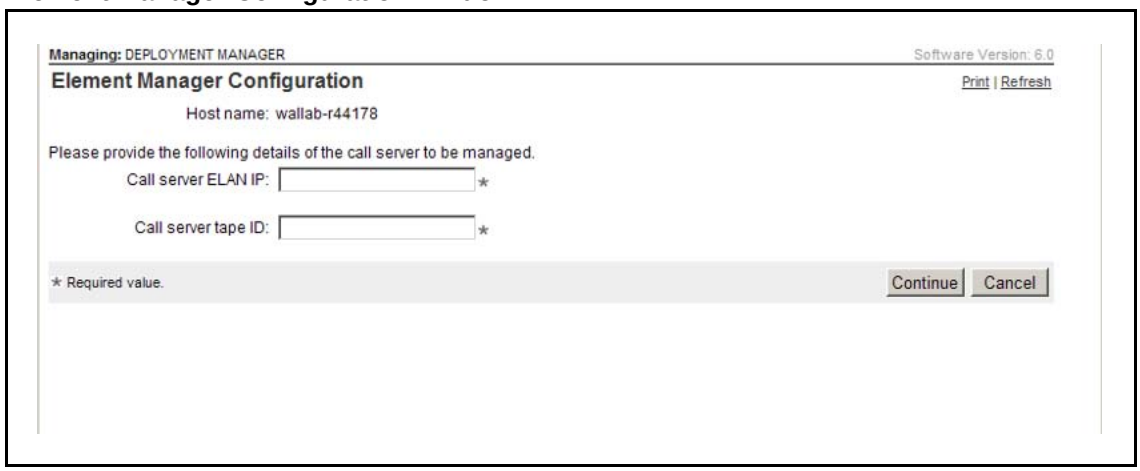


Figure 102
Element Manager Configuration window



If you want to manage a Call Server that is already registered in the security domain, proceed to step 31. If you want to manage an unregistered Call Server, proceed to step 34.

> ***Note:*** If you want to configure EM to manage a Linux call server with a distributor dongle, choose the unregistered call server option even if the Call Server is registered in the security domain.

31 Select the **Existing call server (already registered in the security domain)** option.

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

33 Click **Continue**.

Proceed to step 38.

34 Select the **Unregistered call server** option.

> ***Note:*** If you log on locally, or if there are no Call Servers in the security domain, this step is not necessary. Proceed to step 35.

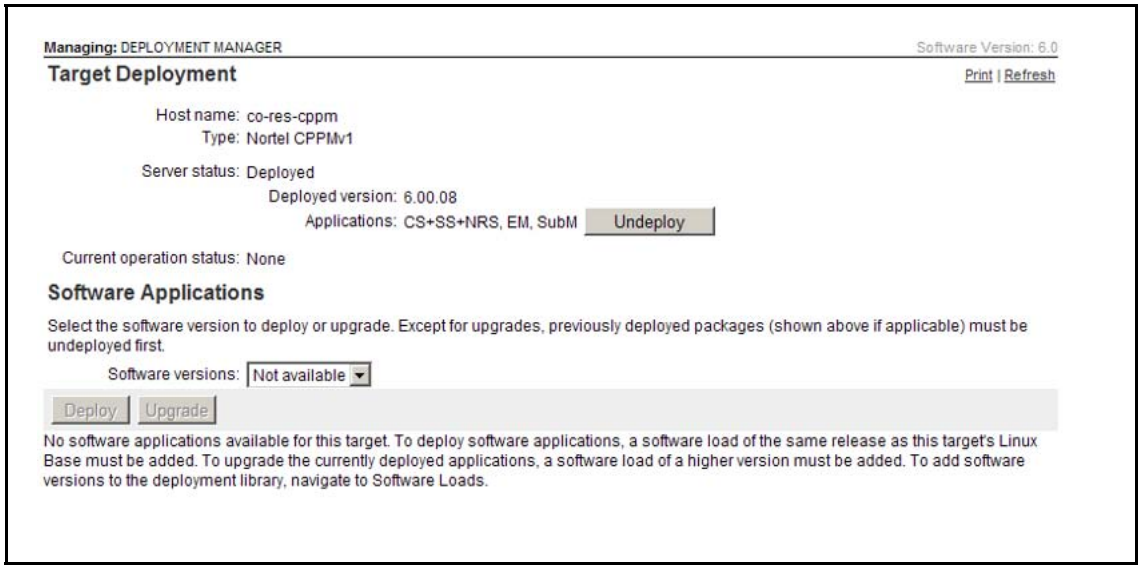
35 In the **Call server ELAN IP** field, enter a value for Call Server ELAN IP.

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

37 Click **Continue**.

The deployment completes. The Target Deployment screen appears, as shown in Figure 103 "Target Deployment window" (page 127). The screen displays the server deployment status and deployed packages.

Figure 103
Target Deployment window



--End--

Application software undeployment

Undeploy software to remove Nortel applications from the server. When you undeploy the Nortel applications, the application data is also erased.

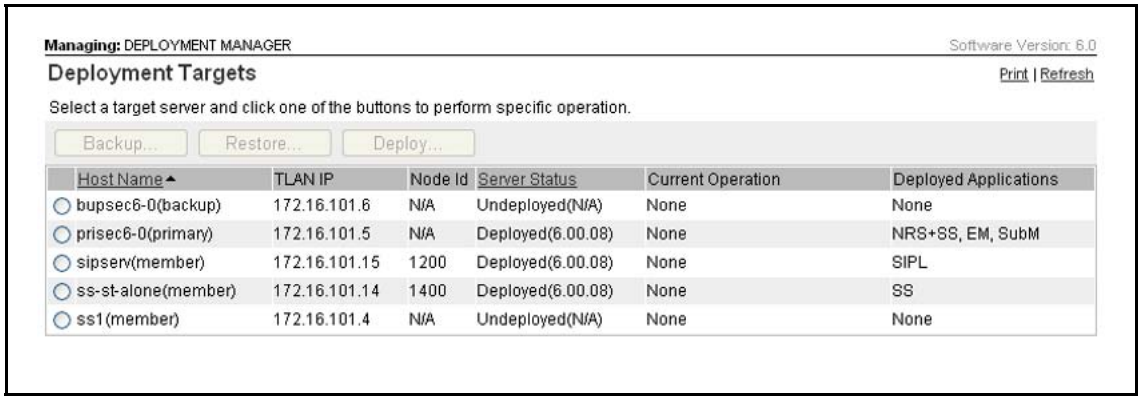
Prerequisites

- The status of the target server must be **Deployed**.

Procedure 8
Undeploying application software from a COTS or CP PM server

Step	Action
1	Log on to UCM. See Procedure 2 “Logging on to UCM” (page 105).
2	In the navigation pane, click **Network**, **CS 1000 Services**, **Software Deployment**, **Deployment Targets**. The Deployment Targets screen appears, as shown in Figure 104 "Deployment Targets window" (page 128).

Figure 104
Deployment Targets window

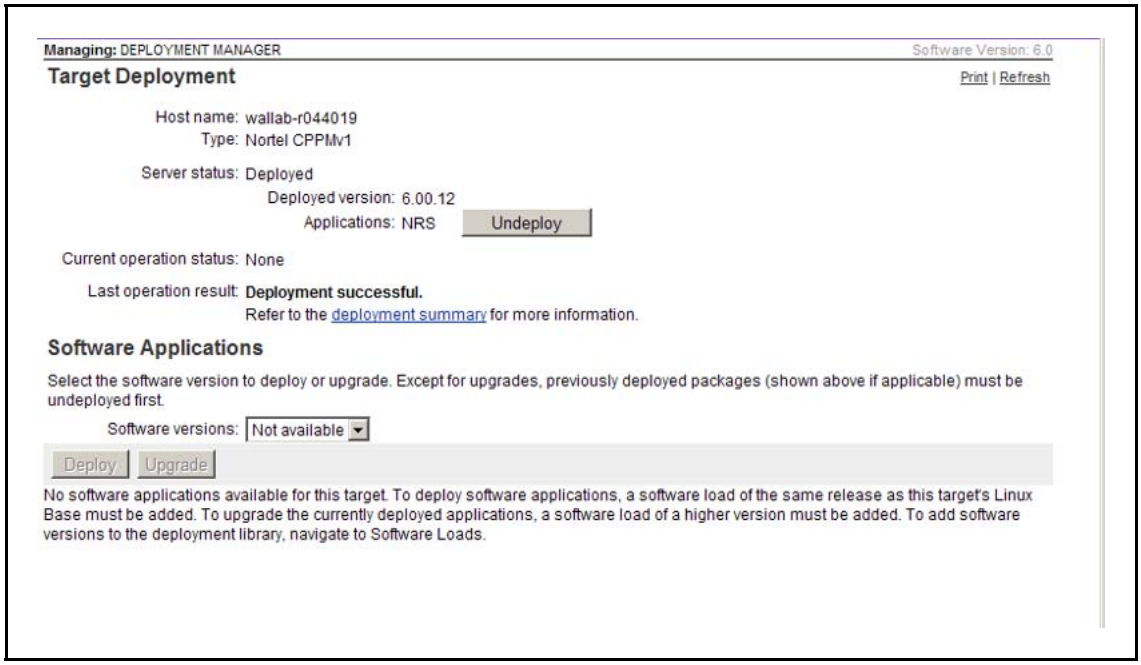


3 Select the target that you want to undeploy.

4 Click **Deploy**.

The Target Deployment and Software Applications screen appears, as shown in Figure 105 "Target Deployment and Software Applications window" (page 128).

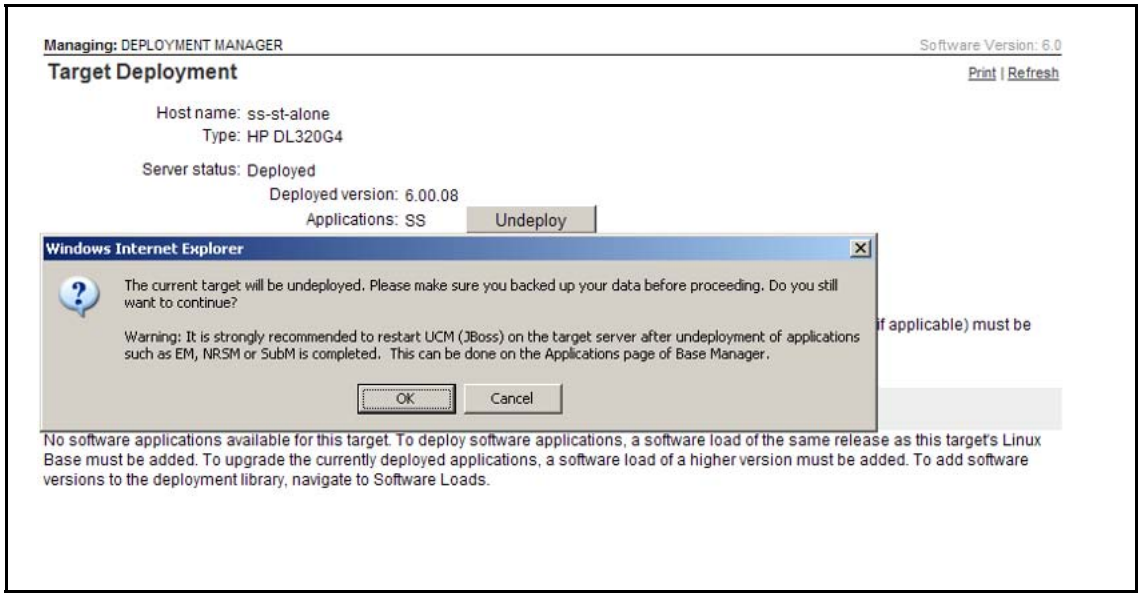
Figure 105
Target Deployment and Software Applications window



5 Click **Undeploy**.

A warning message appears, as shown in Figure 106 "Undeployment warning message" (page 129).

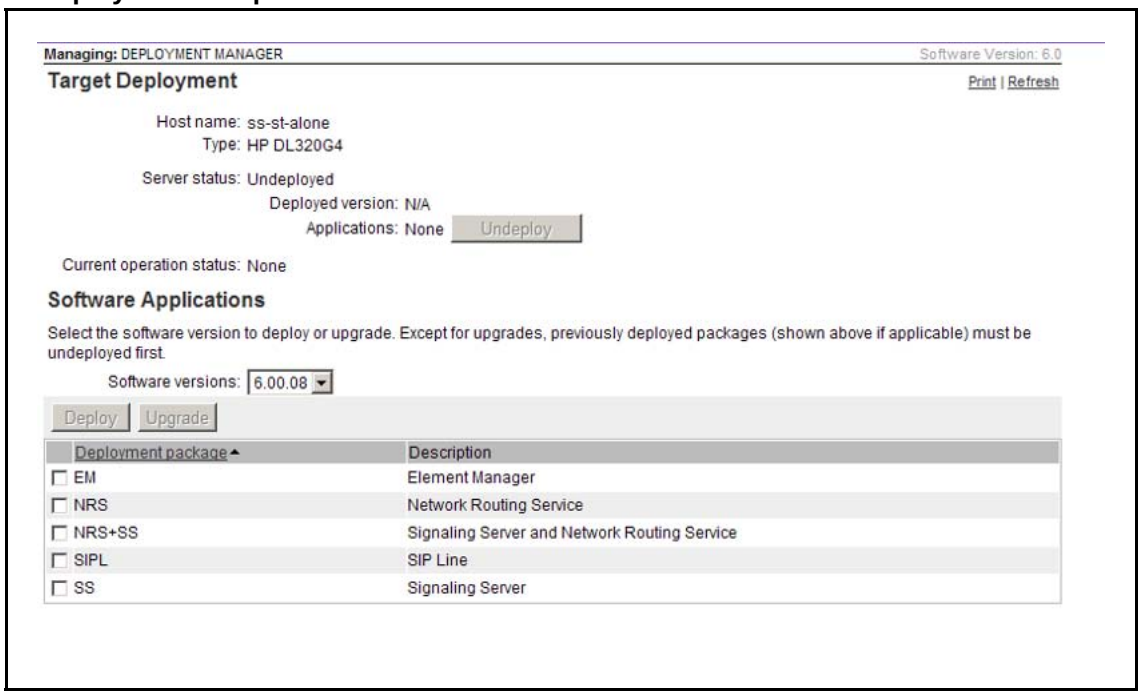
Figure 106
Undeployment warning message



6 Press **OK** to continue undeployment.

The Target Deployment screen appears when the undeployment completes, as shown in Figure 107 "Undeployment complete window" (page 129).

Figure 107
Undeployment complete window



7	In the Target Deployment screen, verify the server status is **Undeployed**.

--End--

Application software upgrades

You can use Procedure 9 “Upgrading application software” (page 130) to upgrade the application software on the current installation of Linux base. If you want to upgrade the application software after an upgrade to the Linux base installation, use Procedure 10 “Upgrading application software after a Linux base upgrade” (page 132).

Upgrade the application software

Perform an application software upgrade to install a more recent version of the application software on the server.

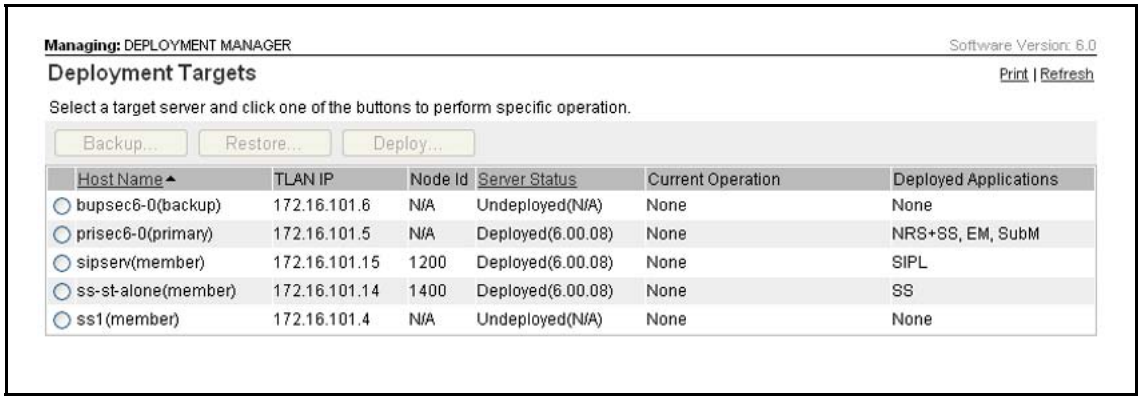
Prerequisites

- The status of the target server must be **Deployed**.
- A higher version of the application software must be available for deployment.

Procedure 9
Upgrading application software

Step	Action
1	Log on to UCM. See Procedure 2 “Logging on to UCM” (page 105).
2	In the navigation pane, click **Network**, **CS 1000 Services**, **Software Deployment**, **Deployment Targets**. The Deployment Targets screen appears, as shown in Figure 108 "Deployment Targets window" (page 131).

Figure 108
Deployment Targets window

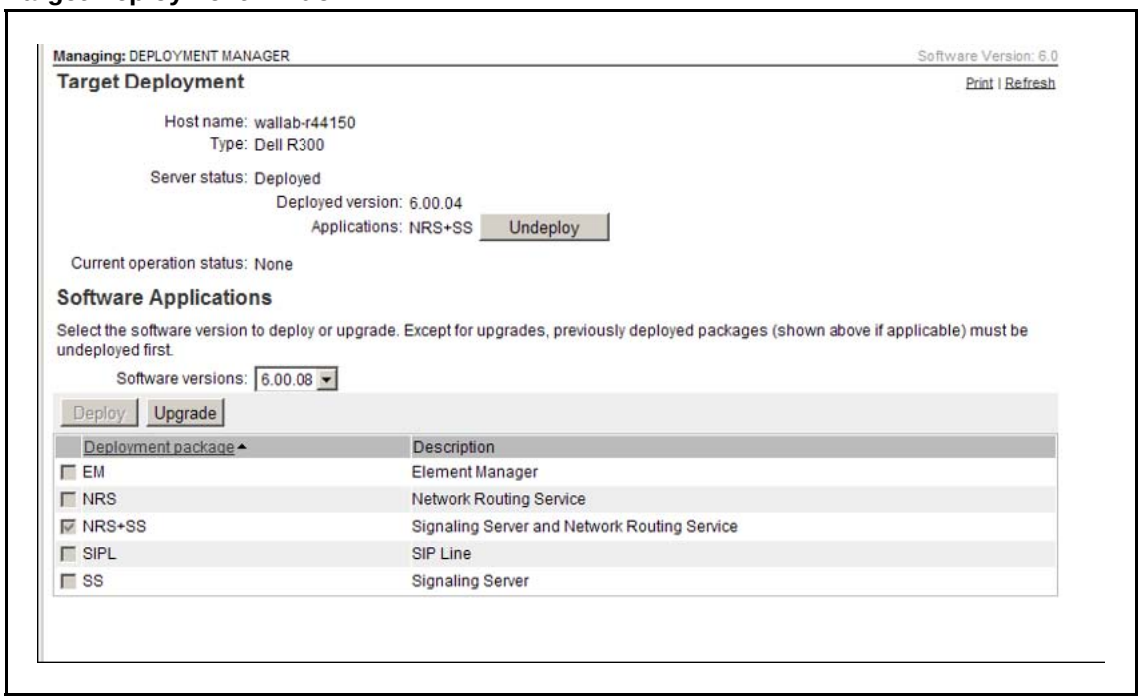


3 In the Deployment Targets screen, select a deployment target.

4 Click **Deploy**.

The Target Deployment screen appears, as shown in Figure 109 "Target Deployment window" (page 131).

Figure 109
Target Deployment window



Note: If the applications on the system include EM or NRSM packages, the links for these managers already exist in the primary UCM. Therefore, the EM preconfiguration page is not presented again.

5 In the **Software versions** list, select the upgrade software version.

> ***Note:*** The upgrade software version must be greater than the current software version; you cannot perform a downgrade using this procedure. To downgrade the software version, you must perform Procedure 8 “Undeploying application software from a COTS or CP PM server” (page 127) and then deploy the downgrade software version using Procedure 7 “Deploying application software to a COTS or CP PM server” (page 116).

6 Click **Upgrade**.

7 If a Call Server package is part of the upgrade, you must perform Procedure 11 “Preconfiguring the Call Server” (page 136).

OR

If a Call Server package is not part of the upgrade, navigate to the Target Deployment section and view the **Deployed version** value to verify the upgrade.

--End--

Upgrade the application software after a Linux server upgrade

Use Procedure 10 “Upgrading application software after a Linux base upgrade” (page 132) to perform an application software upgrade after you perform a Linux server upgrade.

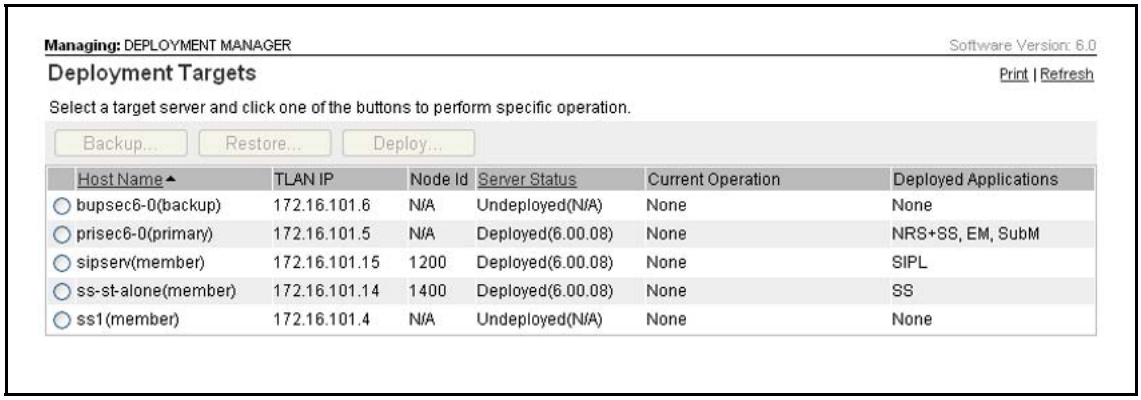
Prerequisites

- You must complete a successful upgrade of the Linux base.
- The status of the target server must be Undeployed.
- The base version of the target server must be the newly upgraded Linux base version.

Procedure 10
Upgrading application software after a Linux base upgrade

Step	Action
1	Log on to UCM. See Procedure 2 “Logging on to UCM” (page 105).
2	In the navigation pane, click **Network**, **CS 1000 Services**, **Software Deployment**, **Deployment Targets**. The Deployment Targets screen appears, as shown in Figure 110 "Deployment Targets window" (page 133).

Figure 110
Deployment Targets window

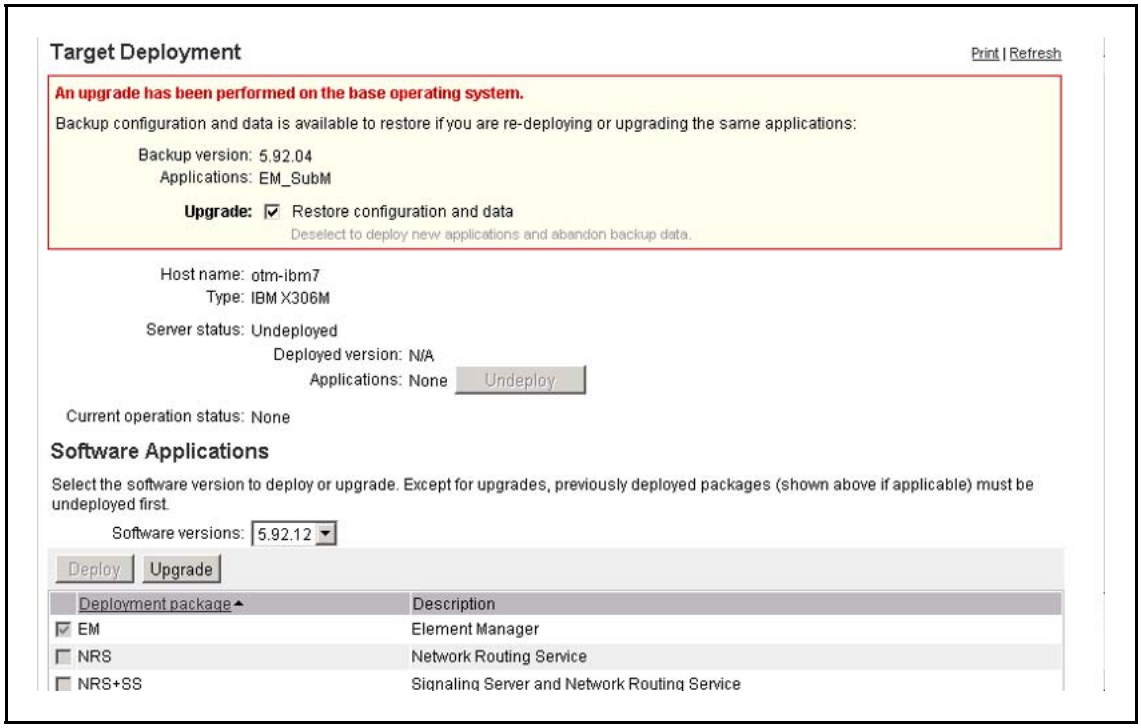


3 In the Deployment Targets screen, select a deployment target.

4 Click **Deploy**.

If you are upgrading within Release 6.0, the Target Deployment screen appears, as shown in Figure 111 "Target Deployment window" (page 134).

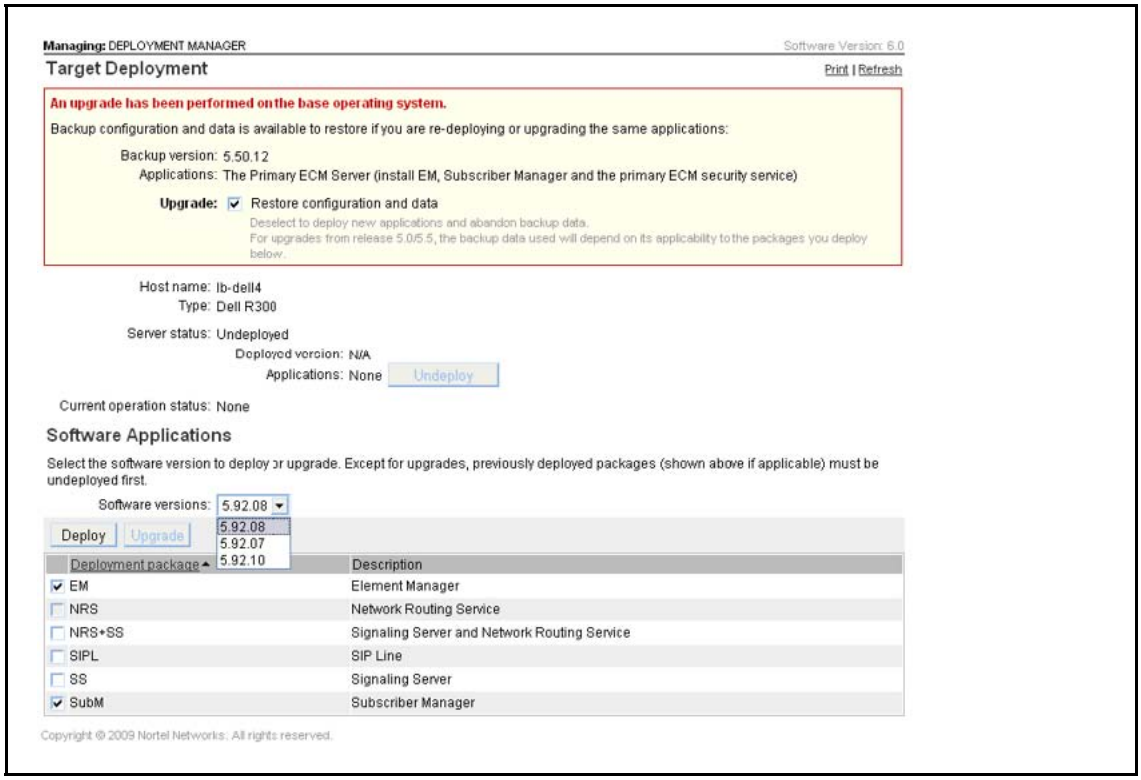
Figure 111
Target Deployment window



Note: If the applications on the system include EM or NRSM packages, the links for these managers already exist in the primary UCM. Therefore, the EM preconfiguration page is not presented again. If you uncheck the upgrade check box and decide to select other packages for deployment, you must go into the primary UCM elements page and delete any EM or NRSM links associated with this element, before performing the deployment. Otherwise, there will be two EMs (original and a duplicate link) and two NRSMs (original and duplicate link) showing in the UCM elements table.

If you are upgrading from Release 5.x to Release 6.0, the Target Deployment screen appears, as shown in Figure 112 "Target Deployment window" (page 135).

Figure 112
Target Deployment window



Note: Choose previously deployed packages if you want to restore the data. If you choose different packages, the data is not restored during the deployment. The only package that have backup data from release 5.0/5.5 are NRS packages.

5 In the **Software versions** list, select the upgrade software version.

Note: The upgrade software version must be greater than the current software version; you cannot perform a downgrade using this procedure. To downgrade the software version, you must perform Procedure 8 “Undeploying application software from a COTS or CP PM server” (page 127) and then deploy the downgrade software version using Procedure 7 “Deploying application software to a COTS or CP PM server” (page 116).

6 Click **Upgrade**.

7 If a Call Server package is part of the upgrade, you must perform Preconfiguring the Call Server.

OR

If a Call Server package is not part of the upgrade, navigate to the Target Deployment section and view the **Deployed version** value to verify the upgrade.

--End--

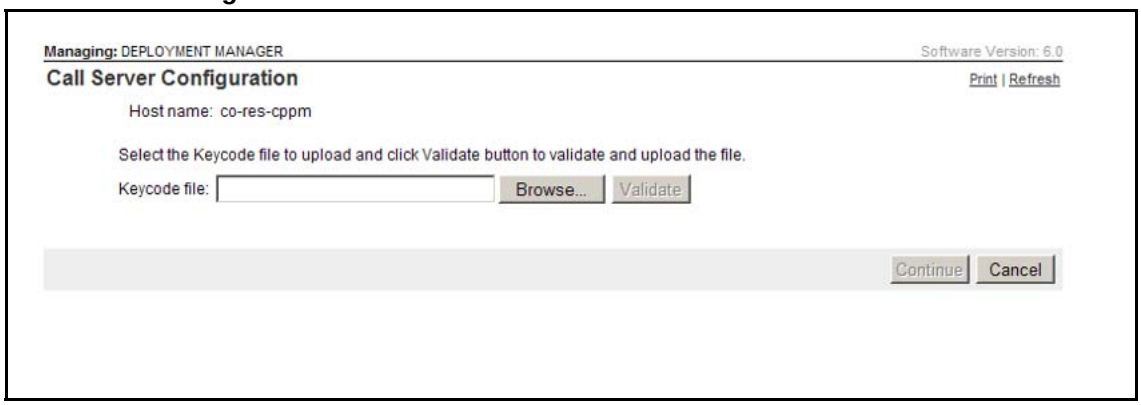
Call Server pre-configuration

If you chose to upgrade a Call Server package, you must provide Call Server configuration details.

Procedure 11
Preconfiguring the Call Server

Step	Action
1	If you upgrade a package that includes Call Server, the Call Server Configuration screen appears, as shown in Figure 113 "Call Server Configuration window" (page 136).

Figure 113
Call Server Configuration window

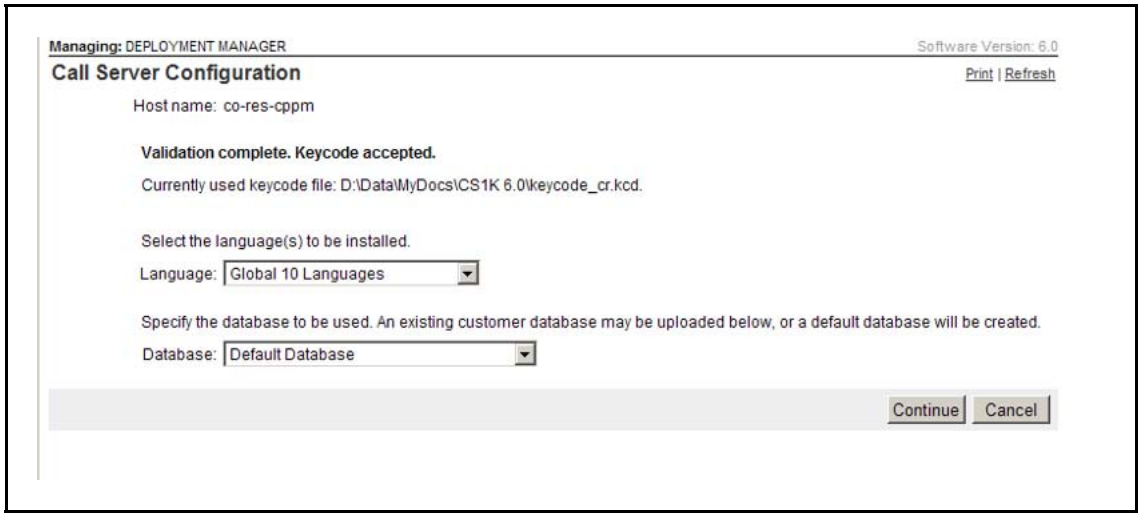


2 In the **Keycode file** box, click **Browse** to browse for the keycode file.

3 Click **Validate** to validate the file selection.

After the keycode file validates successfully, language and database options are displayed, as shown in Figure 114 "Call Server Configuration language and database selection window" (page 137).

Figure 114
Call Server Configuration language and database selection window



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

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

If you want to select the default database, proceed to step 6.

If you want to select a customer database on the client machine, proceed to step 8.

If you want to select a customer database on compact flash, proceed to step 16.

If you want to select an existing database, proceed to step 18.

> ***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.

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

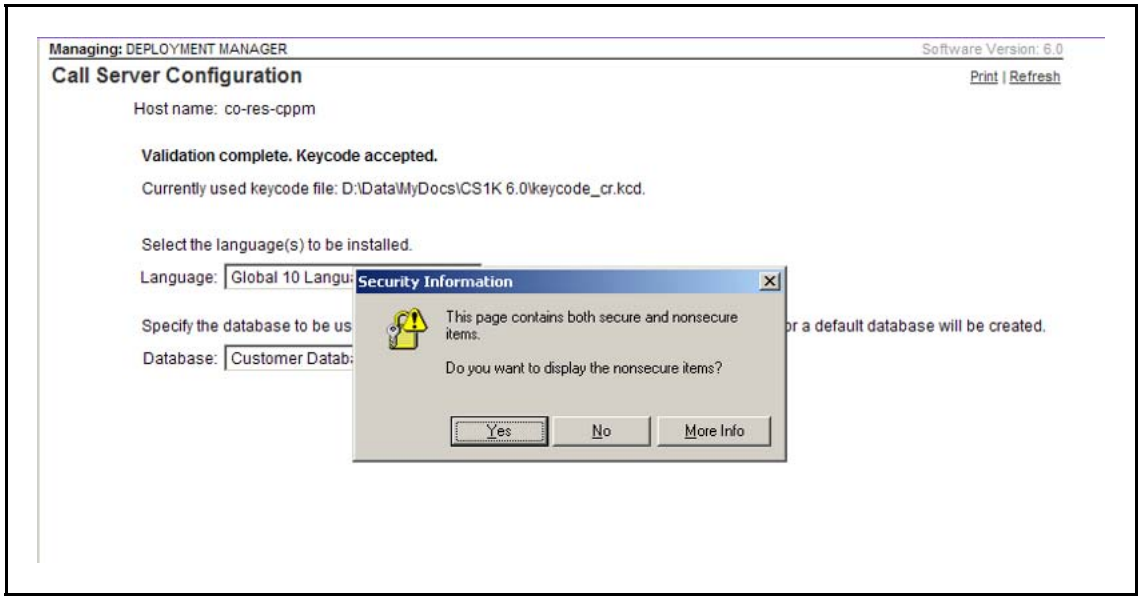
7 Click **Continue**.

Call Server preconfiguration is complete at this point.

8 In the **Database** list, select **Customer Database on Client Machine**.

The Security Information screen appears, as shown in Figure 115 "Security Information window" (page 138).

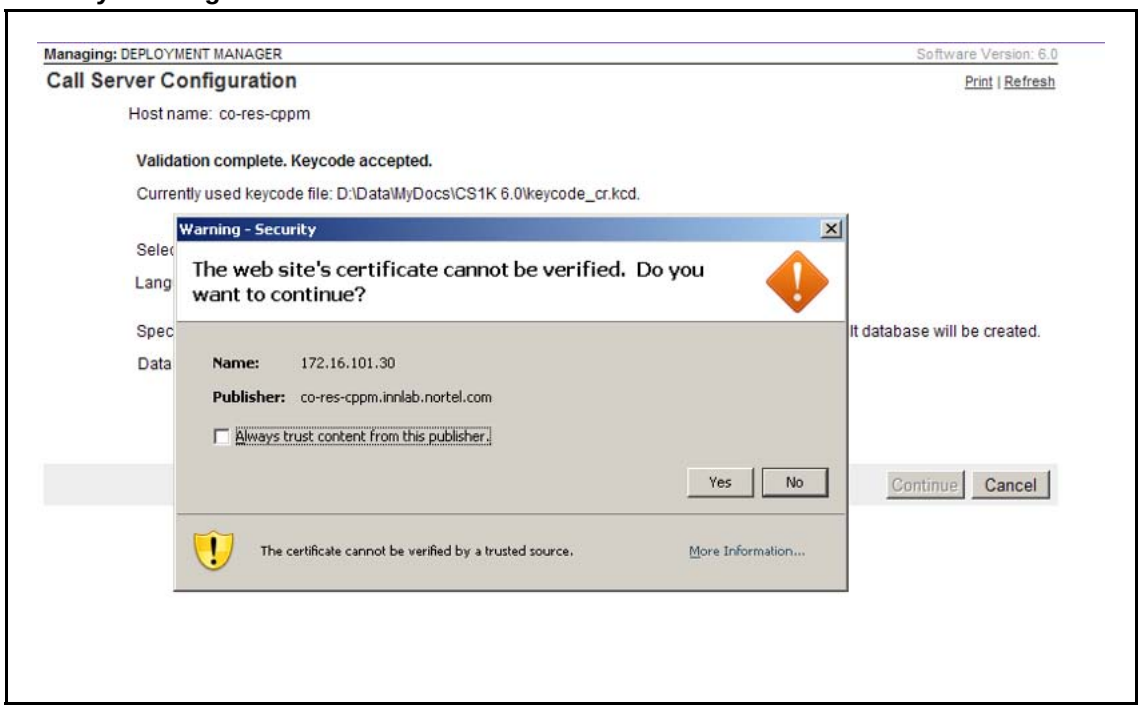
Figure 115
Security Information window



9 Click **Yes**.

The Security warning 1 screen appears, as shown in Figure 116 "Security warning 1 window" (page 138).

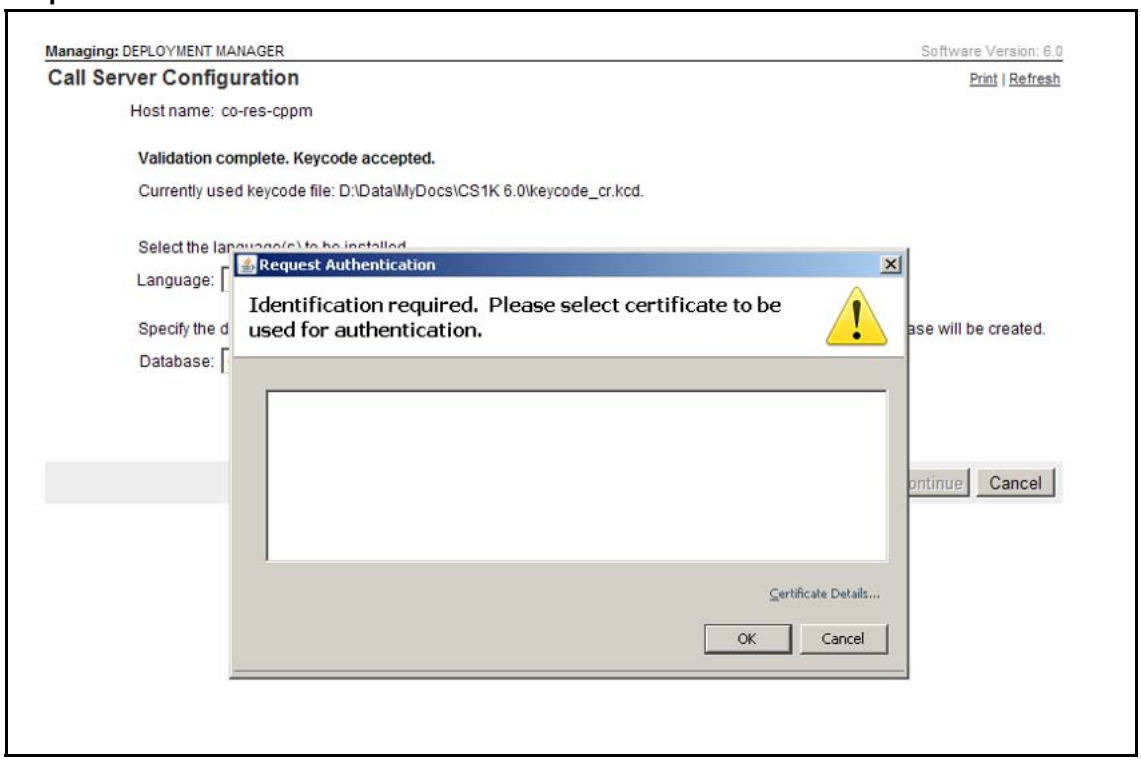
Figure 116
Security warning 1 window



10 Click **Yes**.

The Request Authentication screen appears, as shown in Figure 117 "Request Authentication window" (page 139).

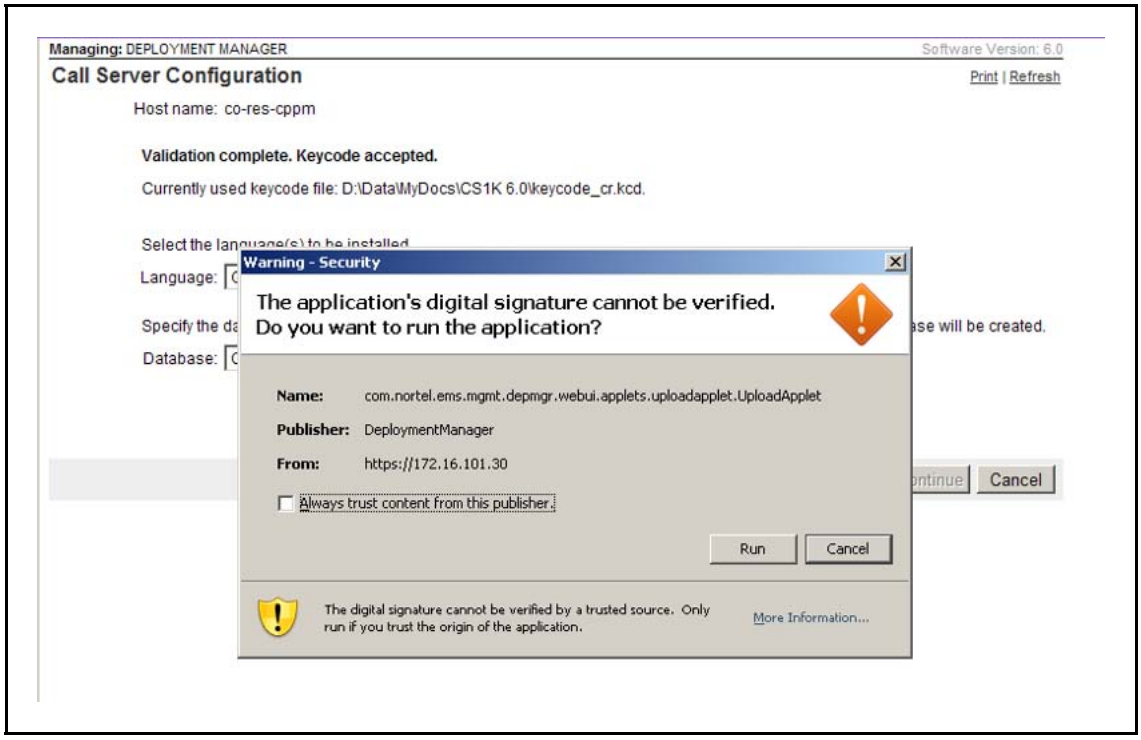
Figure 117
Request Authentication window



11 Click **OK**.

The Security warning 2 screen appears, as shown in Figure 118 "Security warning 2 window" (page 140).

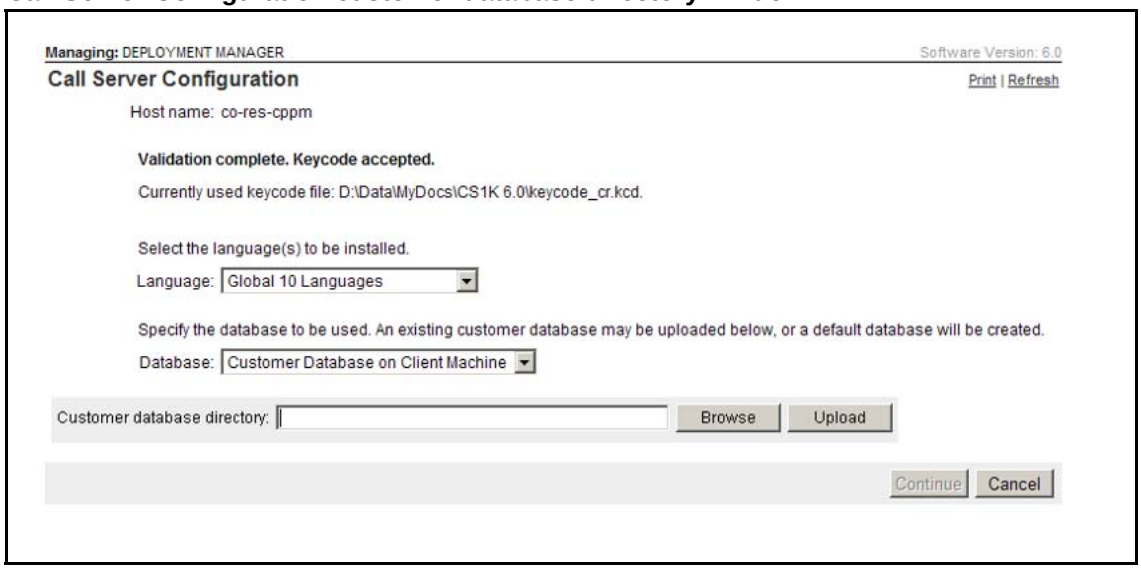
Figure 118
Security warning 2 window



12 Click **Run**.

The **Customer database directory** field appears, as shown in Figure 119 "Call Server Configuration customer database directory window" (page 140).

Figure 119
Call Server Configuration customer database directory window



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

OR

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

14 Click **Upload**.

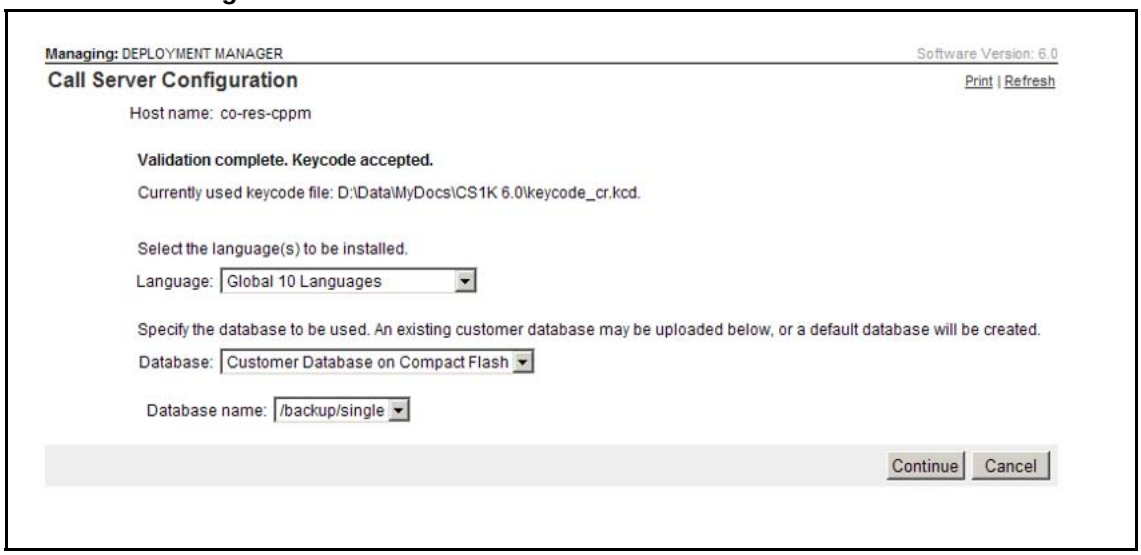
15 Click **Continue**.

Call Server preconfiguration is complete at this point.

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

The **Database name** list appears, as shown in Figure 120 "Call Server Configuration database name window" (page 141).

Figure 120
Call Server Configuration database name window



17 Click **Continue**.

Call Server preconfiguration is complete at this point.

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

19 Click **Continue**.

Call Server preconfiguration is complete at this point.

--End--

System data backup including application data

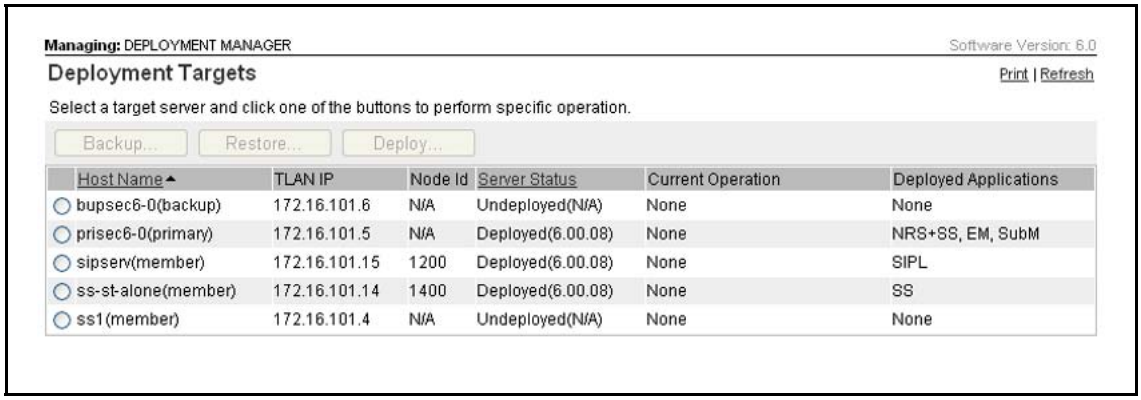
Back up application data for Base and Nortel applications. The type of data backed up is dependant on the applications running on the host server. For example:

- Data backup always includes Linux base system settings and parameters.
- If the server is a primary security server, the backup includes UCM data.
- If the server is a primary security server running Subscriber Manager, the backup includes Subscriber Manager data.
- Data backup includes the Call Server database if the following deployment packages are installed:
  - CS and SS
  - CS, SS, and NRS
- Data backup includes NRS data if the following deployment packages are installed:
  - NRS
  - SS and NRS
  - CS, SS, and NRS
- Data backup includes Personal Directory (PD) data if PD is running on the server and the following deployment packages are installed:
  - SS
  - SS and NRS
  - CS and SS
  - CS, SS, and NRS

Procedure 12
Backing up system data including application data

Step	Action
1	Log on to UCM. See Procedure 2 “Logging on to UCM” (page 105).
2	In the navigation pane, click **Network**, **CS 1000 Services**, **Software Deployment**, **Deployment Targets**. The Deployment Targets screen appears, as shown in Figure 121 "Deployment Targets window" (page 143).

Figure 121
Deployment Targets window



3 Select the target server for the upgrade.

When you select the target server, the **Backup** button becomes active.

4 Click **Backup**.

The Backup screen appears, as shown in Figure 122 "Backup window" (page 143).

Figure 122
Backup window

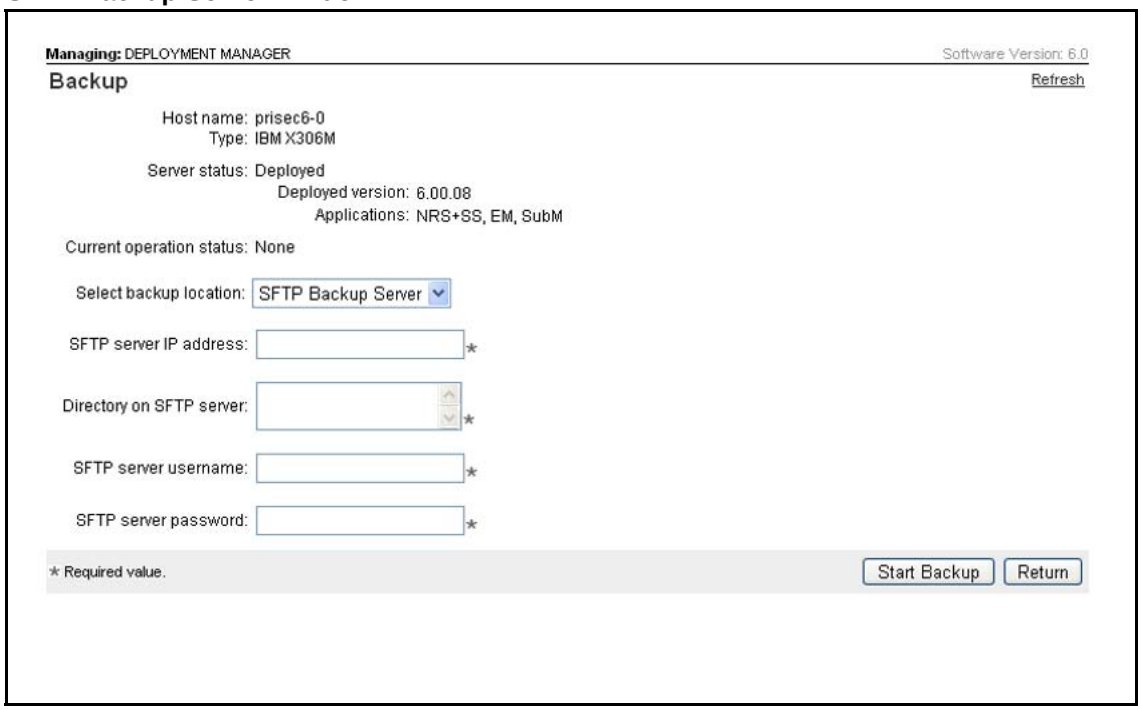
5 In the **Select backup location** list, select a location to store the backup data.

If you select **Deployment Server** as the backup location, proceed to step 10.

Note: There must be sufficient available space on the target server hard drive for the backup file. If there is insufficient capacity for the backup file, you must delete a previous backup file to proceed. A maximum of 3 backup files can be stored on the target server hard drive; once 3 backup files are stored, you must delete a backup file before adding another. For information on deleting backup files from the target server hard drive, see Procedure 14 “Deleting a system data backup file” (page 147).

If you select **SFTP Backup Server** as the backup location, the Backup screen displays additional Secure File Transfer Protocol (SFTP) fields, as shown in Figure 123 "SFTP Backup Server window" (page 144). Proceed to step 6.

Figure 123
SFTP Backup Server window



6 In the **SFTP server IP address** box, type a value for the SFTP server IP address.

7 In the **Directory on SFTP server** field, type a value for the SFTP server directory.

8 In the **SFTP server username** box, type a value for SFTP server user name.

9 In the **SFTP server password** box, type a value for SFTP server password.

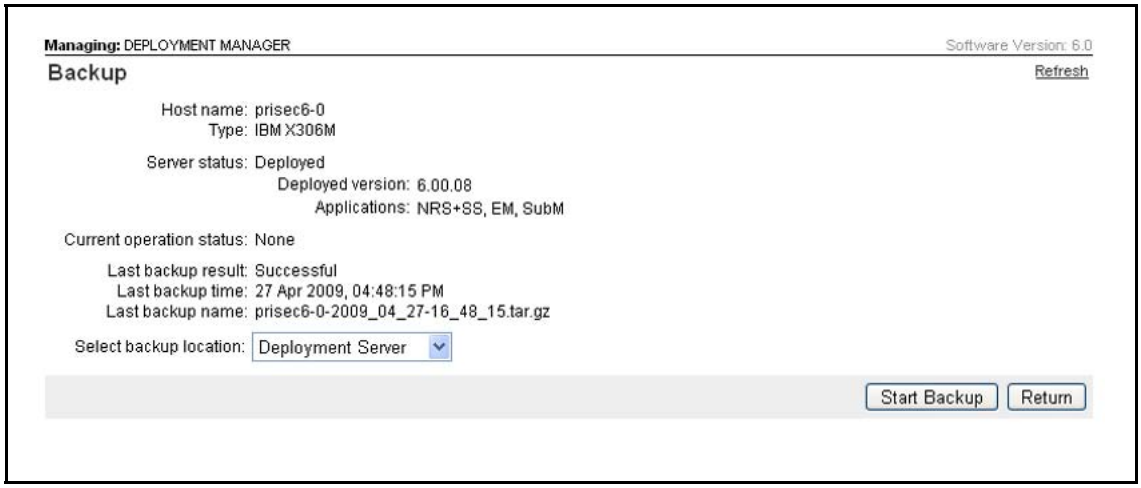
10 Click **Start Backup** to start the backup.

OR

Click **Return** to cancel the backup and return to the Deployment Targets screen.

The Backup screen displays the **Last backup result**, **Last backup time**, and **Last backup name** , as shown in Figure 124 "Backup results window" (page 145).

Figure 124
Backup results window



--End--

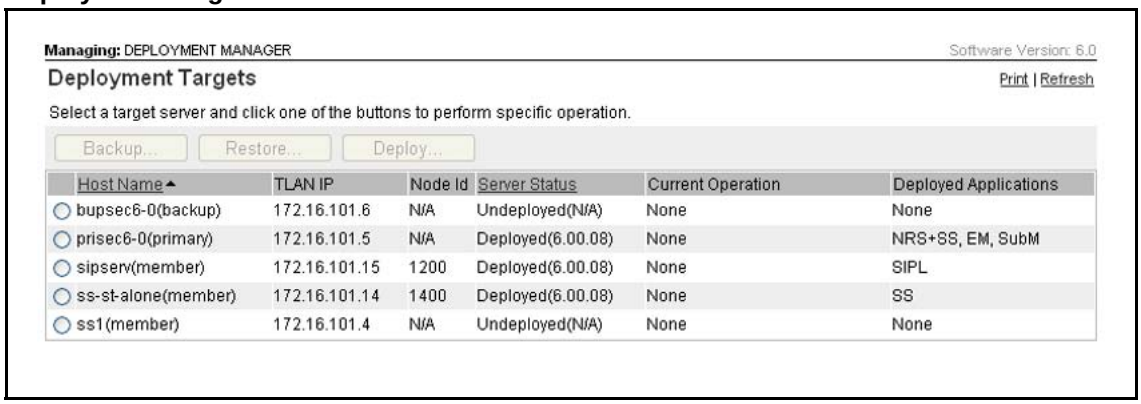
Restore system data including application data

Use an existing backup file to restore application data.

Procedure 13
Restoring system data including application data

Step	Action
1	Log on to UCM. See Procedure 2 “Logging on to UCM” (page 105).
2	In the navigation pane, click **Network**, **CS 1000 Services**, **Software Deployment**, **Deployment Targets**. The Deployment Targets screen appears, as shown in Figure 125 "Deployment Targets window" (page 145).

Figure 125
Deployment Targets window

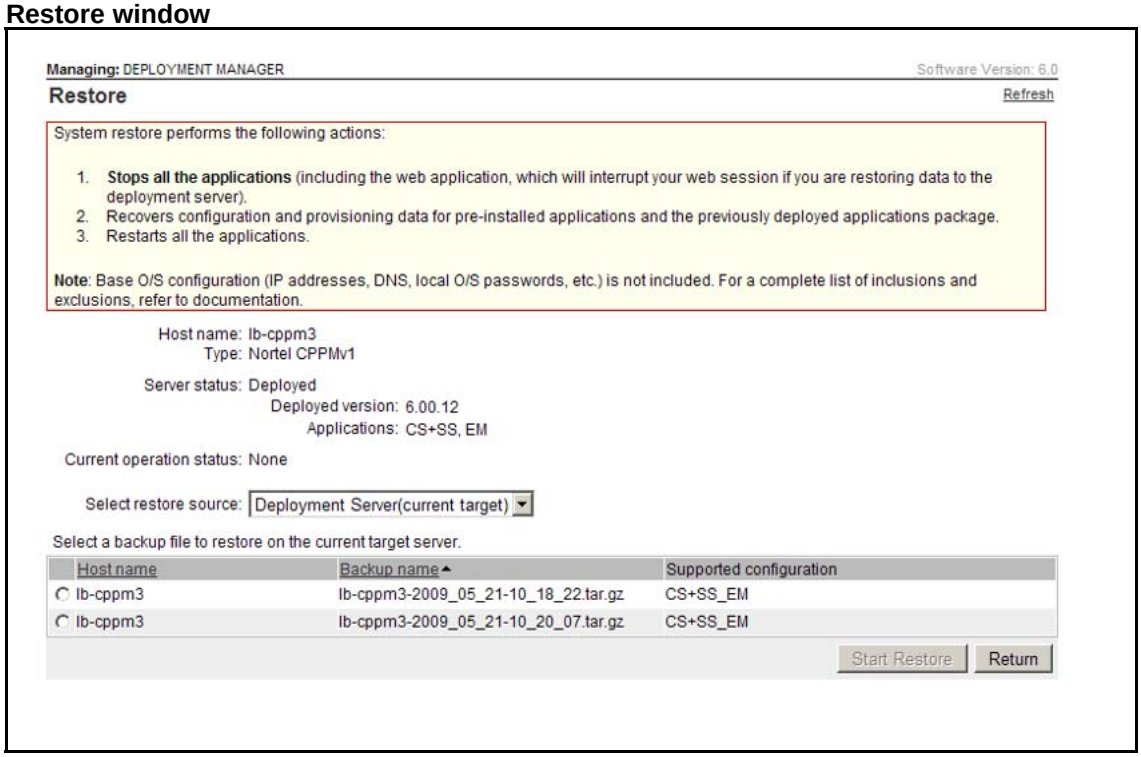


3 Select the target server to restore.

4 Click **Restore**.

The **Restore** screen appears, as shown in Figure 126 "Restore window" (page 146).

Figure 126
Restore window



5 In the **Select restore source** select the source of the application data backup file.

If you select **Deployment Server (current target)** as the backup file source, proceed to step 6.

If you select **Deployment Server (all targets)** as the backup file source, proceed to step 7.

If you select **Client Machine** as the backup file source, proceed to step 8.

If you select **SFTP Backup Server** as the backup file source, Proceed to step 9.

6 Select the backup file from the list of backup files stored on the current target server and proceed to step 13.

7 Select the backup file from the list of backup files stored on all targets in the security domain and proceed to step 13.

8 Type the backup file name in the **Specify restore file name**

OR

Click **Browse** to browse to the backup file.

Proceed to step 13.

9 In the **SFTP server IP address** box, type a value for the SFTP server IP address.

10 In the **File path of backup on SFTP server** field, type the complete file path for the backup file.

Note: You must enter the complete file path, including the file name.

11 In the **SFTP server username** box, type a value for SFTP server user name.

12 In the **SFTP server password** box, type a value for SFTP server password.

Proceed to step 13.

13 Click **Restore** to restore the application data .

OR

Click **Return** to cancel the restore process and return to the Deployment Targets screen.

--End--

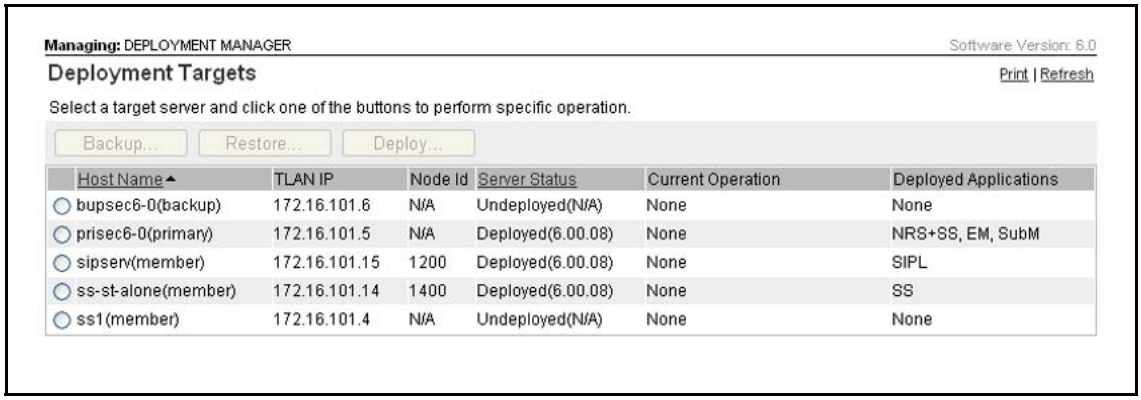
System data backup management

Delete system data backup files on the target server to create room for new backup files.

Procedure 14
Deleting a system data backup file

Step	Action
1	Log on to UCM. See Procedure 2 “Logging on to UCM” (page 105).
2	In the navigation pane, click **Network**, **CS 1000 Services**, **Software Deployment**, **Deployment Targets**. The Deployment Targets screen appears, as shown in Figure 127 "Deployment Targets window" (page 148).

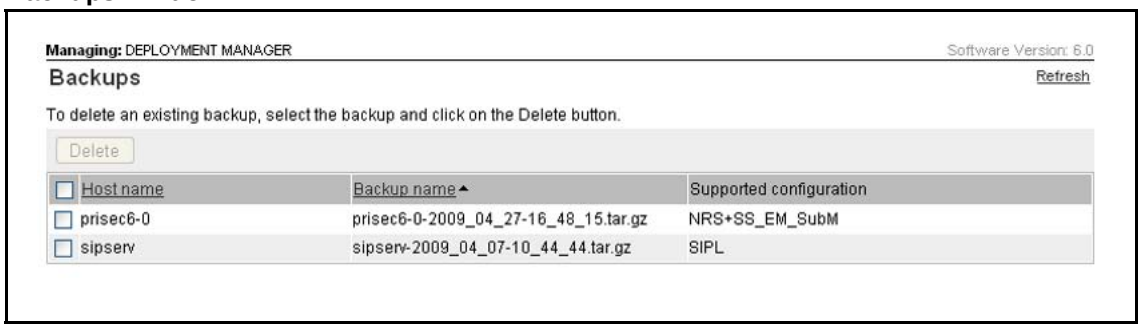
Figure 127
Deployment Targets window



3 In the navigation pane, select **Backups**.

The **Backups** screen appears, as shown in Figure 128 "Backups window" (page 148).

Figure 128
Backups window



4 Select the application backup file to delete.

5 Click **Delete**.

The application backup file is deleted from the hard drive.

--End--

Base Manager

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

- Base System
  - Networking (Network Identity, DNS and Hosts, Route Table).
  - Explicit Congestion Notification
  - Date and Time
- Software
  - Applications
  - Deployment (See “Application installation using Deployment Manager” (page 99))
  - Patches
- Tools
  - Logs

You must access Base Manager (BM) to perform configuration procedures. Use Procedure 15 “Accessing Base Manager through UCM” (page 151) to log on to UCM and access BM. Use Procedure 16 “Accessing Base Manager through local logon” (page 153) to log on to the target server locally and access BM.

Note: The server must be part of the security domain before you can perform BM configuration procedures through UCM. For a more details about UCM configuration of primary, backup, and member servers, see *Unified Communications Management* (NN43001-116). For more information about security management, see *Security Management Fundamentals* (NN43001-604).

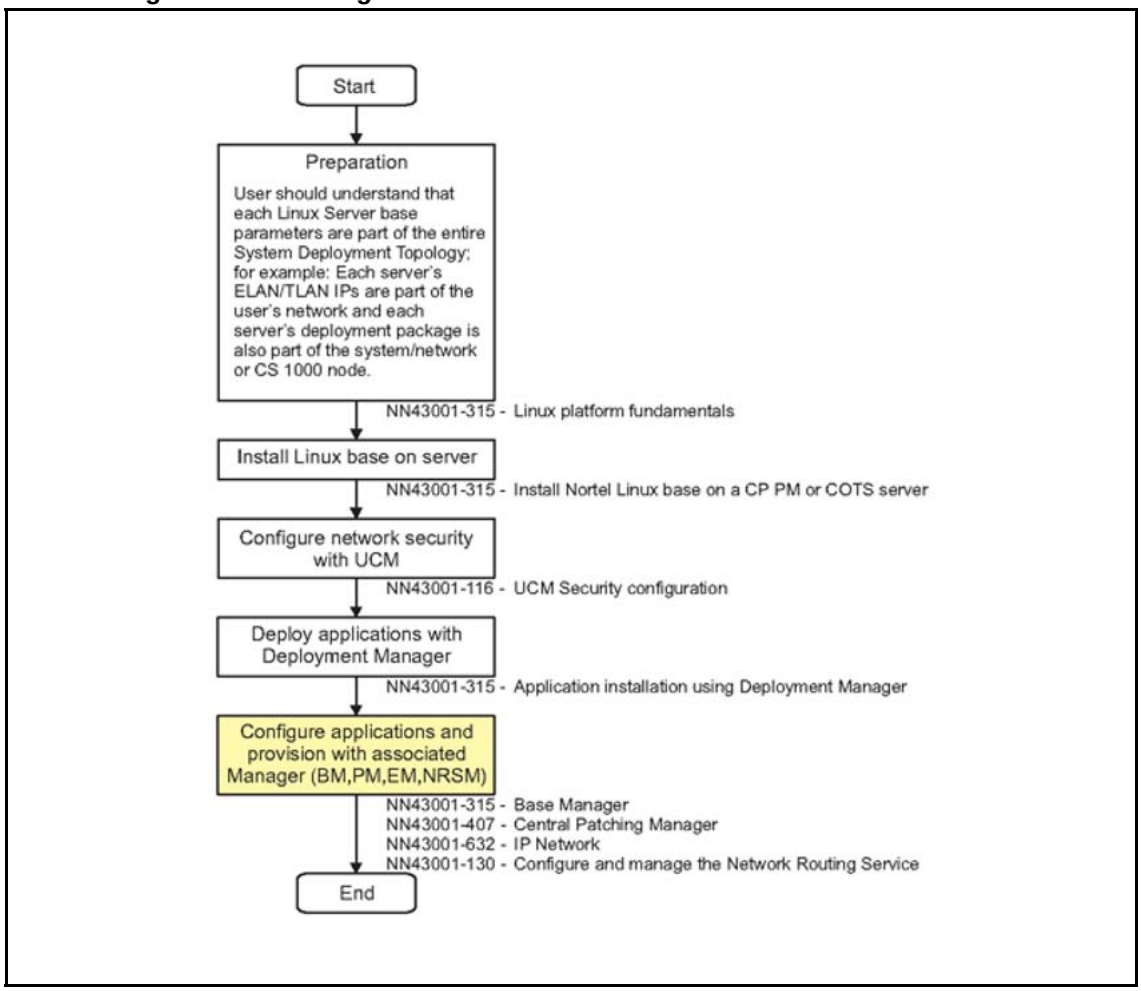
Base Manager workflow stage

"Base Manager" (page 149) contains information rand procedures you need to manage the base system and applications using Base Manager. This chapter also provides references to documentation for Element Manager, Network Routing Service Manager, and Patching Manager where appropriate. Figure 129 "Base Manager workflow stage" (page 150) shows the position of base system and applications configuration and provisioning in the overall workflow.

This chapter provides information and procedures in the following areas:

- "Base system configuration using Base Manager" (page 156)
- "Software maintenance using Base Manager" (page 183)
- "View and export logs using Base Manager" (page 185)

Figure 129
Base Manager workflow stage



Base Manager access

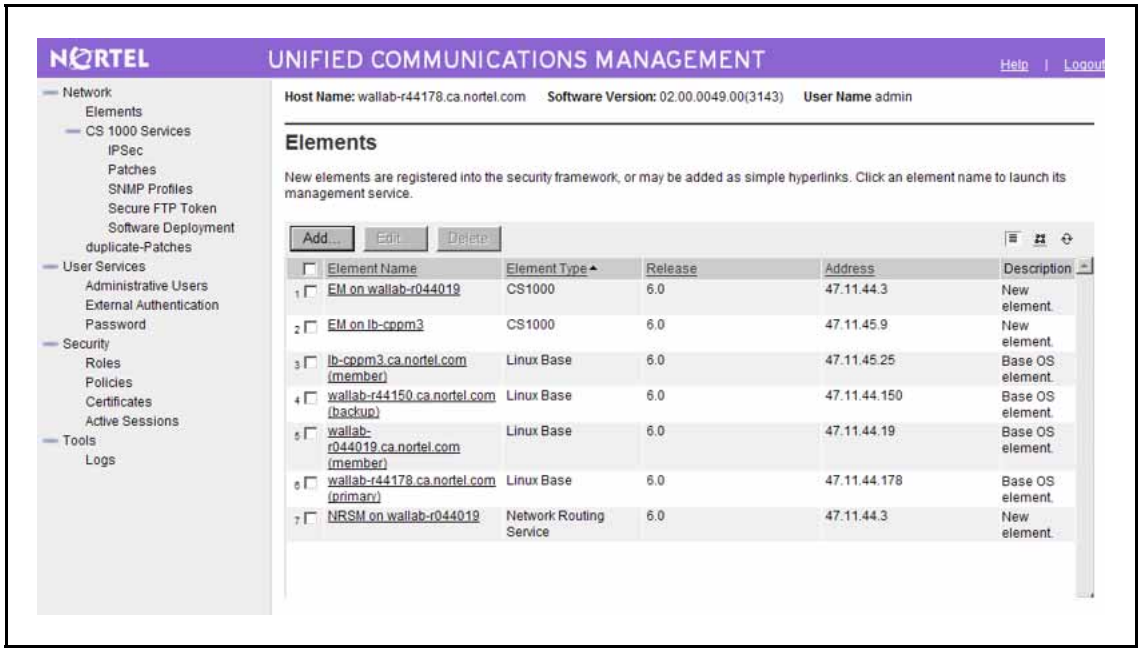
Base Manager access through UCM

Use Procedure 15 “Accessing Base Manager through UCM” (page 151) to access to Base Manager through UCM.

Procedure 15
Accessing Base Manager through UCM

Step	Action
1	Open the Web browser. ***Note:*** You must use Microsoft Internet Explorer 6.02600 or later.
2	Enter one of the following in the Address bar, and then press **Enter**: • Unified Communications Management (UCM) framework IP address. After you enter the UCM framework IP address, a Web page appears stating that you must access Unified Communications Management 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. • 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 user ID.
5	In the **Password** field, enter your password.
6	Click **Log In**. The UCM default navigation screen appears, as shown in Figure 130 "UCM default navigation window" (page 152).

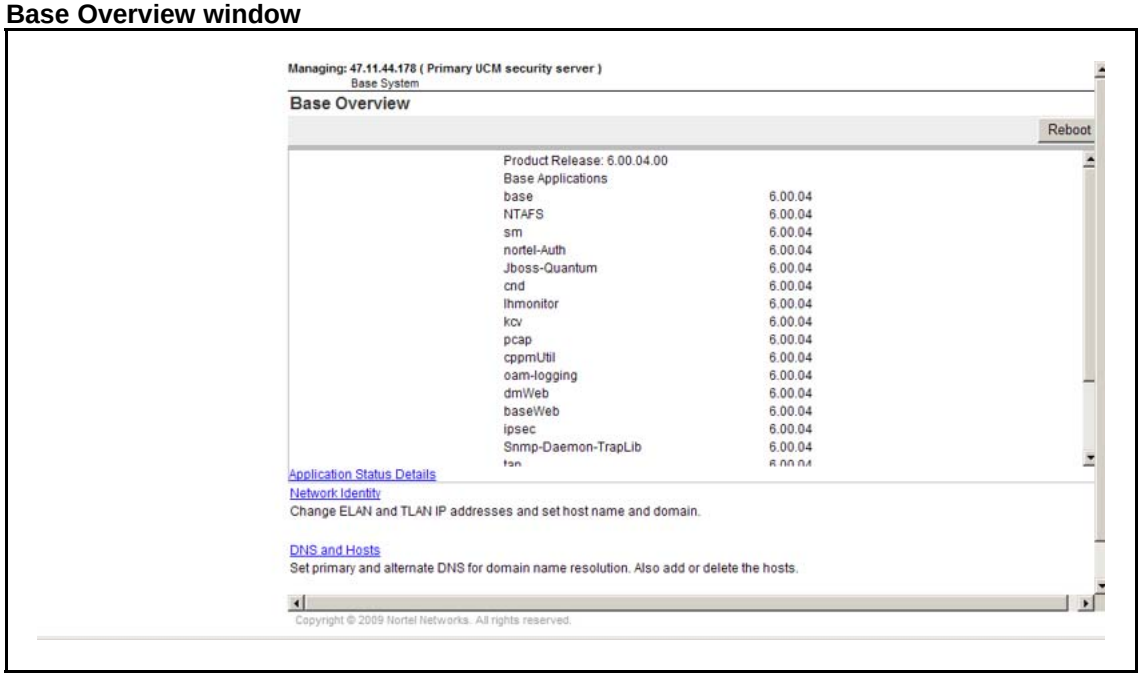
Figure 130
UCM default navigation window



7 On the **Elements** page of Unified Communications Management, under the **Element Name** column, click on an element of type Linux Base to navigate to Base Manager for that element.

The Base Overview page appears, as shown in Figure 131 "Base Overview window" (page 153).

Figure 131
Base Overview window



--End--

Base Manager access through local logon

Use Procedure 16 “Accessing Base Manager through local logon” (page 153) to log on to the server locally and access BM.

Procedure 16
Accessing Base Manager through local logon

Step	Action
1	Open the Web browser. ***Note:*** You must use Microsoft Internet Explorer 6.02600 or later.
2	Enter the following in the Address bar: http://<FQDN>/local-login The Server logon screen appears, as shown in Figure 132 "Server logon window" (page 154).

Figure 132
Server logon window

3 In the **User ID** type, enter a value for User ID.

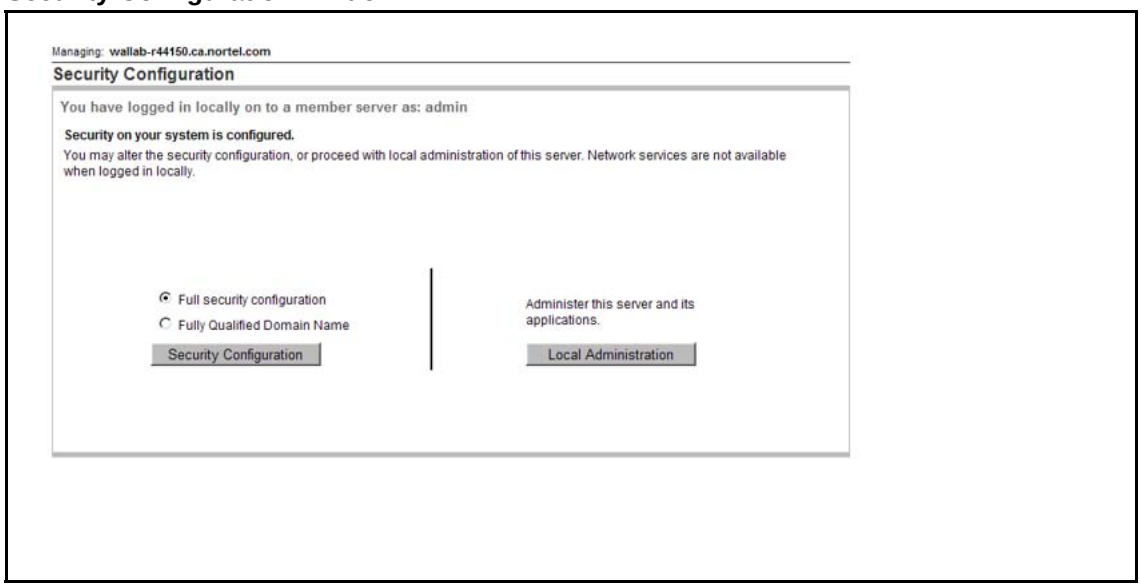
Note: You must use the **nortel** account to log on to the server locally.

4 In the **Password** field, type the password.

5 Click **Log In**.

The Security Configuration screen appears, as shown in Figure 133 "Security Configuration window" (page 154).

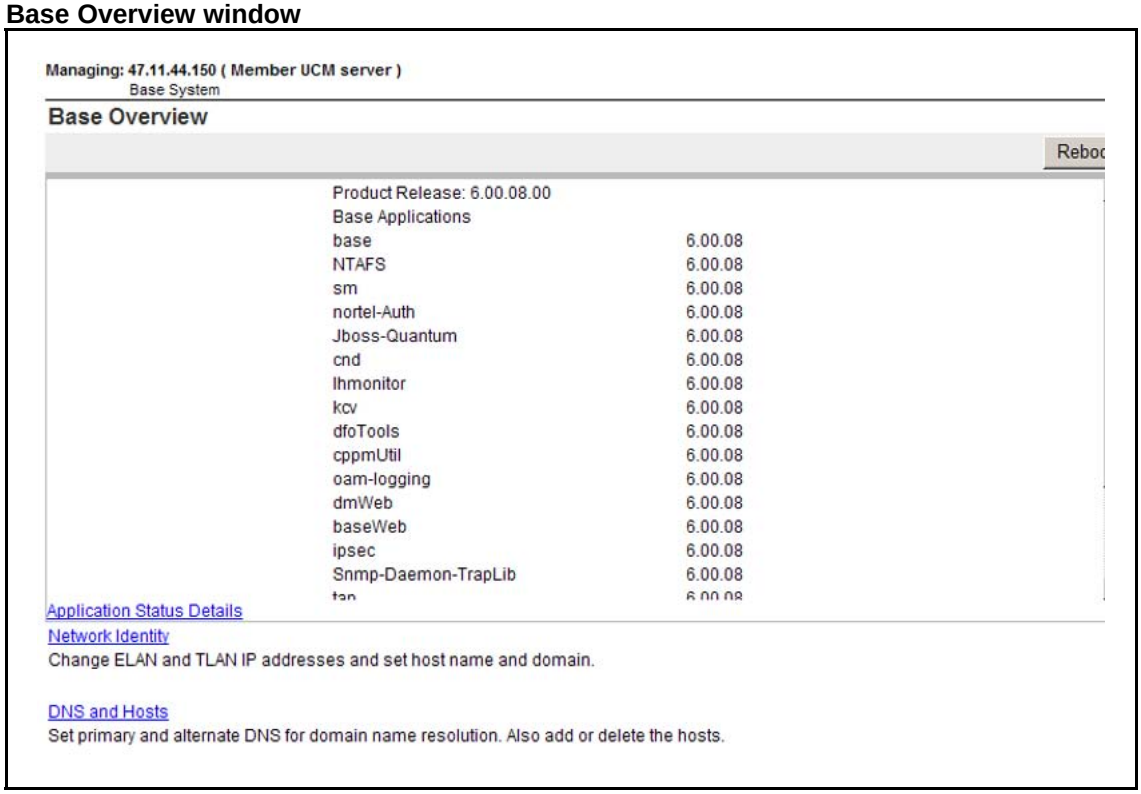
Figure 133
Security Configuration window



6 Click **Local Administration**.

Base Manager opens and the Base Overview screen appears, as shown in Figure 134 "Base Overview window" (page 155).

Figure 134
Base Overview window



--End--

Server reboot

Some procedures require a server reboot for configuration changes to take effect. Use Procedure 17 “Rebooting the server” (page 155) to reboot the server.

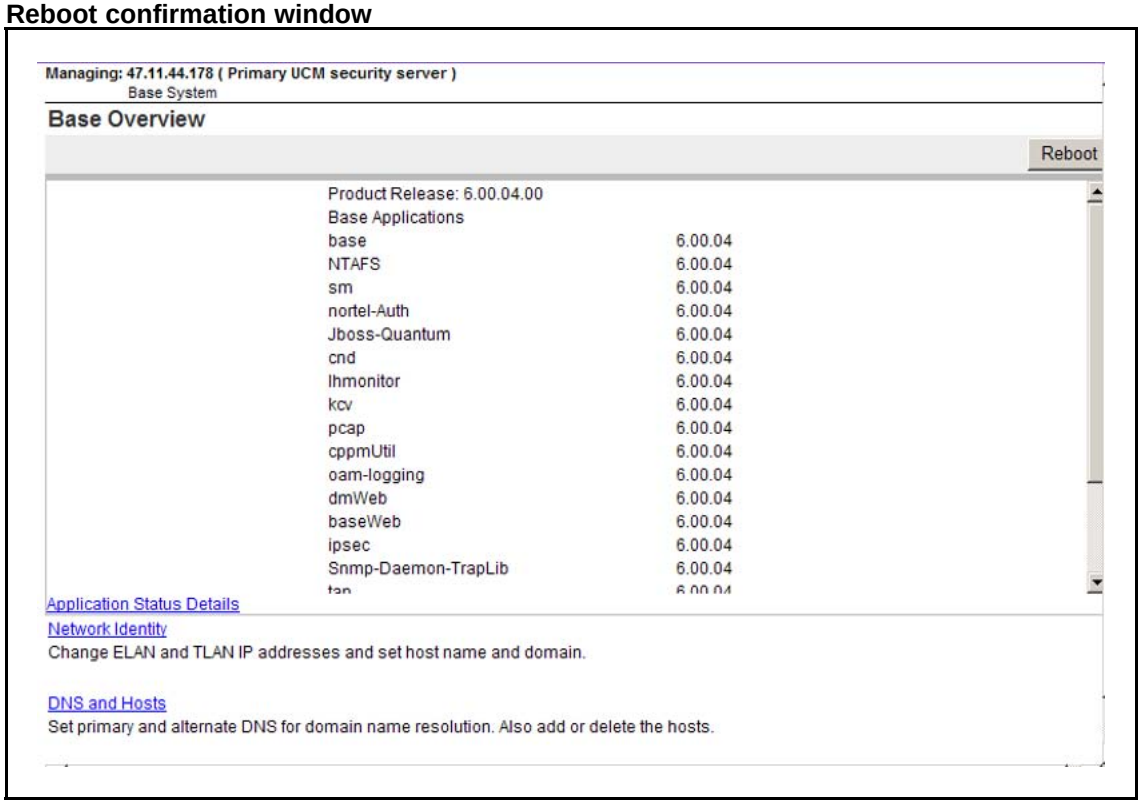
Procedure 17
Rebooting the server

Step	Action
1	Log on to UCM and navigate to Base Manager. See Procedure 15 “Accessing Base Manager through UCM” (page 151).
2	Press **Reboot**.

Note: You must have a user role of System Administrator to reboot the server. If you do not have a user role of System Administrator, the Reboot button is not active.

A confirmation screen appears, as shown in Figure 135 "Reboot confirmation window" (page 156).

Figure 135
Reboot confirmation window



3 Press **OK** to confirm the server restart.

--End--

Base system configuration using Base Manager

You can configure networking values by using BM. You can alter Telephony LAN (TLAN) and Embedded LAN (ELAN) values to edit the network identity, or add or delete hosts. You can add or delete routes to update route tables.

Use BM to configure date and time values. Set system values or configure automatic date and time values using network time servers.

You can also use BM to enable or disable Explicit Congestion Notification (ECN).

Edit the network identity

Note: You cannot change the FQDN or host name of the primary or backup server using BM; you must use CLI commands. Changing the FQDN or host name can have serious implications for the network. Consult *Unified Communications Management Fundamentals* (NN43001-116) before you attempt to change the FQDN or host name.

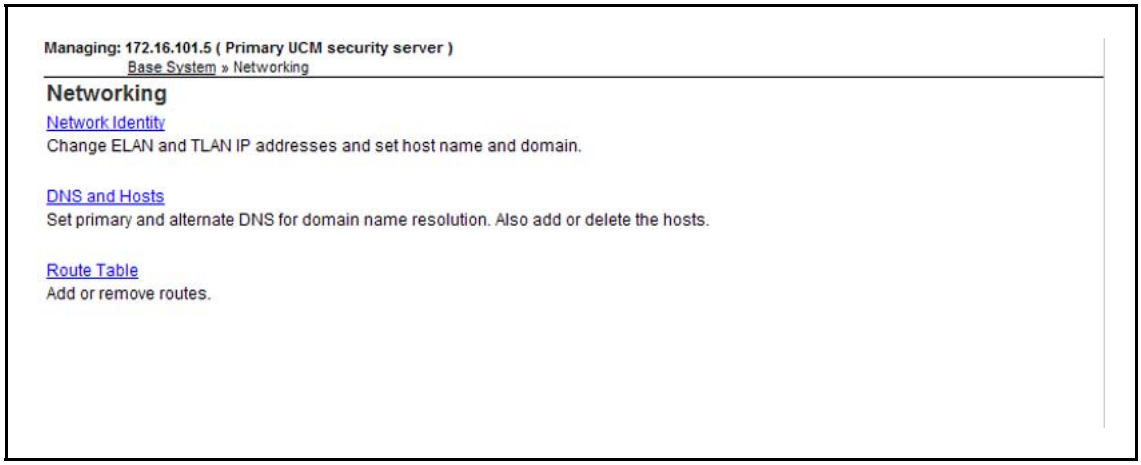
Use Procedure 18 “Editing network identity” (page 157) to manually edit values for ELAN and TLAN.

Note: After you edit the network identity, you must manually restart the server for the changes to take effect.

Procedure 18
Editing network identity

Step	Action
1	Log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing Base Manager, see Procedure 15 “Accessing Base Manager through UCM” (page 151). **OR** Log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, see Procedure 16 “Accessing Base Manager through local logon” (page 153).
2	In the navigation pane, select **Networking**. The Networking screen appears, as shown in Figure 136 "Networking window" (page 157).

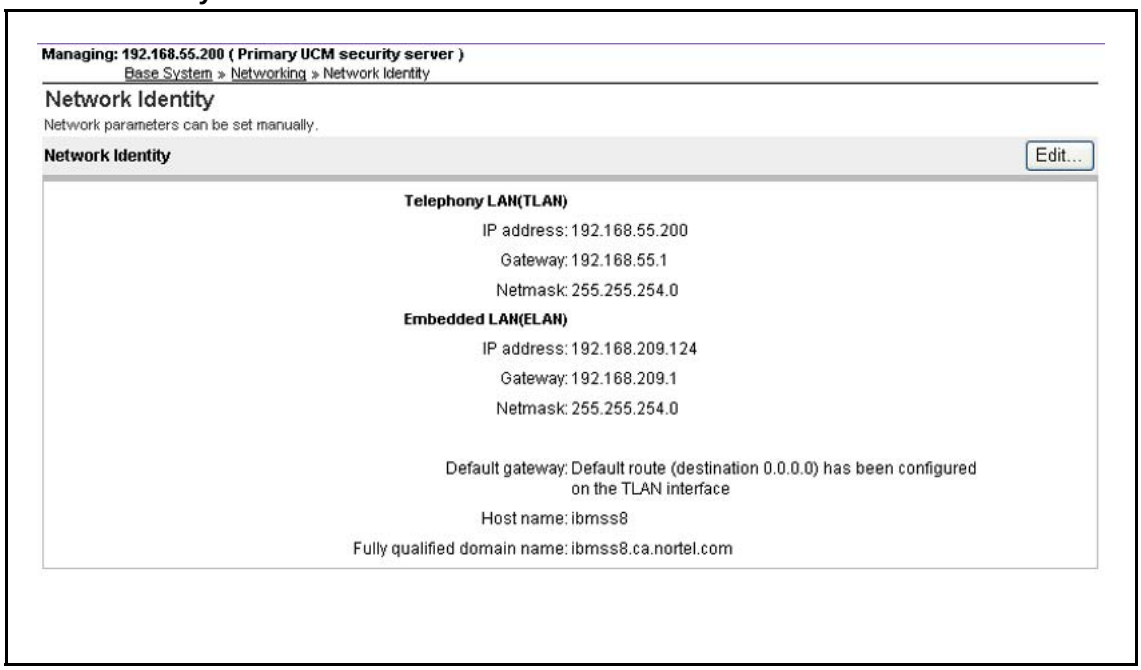
Figure 136
Networking window



3	In the Networking screen, click **Network Identity** .

The Network Identity screen appears, as shown in Figure 137 "Network Identity window" (page 158).

Figure 137
Network Identity window

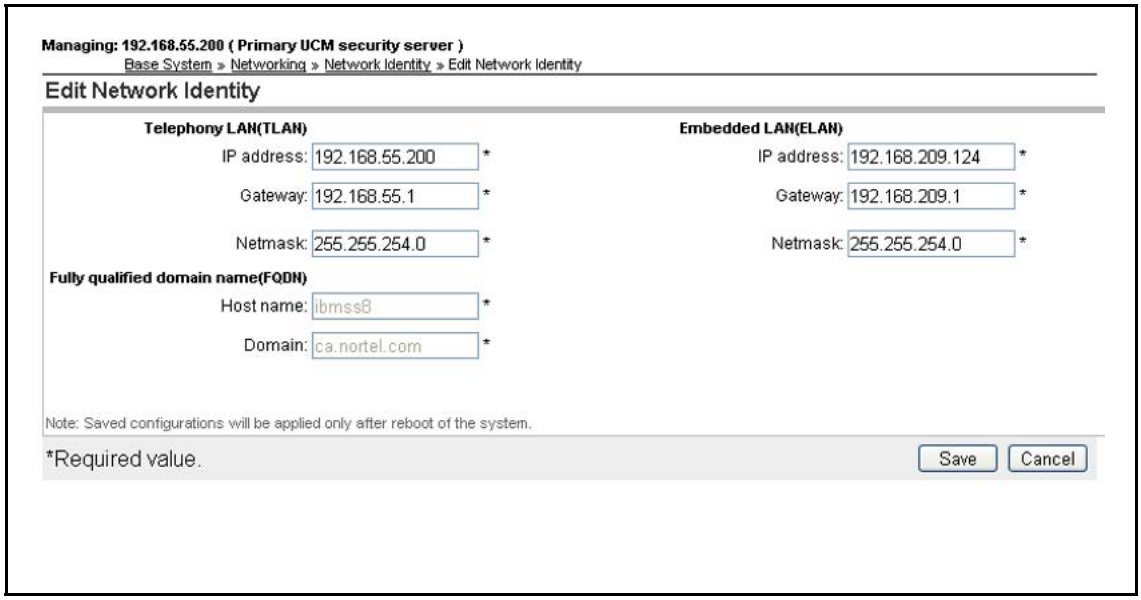


Note: If the TLAN IP address is not the default gateway value, a warning appears that indicates that the default gateway value is an IP address other than the TLAN IP address.

4 Click **Edit**.

The Edit Network Identity screen appears, as shown in Figure 138 "Edit Network Identity window" (page 159).

Figure 138
Edit Network Identity window



5 In the **TLAN IP address** box, you can enter a new value for TLAN IP address.

6 In the **TLAN Gateway** box, you can enter a value for TLAN gateway.

7 In the **TLAN Netmask** box, you can enter a value for TLAN netmask.

8 In the **ELAN IP address** box, you can enter a value for ELAN IP address.

9 In the **ELAN Gateway** box, you can enter a value for ELAN gateway.

10 In the **ELAN Netmask** box, you can enter a value for ELAN netmask.

11 Press **Save** to save your configuration changes.

OR

Press **Cancel** to discard your changes and return to the Network Identity screen.

12 Restart the server to apply configuration changes. See Procedure 17 “Rebooting the server” (page 155).

13 Verify the changes; log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing

Base Manager, see Procedure 15 “Accessing Base Manager through UCM” (page 151).

OR

Verify the changes; log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, see Procedure 16 “Accessing Base Manager through local logon” (page 153).

You can also verify network identity changes using the CLI commands **`ifconfig`** or **`networkconfig -show`**. For more information about Nortel Linux base CLI commands, see “ Nortel Linux base CLI commands” (page 265).

14 In the navigation pane select **Networking**, **Network Identity**.

The Network Identity screen displays any changes you have made.

--End--

DNS and Hosts

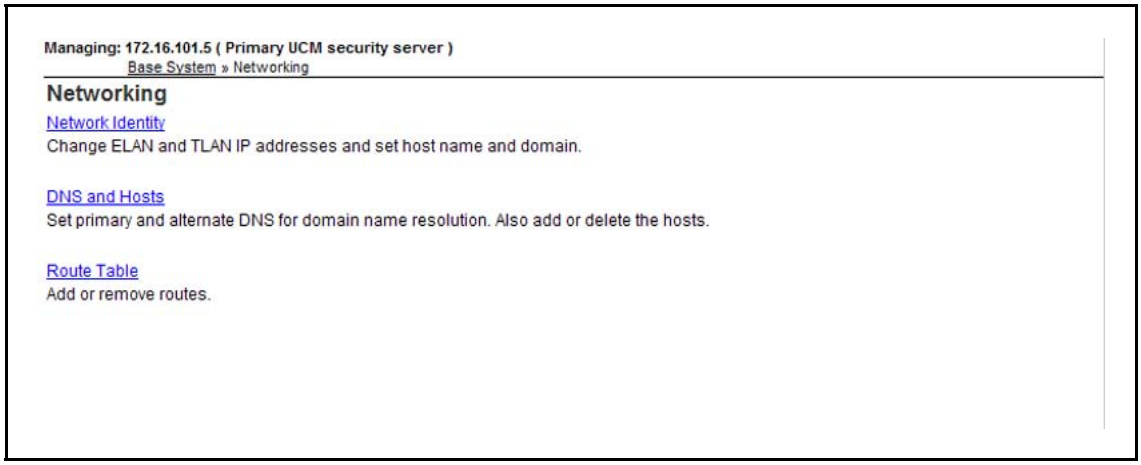
Use Procedure 19 “Adding a host” (page 160) to add a new host and Procedure 20 “Deleting a host” (page 163) to remove an existing host.

Use Procedure 19 “Adding a host” (page 160) to add a host value to the host table.

Procedure 19
Adding a host

Step	Action
1	Log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing Base Manager, see Procedure 15 “Accessing Base Manager through UCM” (page 151). **OR** Log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, see Procedure 16 “Accessing Base Manager through local logon” (page 153).
2	In the navigation pane, select **Networking**. The Networking screen appears, as shown in Figure 139 "Networking window" (page 161).

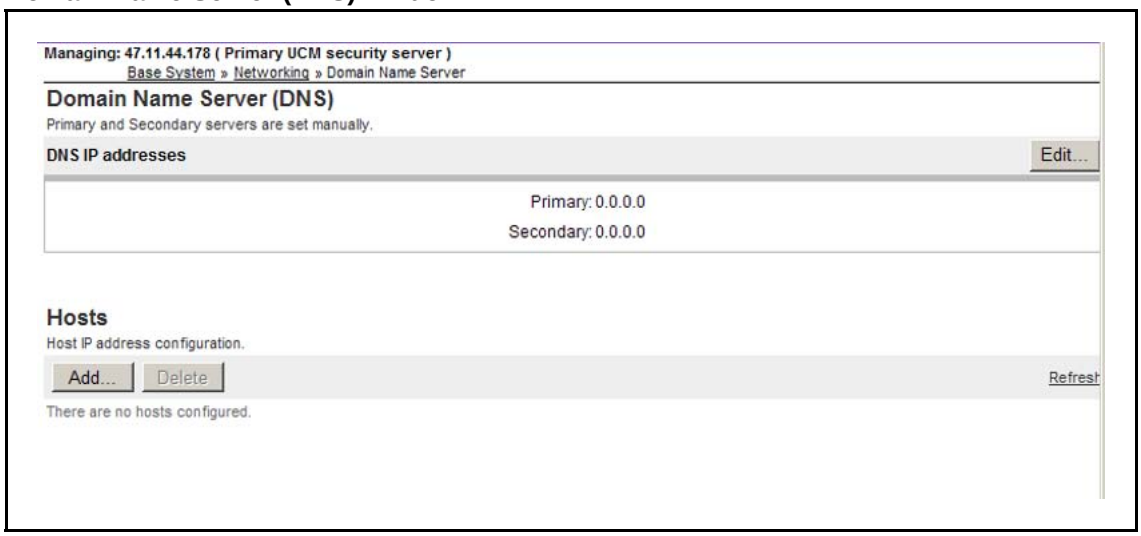
Figure 139
Networking window



3 In the Networking screen, select **DNS and Hosts**.

The Domain Name Server (DNS) screen appears, as shown in Figure 140 "Domain Name Server (DNS) window" (page 161).

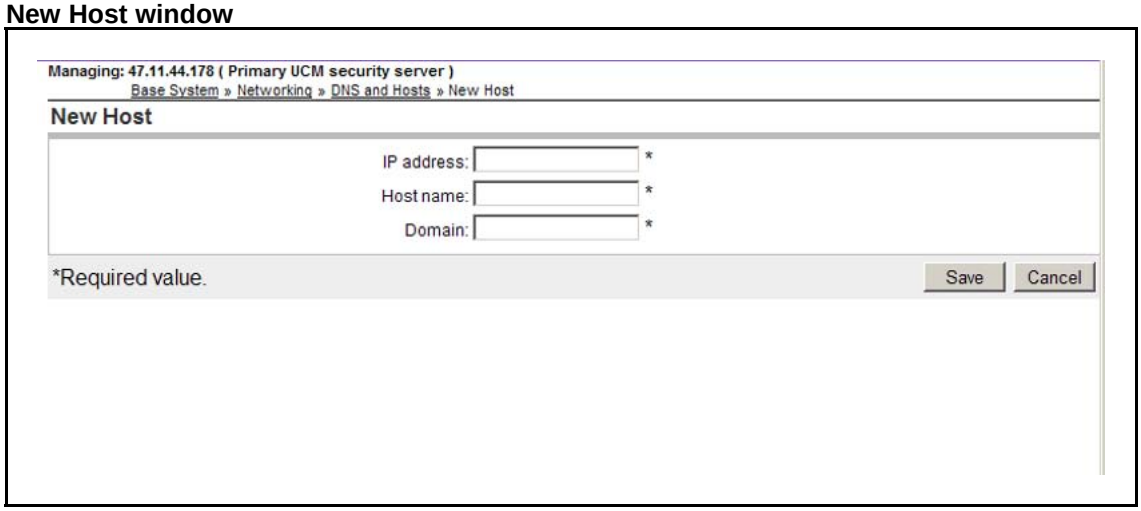
Figure 140
Domain Name Server (DNS) window



4 Click **Add**.

The New Host screen appears, as shown in Figure 141 "New Host window" (page 162).

Figure 141
New Host window



5 In the **IP address** field, enter a value for IP address.

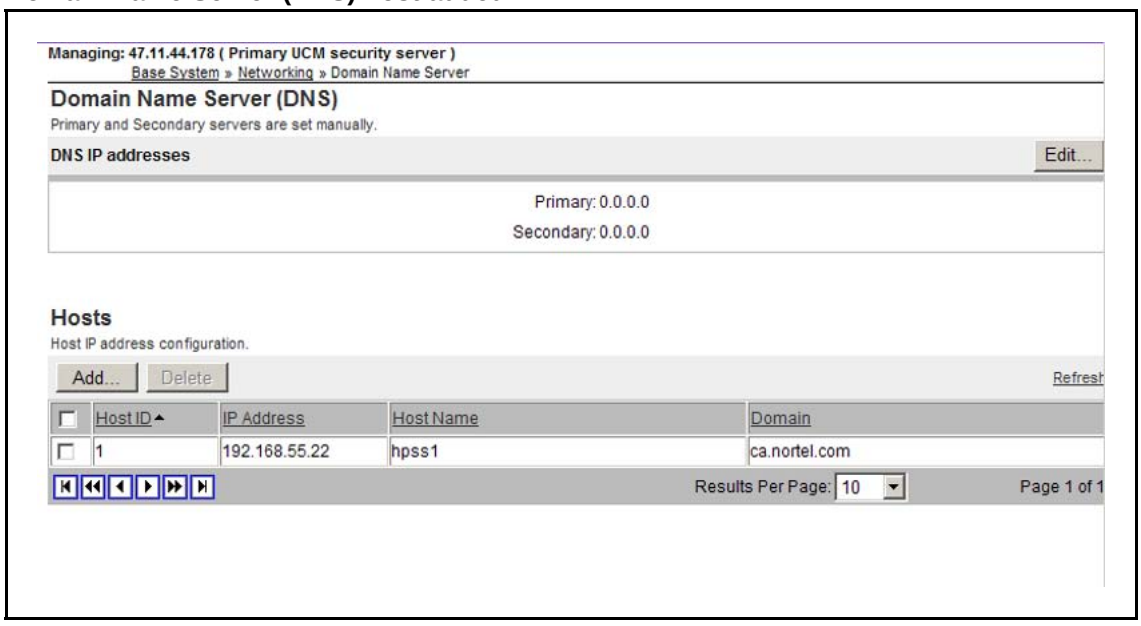
6 In the **Host name** field, enter a value for host name.

7 In the **Domain** field, enter a value for Domain.

8 Click **Save**.

The Domain Name Server (DNS) screen displays the new host, as shown in Figure 142 "Domain Name Server (DNS) host added" (page 162) .

Figure 142
Domain Name Server (DNS) host added



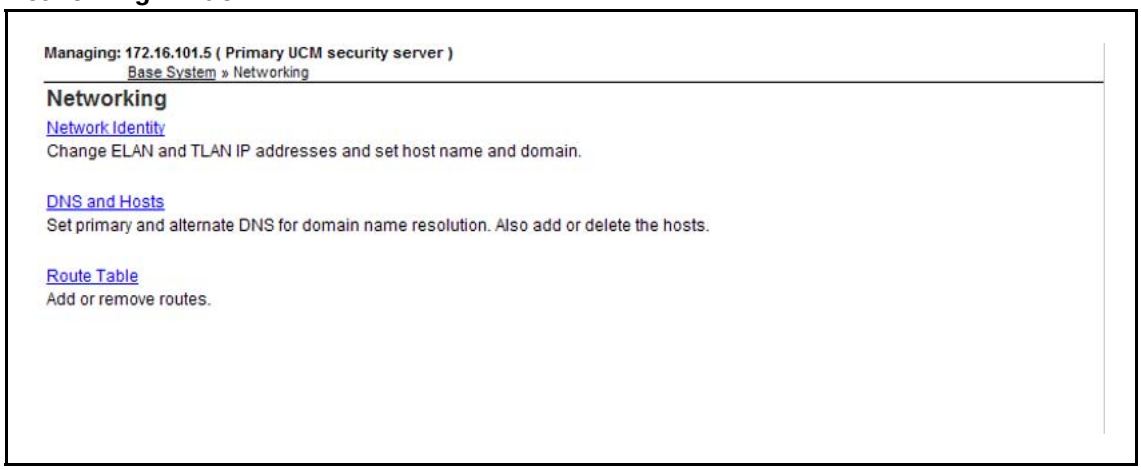
--End--

Use Procedure 20 “Deleting a host” (page 163) to delete a host value from the host table.

Procedure 20
Deleting a host

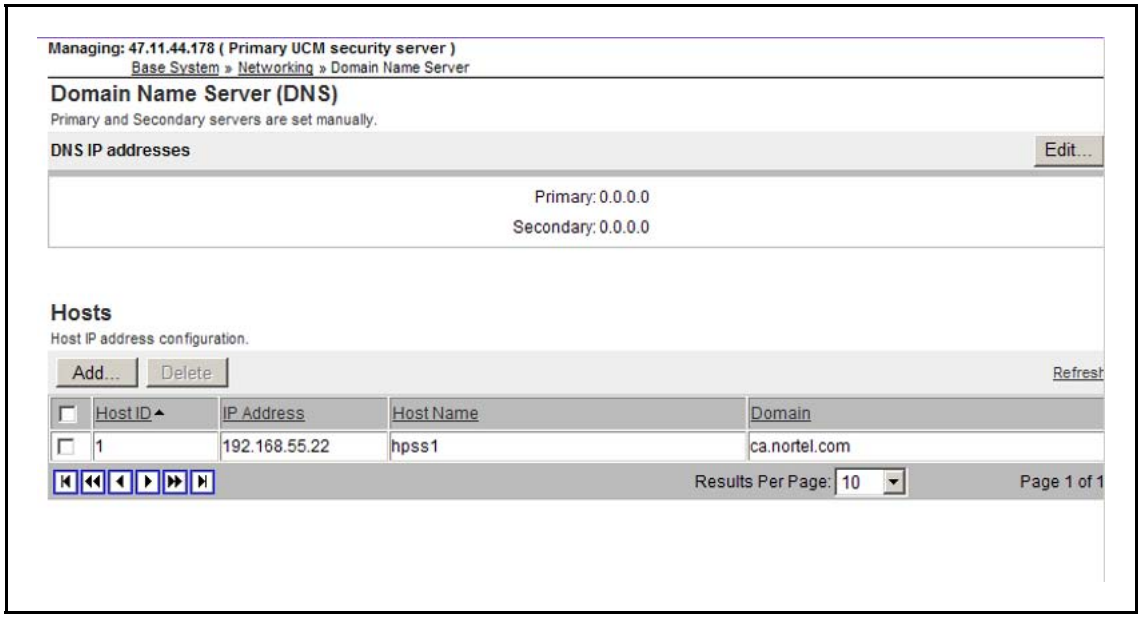
Step	Action
1	Log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing Base Manager, see Procedure 15 “Accessing Base Manager through UCM” (page 151). **OR** Log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, seeProcedure 16 “Accessing Base Manager through local logon” (page 153).
2	In the navigation pane, select **Networking**. The Networking screen appears, as shown in Figure 143 "Networking window" (page 163).

Figure 143
Networking window



3	In the Networking screen, select **DNS and Hosts**. The Domain Name Server (DNS) screen appears, as shown in Figure 144 "Domain Name Server (DNS) window" (page 164).

Figure 144
Domain Name Server (DNS) window



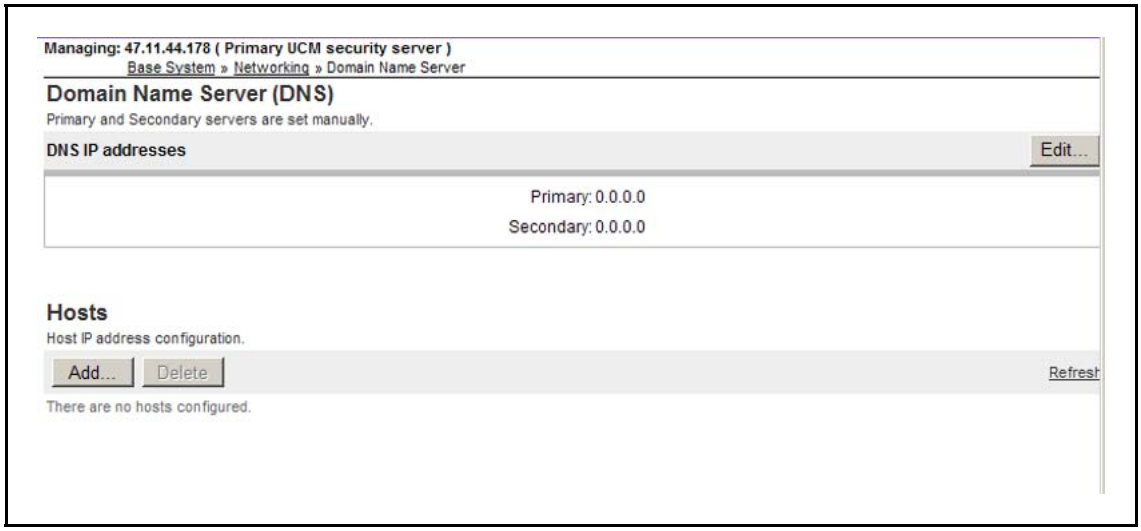
4 Select the host that you want to delete.

The Delete button becomes active.

5 Click **Delete**.

The Domain Name Server (DNS) screen appears and the host is removed, as shown in Figure 145 "Domain Name Server (DNS) host removed" (page 164).

Figure 145
Domain Name Server (DNS) host removed

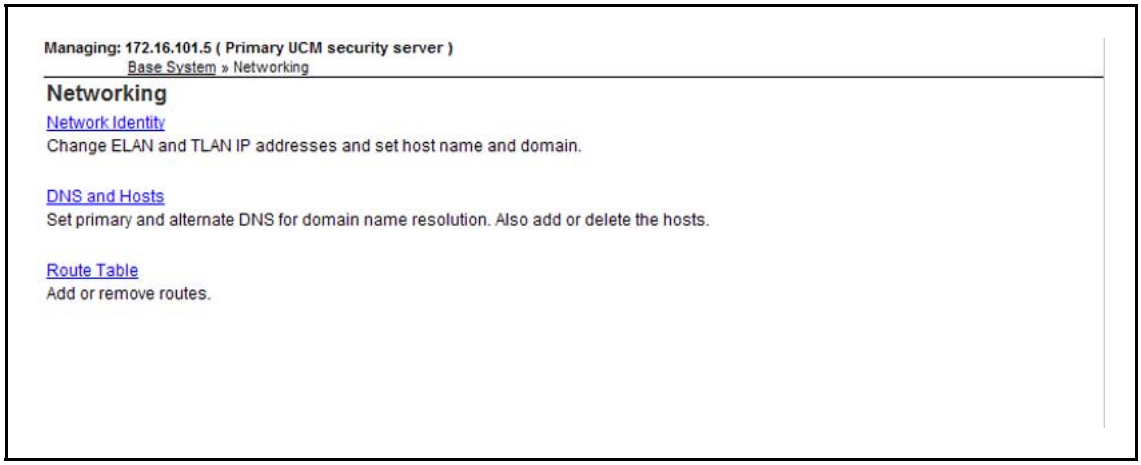


--End--

Procedure 21
Adding a route entry

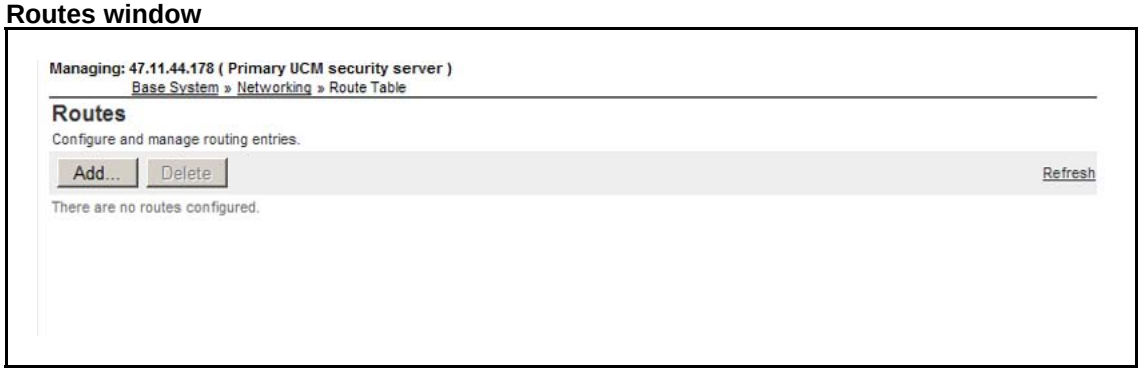
Step	Action
1	Log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing Base Manager, see Procedure 15 “Accessing Base Manager through UCM” (page 151). **OR** Log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, seeProcedure 16 “Accessing Base Manager through local logon” (page 153).
2	In the navigation pane, select **Networking**. The Networking screen appears, as shown in Figure 146 "Networking window" (page 165).

Figure 146
Networking window



Step	Action
3	In the Networking screen, select **Route Table**. The Routes screen appears, as shown in Figure 147 "Routes window" (page 165).

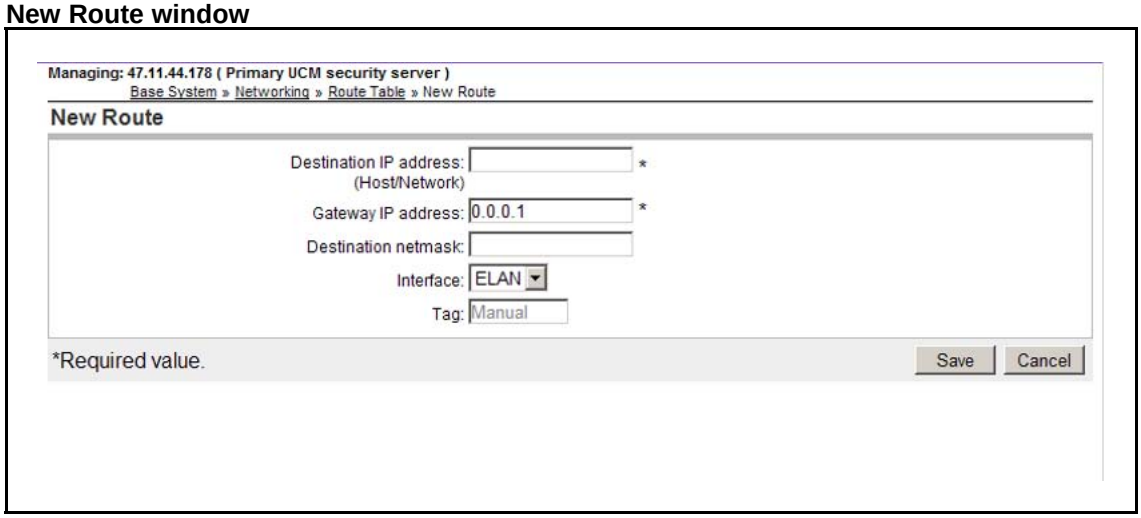
Figure 147
Routes window



4 Click **Add**.

The New Route screen appears, as shown in Figure 148 "New Route window" (page 166).

Figure 148
New Route window



5 In the **Destination IP address** box, enter a value for the destination IP address.

Note: Nortel recommends that the Call Server (CS) and Element Manager (EM) reside on the same subnet. When the CS and EM reside on different subnets, you must configure a route from the EM server to the CS server, using the CS IP address as the destination address and the EM server ELAN gateway as the interface value.

6 In the **Gateway IP address** box, enter a value for gateway IP address.

7 In the **Destination netmask** box, you can enter a value for destination netmask.

Note: You do not need to provide a netmask. If you do provide a netmask, the format must be 255.255.255.255.

8 In the **Interface** list, you can select a value for network interface.

9 Press **Save** to save your configuration changes.

OR

Press **Cancel** to discard your changes and return to the Routes screen.

--End--

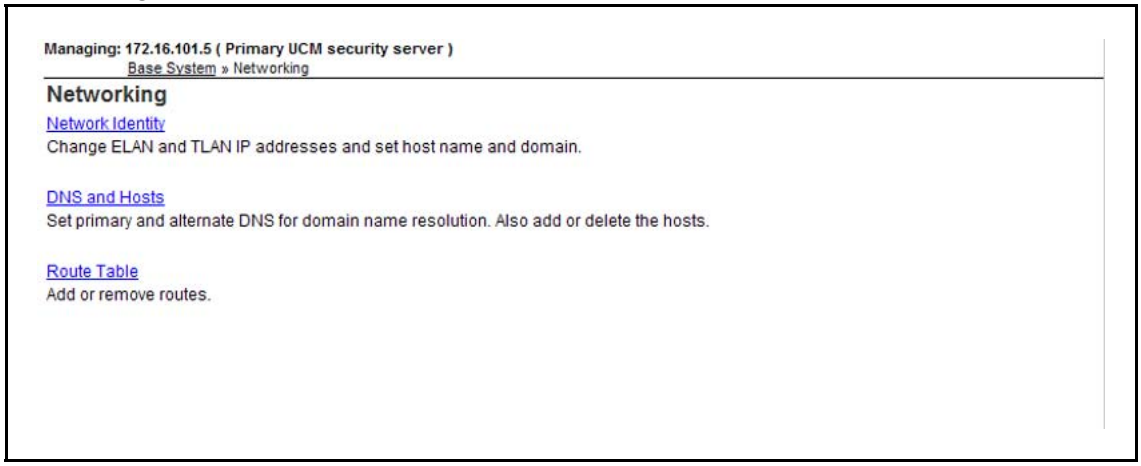
Use Procedure 22 “Deleting a route entry” (page 167) to delete an entry from the routing table.

Note: All routes configured in Base Manager have a Tag value of Manual. Routes with other Tag values are inserted by applications; these routes should only be modified or deleted by configuring the application. Do not use Base Manager to delete a route inserted by an application; this can lead to a malfunction in the application.

Procedure 22
Deleting a route entry

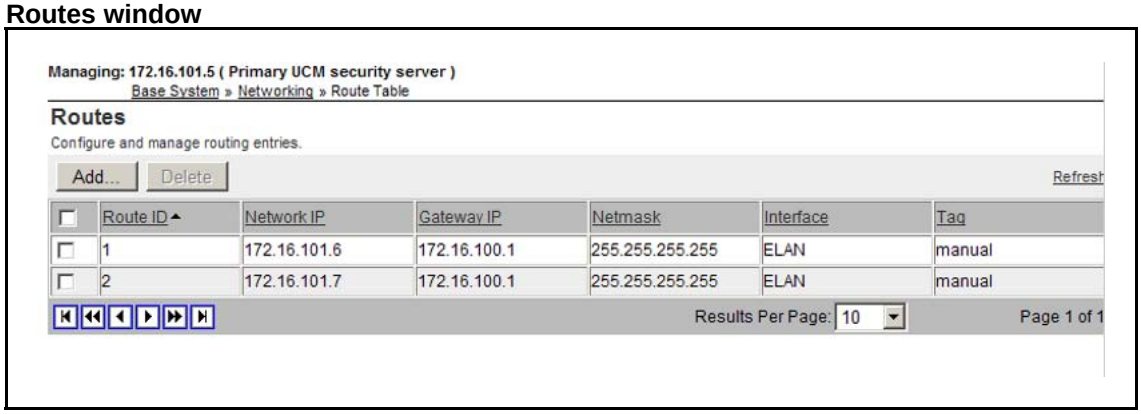
Step	Action
1	Log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing Base Manager, see Procedure 15 “Accessing Base Manager through UCM” (page 151). **OR** Log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, seeProcedure 16 “Accessing Base Manager through local logon” (page 153).
2	In the navigation pane, select **Networking**. The Networking screen appears, as shown in Figure 149 "Networking window" (page 167).

Figure 149
Networking window



3	In the Networking screen, select **Route Table**. The Routes screen appears.

Figure 150
Routes window

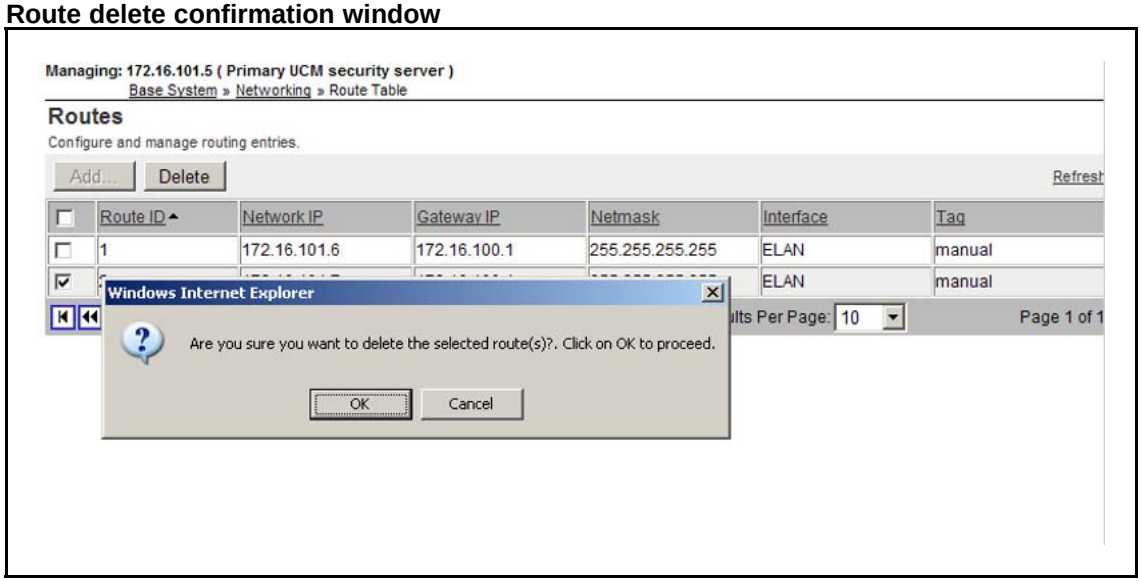


4 Select the route that you want to delete.

5 Click **Delete**.

The Route delete confirmation screen appears, as shown in Figure 151 "Route delete confirmation window" (page 168).

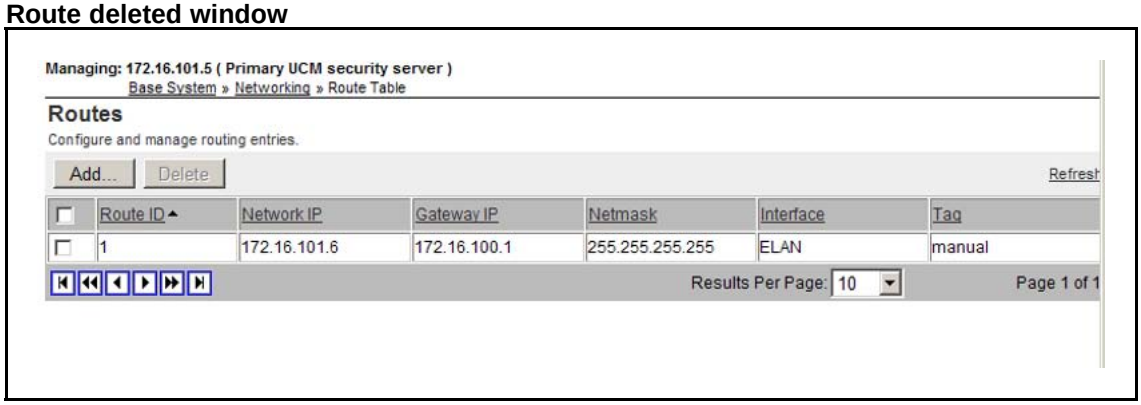
Figure 151
Route delete confirmation window



6 Click **OK**.

The route is deleted, as shown in Figure 152 "Route deleted window" (page 169).

Figure 152
Route deleted window



--End--

Explicit network congestion

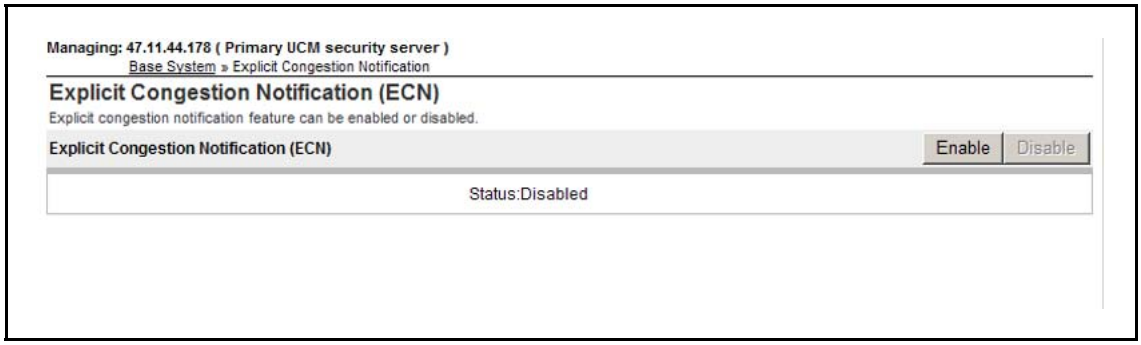
Explicit Congestion Notification in the Internet Protocol allows the server and a router to exchange notifications in cases of network congestion. If the data network is relatively poor the Linux server can be given higher priority network routing treatment by enabling the explicit network congestion setting.

Note: The routers in the network infrastructure must also support the explicit network congestion feature.

Procedure 23
Configuring Explicit Congestion Notification

Step	Action
1	Log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing Base Manager, see Procedure 15 “Accessing Base Manager through UCM” (page 151). **OR** Log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, seeProcedure 16 “Accessing Base Manager through local logon” (page 153).
2	In the navigation pane, select **Explicit Congestion Notification**. The ECN screen appears, as shown in Figure 153 "Explicit Congestion Notification window" (page 170).

Figure 153
Explicit Congestion Notification window



3 Press **Enable** to enable Explicit Congestion Notification.

OR

Press **Disable** to disable Explicit Congestion Notification.

--End--

Date and time

Use Procedure 24 “Configuring system date and time” (page 171) to manually configure system date and time values; use Procedure 25 “Synchronizing date and time with network time servers” (page 174) to configure date and time values using a Network Time Protocol (NTP) server.

The NTP client running on the Linux element obtains time updates by polling an NTP server. The polling interval ranges from 64 to 1024 seconds. After a restart of the element or after NTP synchronization configuration, the initial polling interval is 64 seconds. As the clock stabilizes the interval doubles until it reaches the maximum of 1024 seconds. The polling interval decreases if the clock is not stable; the polling interval increases if the clock cannot be reached. For a newly installed system it can take an additional 15 minutes (approximately) for the clock to stabilize the first time synchronization occurs.

After the clock stabilizes, there can be situations where the NTP clock source time changes. In these situations you can use the Sync Now feature in Base Manager to force an immediate time synchronization, rather than wait as long as 1024 seconds for the next poll to occur.

Note 1: Internally there is no way to distinguish the Sync Now request failure caused by initial configuration having just been performed from other rare error conditions (such as NTP software not responding). Any errors from the Sync Now operation are ignored.

Note 2: You can configure a maximum of 11 external clock source IP addresses for the primary NTP server; you can configure a maximum of 10 IP addresses for the secondary NTP server.

If you configure NTP parameters synchronization is done automatically; you do not need to use the Sync Now feature.

System date and time configuration

Use Procedure 24 “Configuring system date and time” (page 171) to manually configure system values for date and time.

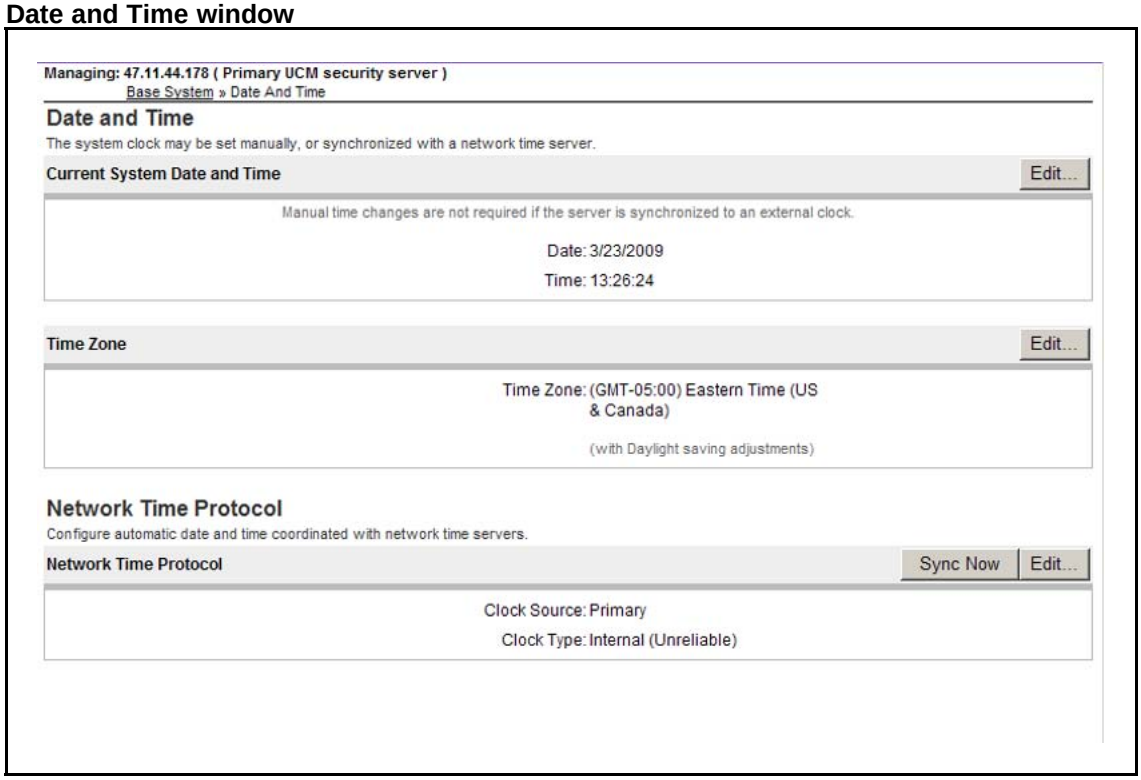
Prerequisites

You must log on using a role from the systemadmin or timeadmin access groups to perform date and time configuration.

Procedure 24
Configuring system date and time

Step	Action
1	Log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing Base Manager, see Procedure 15 “Accessing Base Manager through UCM” (page 151). **OR** Log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, seeProcedure 16 “Accessing Base Manager through local logon” (page 153).
2	In the navigation pane, select **Date and Time**. The date and Time screen appears, as shown in Figure 154 "Date and Time window" (page 172).

Figure 154
Date and Time window

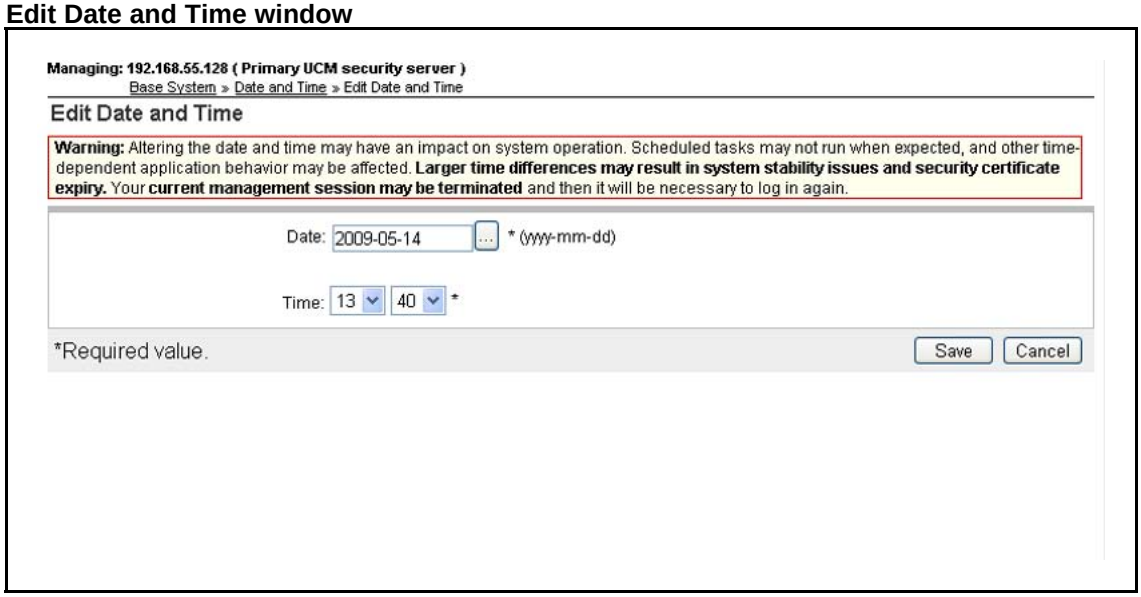


3 Navigate to the **Current System Date and Time** section.

4 Click **Edit**.

The Edit Date and Time screen appears, as shown in Figure 155 "Edit Date and Time window" (page 172).

Figure 155
Edit Date and Time window



5 In the **Date** box, enter the date in the format yyyy-mm-dd.

WARNING
If you modify the date and time to a future value, your session expires and the initial Base Manager screen displays.

OR

Press the Browse (...) button to select the date from a calendar.

6 In the **Time** lists, select values for hours (hh) and minutes (mm).

7 Click **Save** to save your configuration changes.

OR

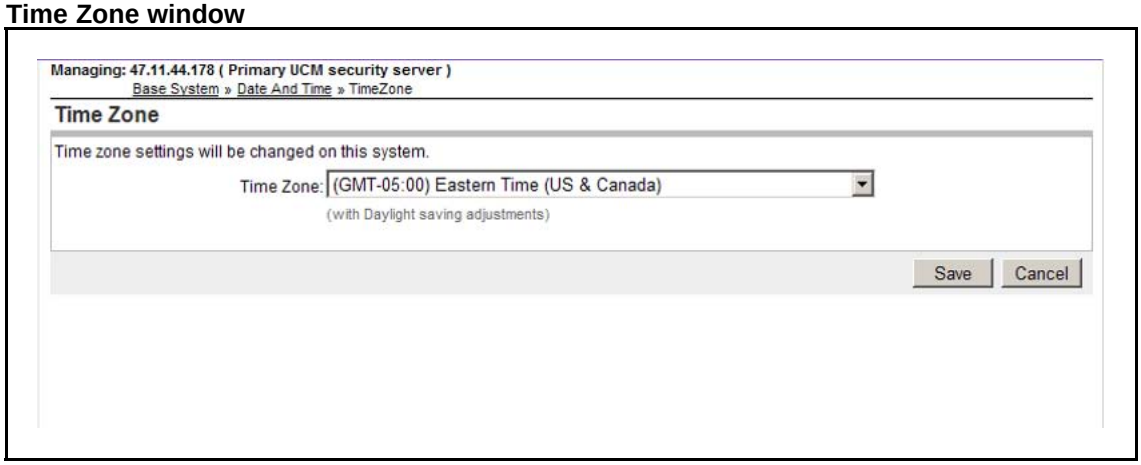
Press **Cancel** to discard your changes and return to the Date and Time screen.

8 Navigate to the **Time Zone** section.

9 Click **Edit**.

The Time Zone screen appears, as shown in .

Figure 156
Time Zone window



10 In the **Time Zone** list, select a value for Time Zone.

11 Click **Save** to save your configuration changes.

OR

Press **Cancel** to discard your changes and return to the Date and Time screen.

--End--

Use Procedure 25 “Synchronizing date and time with network time servers” (page 174)to synchronize system date and time values with network time servers.

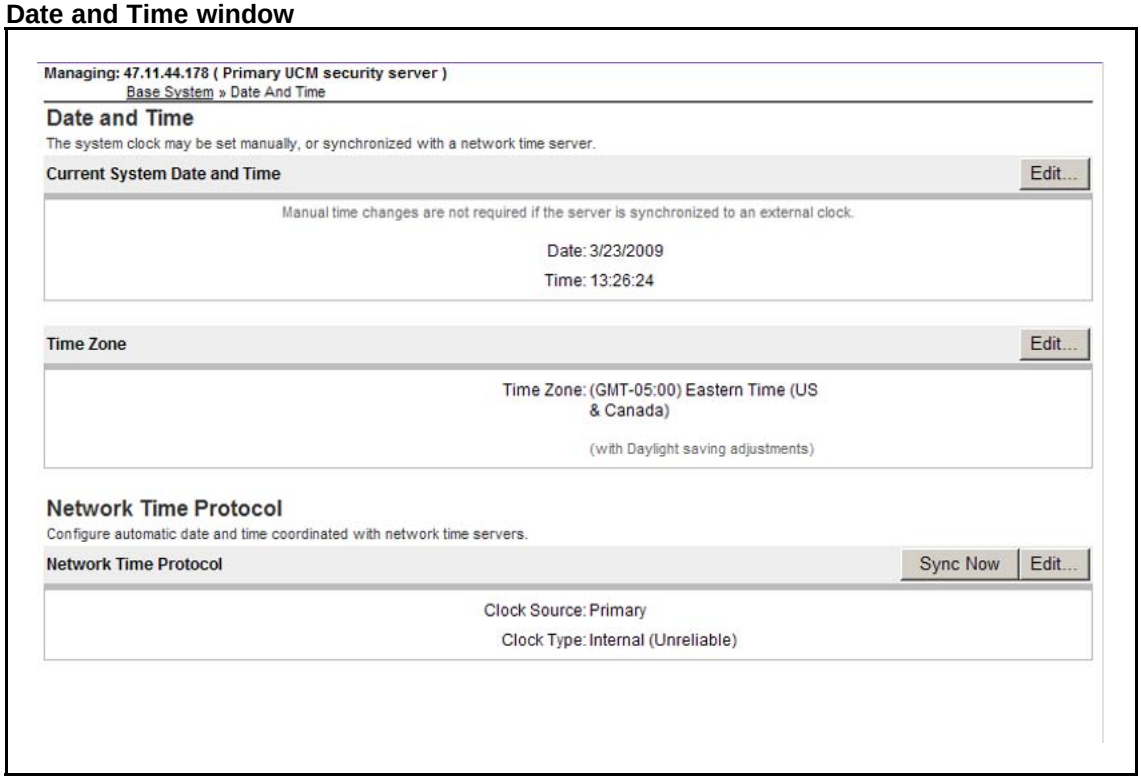
Prerequisites

You must log on using a role from the systemadmin or timeadmin access groups to perform date and time configuration.

Procedure 25
Synchronizing date and time with network time servers

Step	Action
1	Log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing Base Manager, see Procedure 15 “Accessing Base Manager through UCM” (page 151). **OR** Log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, seeProcedure 16 “Accessing Base Manager through local logon” (page 153).
2	In the navigation pane, select **Date and Time**. The date and Time screen appears, as shown in Figure 157 "Date and Time window" (page 175).

Figure 157
Date and Time window



3 Navigate to the **Network Time Protocol** section.

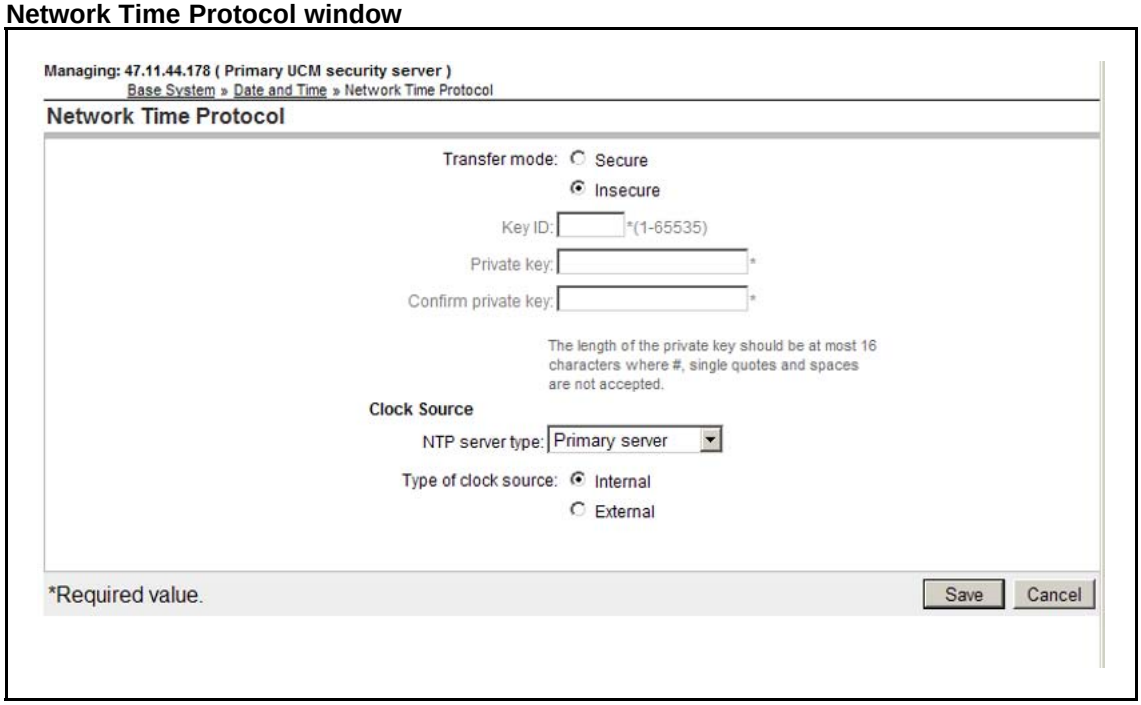
4 If you want to force an immediate time synchronization with the NTP server click **Sync Now**.

The time is synchronized with the NTP server and the procedure ends at this point.

5 Click **Edit**.

The Network Time Protocol screen appears, as shown in Figure 158 "Network Time Protocol window" (page 176).

Figure 158
Network Time Protocol window



6 Perform Procedure 26 “Configuring NTP transfer mode” (page 177)

.

7 If you are configuring the clock source for a primary NTP server, perform Procedure 27 “Configuring the clock source for a primary server” (page 177).

8 If you are configuring the clock source for a secondary NTP server, perform Procedure 28 “Configuring the clock source for a secondary server” (page 179).

9 If you are configuring the clock source for a server that is not a clock source, perform Procedure 29 “Configuring a server that is not a clock server” (page 182).

--End--

NTP transfer mode configuration

Configure NTP to operate using a secure or insecure transfer mode. If you choose a secure transfer mode you must also provide a key ID and private key.

Prerequisites

You must log on using a role from the systemadmin or timeadmin access groups to perform date and time configuration.

Procedure 26
Configuring NTP transfer mode

Step	Action
1	Navigate to the Transfer mode section.
2	If you want an insecure transfer mode select the **Insecure** option. Proceed to step 7 in Procedure 25 “Synchronizing date and time with network time servers” (page 174). **OR** If you want a secure transfer mode select the **Secure** option.
3	In the **Key ID** field, enter a value for key ID.
4	In the **Private key** field, enter a value for private key.
5	Proceed to step 7 in Procedure 25 “Synchronizing date and time with network time servers” (page 174).

--End--

Clock source configuration for a primary server

Configure the clock source for a primary server.

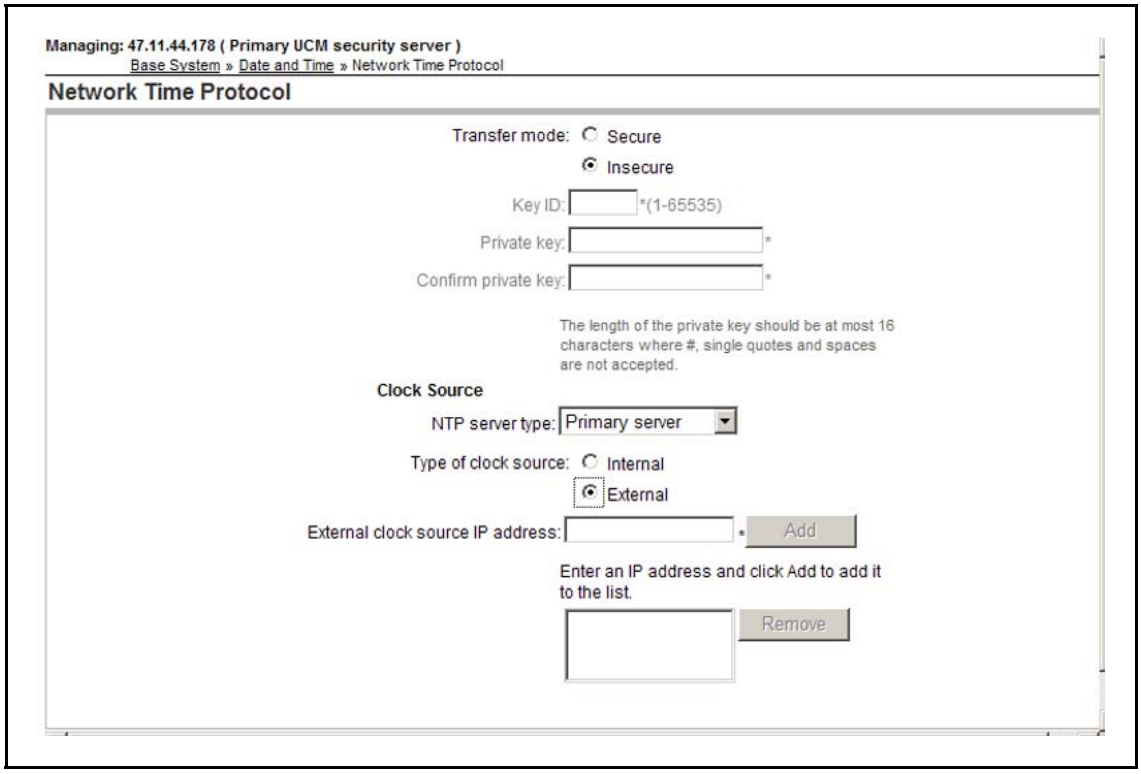
Prerequisites

You must log on using a role from the systemadmin or timeadmin access groups to perform date and time configuration.

Procedure 27
Configuring the clock source for a primary server

Step	Action
1	Navigate to the Clock Source section.
2	Select **Primary** in the **NTP server type** list.
3	In the type of clock source list, select **Internal**. if you want an internal clock source.
4	In the type of clock source list, select **External**. if you want an external clock source. If you select an external clock source, additional fields appear on the screen, as shown in Figure 159 "Primary server clock source window" (page 178).

Figure 159
Primary server clock source window

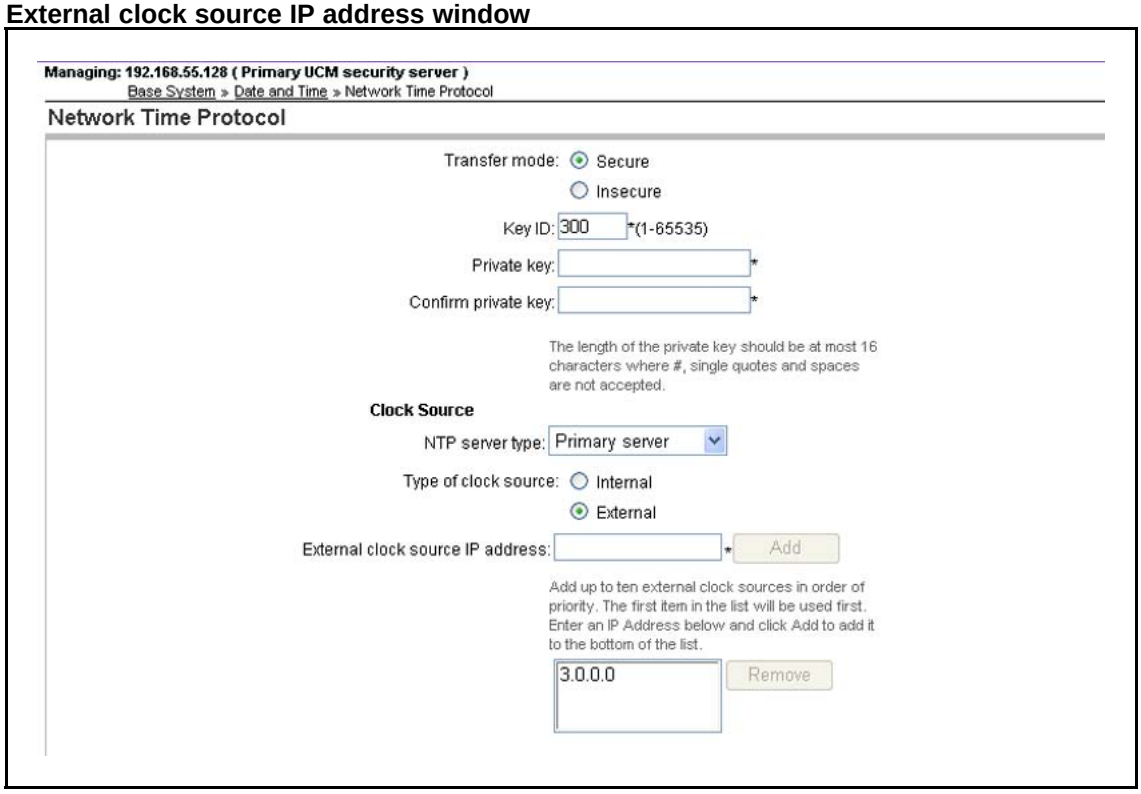


5 In the **External clock source IP address** field, type a value for the external clock source IP address.

6 Click **Add**.

The value is added to the list of IP addresses, as shown in Figure 160 "External clock source IP address window" (page 179).

Figure 160
External clock source IP address window



7 If you want to remove a value from the IP address list, highlight the value and click **Remove**.

8 Click **Save** to save the clock source configuration.

OR

Click **Cancel** to return to the Date and Time screen.

--End--

Clock source configuration for a secondary server

Configure the clock source for a secondary server.

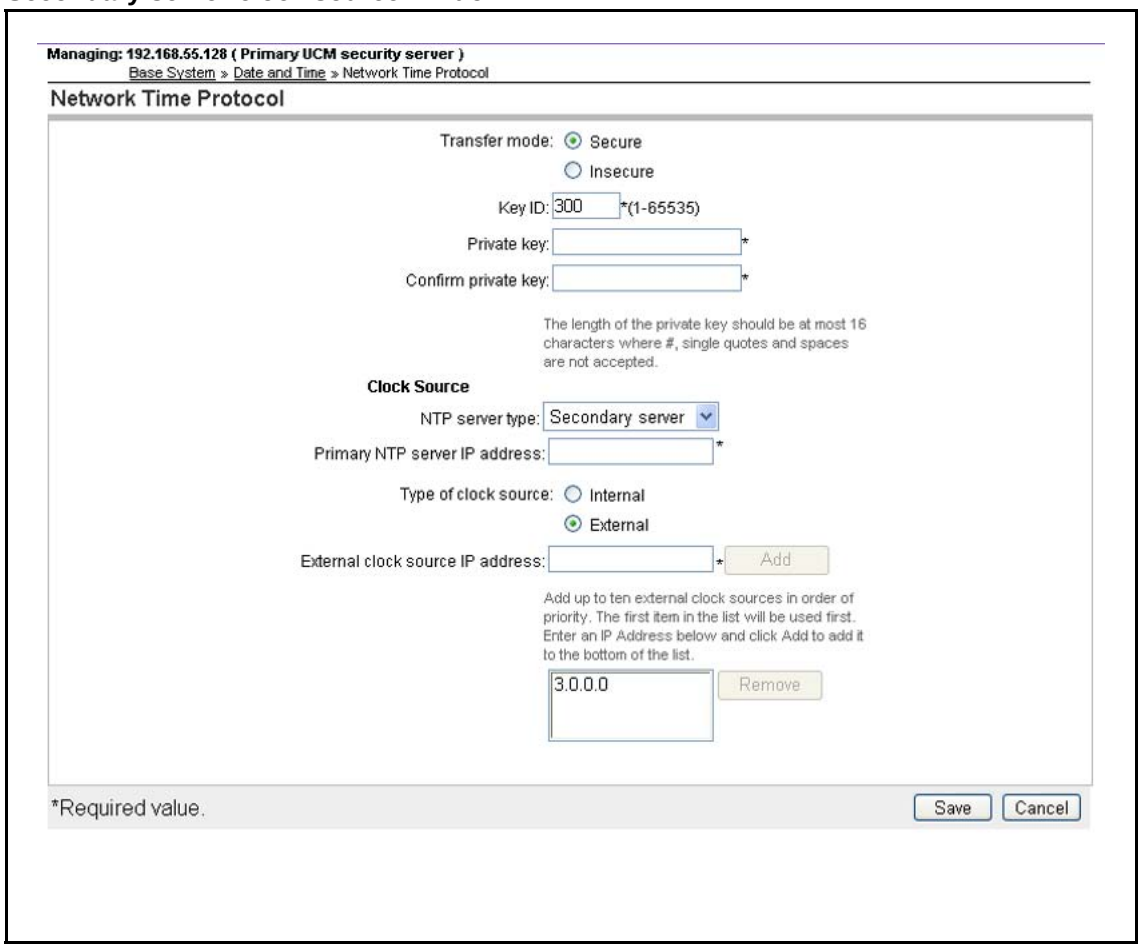
Prerequisites

You must log on using a role from the systemadmin or timeadmin access groups to perform date and time configuration.

Procedure 28
Configuring the clock source for a secondary server

Step	Action
1	Navigate to the Clock Source section.
2	Select **Secondary** in the **NTP server type** list.
3	In the **Primary NTP server IP address** field, type a value for the IP address of the primary NTP server.
4	In the Type of clock source list, select **Internal**. if you want an internal clock source.
5	In the Type of clock source list, select **External**. if you want an external clock source. If you select an external clock source, additional fields appear on the screen, as shown in Figure 161 "Secondary server clock source window" (page 180).

Figure 161
Secondary server clock source window

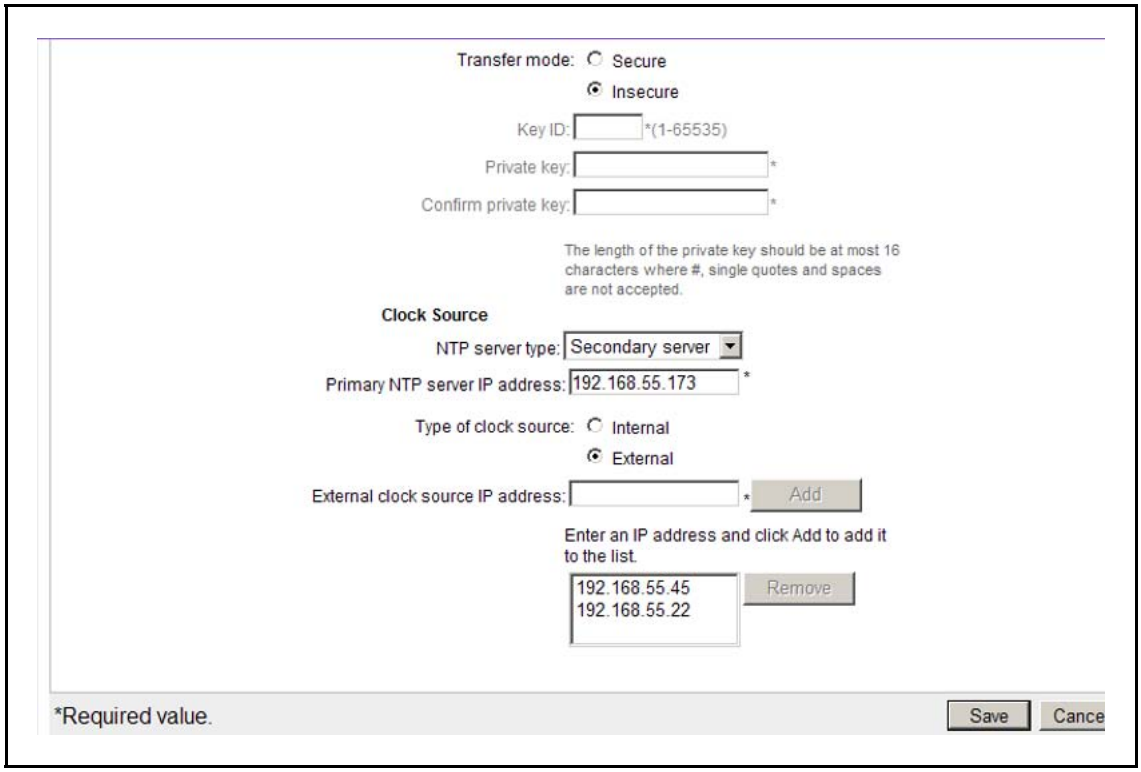


6	In the **External clock source IP address** field, type a value for the external clock source IP address.

7 Click **Add**.

The value is added to the list of IP addresses, as shown in Figure 162 "External clock source IP address (secondary server) window" (page 181).

Figure 162
External clock source IP address (secondary server) window



8 If you want to remove a value from the IP address list, highlight the value and click **Remove**.

9 Click **Save** to save the clock source configuration.

OR

Click **Cancel** to return to the Date and Time screen.

--End--

Clock source configuration for a server that is not a clock server

Configure the clock source for a server that is not a clock server.

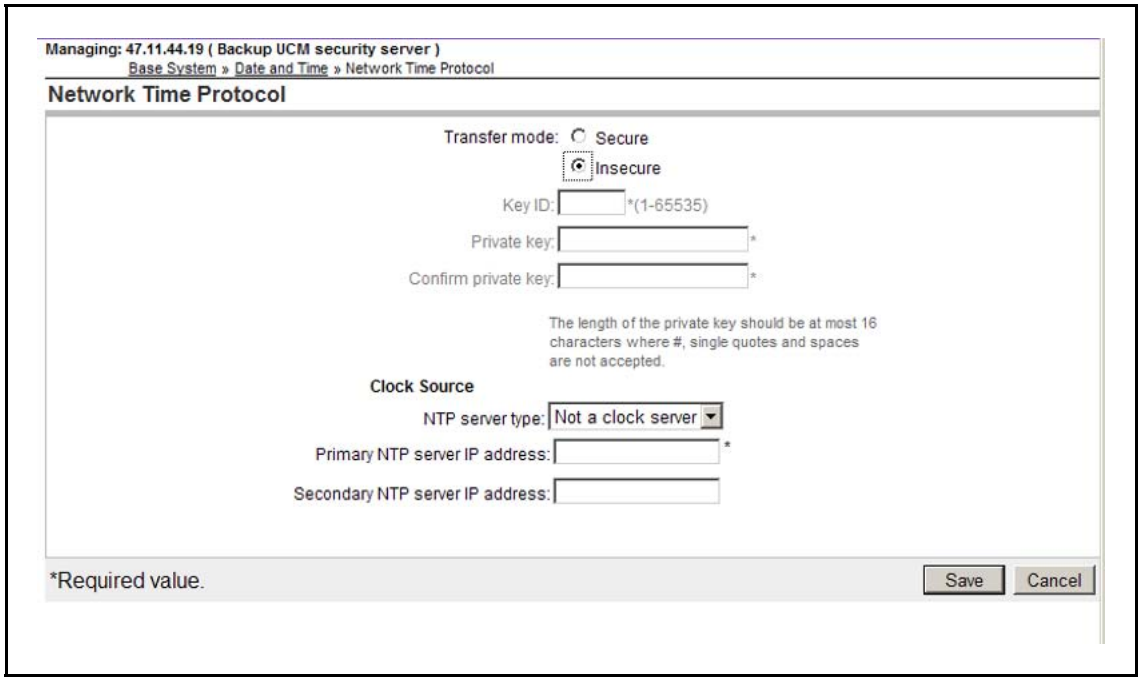
Prerequisites

You must log on using a role from the systemadmin or timeadmin access groups to perform date and time configuration.

Procedure 29
Configuring a server that is not a clock server

Step	Action
1	Navigate to the Clock Source section.
2	Select **Not a clock server** in the **NTP server type** list. The clock source fields appear, as shown in Figure 163 "Clock source fields for a server that is not a clock server" (page 182).

Figure 163
Clock source fields for a server that is not a clock server



3	In the **Primary NTP server IP address** field type a value for the IP address of the primary NTP server.
4	In the **Secondary NTP server IP address** type a value for the IP address of the secondary NTP server. ***Note:*** Use of a secondary NTP server is optional.
5	Click **Save** to save the clock source configuration. **OR** Click **Cancel** to return to the Date and Time screen.

--End--

Software maintenance using Base Manager

Stopping or restarting applications can impact system operations. It may be desirable to gracefully idle down the system or transfer operations to other redundant devices before stopping or restarting. Restarting or stopping an application can affect other systems, as in the case of network wide virtual office or branch office. Restarting or stopping an application can also cause some applications to issue alarms or generate logs.

There are operational impacts and interactions among applications. Before you stop an application it may be necessary to stop dependant applications. Table 5 "Applications and dependencies" (page 183) provides a list of interactions among applications.

Table 5
Applications and dependencies

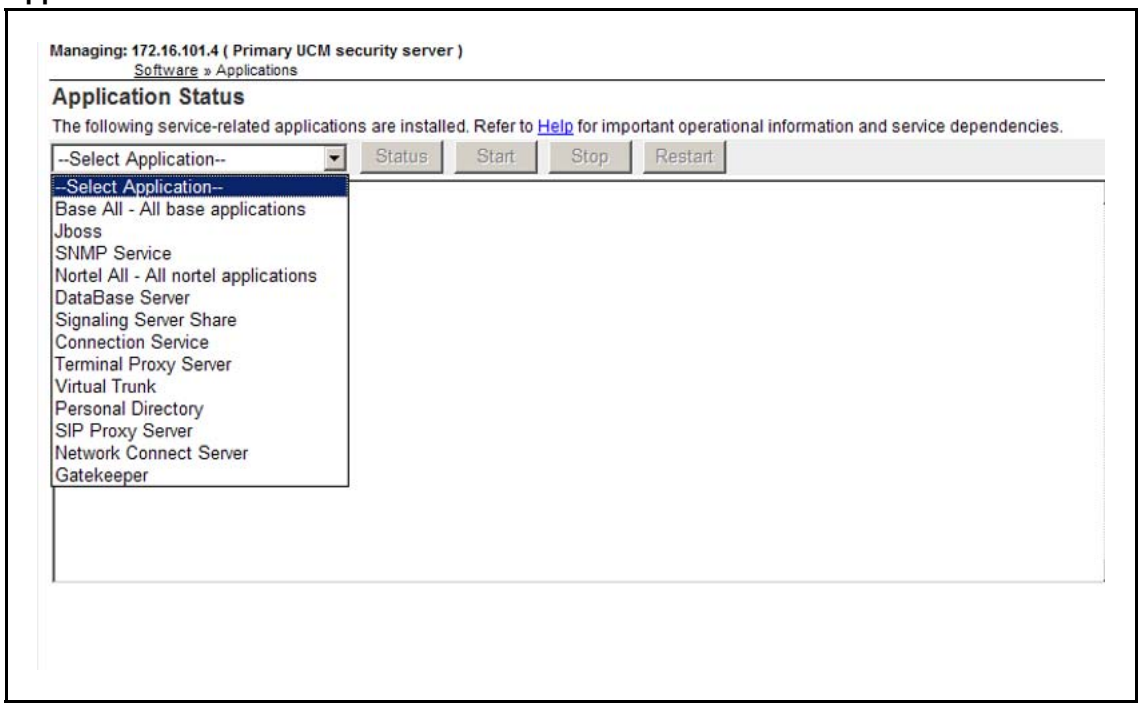
Application	Impact
Base - all	Impacts base and all Nortel applications.
Jboss	Impacts all management applications. ***Note:*** The web session is disrupted if you restart Jboss.
SNMP	Affects the ability of other applications to send traps.
Database server	Impacts most applications (CS, SS, PD, SIPL, NRS, SubM, EM).
Signaling Server	Impacts TPS, CSV, VTRK, and PD.
Virtual Trunk (VTRK)	Impacts SS applications.
Connection Service (CSV)	Impacts TPS.
Terminal Proxy Server (TPS)	Can be stopped independently.
Personal Directory (PD)	Can be stopped independently.
SIP Proxy server	Can be stopped independently.
Gatekeeper	Can be stopped independently.
Network Connect Server	Can be stopped independently.
Nortel - all	Impacts all higher level applications (all related to call processing).

Use Procedure 30 “Managing application status” (page 183) to view the status of installed applications and to start, stop, or restart the applications.

Procedure 30
Managing application status

Step	Action
1	Log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing Base Manager, see Procedure 15 “Accessing Base Manager through UCM” (page 151). **OR** Log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, seeProcedure 16 “Accessing Base Manager through local logon” (page 153).
2	In the navigation pane, select **Software**, **Applications**. The Application Status screen appears, as shown in Figure 164 "Application Status window" (page 184).

Figure 164
Application Status window



3	Select an application from the application list. ***Note 1:*** If you select **Base All** you can only perform the status operation. If you select **Jboss** you can only perform status and restart operations. For all other applications status, start, stop, and restart operations are valid. ***Note 2:*** For start, stop, and restart operations, a confirmation message is displayed when you select the operation.
4	Click **Status** to display the status of the application.
5	Click **Start** to start the application.

6 Click **Stop** to stop the application.

7 Click **Restart** to restart the application.

--End--

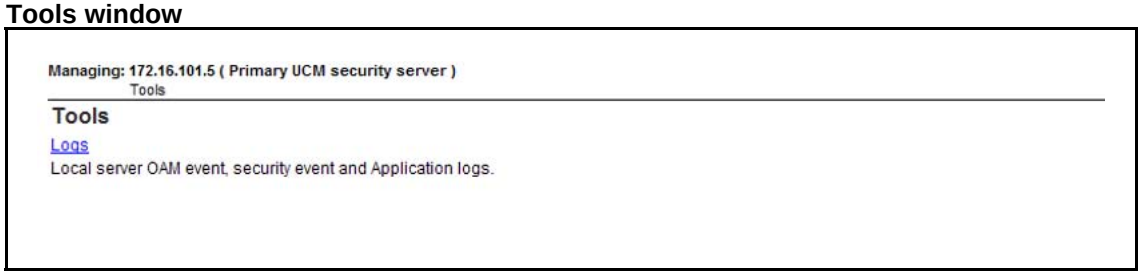
View and export logs using Base Manager

Base Manager provides access to logs generated by installed applications. You can choose to view the logs in BM, or you can export the logs to a file which can be saved locally.

Procedure 31
Viewing application logs

Step	Action
1	Log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing Base Manager, see Procedure 15 “Accessing Base Manager through UCM” (page 151). **OR** Log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, seeProcedure 16 “Accessing Base Manager through local logon” (page 153).
2	In the navigation pane. select **Tools**, The Tools screen appears, as shown in Figure 165 "Tools window" (page 185).

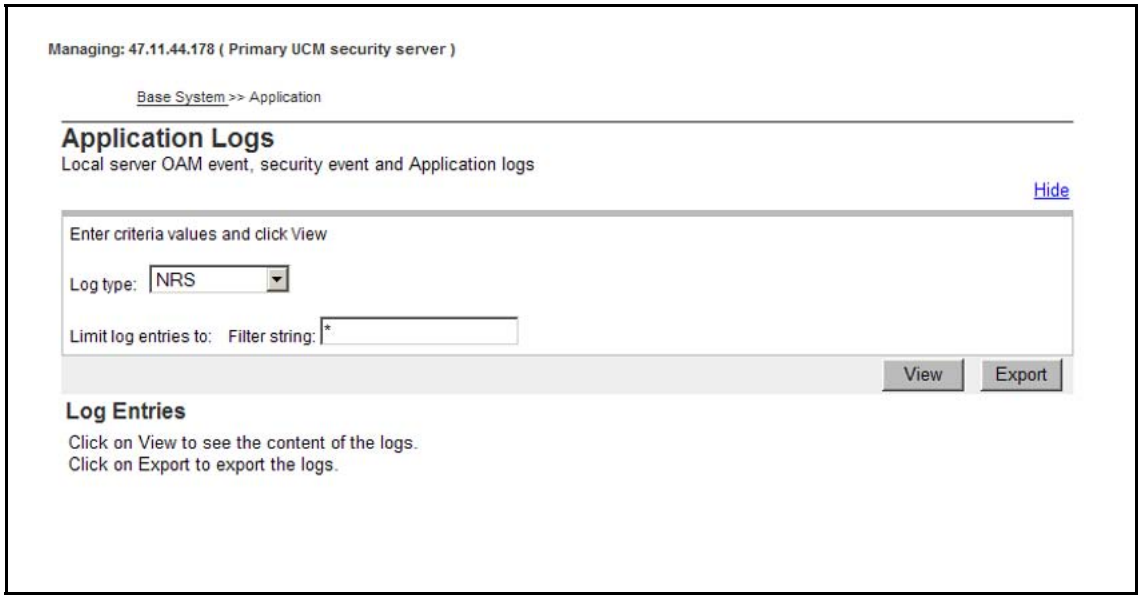
Figure 165
Tools window



3 In the Tools window, click **Logs**.

The Application Logs screen appears, as shown in Figure 166 "Application Logs window" (page 186).

Figure 166
Application Logs window



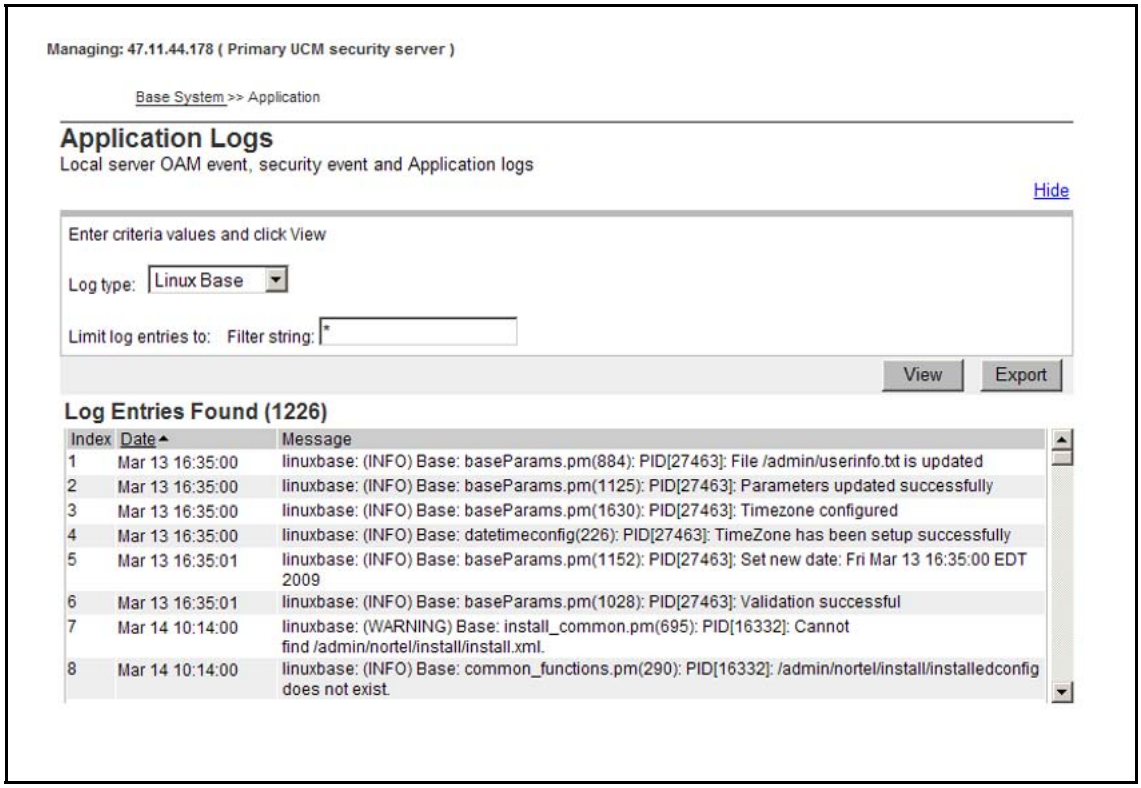
4 In the **Log type** list, select an application log type.

5 In the **Limit log entries to: Filter string** box, enter a character string to limit the log entry search. If you leave the **Limit log entries to: Filter string** blank, the search returns all log entries.

6 Press **View**.

The application log entries appear, as shown in Figure 167 "Application Logs - search results window" (page 187)

Figure 167
Application Logs - search results window

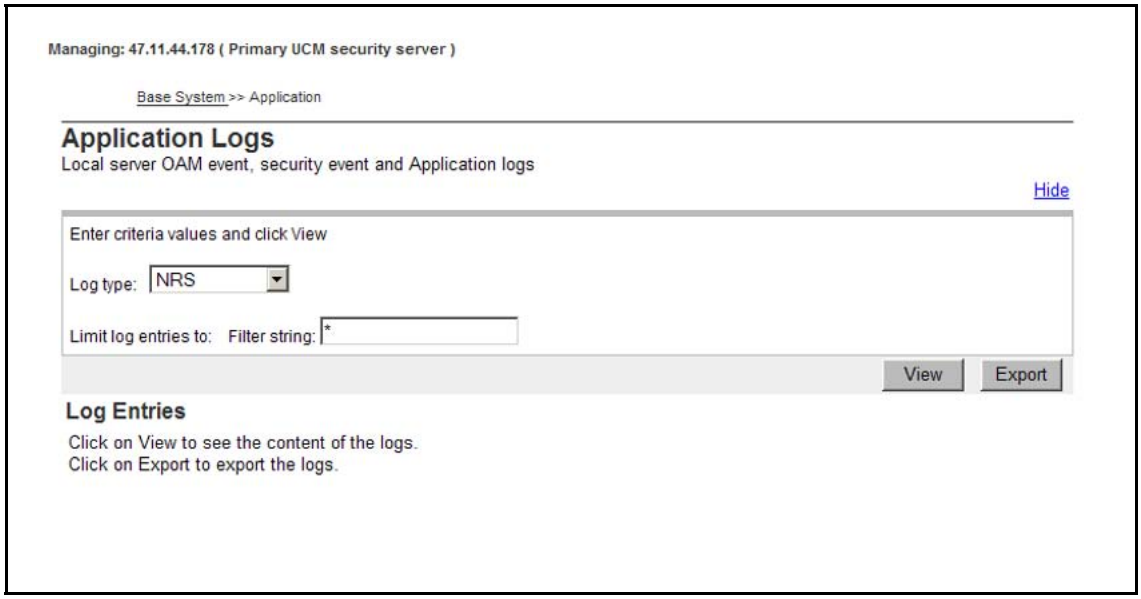


--End--

Procedure 32
Exporting application logs

Step	Action
1	Log on to UCM and navigate to Base Manager. For details about logging on to UCM and accessing Base Manager, see Procedure 15 “Accessing Base Manager through UCM” (page 151). **OR** Log on to the target server locally and navigate to Base Manager. For details about logging on to the target server locally and accessing Base Manager, seeProcedure 16 “Accessing Base Manager through local logon” (page 153).
2	In the navigation pane. select **Tools**, **Logs**, **Application**. The Application Logs screen appears, as shown in Figure 168 "Application Logs window" (page 188).

Figure 168
Application Logs window



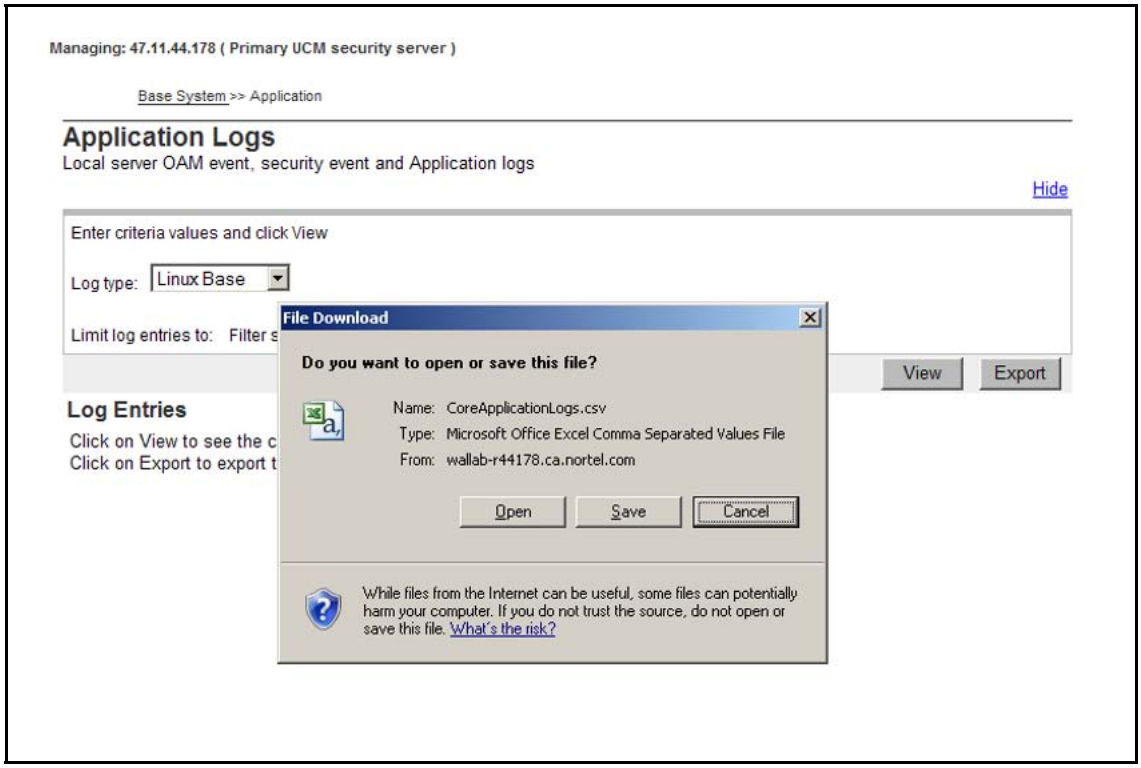
3 In the **Log type** list, select an application log type.

4 In the **Limit log entries to: Filter string** box, enter a character string to limit the log entry search. If you leave the **Limit log entries to: Filter string** blank, the search returns all log entries.

5 Press **Export**

. A file download prompt appears, as shown in Figure 169 "Application Logs - file download prompt window" (page 189).

Figure 169
Application Logs - file download prompt window



6 Press **Open** to open a file that contains the application log entries.

OR

Press **Save** to save the application logs entries file locally.

--End--

Appendix Passthrough end user license agreement

ATTENTION
Do not contact Red Hat for technical support for your Nortel version of the Linux base operating system. If you require technical support, contact Nortel technical support through your regular channels.

This section governs the use of the Red Hat Software and any updates to the Red Hat Software, regardless of the delivery mechanism and is governed by the laws of the state of New York in the U.S.A. The Red Hat Software is a collective work under U.S. Copyright Law. Subject to the following terms, Red Hat, Inc. (“Red Hat”) grants to the user (“Customer”) a license to this collective work pursuant to the GNU General Public License. Red Hat Enterprise Linux (the “Red Hat Software”) is a modular operating system consisting of hundreds of software components. The end user license agreement for each component is located in the component’s source code. With the exception of certain image files identified below, the license terms for the components permit Customer to copy, modify, and redistribute the component, in both source code and binary code forms. This agreement does not limit Customer’s rights under, or grant Customer rights that supersede, the license terms of any particular component.
The Red Hat Software and each of its components, including the source code, documentation, appearance, structure and organization are owned by Red Hat and others and are protected under copyright and other laws. Title to the Red Hat Software and any component, or to any copy, modification, or merged portion shall remain with the aforementioned, subject to the applicable license. The “Red Hat” trademark and the “Shadowman” logo are registered trademarks of Red Hat in the U.S. and other countries. This agreement does not permit Customer to distribute the Red Hat Software using Red Hat’s trademarks. If Customer makes a commercial redistribution of the Red Hat Software, unless a separate agreement with Red Hat is executed or other permission granted, then Customer must modify any files identified as “REDHAT-LOGOS” and

“anaconda-images” to remove all images containing the “Red Hat” trademark or the “Shadowman” logo. As required by U.S. law, Customer represents and warrants that it: (a) understands that the Software is subject to export controls under the U.S. Commerce Department’s Export Administration Regulations (“EAR”); (b) is not located in a prohibited destination country under the EAR or U.S. sanctions regulations (currently Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria); (c) will not export, re-export, or transfer the Software to any prohibited destination, entity, or individual without the necessary export license(s) or authorizations(s) from the U.S. Government; (d) will not use or transfer the Red Hat Software for use in any sensitive nuclear, chemical or biological weapons, or missile technology end-uses unless authorized by the U.S. Government by regulation or specific license; (e) understands and agrees that if it is in the United States and exports or transfers the Software to eligible end users, it will, as required by EAR Section 740.17(e), submit semi-annual reports to the Commerce Department’s Bureau of Industry & Security (BIS), which include the name and address (including country) of each transferee; and (f) understands that countries other than the United States may restrict the import, use, or export of encryption products and that it shall be solely responsible for compliance with any such import, use, or export restrictions. Red Hat may distribute third party software programs with the Red Hat Software that are not part of the Red Hat Software. These third party programs are subject to their own license terms. The license terms either accompany the programs or can be viewed at http://www.redhat.com/licenses/. If Customer does not agree to abide by the applicable license terms for such programs, then Customer may not install them. If Customer wishes to install the programs on more than one system or transfer the programs to another party, then Customer must contact the licensor of the programs. If any provision of this agreement is held to be unenforceable, that shall not affect the enforceability of the remaining provisions. Copyright © 2003 Red Hat, Inc. All rights reserved. "Red Hat" and the Red Hat "Shadowman" logo are registered trademarks of Red Hat, Inc. "Linux" is a registered trademark of Linus Torvalds. All other trademarks are the property of their respective owners.

Appendix Hardware platforms

The Linux base is installed on one the following commercial off-the-shelf (COTS) servers; the Dell R300 server, the Hewlett Packard (HP) DL320-G4 1U server, the International Business Machines (IBM) x306m 1U server, or the IBM x3350 server. Linux base is also installed on the Nortel CP PM card.

This appendix briefly describes each of the following platforms:

CP PM card

This section contains the following information:

Introduction

This chapter contains general instructions to install a Nortel CP PM server. It contains no instructions for installing an IBM X306m or HP DL320-G4 COTS 1U server. See the *IBM xSeries 306m Types 8848 and 8491 User Guide* or the *HP ProLiant DL320 Generation 4 Server User Guide* shipped with the COTS servers for installation instructions.

ATTENTION
Instructions to install an IBM X306m or HP DL320-G4 COTS 1U server are not included in this chapter. Detailed installation instructions can be found in the *IBM xSeries 306m Types 8848 and 8491 User Guide* or the *HP ProLiant DL320 Generation 4 Server User Guide* shipped with the server.

The chapter also contains instructions to connect all types of server to the ELAN and TLAN subnets of a CS 1000 system, and to connect a maintenance terminal to each type of Signaling Server.

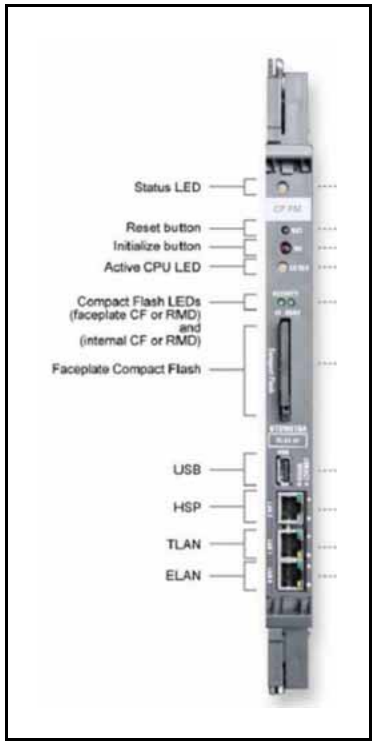
Nortel CP PM features

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

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

Figure 170 "CP PM faceplate" (page 195) shows the faceplate of the NTDW61BAE5.

Figure 170
CP PM faceplate



The Nortel CP PM server provides the following features:

- Intel Pentium M processor (1.4 GHz)
- Fixed Media Device (FMD)
  - an internal hard drive (NTDW6102E5)
  - hosts all Call Server and Signaling Server software and applications
- Removable Media Device (RMD)
  - hot-pluggable Compact Flash (CF) card slot in the faceplate
  - used to back up and restore Signaling Server IP configuration data
- 2 Gb of SDRAM
- One 1 Gb/s Ethernet port (HSP)
  - not used when configured as a Signaling Server, not used in Co-resident CS and SS mode
- Two 100BaseT Ethernet ports

— TLAN port to connect the server to a TLAN Layer 2 Ethernet switch port

— ELAN port to connect the server to an ELAN Layer 2 Ethernet switch port

- Two serial ports

  — to connect a maintenance terminal to the server

- Nortel NTAK19EC cabling kit

  — to adapt the 50-pin MDF connector at the back of the CS 1000E Media Gateway or the CS 1000M Universal Equipment Module (UEM) to a 25-pin DB connector

  — a 25-pin to 9-pin straight-through serial cable (not supplied) is required to connect the 25-pin DB connector to a 9-pin serial port on the maintenance terminal

- One USB port

  — used to backup and restore Linux Base and Application Data. It is also used to install Nortel applications that run on the Linux base.

- An RST (Reset) button

  — to cold-restart the server

- An INI (Initialize) button

  — to warm-restart the server

CP PM hard drive, memory, and BIOS procedures

Nortel Linux base requires CP PM servers to meet criteria for disk size, memory size, and BIOS version. Use the following procedures to determine CP PM disk size, CP PM memory size, and CP PM BIOS version, and to upgrade the CP PM BIOS version.

- Procedure 33 “Determining CP PM disk size” (page 196)
- Procedure 34 “Determining CP PM memory size” (page 197)
- Procedure 35 “Determining CP PM BIOS Method 1 ” (page 198)
- Procedure 36 “Determining CP PM BIOS Method 2” (page 199)
- Procedure 37 “Upgrading the CP PM BIOS” (page 199)

Procedure 33
Determining CP PM disk size

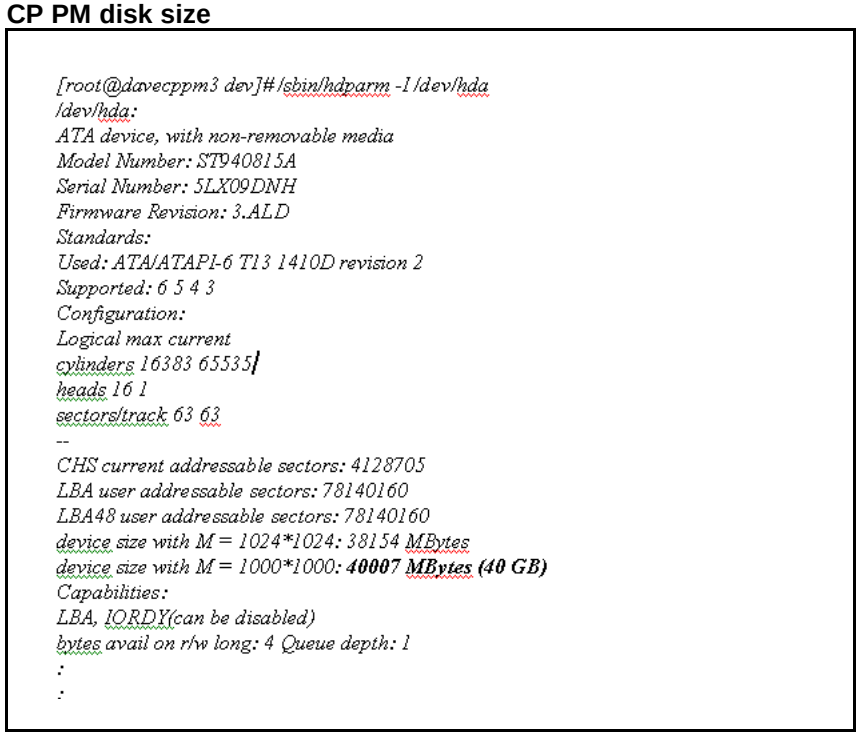
Step	Action
1	Connect to the CP PM server remotely by using SSH or locally by using a serial port.

2 Log on to the CP PM server in a systemadmin role.

3 Issue the Linux hdparm command:

The disk size appears as shown in Figure 171 "CP PM disk size " (page 197).

Figure 171
CP PM disk size

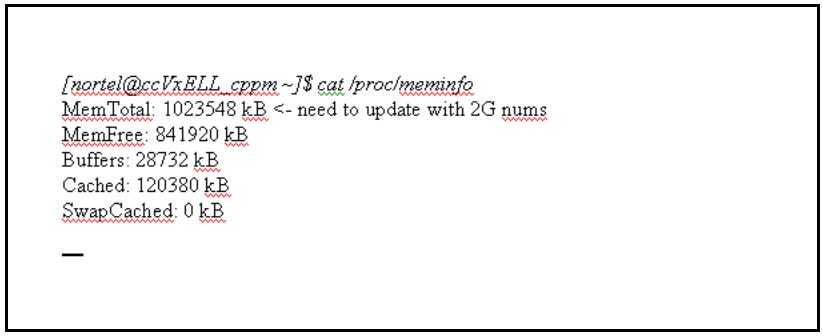


--End--

Procedure 34
Determining CP PM memory size

Step	Action
1	Connect to the CP PM server remotely by using SSH or locally by using a serial port.
2	Log on to the CP PM server.
3	Issue the Linux command to read the /proc/meminfo file. The command and results appear in Figure 172 "CP PM memory size " (page 198).

Figure 172
CP PM memory size

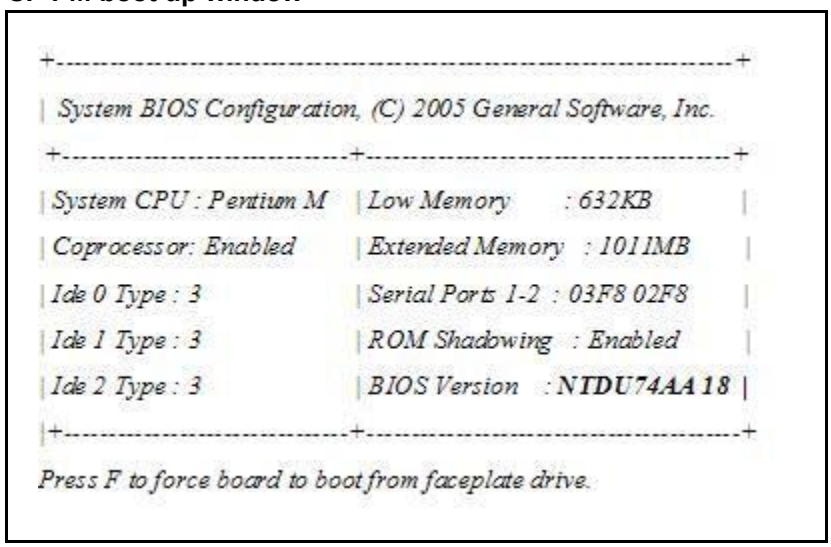


--End--

Procedure 35
Determining CP PM BIOS Method 1

Step	Action
1	Power up the CP PM hardware.
2	Observe the CP PM BIOS output in the bootup screen, as shown in Figure 173 "CP PM boot up window" (page 198).

Figure 173
CP PM boot up window



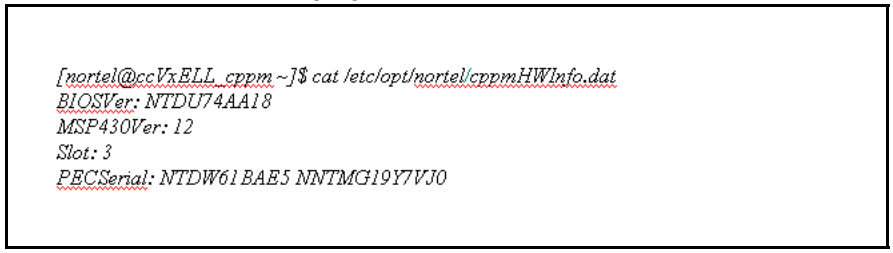
3	If the BIOS needs to be updated, complete Procedure 37 “Upgrading the CP PM BIOS” (page 199)

--End--

Procedure 36
Determining CP PM BIOS Method 2

Step	Action
1	Connect to the CP PM server remotely by using SSH or locally by using a serial port.
2	Log on to the CP PM server.
3	Issue the Linux command to read the cppmHWInfo.dat file in the /etc/opt/nortel/base folder. The BIOS version appears as shown in Figure 174 "CP PM BIOS version display" (page 199).

Figure 174
CP PM BIOS version display



--End--

CP PM BIOS upgrade

Use Procedure 37 “Upgrading the CP PM BIOS” (page 199) to upgrade the BIOS on a CP PM server.

Prerequisites

- You must have a bootable Removable Media Device (RMD) Compact Flash (CF). For instructions about creating an RMD CF, see Procedure 38 “Creating a CF RMD for Linux base installation on a CP PM server” (page 203).

Procedure 37
Upgrading the CP PM BIOS

Step	Action
1	Connect to serial port 1 on the CP PM server.
2	Insert the Linux base installation CF card into the faceplate CF slot.

3 Power on the system.

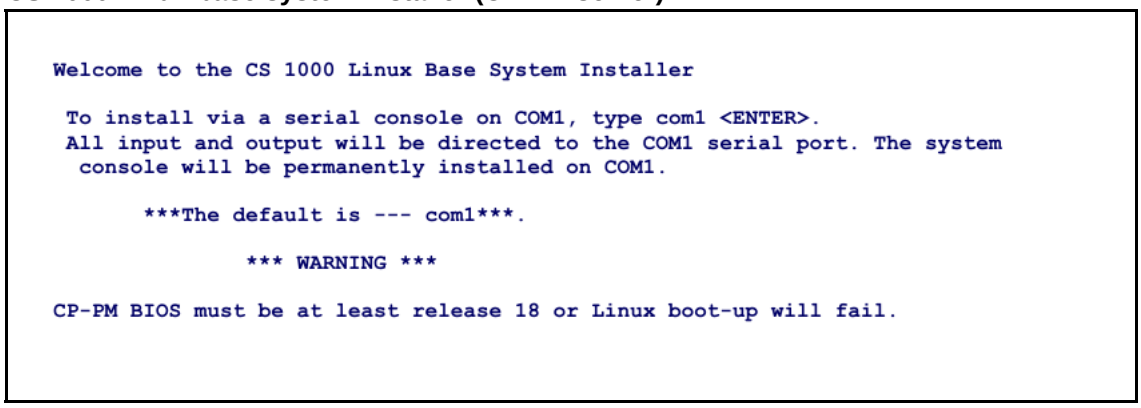
Once the initial boot and memory check completes, the CP PM initial boot screen screen appears..

4 Press the **F** key to boot from the Linux base installation faceplate CF card.

5 Press ENTER to direct the input and output to COM1.

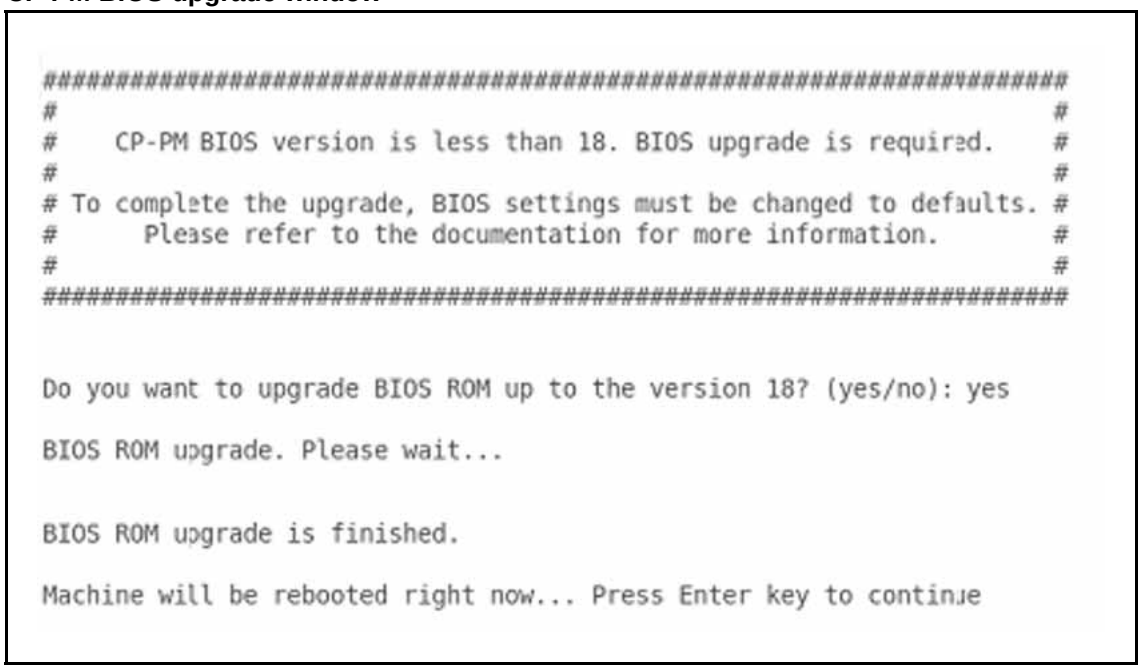
The CS 1000 Linux base system installer (CP PM server) screen appears, as shown in Figure 175 "CS 1000 Linux base system installer (CP PM server)" (page 200).

Figure 175
CS 1000 Linux base system installer (CP PM server)



If the CP PM server BIOS version is lower than 18, the BIOS upgrade screen appears, as shown in Figure 176 "CP PM BIOS upgrade window" (page 200).

Figure 176
CP PM BIOS upgrade window



6 Type **yes** to proceed with the automatic upgrade.

7 Verify that the BIOS upgrade is finished.

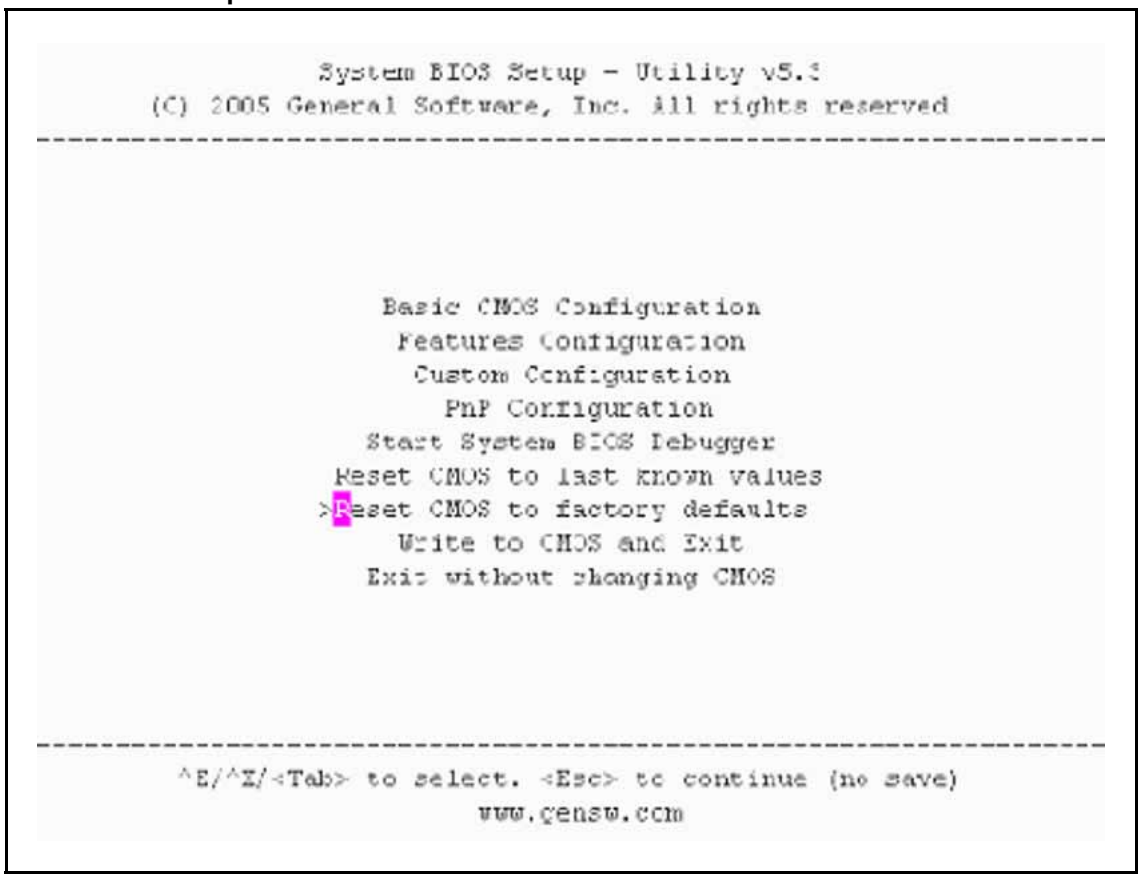
8 Press **F** to restart the server.

9 During the restart memory check, press **Ctrl c** to access the CP PM BIOS setup menu.

Note: If you miss the timing to press Ctrl c you must restart the system and try again. The Linux base installation software displays a warning if you do not reset the CP PM BIOS to factory defaults.

The CP PM BIOS setup screen appears, as shown in Figure 177 "CP PM BIOS setup window" (page 201).

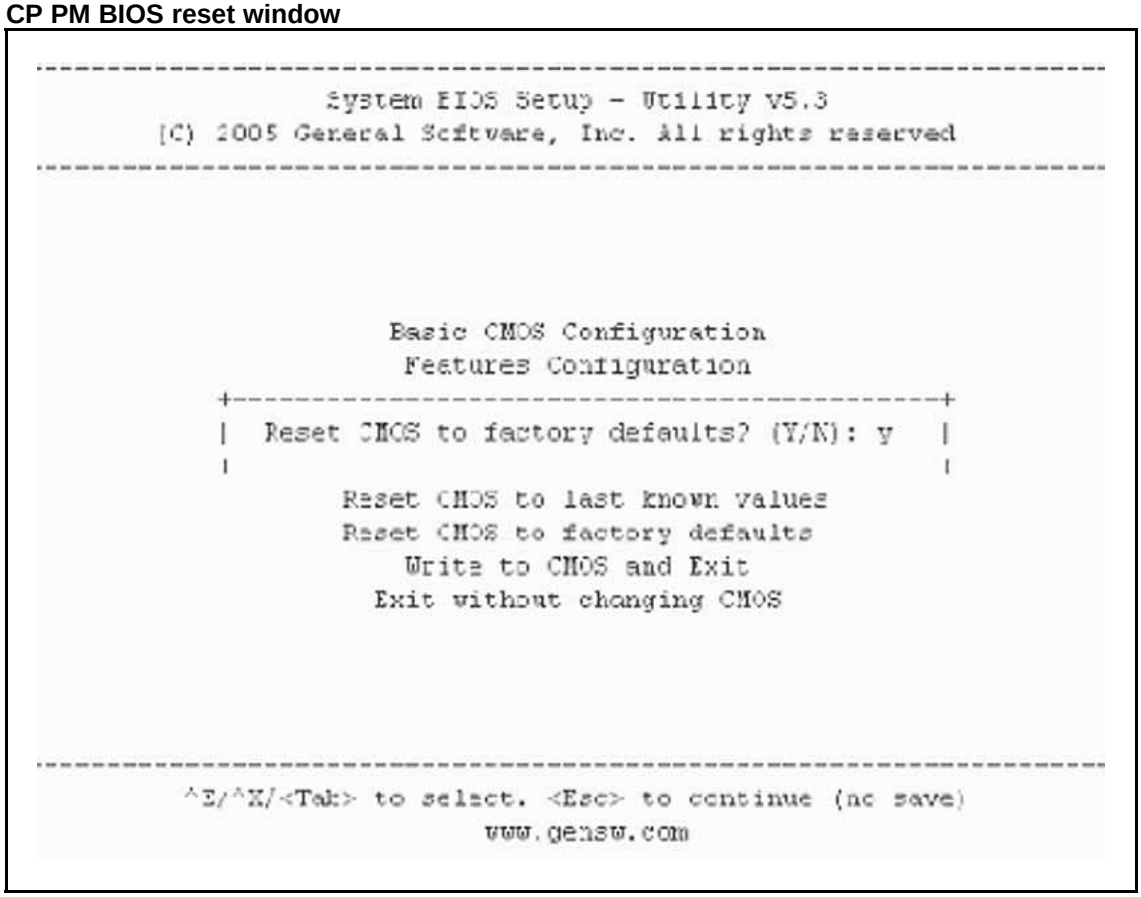
Figure 177
CP PM BIOS setup window



10 Select **Reset CMOS to factory defaults** from the menu.

The CP PM BIOS reset screen appears, as shown in Figure 178 "CP PM BIOS reset window" (page 202).

Figure 178
CP PM BIOS reset window



11 Press **y** to reset CMOS to factory defaults.

12 The system restarts. After initial boot, the CP PM initial boot screen appears and the new BIOS version is displayed. Verify the BIOS version is 18. You can now press the F key to boot from the faceplate CF card and proceed with the Linux base software installation.

--End--

Compact Flash RMD creation for a CP PM server

Linux base installation on a CP PM server requires a Compact Flash (CF) Removable Media Device (RMD). Use Procedure 38 “Creating a CF RMD for Linux base installation on a CP PM server” (page 203) to create an RMD

Prerequisites

- You must have a CF with a capacity of at least 2Gb.

Procedure 38
Creating a CF RMD for Linux base installation on a CP PM server

Step	Action
1	Open a Web browser window and navigate to www.nortel.com.
2	Navigate to Support & Training, Software Downloads.
3	Select the correct software load zip file for the CP PM platform.
4	Download the software load zip file.
5	Extract all of the files in the software load zip file to a temporary folder. The following folders appear in the root directory: • — temp/ — /baseapps — /extra — /license — /pre-configs — /relnotes — /scripts — /utilities
6	Navigate to the utilities directory.
7	Double click the mkbootrmd.bat file.
8	Input the letter for the CF RMD drive. **WARNING** This tool does not validate whether the drive letter that you enter is a valid CF RMD drive. Make sure that you provide the correct letter for the CF RMD drive. The mkbootrmd.bat file formats the drive you select; any information stored on the drive is lost.
9	When the script execution is complete, copy the contents of the temporary folder and paste it to the CF RMD.

--End--

Hardware installation

Installation checklist

Before you start to install a Signaling Server in a CS 1000 system, complete the following checklist.

Table 6
Installation checklist

Have you:
Received all server equipment and peripherals? • For Signaling Server: — installation accessories for rack-mounting the server — AC power cord **WARNING** Do not modify or use a supplied AC power cord if it is not the exact type required in the region where the Signaling Server is installed and used. Be sure to replace the cord with the correct type. — a DTE-DTE null modem serial cable (supplied) • for CS 1000E Nortel CP PM Signaling Server (NTDW61BAE5): — NTDW6102E5: CP PM Signaling Server Hard Drive kit — N0118766: CP PM Signaling Server Hard Drive Installation instructions — NTAK19ECE6: CP PM Signaling Server 2 port SDI Cable assembly kit — a 25-pin to 9-pin straight-through serial cable (not supplied) • for a CS 1000M Nortel CP PM Signaling Server (NTDW66AAE5 model) — NTDW6102E5: CP PM Signaling Server Hard Drive kit — N0118766: CP PM Signaling Server Hard Drive Installation instructions — NTAK19ECE6: CP PM Signaling Server 2 port SDI Cable assembly kit — NTDW69AAE5: CP PM Signaling Server Large System Cabling kit — N0106745: CP PM Signaling Large System Cabling kit installation instructions — a 25-pin to 9-pin straight-through serial cable (not supplied) ***Note:*** Save the packaging and packing materials in case you must reship the equipment or peripherals.
Made sure the area meets all environmental requirements?
Checked for all power requirements?
Checked for correct grounding facilities?

Have you:
Obtained the following? • screwdrivers • an ECOS 1023 POW-R-MATE or similar type of multimeter • appropriate cable terminating tools • a computer (maintenance terminal) to connect directly to the Signaling Server, with: — teletype terminal (ANSI-W emulation, serial port, 9600 bps) — a Web browser for Element Manager (configure cache settings to check for new Web pages every time the browser is invoked, and to empty the cache when the browser is closed)
Prepared the network data as suggested in *Converging the Data Network with VoIP* (NN43001-260) and *Communication Server 1000E: Planning and Engineering* (NN43041-220) or *Communication Server 1000M and Meridian 1: Large System Planning and Engineering* (NN43021-220), as appropriate for your CS 1000 system?
Read all safety instructions in *Communication Server 1000E Installation and Commissioning* (NN43041-310) or *Communication Server 1000M and Meridian 1 Large System Installation and Commissioning* (NN43021-310), as appropriate for your CS 1000 system?

Install a Nortel CP PM server

The Nortel CP PM server is a circuit card and therefore is not mounted in a rack. This section contains instructions to install a Nortel CP PM Signaling Server in a CS 1000E and a CS 1000M system.

Installation in a Nortel CS 1000E system The NTDW61BAE5 model of the Nortel CP PM server is designed for use in a CS 1000E system. The first task that must be performed is to install the hard drive shipped with the server.

You can insert the NTDW61BAE5 model of the Nortel CP PM server into any slot of a CS 1000E Media Gateway (MG 1000E or MG 1000B) or 11C cabinet or chassis, except slot 0. Slot 0 is reserved for a Small System Controller (SSC) card or a Media Gateway Controller (MGC) card. Keying prevents the NTDW61BAE5 model from being inserted into this slot.

WARNING
Do not insert the NTDW61BAE5 model of the Nortel CP PM server into any slot of a CS 1000M Universal Equipment Module (UEM). Doing so can cause electrical shorts on adjacent circuit cards.

Connect a Nortel CP PM server

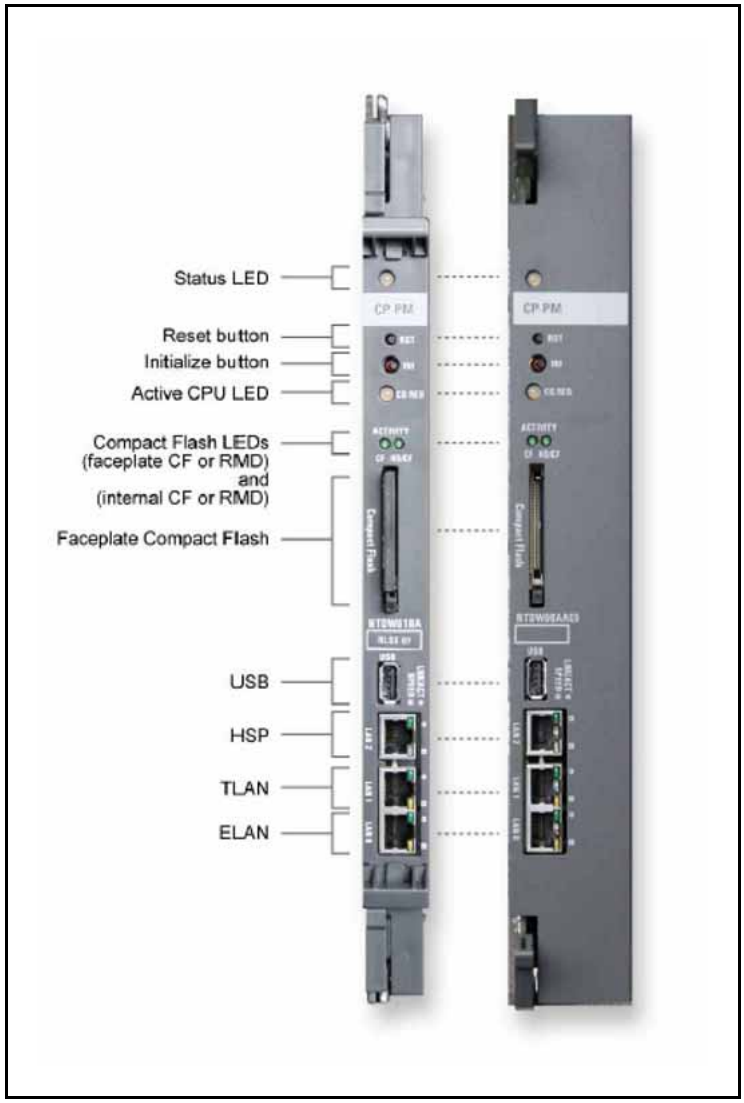
This section contains instructions to connect the NTDW61BAE5 and NTDW66AAE5 models of the Nortel CP PM Signaling Server to the ELAN and TLAN subnets of a CS 1000E and CS 1000M system, respectively. This section also contains instructions to connect a maintenance terminal to the Nortel CP PM Signaling Server.

The NTDW61BAE5 model of the Nortel CP PM Signaling Server is designed for use in a CS 1000E system. It is inserted into a slot of the Media Gateway (MG 1000E or MG 1000B). The Media Gateway also hosts the Media Gateway Controller (MGC) that has Ethernet ports for connecting to the ELAN and TLAN subnets of your CS 1000 system. However, it is common in a CS 1000E system for the Call Server to connect to the MGC through the ELAN port. If the Call Server does not connect to the MGC through this port, the NTDW61BAE5 model of the CP PM Signaling Server uses it to connect to the ELAN subnet of the CS 1000E system. If the Call Server uses the MGC ELAN port, the Nortel CP PM Signaling Server connects directly to the ELAN and TLAN Ethernet switches from the faceplate ELAN and TLAN Ethernet ports.

The NTDW66AAE5 model of the Nortel CP PM Signaling Server is designed for use in a CS 1000M system. It is inserted into a slot of a Universal Equipment Module (UEM). UEMs do not have built-in ELAN and TLAN Ethernet ports. These Ethernet ports must be installed on the back of the UEM to enable the Nortel CP PM Signaling Server to connect to the ELAN and TLAN subnets of your CS 1000 system.

The following figure shows the faceplates of the two models of the Nortel CP PM server with labeling for all components (NTDW61BAE5 on the left and NTDW66AAE5 on the right).

Figure 179
Faceplates of the Nortel CP PM server



Refer to the preceding figure when you perform the following procedure.

Procedure 39
Connecting a Nortel CP PM Signaling Server

Step	Action
1	Establish a maintenance terminal connection at the back of the Media Gateway (CS 1000E) or Universal Equipment Module (CS 1000M) shelf. The com (SDI) port of the Nortel CP PM server is routed through the backplane to the 50-pin MDF connector on the back of the MG or UEM shelf. A special cable (NTAK19EC) ships with the

Nortel CP PM server that adapts the 50-pin MDF connector to a 25-pin DB connector. You need a 25-pin to 9-pin straight-through serial cable to connect from the 25-pin DB connector to the serial port on the back of your PC.

a Connect the NTAK19EC cable (shipped with the Nortel CP PM server) to the 50-pin MDF connector on the back of the shelf.

b Connect a 25-pin to 9-pin straight-through serial cable to the 25-pin DB connector at the end of the NTAK19EC cable.

c Connect the other end of the serial cable to the serial port on the maintenance terminal.

2 Insert the Nortel CP PM server into the slot corresponding to the shelf where you connected the NTAK19EC cable.

The server is hot-pluggable so you can insert it without powering off the system.

The maintenance terminal is now connected to the server.

3 Connect the Nortel CP PM Signaling Server to the ELAN and TLAN subnets of the CS 1000 system.

- If you have a CS 1000E system, perform Procedure 40 “Connecting a CP PM Signaling Server to the ELAN and TLAN subnets of a CS 1000E system ” (page 209).
- If you have a CS 1000M system, perform Procedure 41 “Connecting a CP PM Signaling Server to the ELAN and TLAN subnets of a CS 1000M system ” (page 210).

4 Configure the baud rate for the serial port on the Signaling Server to 9600 b/ps.

Note: The Nortel CP PM Signaling Server ships with the serial port configured to 9600 b/ps.

To verify or change the baud rate on a Nortel CP PM Signaling Server, see Procedure 42 “Changing the baud rate on a Nortel CP PM Signaling Server” (page 211).

5 Configure the connected maintenance terminal.

--End--

Perform the following procedure to connect a Nortel CP PM Signaling Server (model NTDW61BAE5) to the ELAN and TLAN subnets of a CS 1000E system.

Procedure 40
Connecting a CP PM Signaling Server to the ELAN and TLAN subnets of a CS 1000E system

Step	Action
1	Connect the Signaling Server to the ELAN subnet. • if the CS 1000 Call Server is not connected to the Media Gateway Controller (MGC) — Insert the end of one customer supplied 25-cm RJ-45 CAT5 Ethernet cable into the ELAN network interface port (ELAN port) on the faceplate of the CP PM Signaling Server. — Insert the other end of the 25-cm RJ-45 CAT5 Ethernet cable into the MGC ELAN Ethernet port. • if the CS 1000 Call Server is connected to the MGC — Insert the end of a longer RJ-45 CAT5 Ethernet cable (not supplied) into the ELAN network interface port (ELAN port) on the faceplate of the CP PM Signaling Server. — Insert the other end of the RJ-45 CAT5 Ethernet cable into an Ethernet port on the ELAN Ethernet switch.
2	Connect the Signaling Server to the TLAN subnet. • if the CS 1000 Call Server is not connected to the Media Gateway Controller (MGC) — Insert the end of one customer supplied 25-cm RJ-45 CAT5 Ethernet cable into the TLAN network interface port (TLAN port) on the faceplate of the CP PM Signaling Server. — Insert the other end of the 25-cm RJ-45 CAT5 Ethernet cable into the MGC TLAN Ethernet port. • if the Call Server is connected to the MGC

— Insert the end of a longer RJ-45 CAT5 Ethernet cable (not supplied) into the TLAN network interface port (TLAN port) on the faceplate of the CP PM Signaling Server.

— Insert the other end of the RJ-45 CAT5 Ethernet cable into an Ethernet port on the TLAN Ethernet switch.

--End--

Note: If the Call Server is connected to the Media Gateway Controller, you must obtain CAT5 Ethernet cables that are long enough to connect the Signaling Server directly to the ELAN and TLAN Ethernet switches from the faceplate ELAN and TLAN Ethernet ports.

Perform this procedure to connect a Nortel CP PM Signaling Server (model NTDW66AAE5) to the ELAN and TLAN subnets of a CS 1000M system.

ATTENTION
Connecting a Nortel CP PM Signaling Server to the ELAN and TLAN subnets of a CS 1000M system causes a service disruption.

Procedure 41
Connecting a CP PM Signaling Server to the ELAN and TLAN subnets of a CS 1000M system

Step	Action
1	Insert the end of an RJ-45 CAT5 Ethernet cable (not supplied) into the ELAN network interface port (ELAN port) on the back of the CS 1000M UEM. You installed this ELAN port at the back of the UEM when you installed the Signaling Server in the UEM.
2	Insert the other end of the RJ-45 CAT5 Ethernet cable into an Ethernet port on the ELAN Ethernet switch.
3	Insert the end of another RJ-45 CAT5 Ethernet cable (not supplied) into the TLAN network interface port (TLAN port) on the back of the CS 1000M UEM. You installed this TLAN port at the back of the UEM when you installed the Signaling Server in the UEM.
4	Insert the other end of the RJ-45 CAT5 Ethernet cable into an Ethernet port on the TLAN Ethernet switch.

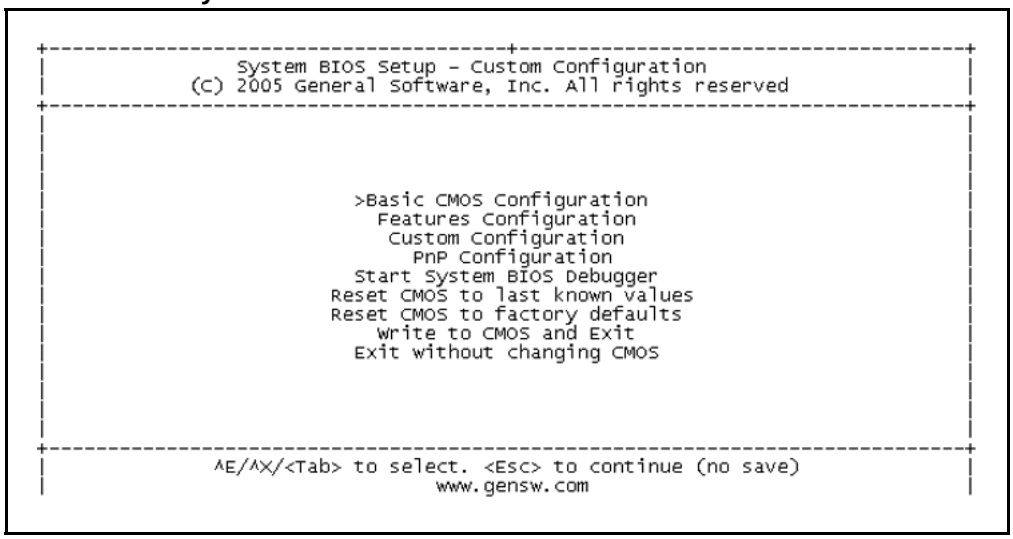
--End--

Perform this procedure to verify or change the baud rate on a Nortel CP PM Signaling Server.

Procedure 42
Changing the baud rate on a Nortel CP PM Signaling Server

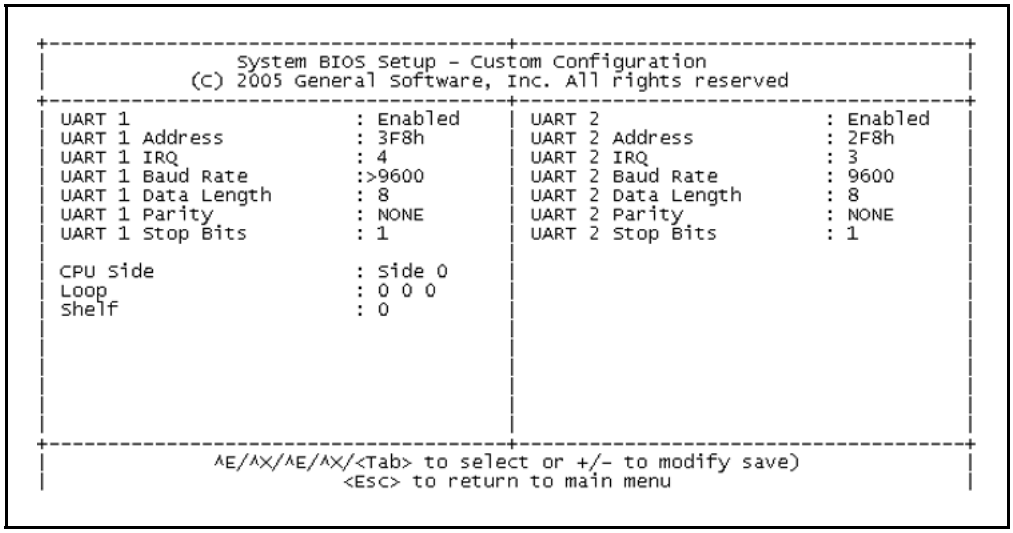
Step	Action
1	Press the **RST** button on the faceplate of the Signaling Server to boot the Signaling Server.
2	Press **Ctrl+C** keys at the same time to invoke the BIOS Setup menu. The Nortel CP PM System BIOS Menu screen appears.

Figure 180
Nortel CP PM System BIOS menu



3	Navigate to **Custom Configuration** and select the option. The Custom Configuration screen appears.

Figure 181
Nortel CP PM Customer Configuration



4 Navigate to the **UART 1 Baud Rate** option and change as necessary.

5 Navigate to the **UART 2 Baud Rate** option and change as necessary.

Note: UART 2 connection does not print BIOS messages.

6 Press **Esc** to save the settings and return to the BIOS Menu screen.

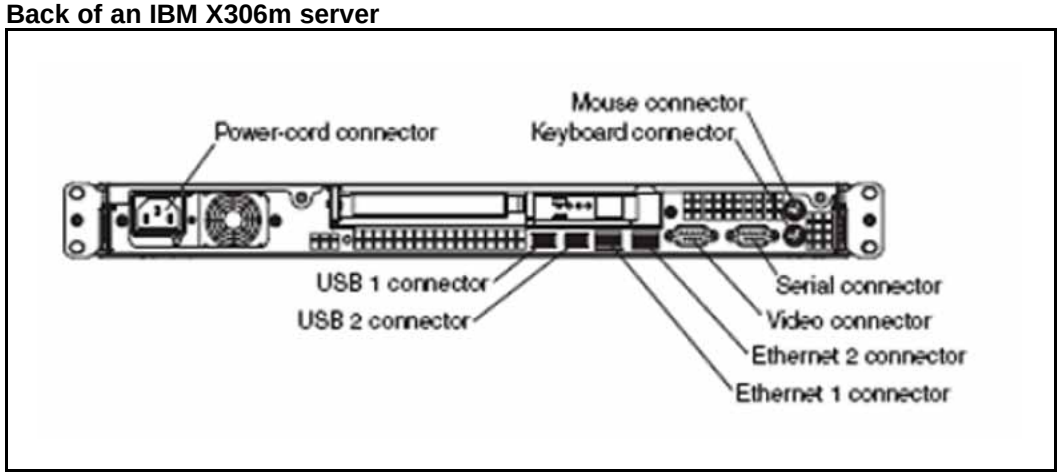
7 Select **Write to CMOS and Exit** to exit the Nortel CP PM server BIOS menu.

--End--

Connect an IBM X306m server

In geographic regions that are susceptible to electrical storms, Nortel recommends that you plug the IBM X306m server into an AC surge suppressor.

Figure 182
Back of an IBM X306m server



Refer to the preceding figure when you perform this procedure.

Procedure 43
Connecting an IBM X306m server

Step	Action
1	Connect the server to the TLAN subnet. Insert the RJ-45 CAT5 (or better) cable into the Ethernet 1 connector (TLAN network interface) on the back of the server.
2	Connect the server to the ELAN subnet. Insert the RJ-45 CAT5 (or better) cable into the Ethernet 2 connector (ELAN network interface) on the back of the server.
3	Connect a DTE–DTE null modem serial cable from the serial port on the back of the Signaling Server to the serial port on a maintenance terminal.
4	Connect the server power cord. **a** Check that the power cord is the type required in the region where you use the server. Do not modify or use the supplied AC power cord if it is not the correct type. **b** Attach the female end of the power cord to the mating AC power receptacle on the left side of the server back panel. Plug the male end of the AC power cord into the AC power source (wall outlet).

5 Configure the baud rate for the serial port on the Signaling Server to 9 600 b/ps. See Procedure 44 “Changing the baud rate on an IBM X306m Signaling Server” (page 214) for instructions.

Note: The IBM X306m Signaling Server ships with the serial port configured to 9600 b/ps.

6 Configure the connected maintenance terminal.

--End--

Perform the following procedure to verify or change the baud rate on an IBM X306m Signaling Server.

Procedure 44
Changing the baud rate on an IBM X306m Signaling Server

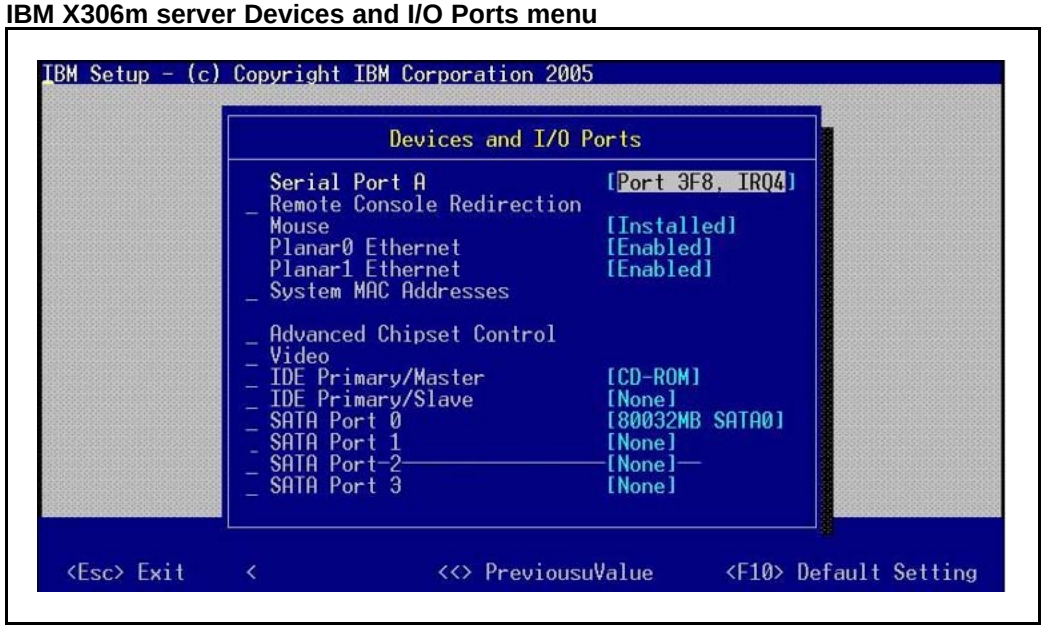
Step	Action
1	Press the Power switch to boot the server. The server boots and a **Press F1 for Configuration/Setup** message appears on the maintenance terminal. ***Note:*** If the server is running, press the **Reset** button on the front of the IBM X306m server to restart and receive the **Press F1 for Configuration/Setup** message.
2	Press **F1** to invoke the IBM X306m server Configuration/Setup Utility. The Configuration/Setup Utility menu screen appears.

Figure 183
IBM X306m server Configuration/Setup Utility menu

3 Navigate to the **Devices and I/O Ports** option and press **Enter**.

The Devices and I/O Ports menu screen appears.

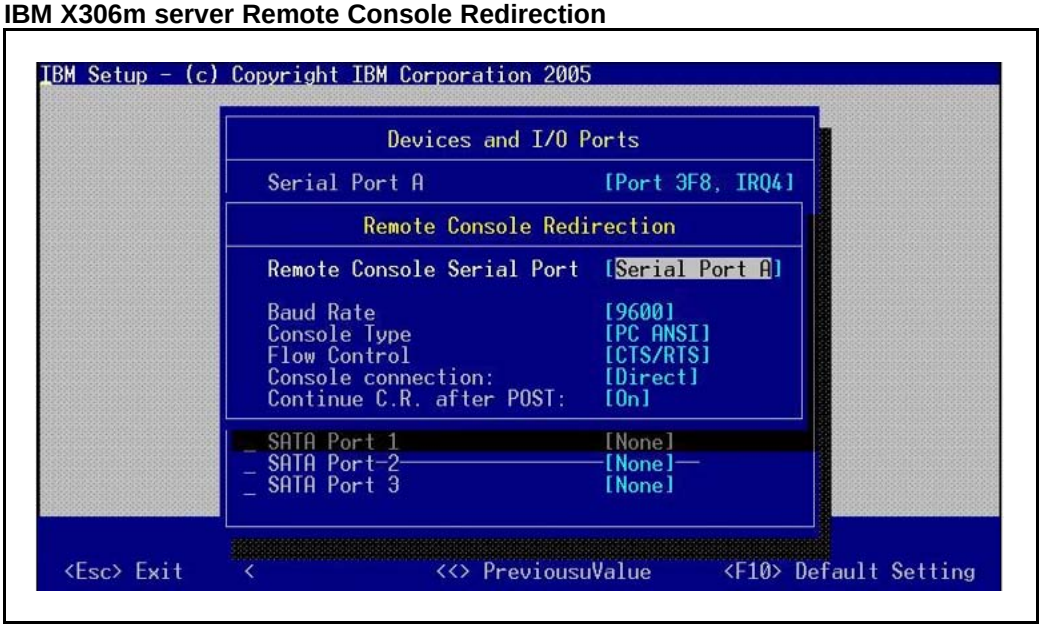
Figure 184
IBM X306m server Devices and I/O Ports menu



4 Navigate to the **Remote Console Redirection** option and press **Enter**.

The Remote Console Redirection screen appears.

Figure 185
IBM X306m server Remote Console Redirection



5 Navigate to the **Baud Rate** option and enter the value 9600.

6 Press **Enter** to change the serial port speed to 9600 b/ps.

7 Press **ESC** to exit the **Remote Console Redirection** option.

The Devices and I/O Ports menu screen appears.

8 Press **ESC** to exit the **Devices and I/O Ports** option.

The Configuration/Setup Utility menu screen appears.

9 Navigate to the **Save Settings** option and press **Enter** to save the changed parameters.

10 Navigate to the **Exit Setup** option and press **Enter** to exit the IBM X306m Configuration/Setup Utility.

The server restarts automatically.

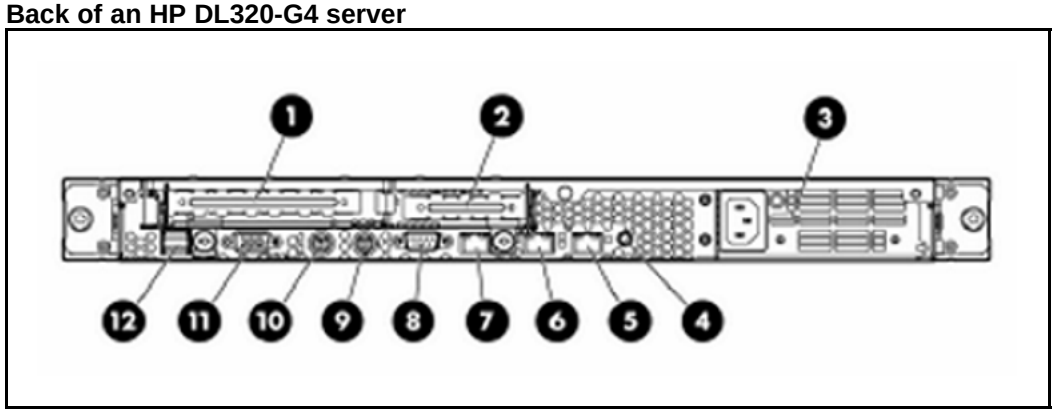
--End--

Refer to the Server Product Guide on the resource CD-ROM shipped with the IBM X306m server for additional operating information.

Connect an HP DL320-G4 Signaling Server

In geographic regions that are susceptible to electrical storms, Nortel recommends that you plug the HP DL320-G4 server into an AC surge suppressor.

Figure 186
Back of an HP DL320-G4 server



Refer to the preceding figure when you perform this procedure.

Procedure 45
Connecting an HP DL320-G4 server

Step	Action
1	Connect the server to the TLAN subnet. Insert the RJ-45 CAT5 (or better) cable into the connector labeled with the number 5 (TLAN network interface) on the back of the server.
2	Connect the server to the ELAN subnet. Insert the RJ-45 CAT5 (or better) cable into the connector labeled with the number 6 (ELAN network interface) on the back of the server.
3	Connect a DTE–DTE null modem serial cable from the serial port on the back of the server (COM1) to a maintenance terminal.
4	Connect the server power cord. **a** Check that the power cord is the type required in the region where you are installing the server. Do not modify or use the supplied AC power cord if it is not the correct type. **b** Attach the female end of the power cord to the mating AC power receptacle on the right side of the back panel. Plug the male end of the AC power cord into the AC power source (wall outlet).
5	Configure the COM1 serial port as the communication port for the connected maintenance terminal. See Procedure 46 “Configuring the COM1 serial port on an HP DL320-G4 Signaling Server” (page 218) for instructions.

6 Set the baud rate for the COM1 serial port on the Signaling Server to 9 600 b/ps.

See Procedure 47 “Changing the baud rate on an HP DL320-G4 Signaling Server” (page 220) for instructions.

Note: The HP DL320-G4 Signaling Server ships with the serial port configured to 9600 b/ps.

7 Configure the connected maintenance terminal.

--End--

Use the following procedure to configure the COM1 port of an HP DL320-G4 Signaling Server as the communication port for the connected maintenance terminal.

Procedure 46
Configuring the COM1 serial port on an HP DL320-G4 Signaling Server

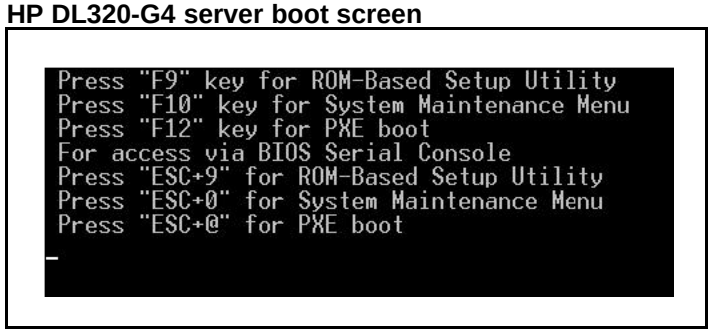
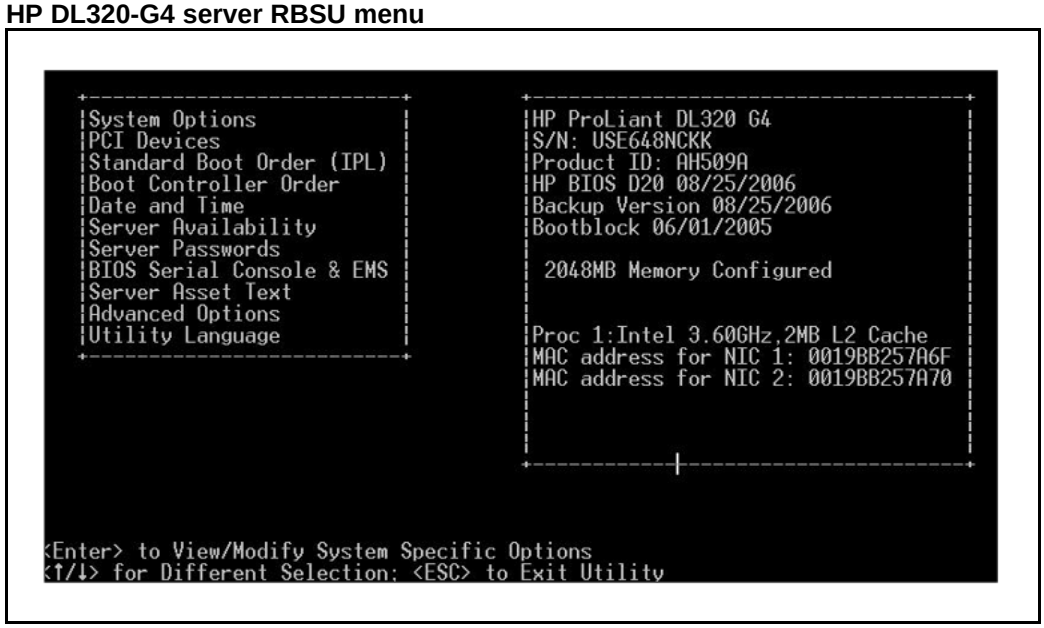
Step	Action
1	Connect a monitor, keyboard and mouse directly to the Signaling Server (through ports on back of Signaling Server) before you power up the Signaling Server. ***Note:*** If you use your maintenance terminal connection (Null Modem cable connected to the serial port), you cannot access the Graphical User Interface (GUI) for the ROM-Based Setup Utility. You must use the command line prompt of the ROM-Based Setup Utility.
2	Press the Power switch to boot the server. The server boots and the HP DL320-G4 boot screen appears. **Figure 187** **HP DL320-G4 server boot screen** 
3	Press **F9** to invoke the ROM-Based Setup Utility (RBSU) menu screen. The RBSU menu screen appears.

Figure 188
HP DL320-G4 server RBSU menu



4 Navigate to the **BIOS Serial Console & EMS** option and press **Enter**.

A BIOS Serial Console & EMS configuration menu screen appears.

5 Navigate to the **BIOS Serial Console Port** option and press **Enter**.

A BIOS Serial Console Port configuration screen appears. This screen display four options:

- 1 | Auto
- 2 | Disabled
- 3 | COM1
- 4 | COM2

6 Navigate to the **COM1** option and press **Enter**.

The COM1 port is configured as the serial port to communicate with the connected maintenance terminal.

The BIOS Serial Console & EMS configuration menu screen reappears.

7 Press **ESC** to exit the BIOS Serial Console & EMS configuration menu screen.

The RBSU menu screen reappears.

8 Press **ESC** to exit the ROM-Based Setup Utility.

9 Press **F10** to Confirm Exit Utility and restart the Signaling Server.

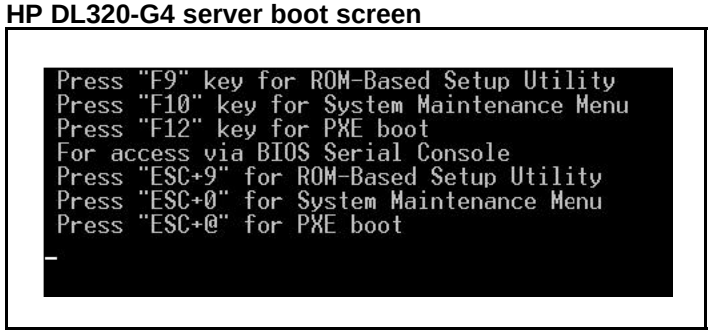
--End--

Use the following procedure to verify or change the baud rate on an HP DL320-G4 Signaling Server.

Procedure 47
Changing the baud rate on an HP DL320-G4 Signaling Server

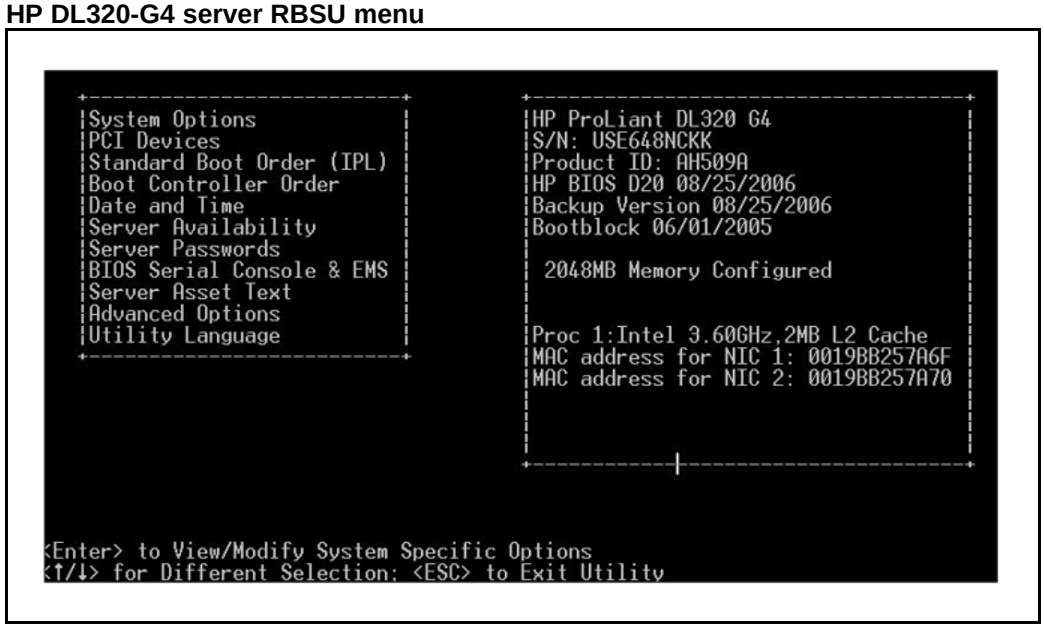
Step	Action
1	Connect a monitor, keyboard, and mouse directly to the Signaling Server (through back plane) before you power up the Signaling Server. ***Note:*** If you use a Null Modem cable connected to the serial port, you cannot access the ROM-Based Setup Utility.
2	Press the Power switch to boot the server. The server boots and the HP DL320-G4 boot screen appears.

Figure 189
HP DL320-G4 server boot screen



3	Press **F9** to invoke the ROM-Based Setup Utility (RBSU) menu screen. The RBSU menu screen appears.

Figure 190
HP DL320-G4 server RBSU menu



4 Navigate to the **BIOS Serial Console & EMS** option and press **Enter**.

A BIOS Serial Console & EMS configuration screen appears.

5 Navigate to the **BIOS Serial Console Baud Rate** option and press **Enter**.

A BIOS Serial Console Baud Rate configuration window appears. This window display the following four settings for the serial port speed:

- 9600
- 19200
- 57600
- 115200

6 Navigate to the **9600** setting and press **Enter**.

This configures the serial port speed to 9600 b/ps.

The BIOS Serial Console & EMS configuration menu screen reappears.

7 Press **ESC** to exit the BIOS Serial Console & EMS configuration menu screen.

The RBSU menu screen reappears.

8 Press **ESC** to exit the ROM-Based Setup Utility.

9 Press **F10** to Confirm Exit Utility and restart the Signaling Server.

--End--

Refer to the Server Product Guide on the resource CD-ROM shipped with the HP DL320-G4 server for additional operating information.

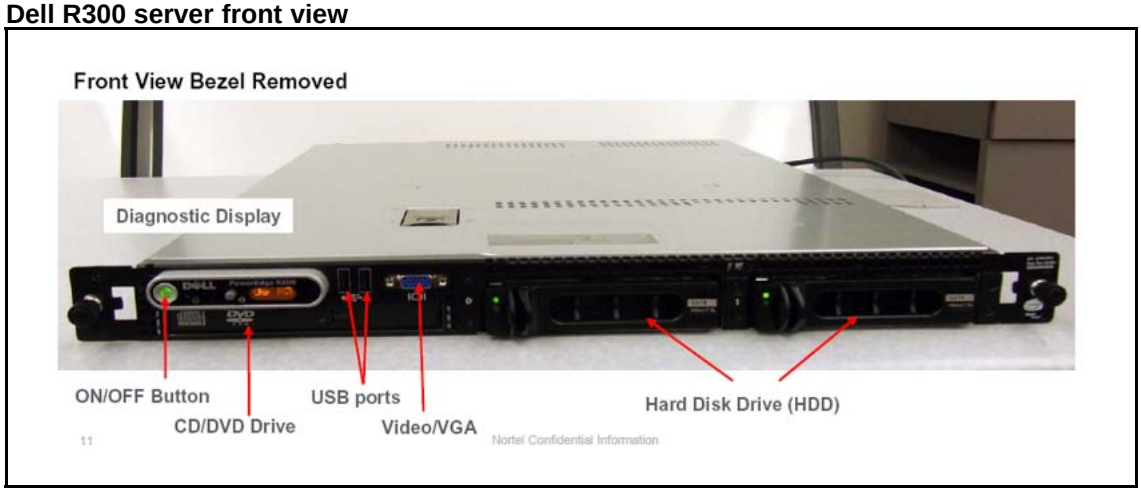
Dell R300 server

The Dell R300 server provides the following features:

- Intel Xeon (quad-core) processor
- Two 80 GB SATA Hard drives (1 configured)
- Four GB PC2-4200 ECC DDR2 SDRAM (2 GB configured)
- Two 10/100/1000BaseT Ethernet ports
- Three USB ports
- One CD-R/DVD ROM drive
- One serial port
- A reset button

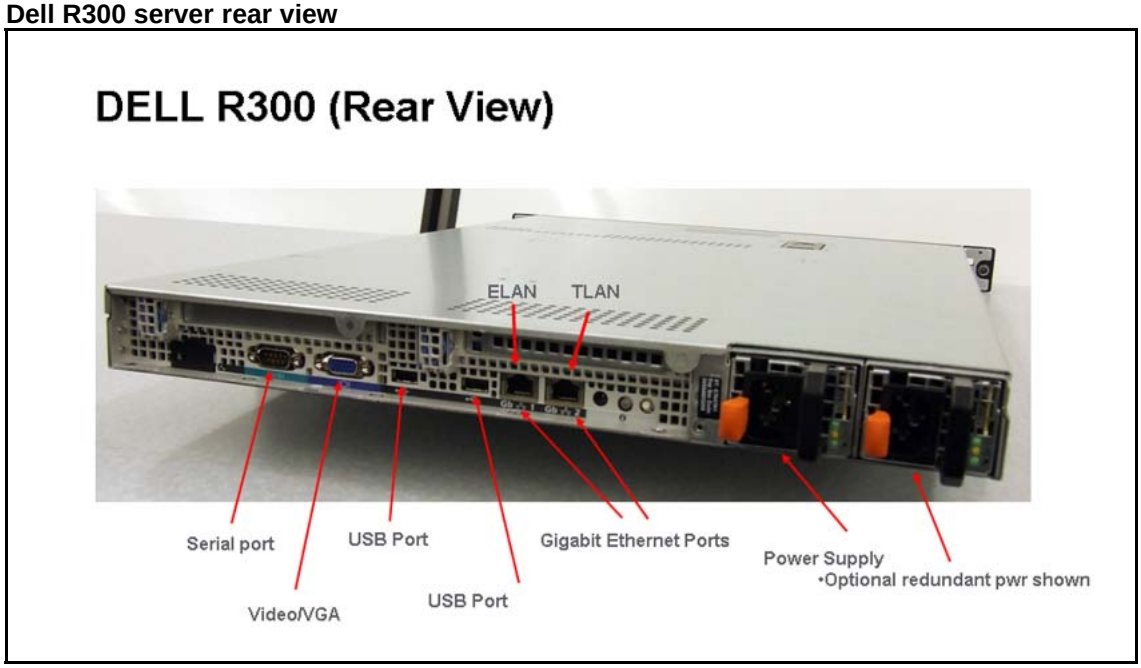
The following figure shows the front view of the Dell R300 server.

Figure 191
Dell R300 server front view



The following figure shows the rear view of the Dell R300 server.

Figure 192
Dell R300 server rear view

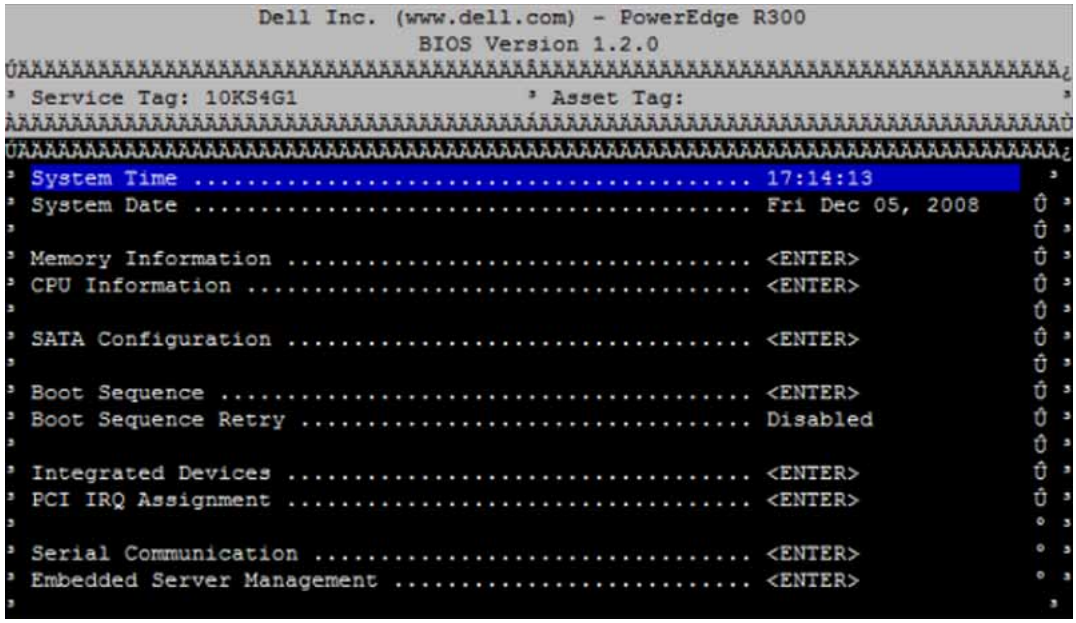


Dell R300 BIOS settings

Procedure 48
Configuring the COM1 serial port on a Dell R300 server

Step	Action
1	Press **F2** to navigate to the BIOS configuration main menu screen using a Keyboard Video Monitor (KVM) terminal. **OR** Press **ESC-2** to navigate to the BIOS configuration main menu screen using the console terminal. The BIOS configuration main menu screen appears, as shown in Figure 193 "BIOS configuration main menu window" (page 225).

Figure 193
BIOS configuration main menu window



2 In the BIOS configuration main menu screen, select **Serial Communication** and press **Enter** to continue. The Serial Communication screen appears.

3 In the Serial Communication line, type **On with Console Redirection via COM1**.

4 In the External Serial Connector line, type **COM1**.

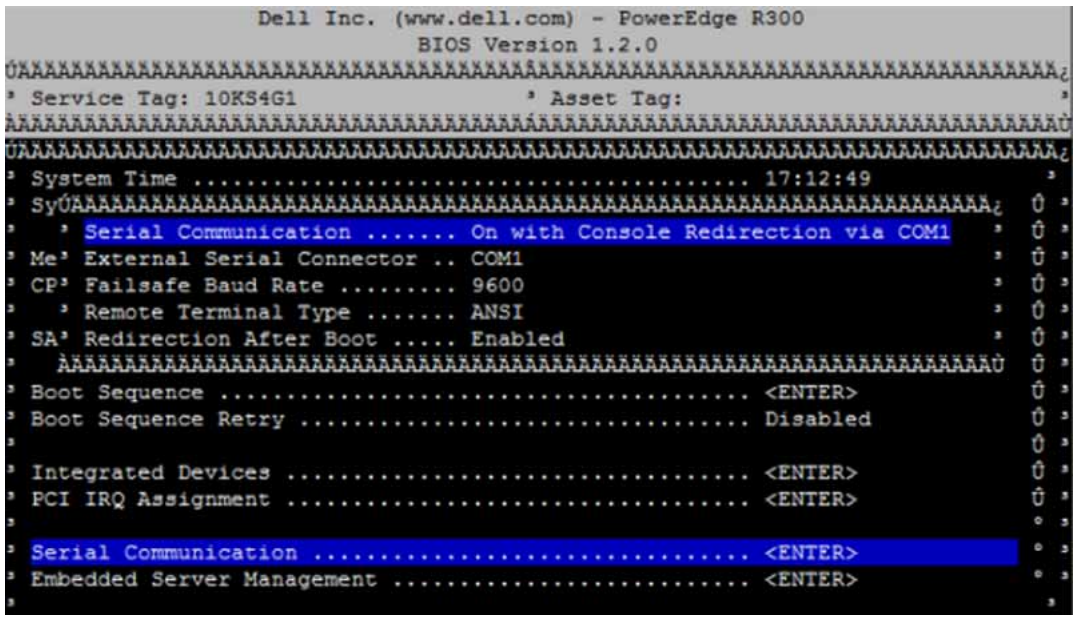
5 In the Failsafe Baud Rate line, type **9600**.

6 In the Remote Terminal Type line, type **Remote Terminal Type**.

7 In the Redirection After Boot line, type **Enabled**.

The Serial Communication screen containing the correct values appears in Figure 194 "Serial Communication window" (page 226).

Figure 194
Serial Communication window



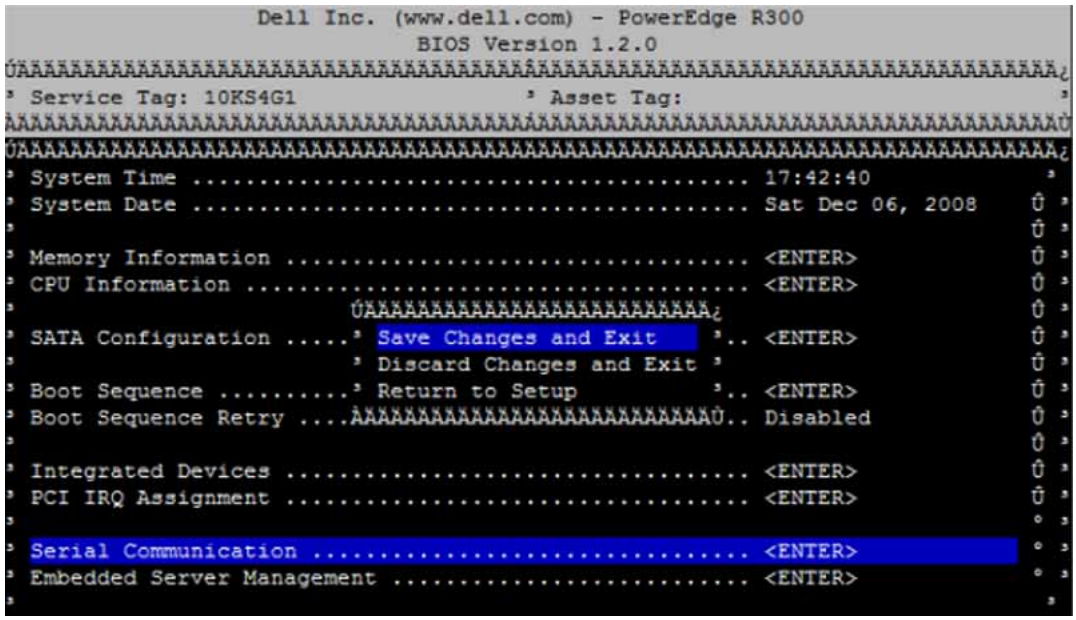
8 Press **Esc** to return to the BIOS configuration main menu.

In the BIOS configuration main menu screen you can perform other changes or you can exit and save the changes you made.

9 If you want to exit and save your changes, press **Esc**.

A prompt to save changes appears, as shown in Figure 195 "Save changes and exit window" (page 227).

Figure 195
Save changes and exit window



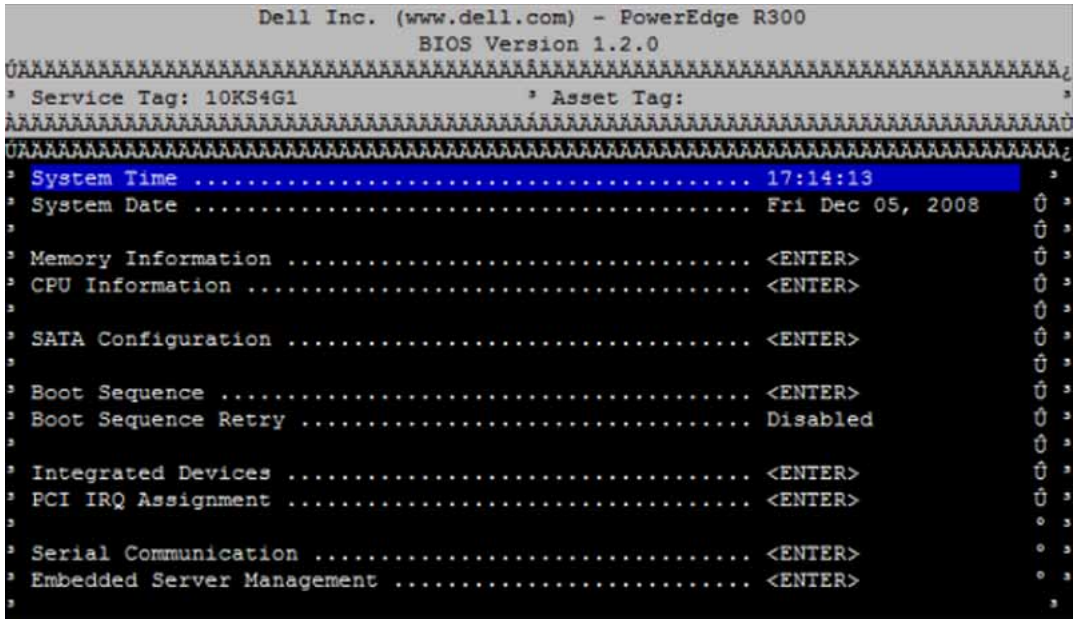
10 Select **Save Changes and Exit**, and then press **Enter**.

--End--

Procedure 49
Setting the BIOS password for the Dell R300 server

Step	Action
1	Press **F2** to navigate to the BIOS configuration main menu screen using a Keyboard Video Monitor (KVM) terminal. **OR** Press **ESC-2** to navigate to the BIOS configuration main menu screen using the console terminal. The BIOS configuration main menu screen appears, as shown in Figure 196 "BIOS configuration main menu window" (page 228).

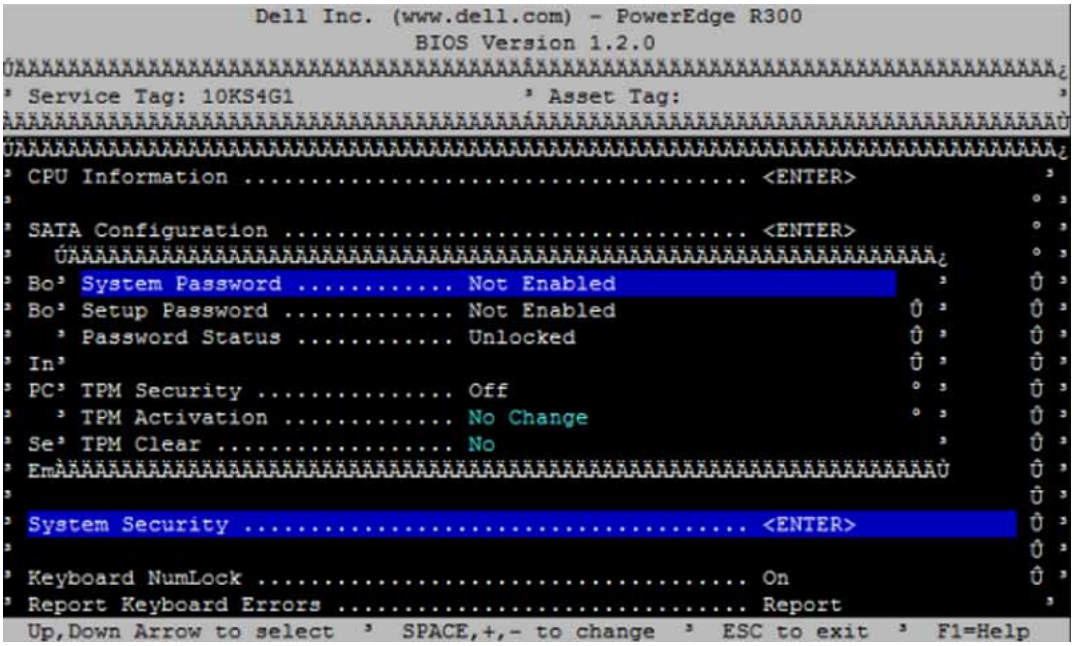
Figure 196
BIOS configuration main menu window



2 In the main menu screen, select **System Security** and press **Enter**.

The System Security menu appears, as shown in Figure 197 "System Security menu" (page 229).

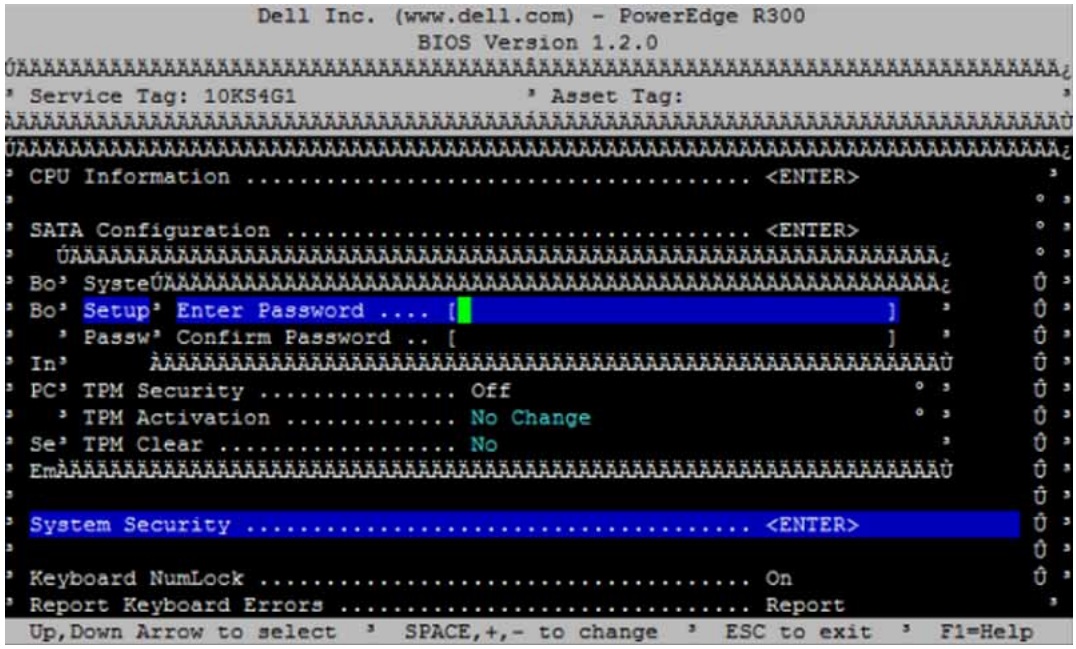
Figure 197
System Security menu



3 In the System Security menu, select **Setup Password** and press **Enter**.

The password entry screen appears, as shown in Figure 198 "Password entry window" (page 230).

Figure 198
Password entry window

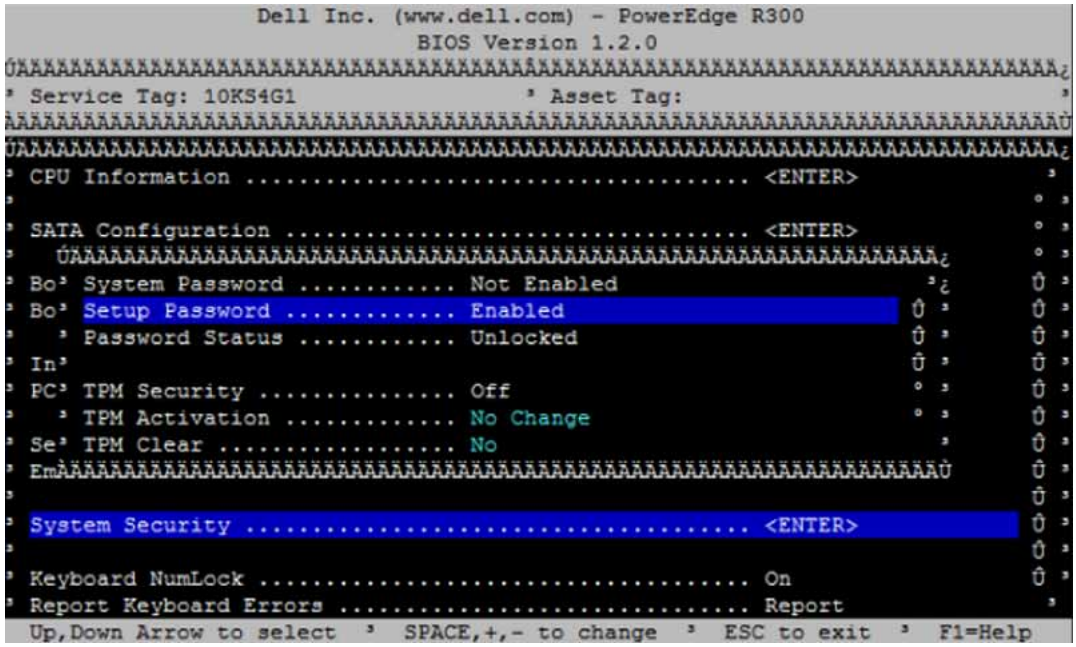


4 Type the new password. Press **Enter** to continue.

5 Type the password again to confirm the values, and then press**Enter**.

The password is now enabled, as shown in Figure 199 "Password enabled window" (page 231).

Figure 199
Password enabled window



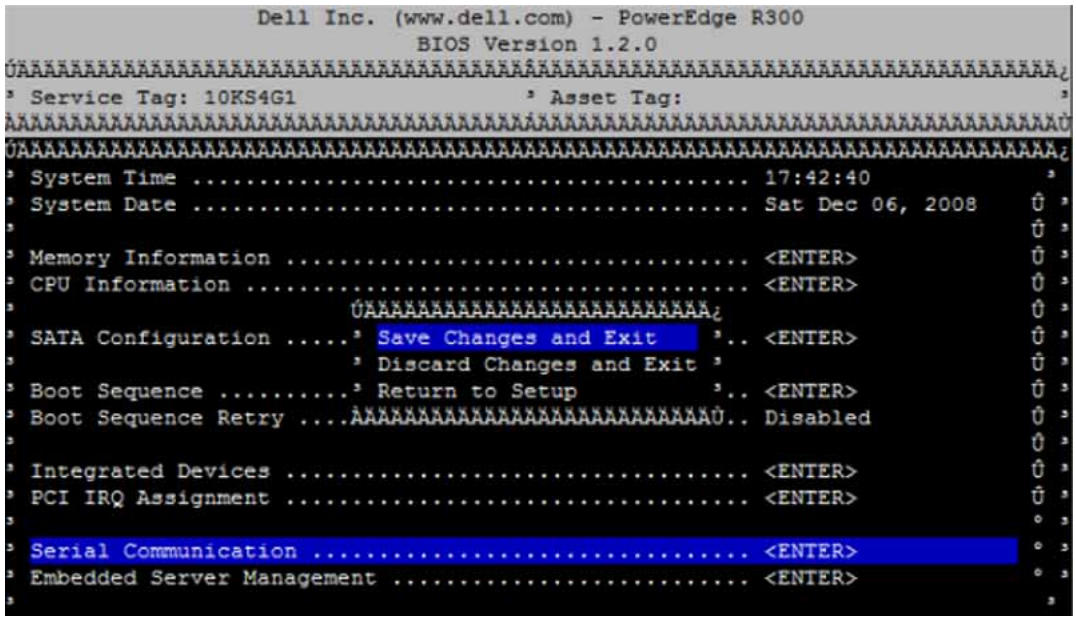
6 Press **Esc** to return to the BIOS configuration main menu.

In the BIOS configuration main menu screen you can perform other changes, or your can exit and save the changes you made.

7 If you want to exit and save your changes, press **Esc**.

A prompt to save changes appears, as shown in Figure 200 "Save changes and exit window" (page 232).

Figure 200
Save changes and exit window



8 Select **Save Changes and Exit**, and then press **Enter**.

--End--

Procedure 50
Configuring RAID settings

Step	Action
1	To configure the RAID settings for the Dell R300 server, go to www.dell.com.

--End--

HP DL320 G4 server

The HP DL320 G4 server provides the following features:

- Intel Pentium 4 processor (3.6 GHz)
- Two 80 GB SATA Hard drives (1 configured)
- Four GB PC2-4200 ECC DDR2 SDRAM (2 GB configured)
- Two 10/100/1000BaseT Ethernet ports
- Three USB ports
- One CD-R/DVD ROM drive
- One serial port
- A reset button

Figure 201 "HP DL320 G4 front view" (page 233) shows the front view of the HP DL320 G4 server.

Figure 201
HP DL320 G4 front view

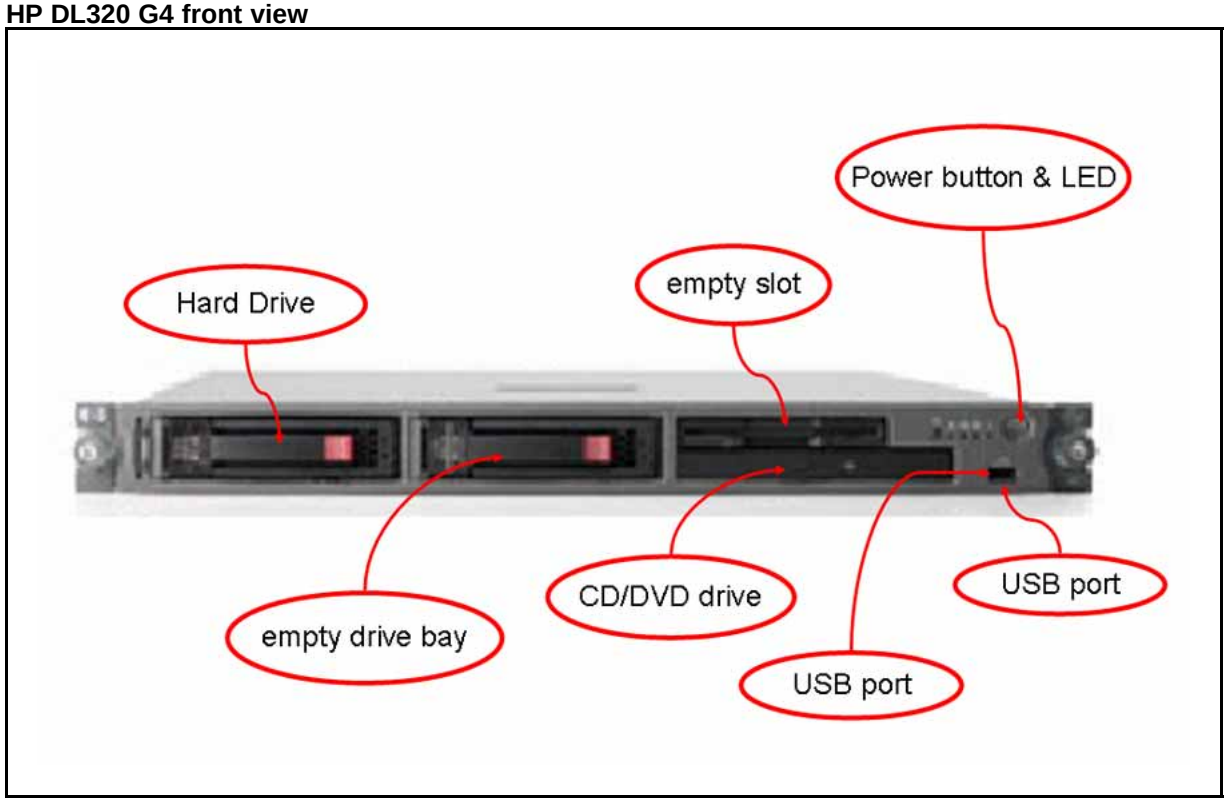
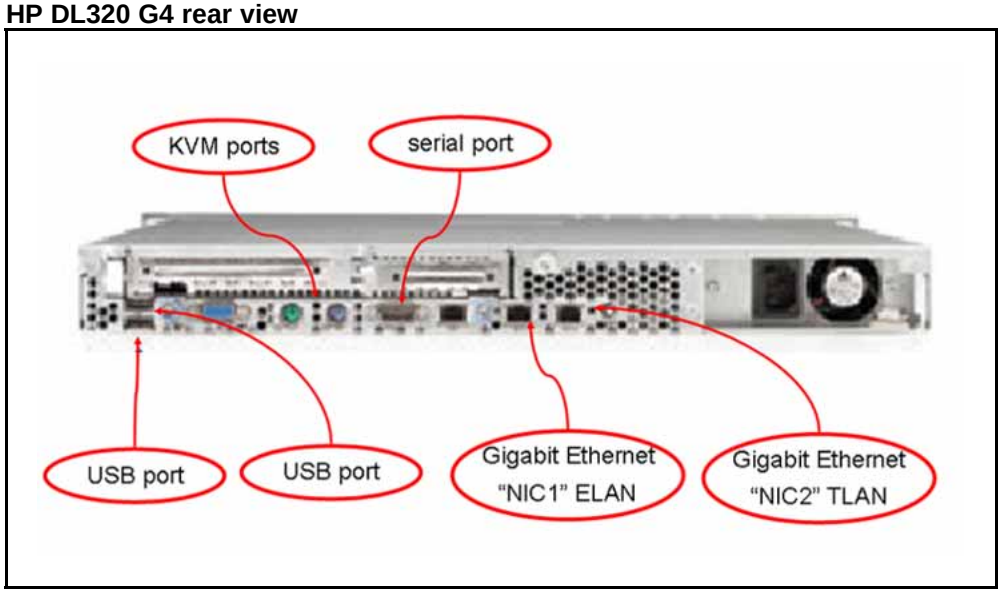


Figure 202
HP DL320 G4 front view: LEDs

Table 7
HP DL320 G4 LED item description and status

Item	Description	Status
1	UID button LED (Unit Identification)	**Blue** – Identification is activated. **Flashing blue** – System is remotely managed. **Off** – Identification is deactivated.
2	Internal health LED	**Green** –- System health is normal. **Amber** – System is degraded. To identify the component, check the system board LEDs. **Red** – Critical. To identify the component in a critical state, check the system board LEDs. **Off** – System health is normal (when in standby mode).
3	NIC 1 link/activity LED	**Green** – Network link exists. **Flashing green** – Network link and activity exist. **Off** – No link to network exists.
4	NIC 2 link/activity LED	**Green** –Network link exists. **Flashing green** – Network link and activity exist. **Off** – No link to network exists.
5	Drive activity LED	**Green** – Drive activity is normal. **Amber** – Drive failure occurred. **Off** – No drive activity.
6	Power button and LED	**Green** – System is on. **Amber** – System is shut down, but power is still applied. **Off** – Power not available.

Figure 203
HP DL320 G4 rear view



ATTENTION
The TLAN and ELAN port positions are reversed (L and R, 1 and 2) compared to the IBM x306m server.

HP DL320 G4 BIOS settings

The Basic Input Output System (BIOS) settings on the HP DL320 G4 server shipped through Nortel are correct. The BIOS settings do not require adjustment unless they are reset due to a fault or through maintenance. If a reset of the BIOS settings occurs, check the serial port option. The HP DL320 G4 BIOS settings can be seen at Table 8 "HP DL320 G4 default BIOS settings" (page 236). The HP DL320 G4 servers provide a physical COM1 serial port and a virtual (ILO) COM2 serial port. If the setting for the serial console port is Auto, output can be directed to either the COM1 port or COM2 ILO port. Set the serial console port option to COM1 to ensure the console output goes to the physical COM1. See “Configuring the COM1 serial port on an HP DL320 G4 server” (page 236) for instructions.

The HP DL320 G4 server shipped through Nortel has a default baud rate of 9600 b/ps and does not require a reset. If an error occurs and you want to reset the baud rate, or if you want to change to another baud rate, see Procedure 47 “Changing the baud rate on an HP DL320-G4 Signaling Server” (page 220)for instructions.

For information about how to enable or disable the BIOS password on the HP DL320 G4 server see “Setting the HP DL320 G4 server BIOS password” (page 240).

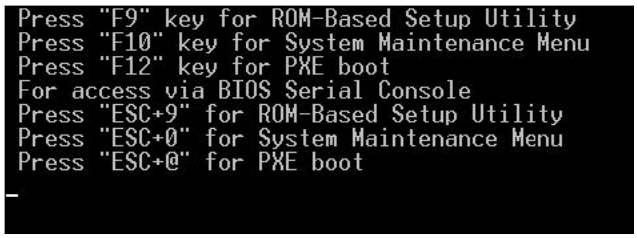
Table 8
HP DL320 G4 default BIOS settings

BIOS value	Default setting
Devices and I/O port - serial port A	Enabled
Devices and I/O port - baud rate	9600 baud
Devices and I/O port - type of connector	9-pin serial female
Start options - legacy USB support	Disabled

Configuring the COM1 serial port on an HP DL320 G4 server

Step	Action
1	Press **Power** to boot the server. The server boots and the HP DL320 G4 boot screen appears.

Figure 204
HP DL320 G4 server boot screen

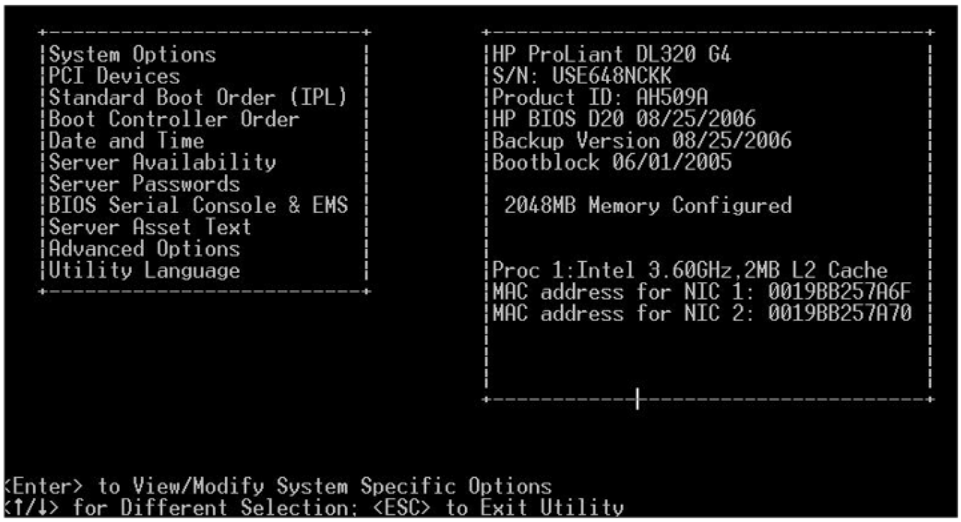


Note: If the server is already up and running, power the server off and on to restart and receive the HP DL320 G4 boot screen.

2 Press **F9** to invoke the ROM-based setup utility (RBSU) menu screen.

The RBSU menu screen appears.

Figure 205
HP DL320 G4 server RBSU menu



3 Navigate to the **BIOS Serial Console & EMS** option and press **Enter**.

A BIOS Serial Console & EMS configuration menu screen appears.

4 Navigate to the **BIOS Serial Console Port** option and press **`Enter`**.

A BIOS Serial Console Port configuration screen appears. This screen presents you with four options:

- 1 | Auto
- 2 | Disabled
- 3 | COM1
- 4 | COM 2

5 Navigate to the **COM1** option and press **`Enter`**.

This configures the COM1 port as the serial port for communicating with the connected maintenance terminal.

The BIOS Serial Console & EMS configuration menu screen reappears.

6 Press **`ESC`** to exit the BIOS Serial Console & EMS configuration menu screen.

The RBSU menu screen reappears.

7 Press **ESC** to exit the ROM-based Setup Utility.

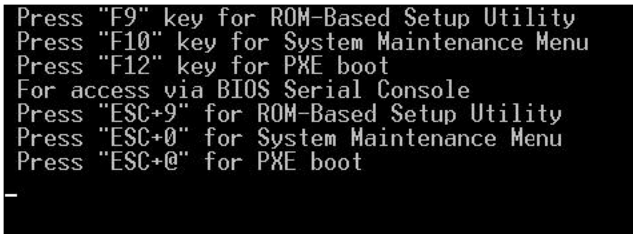
--End--

Changing the baud rate on an HP DL320 G4 Signaling Server

ATTENTION
The HP DL320 G4 server shipped through Nortel has a default Baud rate of 9600 b/ps and does not require a reset. Use this procedure only if you want to use another Baud rate, or to correct the Baud rate after it is reset due to an error.

Step	Action
1	Press **Power** to boot the server. The server boots and the HP DL320 G4 boot screen appears.

Figure 206
HP DL320 G4 server boot screen

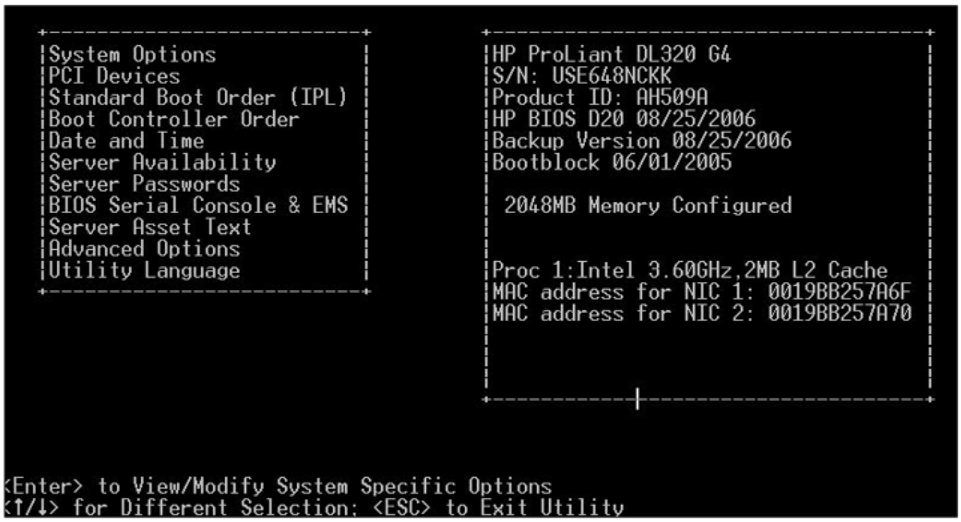


Note: If the server is already up and running, power the server off and on to restart and receive the HP DL320 G4 boot screen.

2 Press **F9** to invoke the ROM-based Setup Utility (RBSU) menu screen.

The RBSU menu screen appears.

Figure 207
HP DL320 G4 server RBSU menu



3 Navigate to the **BIOS Serial Console & EMS** option and press **Enter**.

A BIOS Serial Console & EMS configuration screen appears.

4 Navigate to the **BIOS Serial Console Baud Rate** option and press **Enter**.

A BIOS Serial Console Baud Rate configuration window appears. This window presents you with four settings for the serial port speed:

- 9600
- 19200
- 57600
- 115200

5 Navigate to the **9600** setting and press **Enter**.

This configures the serial port speed to 9600 b/ps.

The BIOS Serial Console & EMS configuration menu screen reappears.

6 Press **ESC** to exit the BIOS Serial Console & EMS configuration menu screen.

The RBSU menu screen reappears.

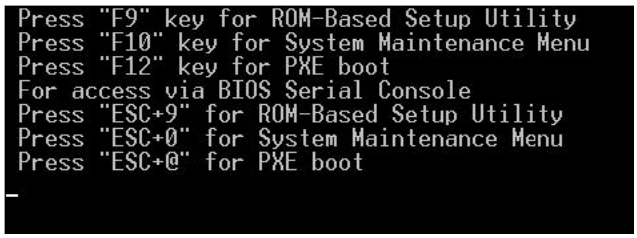
7 Press **ESC** to exit the ROM-based Setup Utility.

--End--

Setting the HP DL320 G4 server BIOS password

Step	Action
1	Press **Power** to boot the server. The server boots and the HP DL320 G4 boot screen appears.

Figure 208
HP DL320 G4 server boot screen



Note: If the server is already up and running, power the server off and on to restart and receive the HP DL320 G4 boot screen.

2 Press **F9** to invoke the ROM-based setup utility (RBSU) menu screen.

The RBSU menu screen appears.

Figure 209
HP DL320 G4 server RBSU menu

3 Select the Server Passwords option and press **Enter**.

4 Select the Set Admin Password option and press **Enter**.

5 At this point refer to the manufacturer's manual for specific instructions on how to enable or disable the BIOS password.

--End--

For additional operating information see the Server Product Guide on the resource CD-ROM shipped with the HP DL320 G4 server .

IBM x306m server

The IBM x306m server provides the following features:

- an Intel Pentium 4 processor (3.6 GHz)
- 2 simple swap Serial ATA, 80 GB (1 drive configured)
- 8 GB of RAM PC4200 DDR II by means of 4 DIMM slots (2 GB configured)
- Two Gigabit Ethernet ports
- Four USB ports (two front, two back)
- One DVD-COMBO (DVD/CD-RW) drive
  - — You use this to load the Signaling Server software files for the Signaling Server, Voice Gateway Media Cards, and IP Phones
- One serial port (back of Signaling Server)
- A reset button

For complete details and specifications about the IBM x306 server, visit the manufacturer's Web site at www.ibm.com.

Figure 210
IBM x306m front view

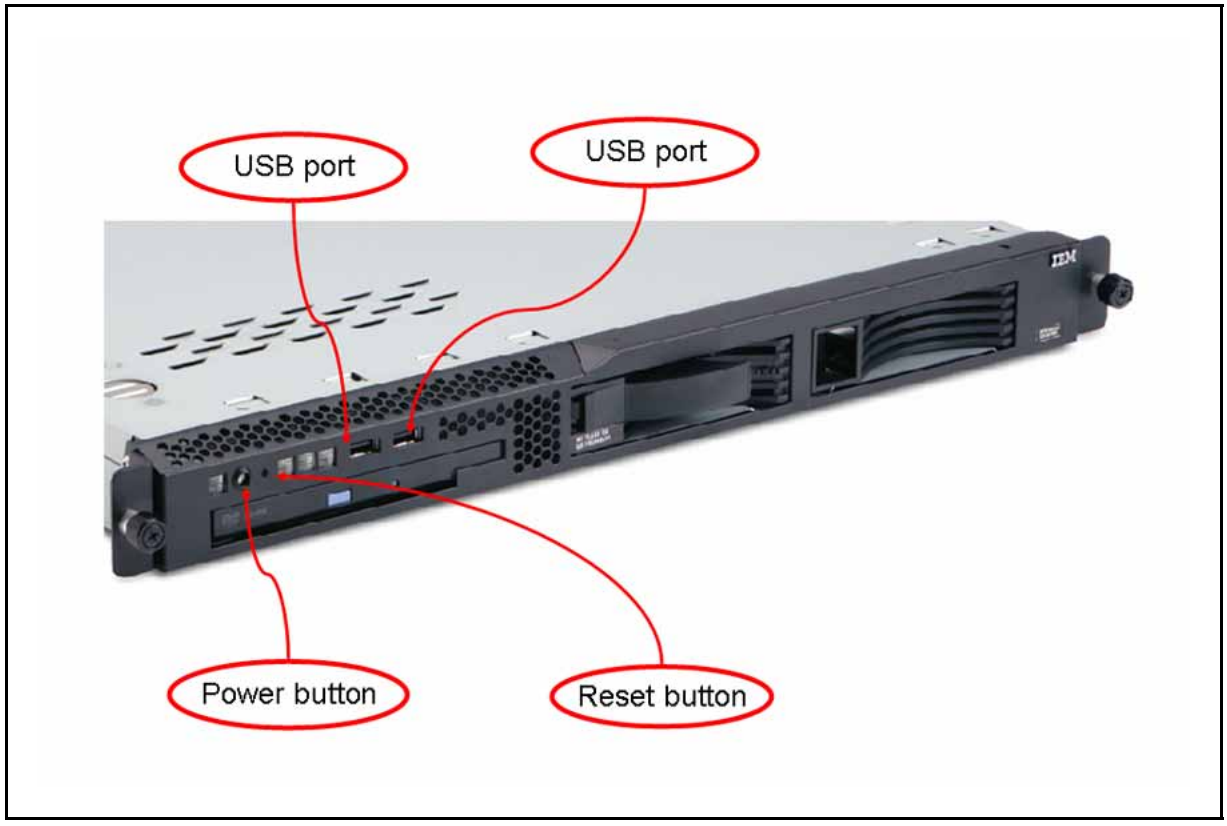


Figure 211
IBM x306m front view: LEDs

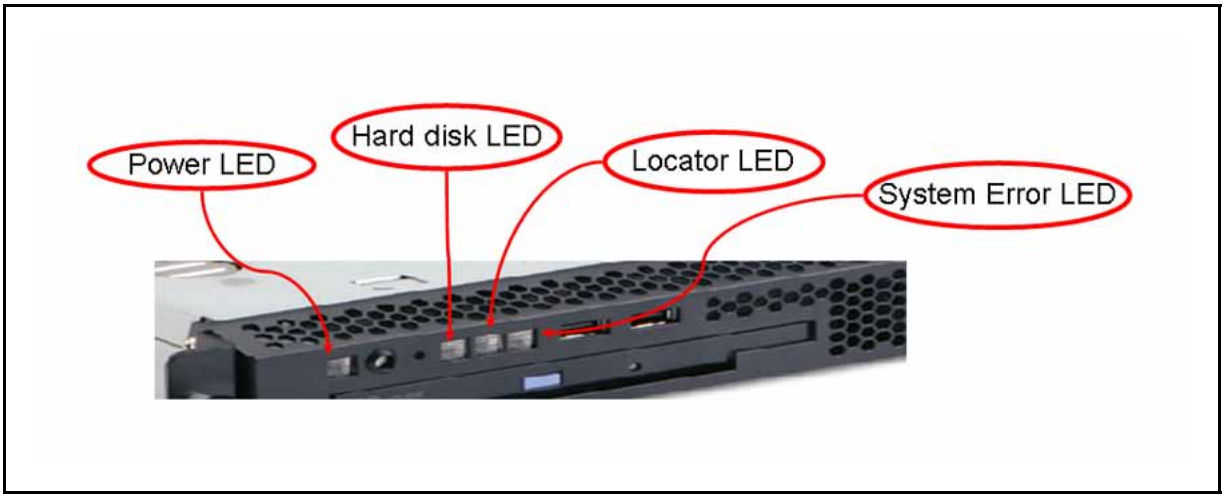
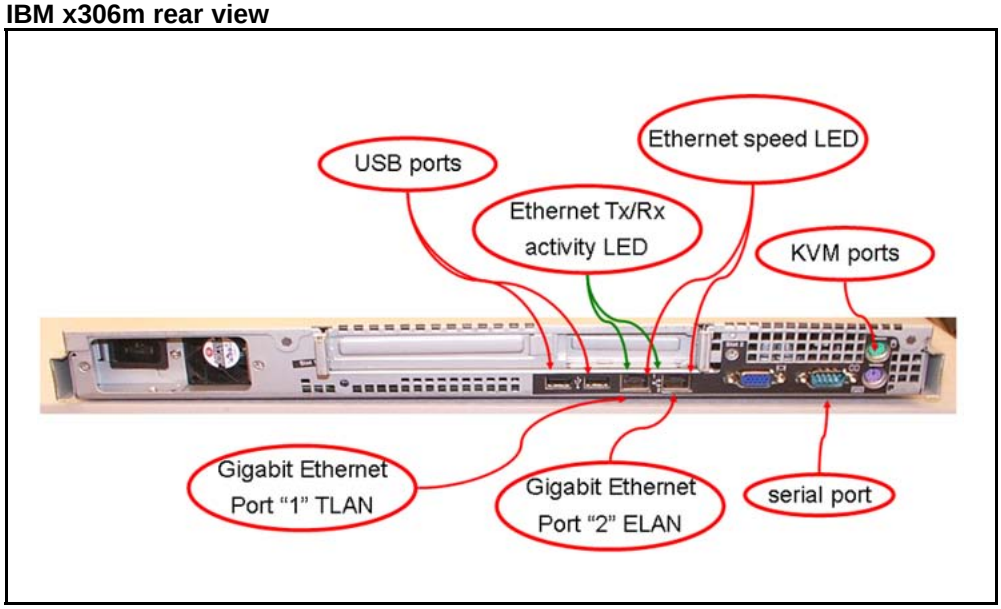


Table 9
IBM x306m LED description and status

Description	Status
Power LED	If this LED is lit, it indicates that the server is turned on. If this LED is off, it indicates that AC power is not present, or the power supply or the LED itself failed.
Hard disk LED	If this LED is lit, it indicates that a hard disk drive is in use.
Locator LED	When this LED is lit, it is lit remotely by the system administrator to aid in visually locating the server.
System Error LED	If this LED is lit, it indicates that a system error occurred.

Figure 212
IBM x306m rear view



ATTENTION
The TLAN & ELAN port positions are reversed (L and R, 1 and 2) compared to the HP DL320 server.Ethernet speed LED:

- Lit indicates Ethernet network speed of 1 Gbps.
- Off indicates Ethernet network speed is 10/100 Mbps.

IBM x306m BIOS settings

The BIOS settings on the IBM x306m server shipped through Nortel are correct. These settings can be viewed at Table 10 "IBM x306m default BIOS settings" (page 244).

Table 10
IBM x306m default BIOS settings

BIOS value	Default setting
Devices and I/O port - serial port A	Enabled
Devices and I/O port - baud rate	9600 baud
Devices and I/O port - console type	PC ANSI
Devices and I/O port - flow control	Off
Devices and I/O port - continue C.R. after POST	On
Devices and I/O port - type of connector	9-pin serial female
Start options - legacy USB support	Disabled

The IBM x306m server default BIOS settings can be changed by a BIOS reset or other maintenance activity. To return the BIOS settings to the appropriate values, see Procedure 44 “Changing the baud rate on an IBM X306m Signaling Server” (page 214) for instructions.

For information about how to enable or disable the BIOS password on the IBM x306m server see “Setting the IBM x306m server BIOS password” (page 247).

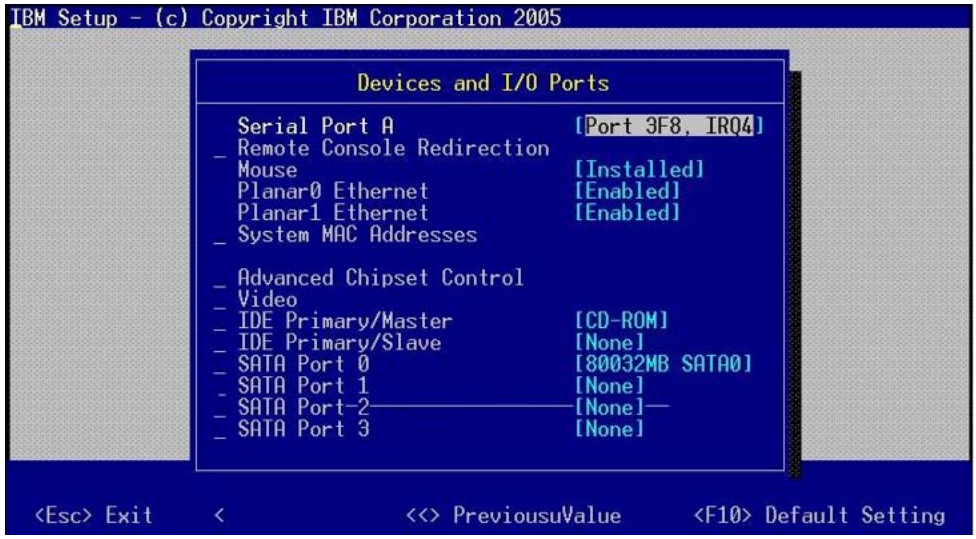
Changing the BIOS settings on an IBM x306m server

Step	Action
1	Press the Power switch to boot the server. The server boots and the Press F1 for Configuration/Setup message appears on the maintenance terminal. ***Note:*** If the server is already up and running, power the server off and on or press the reset button to restart and receive the Press F1 for Configuration/Setup message.
2	Press **F1** to invoke the IBM x306m server Configuration/Setup Utility. The Configuration/Setup Utility menu screen appears.

Figure 213
IBM x306m server Configuration/Setup Utility menu

3	Navigate to the **Devices and I/O Ports** option and press **Enter**. The Devices and I/O Ports menu screen appears.

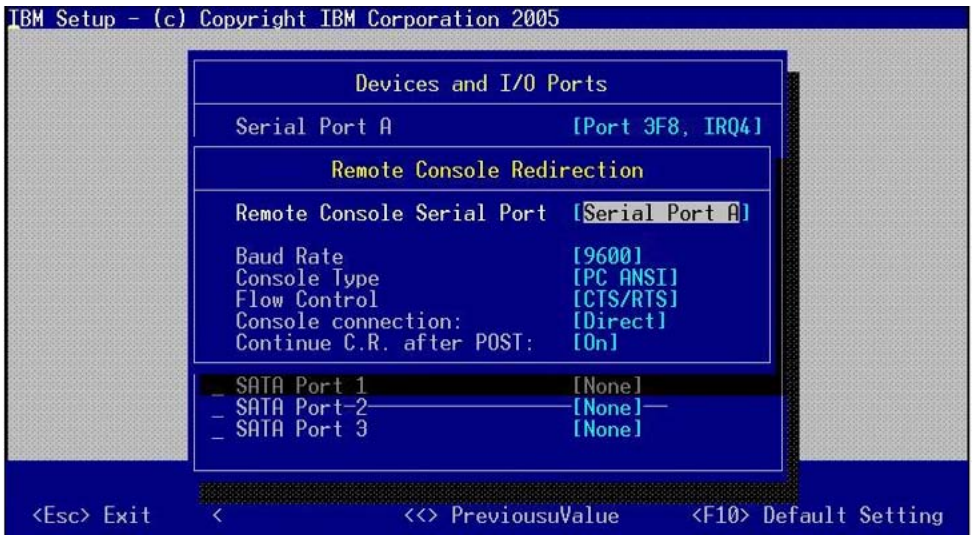
Figure 214
Devices and I/O Ports menu



4 Navigate to the **Remote Console Redirection** option and press **Enter**.

The Remote Console Redirection screen appears.

Figure 215
IBM x306m server Remote Console Redirection



5 Navigate to the option you wish to change and enter the appropriate value.

6 Press **Enter** to change the setting.

7 Press **ESC** to exit the **Remote Console Redirection** option.

The Devices and I/O Ports menu screen appears.

8 Press **ESC** to exit the **Devices and I/O Ports** option.

The Configuration/Setup Utility menu screen appears.

9 Navigate to the **Save Settings** option and press **Enter** to save the changed parameters.

10 Navigate to the **Exit Setup** option and press **Enter** to exit the IBM x306m Configuration/Setup Utility.

The server will restart automatically.

--End--

Setting the IBM x306m server BIOS password

Step	Action
1	Press the Power switch to boot the server. The server boots and the Press F1 for Configuration/Setup message appears on the maintenance terminal. ***Note:*** If the server is already up and running, power the server off and on or press the reset button to restart and receive the Press F1 for Configuration/Setup message.
2	Press **F1** to invoke the IBM x306m server Configuration/Setup Utility. The Configuration/Setup Utility menu screen appears.

Figure 216
IBM x306m server Configuration/Setup Utility menu

3 Select the System Security option and press **Enter**.

4 Select the Administrator Password option and press **Enter**.

5 At this point refer to the manufacturer's manual for specific instructions on how to enable or disable the BIOS password.

--End--

For additional operating information see the Server Product Guide on the resource CD-ROM shipped with the IBM x306m server .

IBM x3350 server

The IBM x3350 server provides the following features:

- Intel Core 2 Quad CPU –2.66GHz
- 250Gb RAID 1 array (2x 250Gb hard drives, hot-swappable)
- 4 Gb memory
- CD-RW/DVD drive
- Redundant power supply (hot-swappable)
- Dual GigaBit ethernet ports
- BIOS and RAID settings preconfigured for Nortel applications

For complete details and specifications about the IBM x3350 server, visit the manufacturer's Web site at www.ibm.com.

Figure 217
IBM x3350 server front view

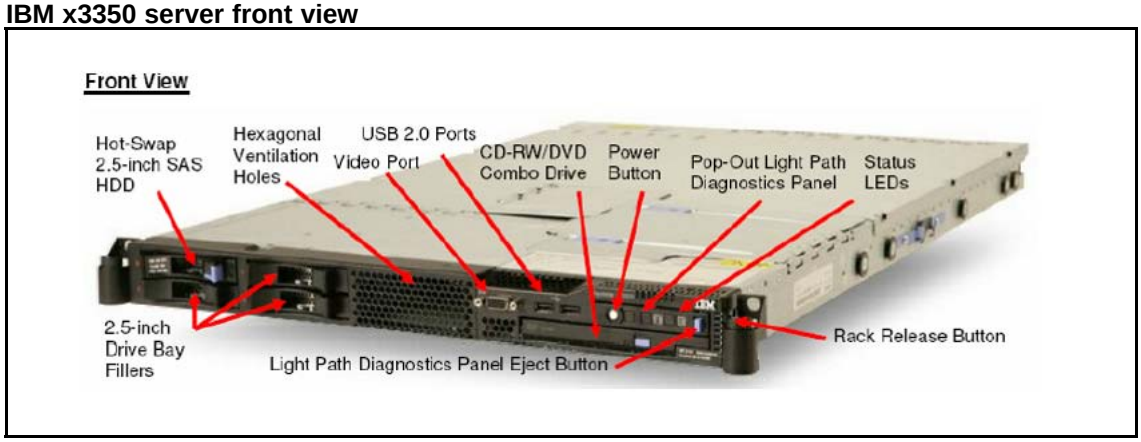
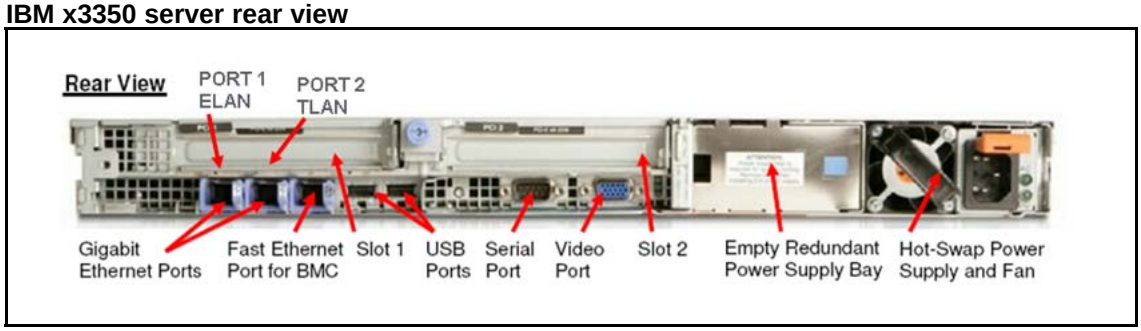


Figure 218
IBM x3350 server rear view



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

NTRX26NPE6 9 pin female to 9 pin female null modem cable is displayed in Figure 219 "NTRX26NPE6 9 pin female to 9 pin female null modem cable" (page 250).

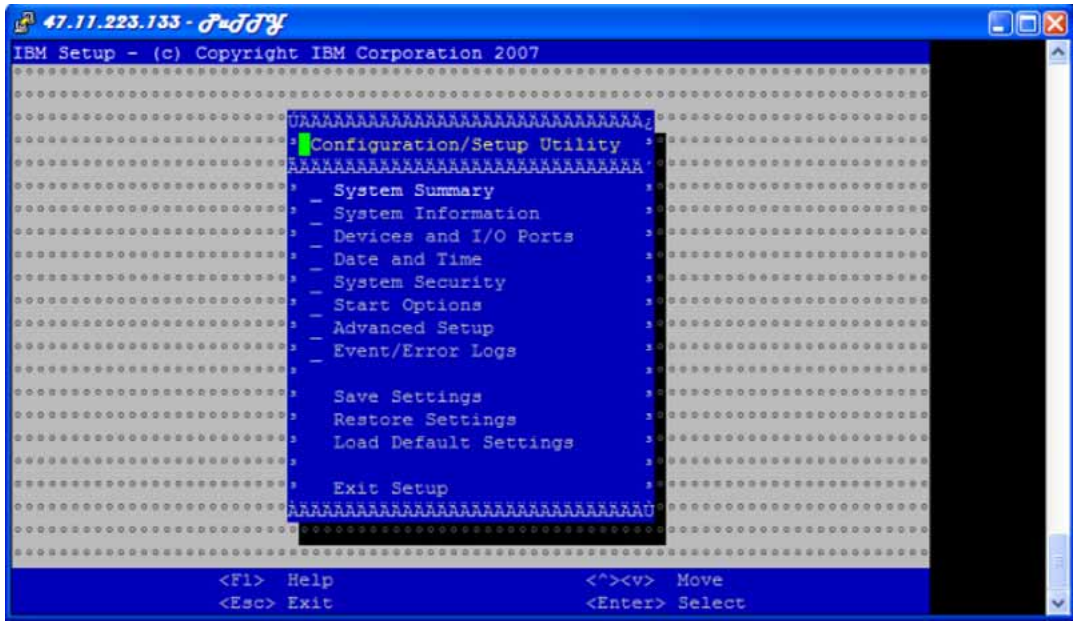
Figure 219
NTRX26NPE6 9 pin female to 9 pin female null modem cable

IBM x3350 BIOS settings

Procedure 51
Configuring COM port settings for the IBM x3350 server

Step	Action
1	Press **F1** to navigate to the BIOS configuration main menu screen using a Keyboard Video Monitor (KVM) terminal. **OR** Press **ESC-1** to navigate to the BIOS configuration main menu screen using the console terminal. The BIOS Configuration/Setup Utility main menu screen appears, as shown in Figure 220 "BIOS Configuration/Setup Utility main menu window" (page 251).

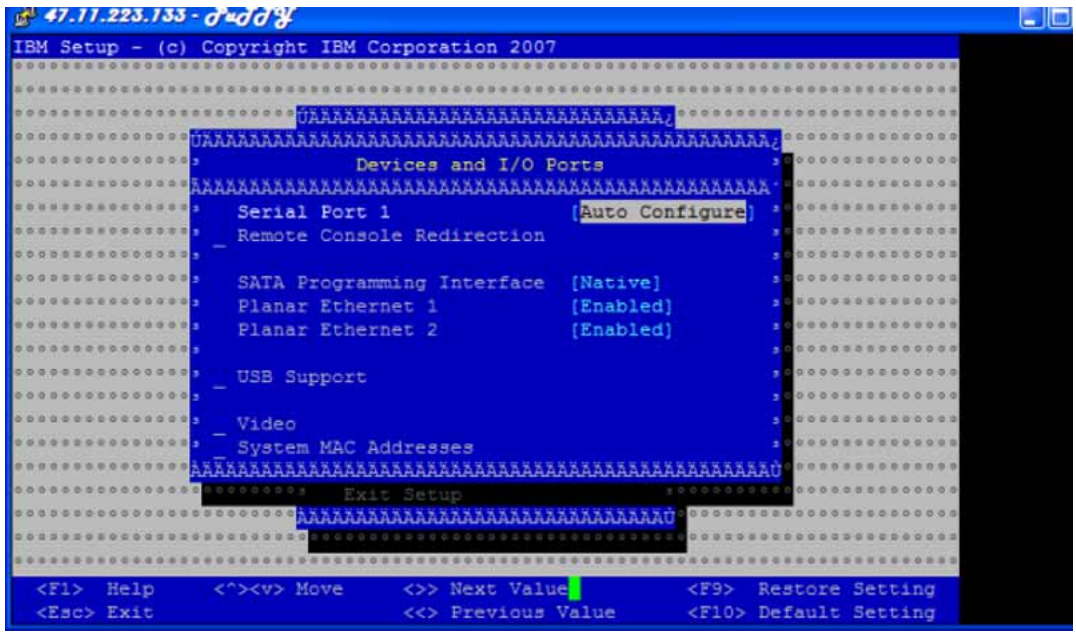
Figure 220
BIOS Configuration/Setup Utility main menu window



2 In the BIOS Configuration/Setup Utility main menu select **Devices and I/O Ports** and press **Enter**.

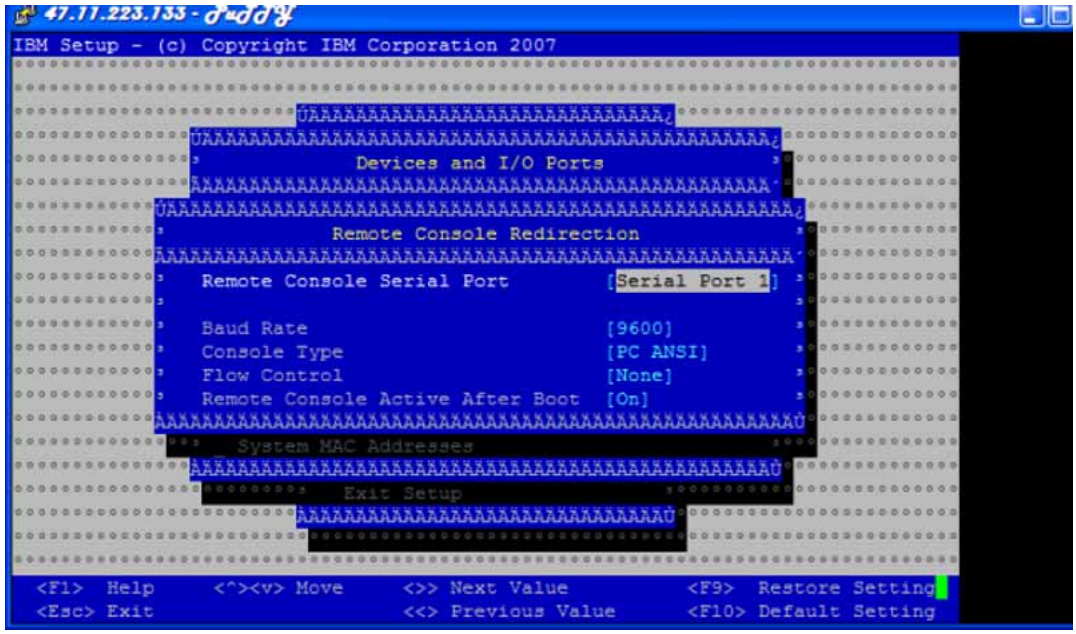
The Devices and I/O Ports screen appears, as shown in Figure 221 "Devices and I/O Ports window" (page 251).

Figure 221
Devices and I/O Ports window



3 In the Devices and I/O Ports screen, select **Remote Console Redirection** and press **Enter**. The Remote Console Redirection screen appears, as shown in Figure 222 "Remote Console Redirection window" (page 252).

Figure 222
Remote Console Redirection window



4 Navigate to Remote Console Serial Port and type **Serial Port 1**.

5 Navigate to Baud Rate and type **9600**.

6 Navigate to Console Type and type **PC ANSI**.

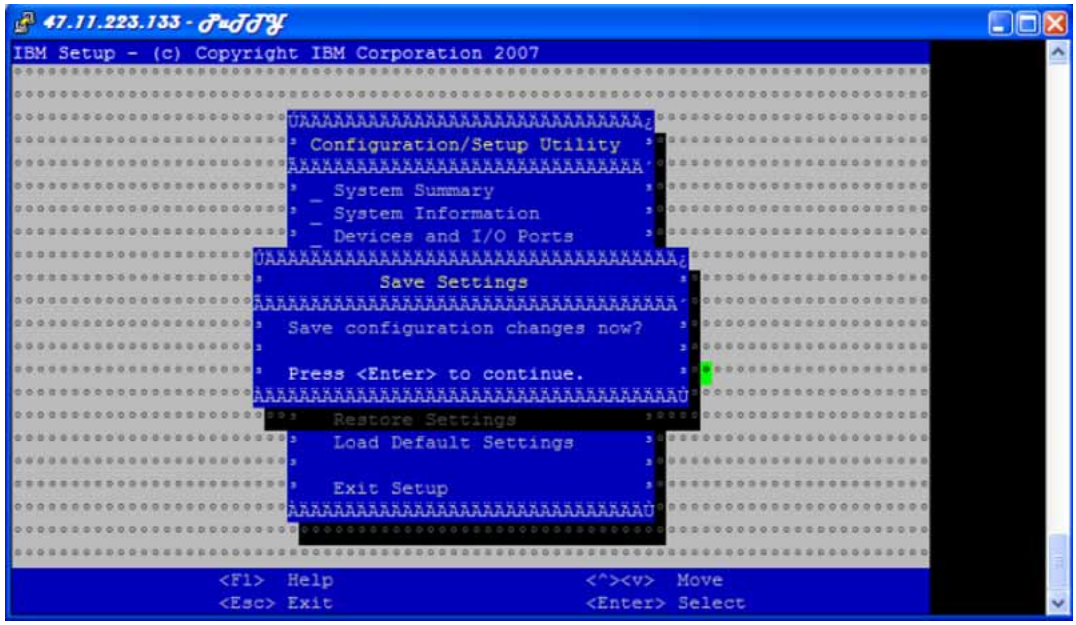
7 Navigate to Flow Control and type **None**.

8 Navigate to Remote Console Active After Boot and type **On**.

9 Press **Esc** twice to return to the BIOS Configuration/Setup Utility main menu.

10 In the BIOS Configuration/Setup Utility main menu screen, select **Save Settings** and press **Enter**. A confirmation prompt appears, as shown in Figure 223 "Save Settings confirmation window" (page 253).

Figure 223
Save Settings confirmation window



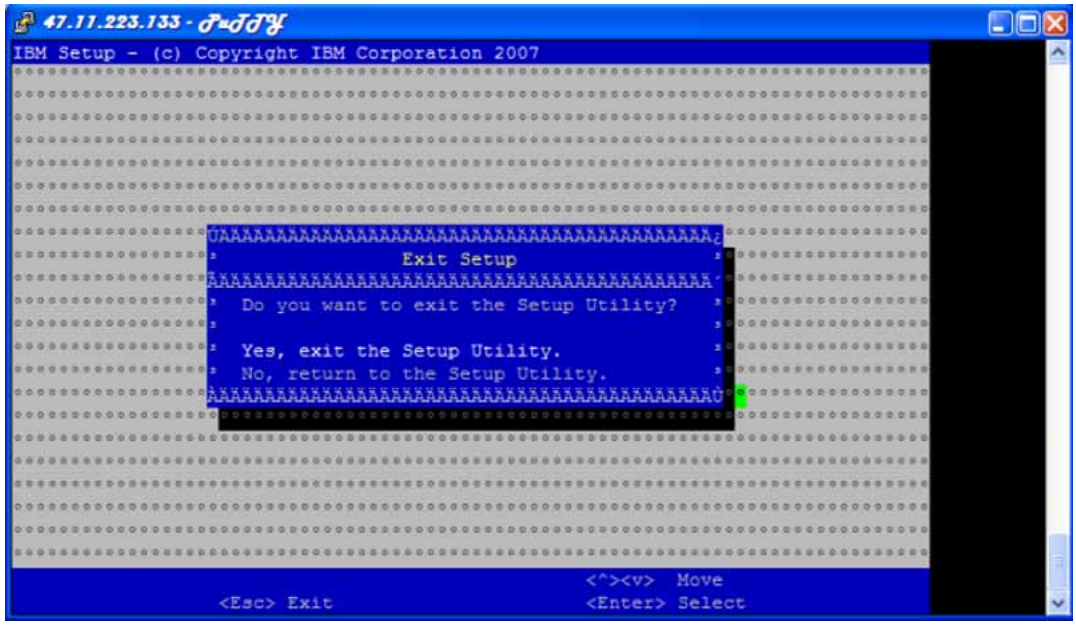
11 In the Save Settings confirmation screen press enter to confirm your changes.

The BIOS Configuration/Setup Utility main menu screen appears.

12 Press **Esc** to exit the BIOS Configuration/Setup Utility main menu.

A confirmation screen appears, as shown in Figure 224 "BIOS Configuration/Setup Utility main menu exit confirmation window" (page 254).

Figure 224
BIOS Configuration/Setup Utility main menu exit confirmation window



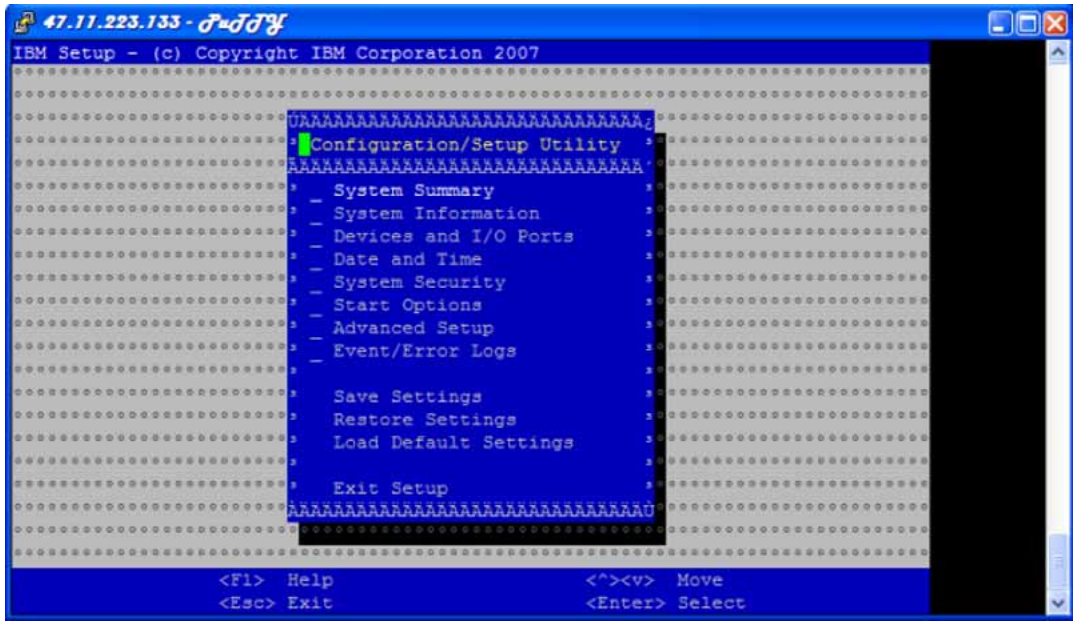
13 Navigate to **Yes, exit the Setup Utility** and press **Enter**.

--End--

Procedure 52
Setting the BIOS password for the IBM x3350 server

Step	Action
1	Press **F1** to navigate to the BIOS configuration main menu screen using a Keyboard Video Monitor (KVM) terminal. **OR** Press **ESC-1** to navigate to the BIOS configuration main menu screen using the console terminal. The BIOS Configuration/Setup Utility main menu screen appears, as shown in Figure 225 "BIOS Configuration/Setup Utility main menu window" (page 255).

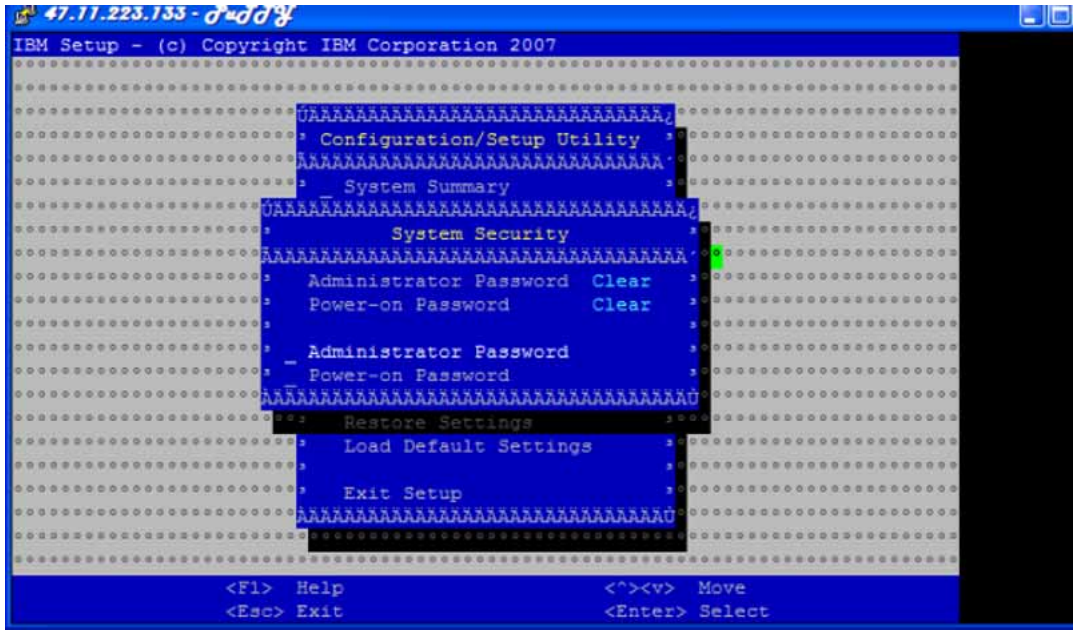
Figure 225
BIOS Configuration/Setup Utility main menu window



2 In the BIOS Configuration/Setup Utility main menu screen, select **System Security** and press **Enter**.

The System Security menu appears, as shown in Figure 226 "System Security menu" (page 255).

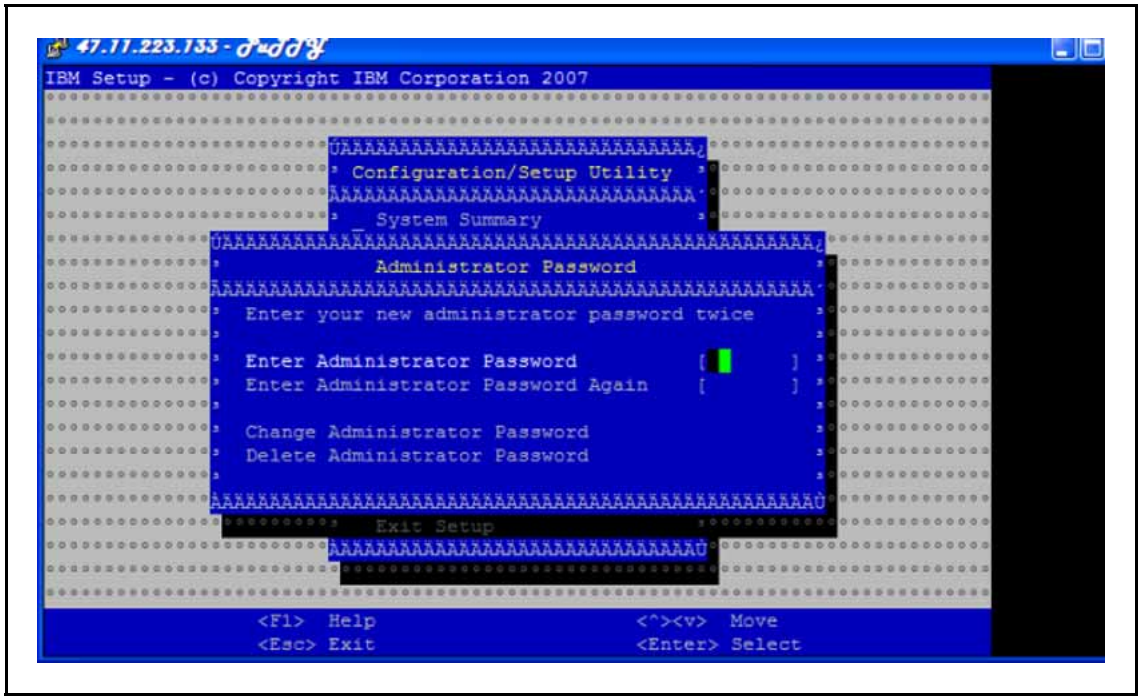
Figure 226
System Security menu



3 In the System Security menu, navigate to **Administrator Password** and press **Enter**.

The Administrator Password menu screen appears, as shown in Figure 227 "Administrator Password menu window" (page 256).

Figure 227
Administrator Password menu window



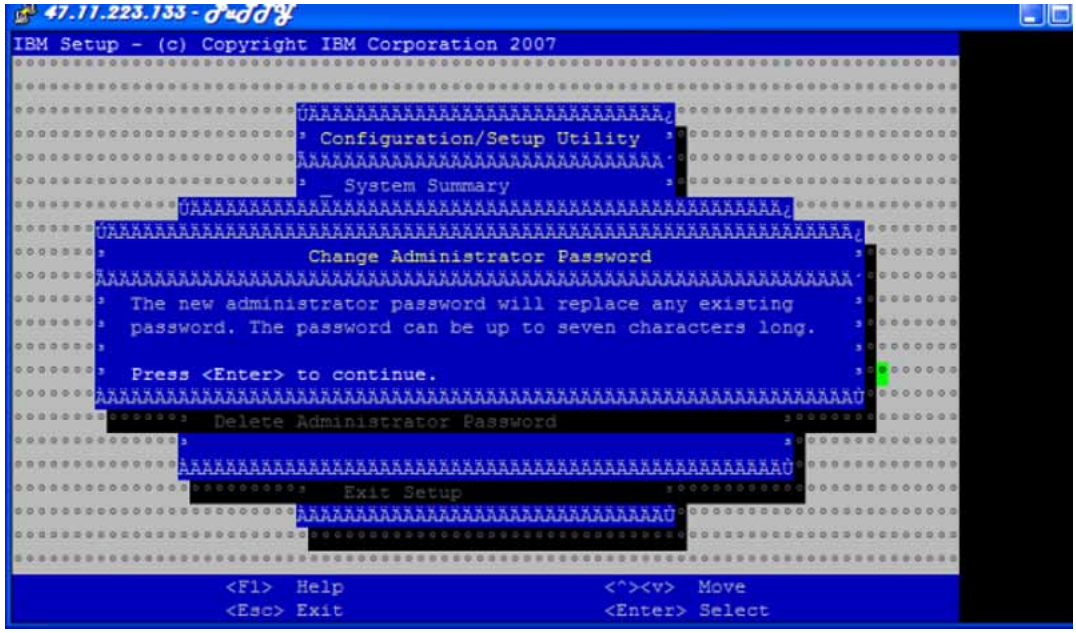
4 In the Administrator Password menu screen, navigate to **Enter Administrator Password** and type a password.

5 Navigate to **Enter Administrator Password Again** an retype the password.

6 Navigate to **Change Administrator Password** and press **Enter**.

The Change Administrator Password confirmation screen appears, as shown in Figure 228 "Change Administrator Password confirmation window" (page 257).

Figure 228
Change Administrator Password confirmation window



--End--

Appendix Installation times

Linux base and base applications installation times

Table 11 "Installation times by hardware platform" (page 259) provides installation times for Linux base and base applications on the CP PM and COTS platforms. Installation times are listed in total and in the following intervals:

- Power on to boot prompt
- Boot prompt to installation prompt
- Copy CD to HD
- Formatting
- Transfer initial image to HD
- Installation of RPMs
- Post installation
- Reboot, including base applications installation
- Total
- Format admin
- Pre-install
- Complete total

Table 11
Installation times by hardware platform

	CP PM	Dell R300	HP DL320	IBM x306	IBM x3350
Power On > Boot Prompt	0:00:25	0:01:55	0:00:45	0:00:33	0:01:22
Boot Prompt > Installation Prompt	0:02:13	0:01:21	0:01:07	0:01:14	0:01:43

	CP PM	Dell R300	HP DL320	IBM x306	IBM x3350
Copy CD to HD	0:04:03	0:01:13	0:01:26	0:02:30	0:02:30
Formatting	0:01:32	0:01:50	0:07:32	0:01:35	0:39:57
Transfer Install Image to HD	0:00:00	0:00:21	0:00:21	0:00:34	0:00:27
Installation of RPMs	0:08:16	0:06:37	0:07:15	0:07:02	0:07:33
Post-Installation	0:00:59	0:00:35	0:01:58	0:00:38	0:01:42
Reboot (Including BaseApps Installation)	0:04:14	0:04:06	0:04:44	0:04:51	0:06:57
Total	0:21:43	0:17:58	0:25:08	0:18:56	1:02:13
Format Admin	0:00:08	0:00:12	0:00:19	0:00:08	0:05:10
Pre-Install	0:01:30	0:01:30	0:01:30	0:01:30	0:01:30
Complete Total	0:23:21	0:19:40	0:26:58	0:20:34	1:08:52

Figure 229 "Total installation times " (page 261) provides a comparison of total installation times for each hardware platform.

Figure 229
Total installation times

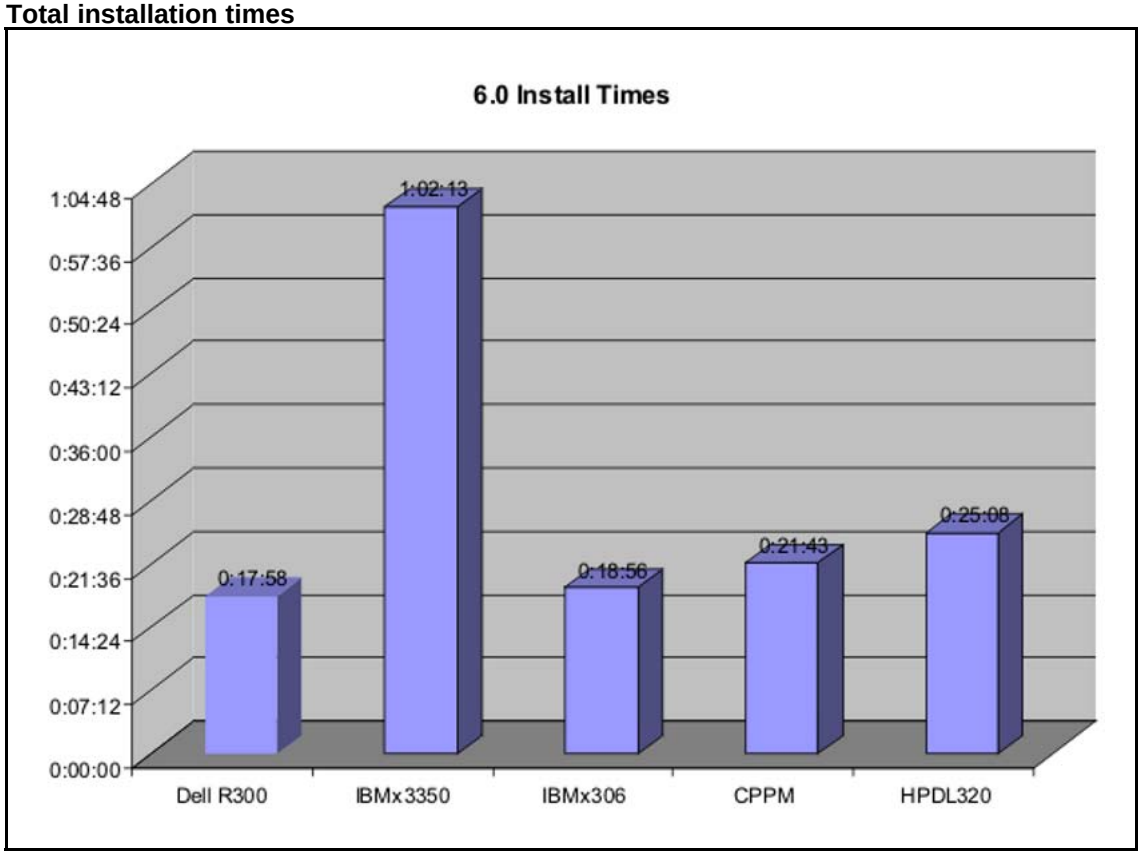


Figure 230 "CP PM installation time analysis" (page 262), Figure 231 "Dell R300 installation time analysis" (page 262), Figure 232 "HP DL320 installation time analysis" (page 263), Figure 233 "IBM x306 installation time analysis" (page 263), and Figure 234 "IBM x3350 installation time analysis" (page 264)provide a graphical view of the time required for the various installation phases on each hardware platform.

Figure 230
CP PM installation time analysis

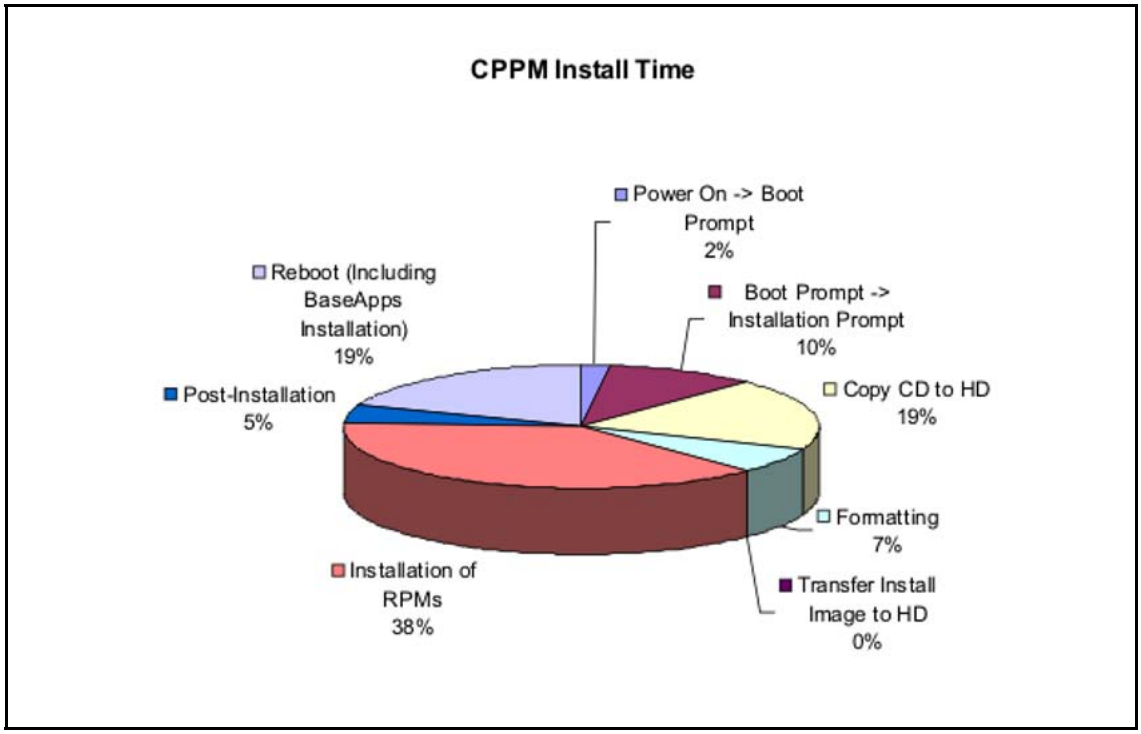


Figure 231
Dell R300 installation time analysis

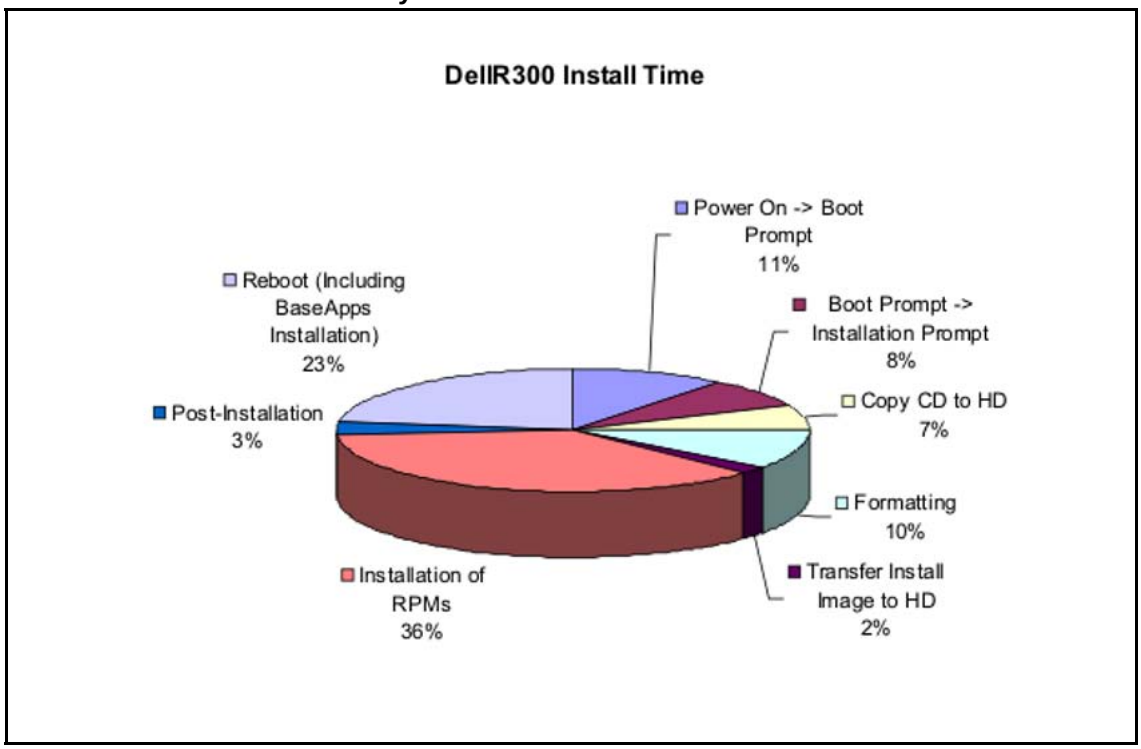


Figure 232
HP DL320 installation time analysis

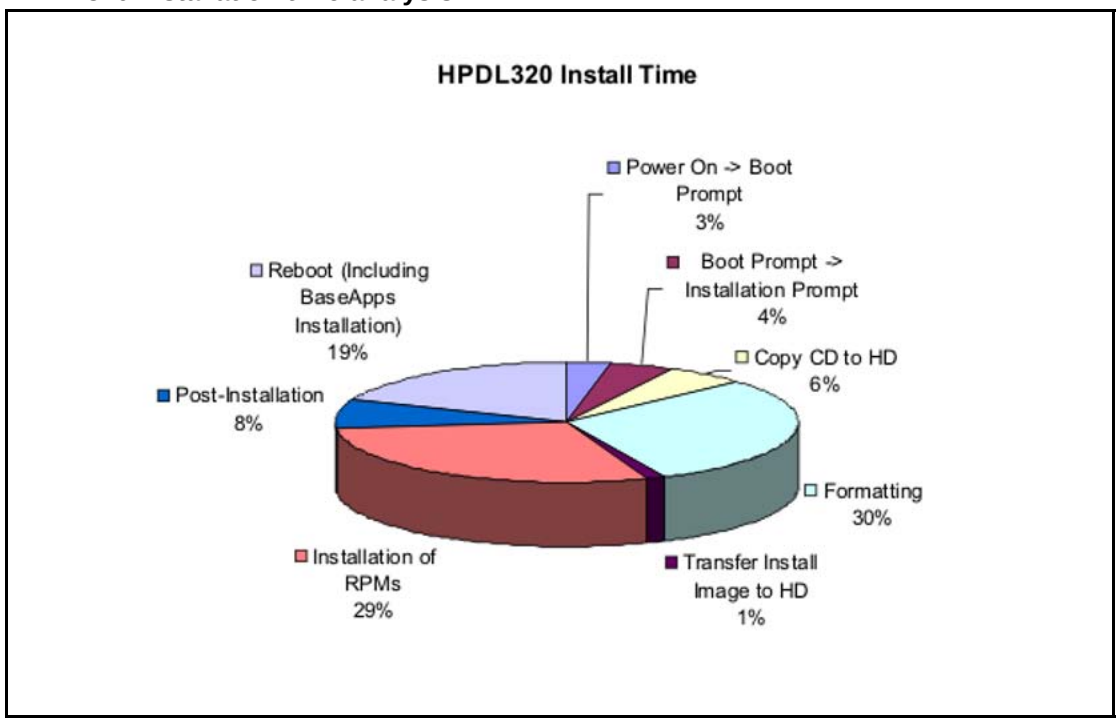


Figure 233
IBM x306 installation time analysis

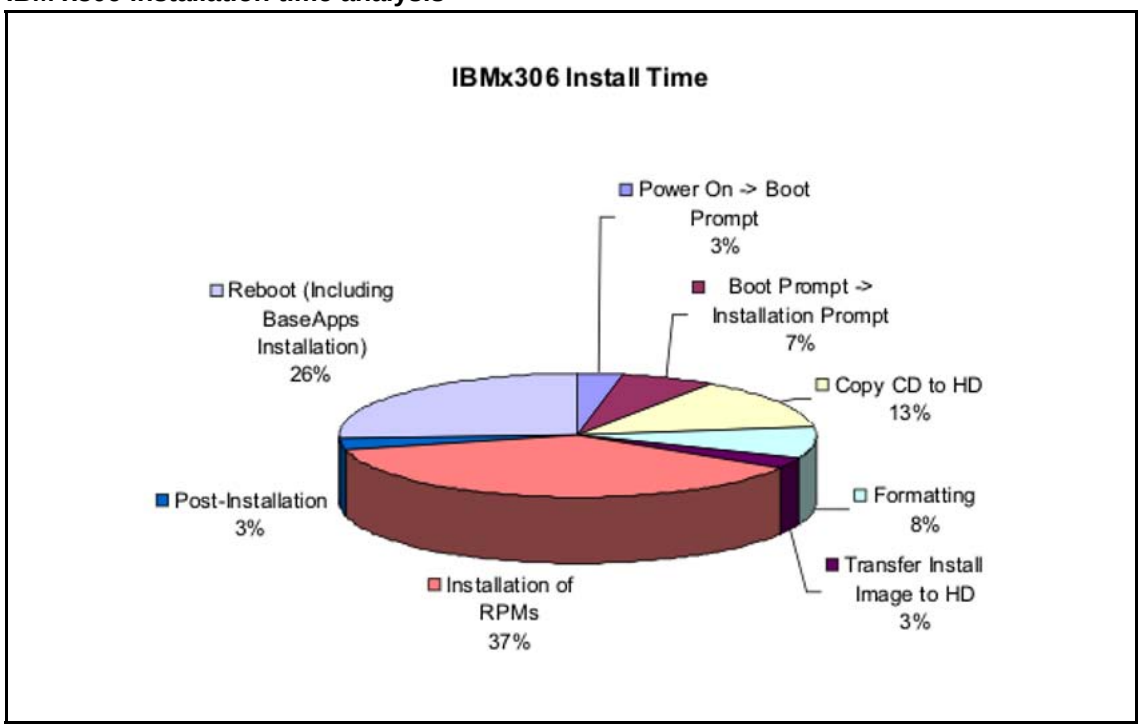
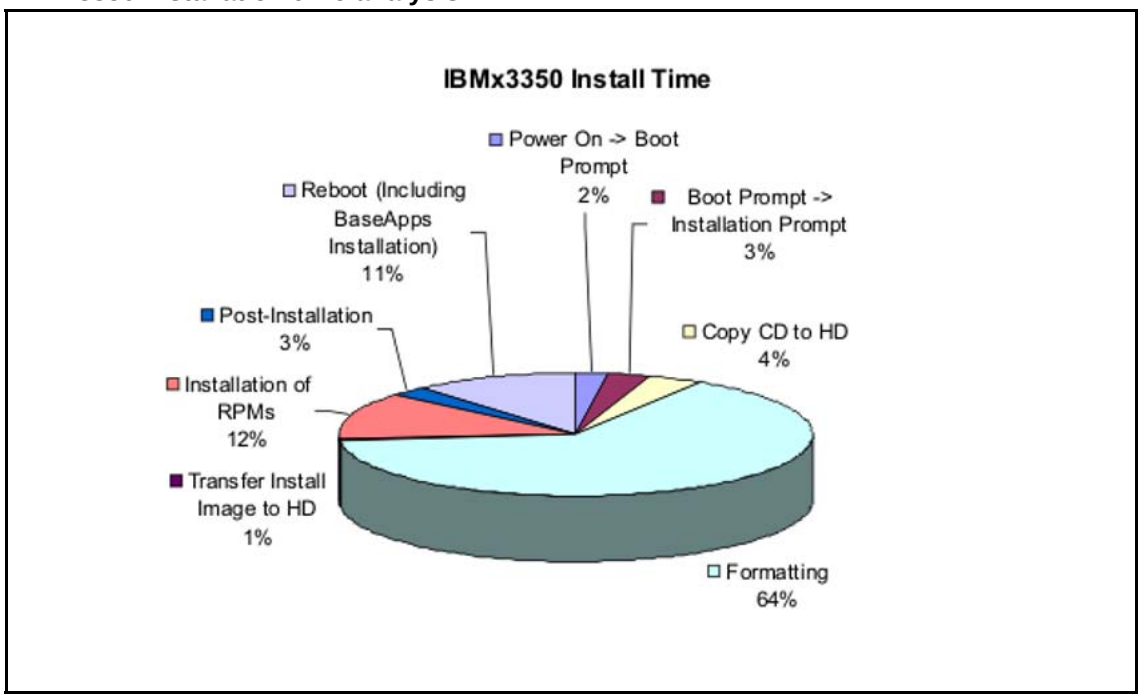


Figure 234
IBM x3350 installation time analysis



Appendix
Nortel Linux base CLI commands

" Nortel Linux base CLI commands" (page 265) contains a list of the command line interface (CLI) commands used in Nortel Linux base. Type **(linuxbase-command) -h | --help | help** at the command prompt to display a brief summary of the CLI command, as shown in Table 12 "Linux CLI command help" (page 265). Type **man (linuxbase-command)** at the command prompt for a more detailed description, as shown in Table 13 "Linux man command example" (page 266).

Table 12
Linux CLI command help

```
$ poos --help
Usage:
poos (patch_id)|-app *(app_name)*|--help,-h

Options:
(patch_id)
Deactivate patch with (patch_id) handle.

-app *(app_name)*
Deactivate all patches for the application (app_name).

--help
Print this help message and exit.
```

Table 13
Linux man command example

```
$ man poos

POOS(1) User Contributed Nortel Documentation POOS(1)

NAME
poos - Put a patch out of service.

SYNOPSIS
poos (patch_id)| -app (app_name) | --help,-h

DESCRIPTION
Remove a patch from service. The patch is removed from service from all processes in which it
was in service.

OPTIONS
(patch_id)
Deactivate patch with (patch_id) handle.

-app (app_name)
Deactivate all patches for the application (app_name).

--help Print this help message and exit.

EXAMPLES
Deactivate patch with 2 handle
$ poos 2
Patch handle: 2
Please ensure that the application solid is stopped before proceeding patch un-installation.
Do you want to continue patch un-installation? (Y/N) [N]? y
Performing the uninstallation:
Performing uninstall RPM patch...
Preparing... ########################################### [100%]
1:nortel-cs1000-solid ########################################### [100%]
executing Solid DB post install...
Installation nortel Solid database server completed.
Unstalling the Solid database server package done

Done.
The RPM patch uninstallation is completed.
The patch 2 has been deactivated successfully.

Deactivate all sunAm patches
$ poos -app sunAm
Patch handle: 0
Performing the uninstallation:
```

```
The patch 0 has been deactivated successfully.

SEE ALSO pload, pout, pins, pstat, plis

5.50 2007-12-18 POOS(1)
```

Nortel Linux base uses common (no access restrictions) CLI commands plus 8 categories of CLI commands that correspond to the 8 Nortel Linux base user groups. The 8 categories of CLI commands are shown in the following list:

- backupadmin
- dbadmin
- logadmin
- maintadmin
- patchadmin
- securityadmin
- systemadmin
- timeadmin

Table 14
Common CLI commands

Command	Description
appVersionShow	Print the server's application software version.
baseVersionShow	Print the server's base software version.
echo	
find	
ftp	
ifconfig	
ls - ll	
man	
printenv	
scp	
sftp	
ssh	
su	
swVersionShow	Print the server's software version.
telnet	
whoami	

Table 15
backupadmin CLI commands

Command	Description
sysbackup	Perform a system backup (both base and applications).

Table 16
maintadmin CLI commands

Command	Description
consoleShow	
gnome-system-monitor	
gryphon	Control script for Apparent Network's AppCritical OEM.
netstat	Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.
pcapConfig	Configure PCAP for Linux.
pcapCtrlRemove	Stops the PCAP for Linux listener interface.
pcapCtrlStart	Start the PCAP for Linux listener interface.
pcapRestart	Restart PCAP for Linux.
pcapStatus	Displays the current status of PCAP for Linux.
pcapStop	Stop PCAP for Linux.
wireshark	
pcap	
ppp	Initiate a PPP connection.
tcpdump	

Table 17
patchadmin CLI commands

Command	Description
issp	Generates a list of installed RPMs, SUs and patches.
pins	Put the patch in service.
plis	Show detailed information about the patch.
pload	Load the patch into the system database.
poos	Put the patch out of service.
pout	Unload the patch from the system database.
pstat	Show a list of installed patches.
spins	Put a Service Pack into service.

Command	Description
spload	Load a Service Pack (bundle of patches and SUs) into the system database.
spout	Unload a Service Pack (bundle of patches and SUs) from the system database.
spstat	Show the installed and in service SPs.

Table 18
securityadmin CLI commands

Command	Description
addipsectarget	
basefirewallconfig	Configure firewall settings.
checkIPsecStatus	
copyipsectarget	
deleteipsectarget	
disableAllTargets	
disableipsectarget	
enablealltargets	
enableipsectarget	
harden	Command to manage CS 1000 hardening items.
harden audit status	Displays the status of the Linux Audit Daemon.
harden banners set/file	Modify the banner text. The banner text will be replaced by the content from the file.
harden banners status	Enables or disables the pre-login banners.
harden coredumps status	Enables or disables the coredump service.
harden ftp status	Shows that FTP service is turned on or off.
harden help	Displays help information for using the command.
harden nettools status	Enables or /disables the nettools service.
harden passwd_days off	Disable previously configured parameters.
harden passwd_days on	Enables previously configured parameters.
harden passwd_days set -max	Set value the value of the PASS_MAX_DAYS parameter. The default value is 90.
harden passwd_days set -min	Set the value of the PASS_MIN_DAYS parameter. ***Note:*** This parameter must be set to a value >or = 1. The default value is 1.

Command	Description
harden passwd_days status	Provides the current value of the parameters from hardening storage.
harden rlogin	Apply hardening to remote logons. ***Note:*** rlogin is only available in Co-Resident configurations where the Call Server is installed.
harden ssh_filter status	Shows the list of the names of the hosts which are allowed to connect to Linux Base by SSH.
harden status	Retrieve the status of Linux Base Enhanced Hardening options.
harden telnet status	Shows that telnet service is turned on or off.
harden tftp status	Shows that TFTP service is turned on or off.
newipsectarget	
printipsecpolicy	
queryipsectarget	
removeipsectarget	
masterfirewallconfig	Master firewall configuration.
masterfirewallcontrol	

Table 19
systemadmin CLI commands

Command	Description
appinstall	Install Nortel applications. ***Note:*** Do not use the appinstall command unless you are directed to use it by Nortel support.
appstart	Stop, start, or restart Nortel applications.
arp	Manipulate the system ARP cache.
baseparamsconfig	Configure base parameters. **WARNING** Do not change the FQDN of the primary or backup security server when you use the baseparamsconfig command.
datetimeconfig	Configure the date and time.
dnsconfig	Configure DNS values.
ecnconfig	Configure Explicit Congestion Notification settings.
hdStat	Displays the size of the hard disk.
hostconfig	Configure the static lookup table for host names.

Command	Description
memShow	Displays available, free, and used server memory.
memSizeShow	Displays the total server memory.
networkconfig	Configure network settings.  **WARNING** Do not change the FQDN of the primary or backup security server when you use the networkconfig command.
ntpconfig	Configure Network Time Protocol settings.
reboot	Restart the entire system.
routeconfig	Configure routing entries. ***Note:*** When you use routeconfig to add a host route you do not need to provide a netmask. If you do provide a netmask, the format must be 255.255.255.255.
stty	Change and print terminal line settings.
sysbackup	Configure system backup.
syslogFacilitySet	Set the facility value.
syslogLevelSet	Set a value for level.
syslogShow	Display syslog processes. ***Note:*** The help key is not valid for **`syslogShow`**. If you want to retrieve help information, you must use the format **`syslogShow -h`** or **`syslogShow -help`**.
sysrestore	Perform a restore of the application data (backed up by sysbackup).
timeadj	Specify system clock parameters.
upgrade	Select the backup data source and reinstall Linux base.

Note: You might need to add the primary host entry in backup and member servers before you can access them using the **`hostconfig`** command.The command syntax is **`nortel user ---> hostconfig add -ip <PRIMARY SERVER IP> -host <PRIMARY SERVER HOST NAME> -domain <PRIMARY SERVER DOMAIN NAME>`**.

Table 20
timeadmin CLI commands

Command	Description
datetimeconfig	Configure the date and time.

Command	Description
ntpconfig	Configure Network Time Protocol settings.
timeadj	

Appendix Network configuration for Secure File Transfer Protocol (SFTP) data backup

Use the guidelines in this appendix to assist in data backup to an SFTP server. The section “Network configuration” (page 273) provides details on network requirements and the section “SFTP logon” (page 273) provides SFTP logon details. The section “SFTP network configuration requirements” (page 274) provides specific Embedded Local Area Network (ELAN) and Telephony Local Area Network (TLAN) requirements for SFTP network configuration.

Network configuration

The network must be configured correctly for data backup to an SFTP server. In order to configure the network you must understand the difference between the ELAN and the TLAN. The ELAN and TLAN are defined as follows:

- ELAN - The ELAN is a secure local area network. The scope of this network is limited to one subnet or node; however the scope of the ELAN network can be expanded to cover multiple nodes with advanced router (data path) configurations.
- TLAN - The TLAN spans the entire enterprise network. Every node on the TLAN has access to every other node.

Note: The definitions of ELAN and TLAN are a subset of the definitions provided in the voice media gateway cards section of *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

SFTP logon

Data backup to an SFTP server requires a user logon, password, and path to access the SFTP server storage. The user logon can contain a maximum of 32 characters comprised of lower and uppercase letters,

numeric digits, and the special characters _ . - and $. You cannot use the character - at the beginning of the logon string and you can use $ only at the end of the logon string.

Nortel Linux base uses the character / to specify paths in the system. Use the / character when you specify the SFTP directory.

SFTP network configuration requirements

The SFTP option requires an operational ELAN network because the backup and recovery of data must use the ELAN interface. Nortel recommends the destination SFTP server reside on the same ELAN network as the source SFTP server. If the destination SFTP server resides outside the subnet of the source SFTP server, use one of the two options shown in Table 21 "SFTP network configuration requirements" (page 274).

Note: Not all Windows based SFTP servers can be used as SFTP backup servers. The following Windows based SFTP servers can be used:

- ***Sysax Multi Server***
- ***OpenSSH for Windows***

The following Windows based SFTP servers are not supported:

- ***Core FTP mini-sftp-server***
- ***CrushFTP***
- ***freeFTPd***
- ***NullFTP***
- ***TitanFTP***
- ***winSSHD***

Table 21
SFTP network configuration requirements

Option	Details
1	The router connecting the two subnets must be configured to allow pings to pass through. This ensures there is a valid data path between the two subnets If the default gateway is set to the TLAN interface gateway, a routing entry is required to ensure that all ELAN data uses only the ELAN NIC. Use the CLI command **`routeconfig`** to add the routing entry. An example of the **`routeconfig`** command is as follows: routeconfig add -net destination_ip -netmask subnet_mask -gw gateway_ip -dev eth0
2	On the source server set the ELAN interface gateway as the default gateway.

Appendix Deployment errors

Deployment errors

It is possible for errors to occur during application deployment. Table 22 "Deployment errors" (page 275)provides a list of error codes that can display during application deployment. For each error code, the table provides the error message corresponding to the error code, as well as a description and user action where applicable.

Table 22
Deployment errors

Error Code	Error Message	Description	Action
AAIN	Applications are already installed.	Possible causes: Case: deploy is called when Nortel Applications are already installed. This case supports auto-recovery – deployment status should reset to correct one automatically.	No action is required, the server status should be reset to correct value.
ANIN	Applications are not installed.	Deployment manager status may not have been correct initially. Case: deploy is called when Nortel Applications are already installed. This case supports auto-recovery – the server status should reset to correct one automatically.	No action is required, the server status should be reset to correct value.

Error Code	Error Message	Description	Action
BKUP	Error occurred while backup of target.	Possible causes: General error for any backup failure. Any one of the backup scripts failed. Network problem.	Check your network (on TLAN) between the deployment server and the target. Check your network between the target and the SFTP server. Check permissions on the file system. Check whether the SFTP server has enough free disk space to keep the backup archive.
CLDF	Failed to clear a directory in pre-installation phase.	Possible causes: Generic error. Could be some permission issue.	Check the permissions. Try the operation again.
CRDF	Failed to create a directory in pre-installation phase.	Possible causes: Generic error. Could be some permission issue.	Check the permissions. Try the operation again.
INPF	Input parameter(s) validation failed.	Possible causes: Provided keycode file does not exist (something must have gone wrong during the keycode file upload).	Browse and validate the keycode again.
INSF	Can't copy installation xml.	Possible causes: Some permission problem which is disallowing the copy of the install.xml file under the /admin partition.	Check file permissions of the /admin partition. Repeat the operation again.
NFLS	No configure.xml files found.	Corrupted .nai file. Damaged installation.	Upload the software load again. Try the application installation again. Backup the data, and reinstall Linux base again.
NUSR	Please login as a user with valid permissions to use Deployment Manager.	Deployment manager is not running as user nortel.	Make sure that Jboss is running as nortel user. Perform "ps –ef | grep jbossd" and check whether the user is nortel.

Error Code	Error Message	Description	Action
PRECFG	Cannot get preconfig data.	Possible causes: Can be set if preconfig data are found on the target but cannot be extracted from an archive file.	Try again, and if problem persists, get Nortel help.
PREDEPF	Failed to prepare or transfer deployment data. Make sure the network connection to your target is in working condition. See Help for more details.	Possible causes: Network connection between the deployment server and the target may have some problem Available disk size and permission problem.	Try the operation again. Check available disk space.
PREP	Installation data preparations error.	Possible causes: Couldn't create the necessary files for this particular target.	Try again, and if problem persists, get Nortel help.
RESF	Restore of applications failed.	Possible causes: General error for any restore failure. Any one of the backup scripts failed. Network problem.	Check network connection, permissions and try one more time. Make sure that there is enough space on the server to keep restore archive. Check the linuxbase.log from base manager.
RPMDB	RPM database is corrupted. Re-installation of Linux Base is required.		
RPMF	RPM installation failed.	Possible causes: Corrupted .nai file.	Check the appinstall_stderr.log, appinstall_stdout.log and linuxbase.log. Check to see whether there is any dependency problems (which will be indicated in the appinstall_stderr.log). Try the operation again.
RPMUF	RPM uninstallation failed.		
RSBLK	Operation is blocked by another process. Please try again.	Possible causes: Applicable for Deploy, Undeploy, Backup, Restore and Upgrade cases. Indicates that semaphore is busy and operation cannot be started to avoid data integrity corruption.	Wait for sometime and try the same operation again.

Error Code	Error Message	Description	Action
RSWF	Remote script failed.	Possible causes: Generic error. Applicable for Deploy, Undeploy, keycode validate and Upgrade cases. Set if for example, remote script cannot be executed, command is not found, not enough permissions and so on.	Check permission of the file system. Check the connection between the deployment server and the target.
TRNSF	Transfer failed.	Possible causes: SCP operation (remote copy command) failed.	Check your network (on TLAN) between the deployment server and the target.
UNER	Undeployment error.	Possible causes: There are some patches that cannot be removed.	Check the appinstall_stderr.log , appinstall_stdout.log, and the linuxbase.log. Check the network connection. Try undeployment again.
UNPA	Undefined parameter.	Possible causes: Some mandatory values are not set in deployment manager properly.	Set all required values, and try the operation again. Seek help from nortel.
WAPPVER	Undefined parameter.	Possible causes: Some mandatory values are not set in deployment manager properly.	Set all required values, and try the operation again. Seek help from nortel.
WC1001	An unexpected error occurred.		Please try the operation again. If not successful seek help from Nortel.
WC1002	Error occurred while restoring Could not retrieve the information for the target on the deployment server.target.	Please try the operation again. If not successful seek help from Nortel.	

Error Code	Error Message	Description	Action
WC1003	Error occurred while saving target.	Possible causes: Problem in writing the target information on the deployment server. Frequency: Very Low Severity: Major	Please try the operation again. Go to the folder /var/opt/nortel/deployment/deployed/<hostname> and check for any permission or disk space issues that could prevent writing to this folder. If not successful seek help from Nortel.
WC1004	Could not retrieve UCM elements temporarily. Please refresh the page.	Possible causes: There was a problem retrieving the linux base element(s) from UCM. Refresh the page by clicking on the refresh link.	Refresh the page by clicking on the refresh link.
WC1005	Target in an invalid status for requested action.	Possible causes: Someone else may have started another operation on the target. The information on the deployment server is corrupted.	Refresh the page. Try again later. If not successful seek help from Nortel.
WC1006	Error occurred while deploying/upgrading/undeploying target.	Possible causes: Could not make the system call to execute the linux base commands to perform the deploy/upgrade/undeploy operation.	Seek help from Nortel.
WC1008	Failed to generate a pre configuration file.	Possible causes: ElementInternalID is blank for the chosen call server. Could not create the cs1000.properties file. Error while writing to the cs1000.properties file. Could not create the csinst.ini file. Could not create the preconfiguration directory.	Check the file system for disk space and permissions.
WC1009	Maximum number (3) of simultaneous deployment reached.	There are already 3 deployment operations in progress.	Wait for at least one deployment to complete before starting a new deployment.

Error Code	Error Message	Description	Action
WC1010	Could not validate keycode. Error occurred during validation process.	Could not make the system call to run the keycode validation base command.	Check whether the keycodeValidate API exists on the server. Also check whether executable permissions are set properly.
WC1011	Keycode file missing on target, or can't read the file.	There has been some problem in the keycode uploading process.	Browse and validate the keycode again. Check whether the keycode is of non-zero size.
WC1012	Version in keycode does not match software version to be installed.		Make sure that the Release and Issue of the keycode are matching the version of the software to be installed. Obtain a proper keycode or use the proper software version.
WC1013	System type in keycode does not match the hardware type.		Browse and validate the keycode again. Obtain a proper keycode or use the proper software version.
WC1014	Keycode file corrupted.		Browse and validate the keycode again. If it does not work, try regenerating the keycode.
WC1015	Can't detect dongle, dongle missing or can't read the dongle.	Dongle is not installed (or not properly installed) on the system. Dongle is bad.	Make sure the dongle is properly installed. Replace the dongle with a good one.
WC1016	Keycode does not match dongle.	Keycode maybe invalid. Dongle maybe invalid.	Make sure the keycode is right and the dongle is right, and they match.
WC1017	Keycode file contains invalid load build cycle.	The load build cycle on the keycode is not valid. Only valid load build cycle is "MR (market release)".	Obtain a keycode with a valid load build cycle.
WC1020	Could not validate keycode. Error occurred during validation process.	Could not execute the keycode validation software.	Make sure that the kcv software is present, and with executable permission.

Error Code	Error Message	Description	Action
WC1021	Could not mount software load: Invalid mount point. Restart the server and try again.		
WC1022	Could not find a valid software load. File or media may be invalid.	Software load .nai file maybe corrupt.	Try uploading the .nai file again.
WC1023	Software load could not be copied to the deployment server.		Check whether there is enough disk space on the deployment server to copy the .nai file.
WC1024	Software Load media is not accessible. Media not present or busy.		Check whether the CD/DVD or Compact Flash is inserted properly in the drive. Check whether the CD/DVD or Compact Flash has the application software or customer database, whichever you are trying to upload.
WC1025	Could not determine hardware type of this server.	The h/w type is not in the baseOs.properties file.	Check the /admin/nortel-linuxbase-info file for the SYSTEM_HW_PLATFORM field. If it is proper, then do a system restart, otherwise seek help from Nortel.
WC1026	Failed to get Software Load information - install.xml file does not exist.	Install.xml file is missing in the load (i.e. corrupted software load)	Try uploading the software load .nai file again. Check the directory /var/opt/nortel/deployment /app_loads/<app_load>/ to see whether the install.xml file is present. Check whether the .nai file you got is of expected size.
WC1027	Failed to get Software Load information - Could not read install.xml.	Could not read install.xml file. Must be corrupted.	Try uploading the software load .nai file again. Check whether the .nai file you got is of expected size.

Error Code	Error Message	Description	Action
WC1028	Failed to access software load data file. Please try again.	Could not access the software load .nai file.	Check whether you can access this file on your PC or the CD/DVD or compact flash that you are trying to upload from. Check whether it has the right permissions.
WC1029	Software load add is already in progress.	Another user has started a software upload process.	Refresh the page. This should show the same page as the other user is getting. Wait until the other upload is done before initiating the software add.
WC1030	Software load already exists. If you would like to replace the existing load, please delete it from the table and add again.	The software load that you are trying to upload already exists on the deployment server.	As suggested, first delete the software load from the table. Then try the add again.
WC1031	Failed to create the preconfig directory for call server configuration.	Could not create the directory /var/opt/nortel/deployment/deployed/<hostname>/preconfig/cs or /var/opt/nortel/deployment/deployed/<hostname>/preconfig/em. Could be disk space issue or permission issue.	Check the disk space and permissions for the above mentioned directory.
WC1032	Unable to retrieve target server details. Please cancel and try again.		
WC1033	Maximum number (3) of software loads reached on this server. Please delete one of the loads before proceeding with an add operation.		
WC1034	Cannot delete the selected software load(s). Make sure all deployment and upgrade operations are completed before deleting a load.	Some other user maybe performing a deployment or upgrade which uses this load.	Wait till other operations are done (can check on the deployment targets page), and then retry the deletion.
WC1041	Backup file is null or the file type is invalid.	Possible causes: Backup file is empty, or the extension is not .tar.gz as expected. Severity: Minor	Browse an appropriate backup file.

Error Code	Error Message	Description	Action
WC1042	Backup file not found.		
WC1043	An I/O error occurred while uploading backup file.		
WC1044	Unexpected error occurred while uploading backup file.		
WC1045	Backup file name is invalid.	Backup filename extension is not .tar.gz as expected.	Make sure that proper backup file is being used.
WC1051	Keycode file is null or the file type is invalid.	Keycode file that was browsed is empty or the extension is not .kcd as expected.	Choose a proper keycode file that ends with .kcd.
WC1052	Keycode file not found.	Keycode file upload had some issues.	Browse and validate the keycode again. Make sure that the keycode is valid.
WC1053	An I/O error occurred while uploading keycode file.	Keycode file upload had some issues.	Browse and validate the keycode again. Make sure that the keycode is valid.
WC1054	Unexpected error occurred while uploading keycode file.	Keycode file upload had some issues.	Browse and validate the keycode again. Make sure that the keycode is valid.
WC1063	An I/O error occurred while uploading customer database file.	Customer database file upload had some issues.	Browse and upload the customer database again. Make sure that the customer database is valid.
WC1064	Unexpected error occurred while uploading customer database file.	Customer database file upload had some issues.	Browse and upload the customer database again. Make sure that the customer database is valid.
WC1065	An I/O error occurred while extracting customer database archive file.	Customer database file upload had some issues.	Browse and upload the customer database again. Make sure that the customer database is valid.

Error Code	Error Message	Description	Action
WC1066	Failed to extract customer database from the archive file.	Customer database file upload had some issues.	Browse and upload the customer database again. Make sure that the customer database is valid.
WC1071	Software version delete failed for one/more selected loads.		
WC1091	Error occurred while backing up target.	Could not make the system call to execute the base commands appBackup.	Check whether the appBackup script exists on the server, with executable permission.
WC1092	Error occurred while restoring target.	Could not make the system call to execute the base commands appRestore. System call got interrupted for some reason.	Check whether the appRestore script exists on the server, with executable permission.
WC1093	Invalid IPv4 format.		
WC1094	Maximum number of backups reached. Please delete any of the existing backups for the same target using Backups management.	Only 3 backups are allowed to be stored on the deployment server, per target.	
WC1095	Failed to delete one/more backups.		Try refreshing the page, and try the delete again.
WC1096	Maximum number (3) of simultaneous restores reached.	Only 3 restore operations are allowed simultaneously.	Wait for sometime, and then try the restore operation.
WC1097	Maximum number (3) of simultaneous backups reached.	Only 3 backup operations are allowed simultaneously.	Wait for sometime, and then try the backup operation.
WC1098	Selected file does not match required format(.tar.gz).		
WC1099	Server path cannot be empty.		
WC1100	Required fields cannot be empty.		
WC1101	Server IP address cannot be empty.		
WC1102	Username cannot be empty.		

Error Code	Error Message	Description	Action
WC1103	Password cannot be empty.		
WC1104	Not enough disk space available for backup. Please ensure that the /var partition has at least 20% space available, and try the backup again.		
WC1105	Could not validate size of the disk. Please try again.		
WC1111	Note - An automatic status update was not available. Click the refresh link (above, right) to verify current status.	Could not retrieve information from UCM regarding the targets. This is a temporary problem due to concurrent access and race conditions.	As suggested, refresh the page again.
WC1200	Failed to delete elements on this target. Please manually delete the elements from UCM elements table.	After undeployment, DM deletes the associated elements (CS1000, NRSM, Subscriber manager depending on what was deployed). For some reason, it couldn't delete these elements.	Go into UCM elements page, and find the corresponding elements and delete them.
WC2001	Call server ELAN IP cannot be empty or invalid IPv4 format.		
WC2003	Call server tape ID cannot be empty.		Check the tape ID on the call server's dongle.
WC2004	Call server tape ID must be alphanumeric		Check the tape ID on the call server's dongle. It cannot have any special characters.
WC2005	MAC address format is invalid.		

Error Code	Error Message	Description	Action
WC3000	The target is performing an operation launched from another deployment server. Please try again later.	If you are performing a operation centrally, then it could be that some other user is performing some operation locally on the box and vice versa.	Make sure that no one else is performing any operation on the box from anywhere else.
WCFG	Can not find install.xml file.	Corrupted .nai file.	Upload the software load again.

Index

Nortel Communication Server 1000

Linux Platform Base and Applications Installation and Commissioning

Release: 6.0
Publication: NN43001-315
Document revision: 03.13
Document release date: 23 March 2010

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

www.nortel.com