Nortel Communication Server 1000

Linux Platform Base and Applications Installation and Commissioning

NN43001-315

Document status: Standard
Document version: 01.01
Document date: 30 May 2007

Sourced in Canada.

Revision history

May 30, 2007
Standard 01.01. This document is issued to support Nortel Communication Server 1000 Release 5.0.

Contents

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.

New in this Release

WARNING
Do not contact Red Hat for technical support on your Nortel version of the Linux base operating system. If technical support is required for the Nortel version of the Linux base operating system, contact Nortel technical support through your regular channels.

This document is a new NTP created to support Nortel Communication Server 1000 (CS1000) Release 5.00.

Subject

This document describes the installation and configuration of Linux base Operating System on the HP DL320 G4 and IBM x306m COTS servers. The Linux base server platform supports the following Nortel CS 1000 application configurations:

- Primary Security Service and Network Routing Service
- Backup Security Service and Network Routing Service
- Network Routing Service
- Primary Security Service and CS 1000 Element Manager
- Backup Security Service and CS 1000 Element Manager
- CS 1000 Element Manager

Introduction

WARNING
Do not contact Red Hat for technical support on your Nortel version of the Linux base operating system. If technical support is required for the Nortel version of the Linux base operating system, contact Nortel technical support through your regular channels.

To view licensing information, see Appendix "Passthrough end user license agreement" (page 69).

Linux base operating system overview

The Communication Server 1000 (CS 1000) Linux base system provides a Linux server platform for applications on a Consumer off the shelf (COTS) Pentium server. The platform can support the new Session Initiation Protocol Network Redirect Server (SIP NRS) and Enterprise Common Manager (ECM) framework.

This system is supported on the HP DL320 G4 1u Pentium server and the IBM x306m 1u Pentium 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)

Install the Linux base operating system

Install the Linux base software on the IBM x306m and HP DL320 G4 servers

Nortel Communication Server 1000 (CS 1000) Linux base introduces a two-stage installation procedure. The operating system is installed, then the applications. In the future, you will be able to upgrade the current application configuration using the existing operating system. You can reinstall an application configuration using the existing operating system.

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

Use the following procedure to install the Linux base software.

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

- Gather the following necessary customer information:
  - ELAN IP address
  - ELAN gateway IP address
  - ELAN netmask
  - Fully Qualified Domain Name (FQDN). The host name of the FQDN is associated with the TLAN.

    Note: An FQDN consists of a host name and a domain name, and includes a top-level domain name. Using www.nortel.com as an example, www is the host name, nortel is the second-level domain name, and .com is the top-level domain name. The FQDN must contain at least two dots.

  - TLAN IP address
  - TLAN gateway IP address

— TLAN netmask

— Timezone

— 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 1: The ELAN and TLAN network interfaces for the HP DL320 G4 server can be seen at Figure 59 "HP DL320 rear view" (page 74). The ELAN and TLAN network interfaces for the IBM x306m server can be seen at Figure 66 "IBM X306m rear view" (page 80).

Note 2: 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. Refer to the appropriate application NTP for more information.

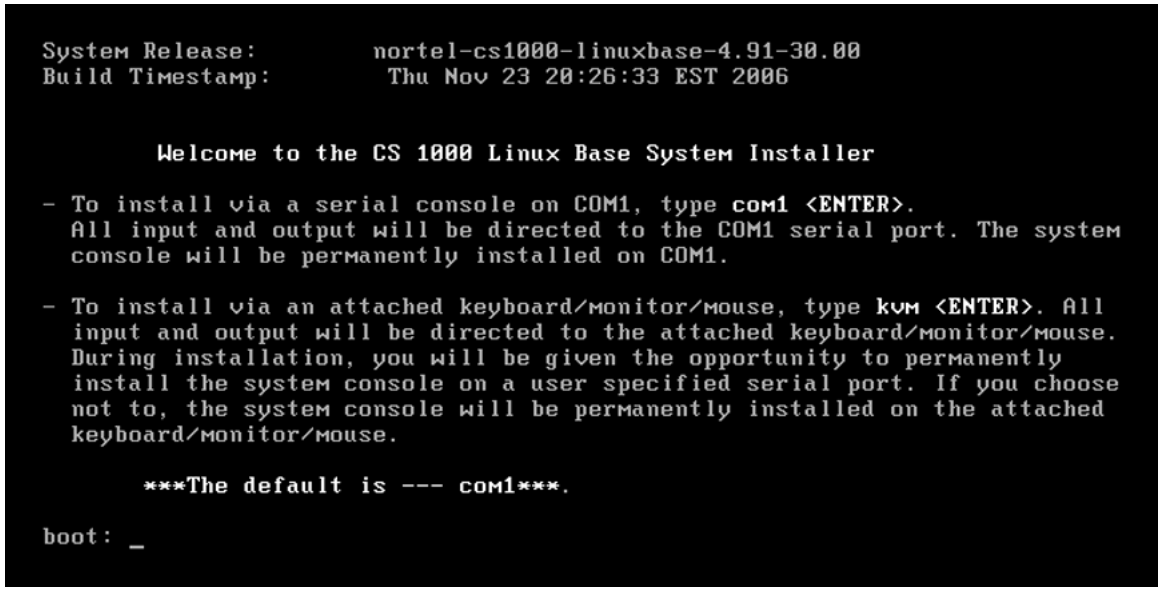
Installing the Linux base on the IBM x306m server or HP DL320 G4

Step	Action
1	Connect to the COTS server using a serial console or keyboard, video monitor, and mouse (kvm).

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

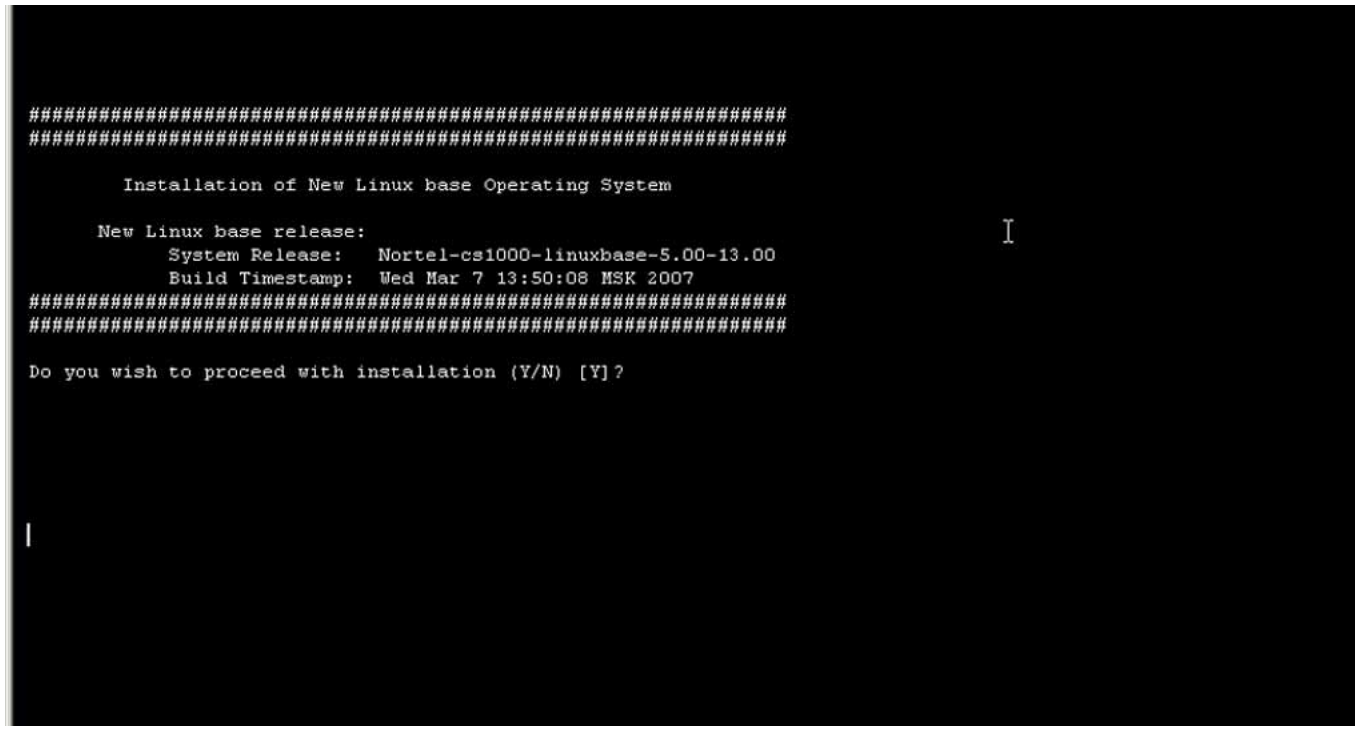
2	Insert the Linux base bootable CD-ROM in the CD-ROM tray.
3	Reboot the server.
4	Choose the method of installation as shown in Figure 1 "CS 1000 Linux base system installer" (page 15). • To install using a serial console on COM1, type **com1** at the boot prompt. • To install using an attached keyboard, video monitor, and mouse, type **kvm** at the boot prompt. ***Note:*** It is not required to attach a keyboard, video monitor and mouse (KVM) to view output. A console based installation will also provide output.

Figure 1
CS 1000 Linux base system installer



5 Type **Y** and press **Enter** as shown in Figure 2 "CS 1000 Linux base system installer" (page 15).

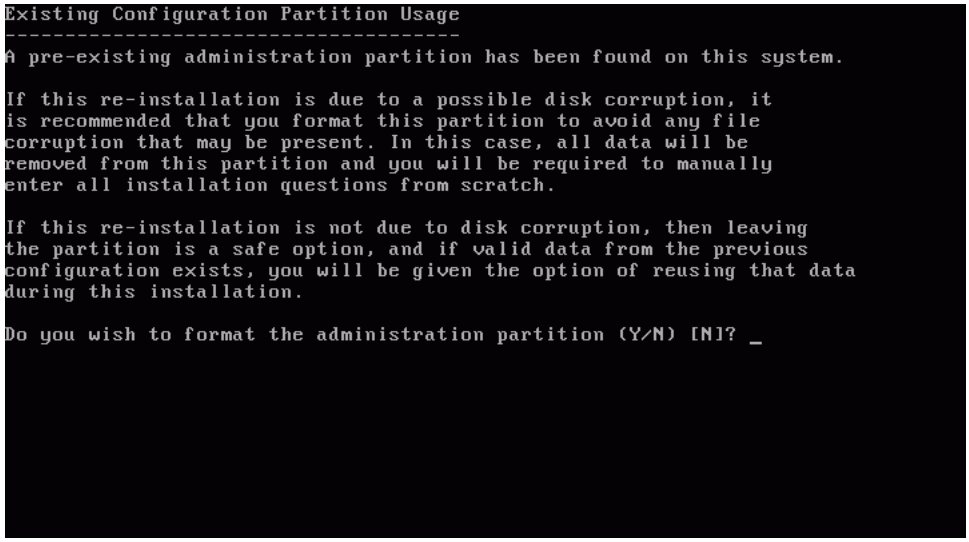
Figure 2
CS 1000 Linux base system installer



If the software was previously installed on the server, the system prompts you to format the administrative partition.

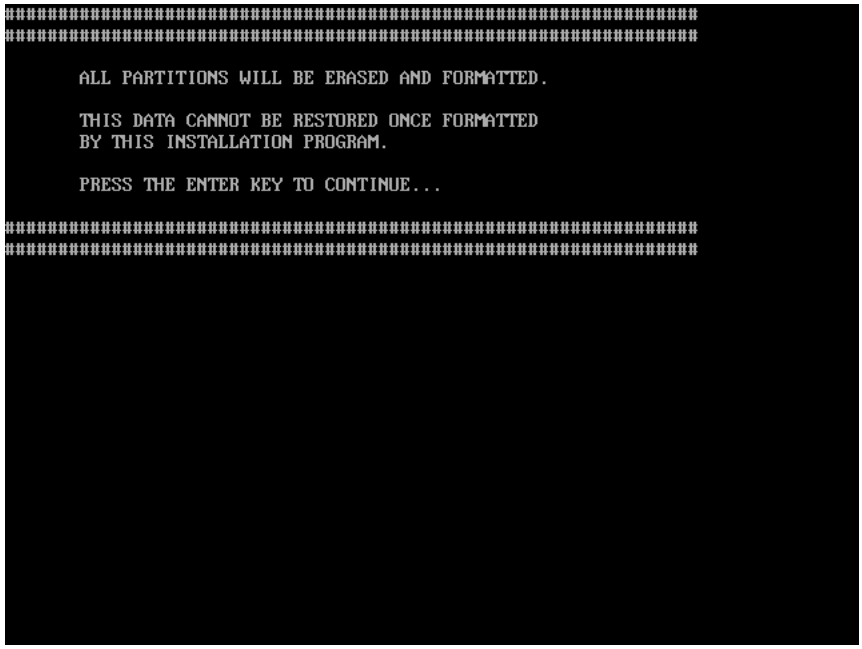
6 Type **Y** for yes or **N** for no as required and press **Enter**, as shown in Figure 3 "Existing configuration partition window" (page 16).

Figure 3
Existing configuration partition window



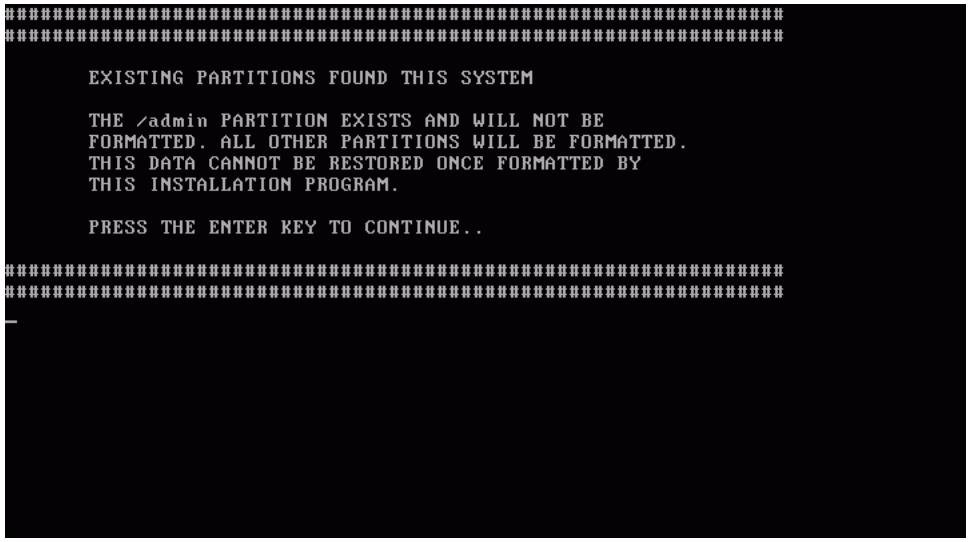
If you selected **Y** , the partitions are configured as shown in Figure 4 "Format all partitions" (page 16). Press **Enter** to continue.

Figure 4
Format all partitions



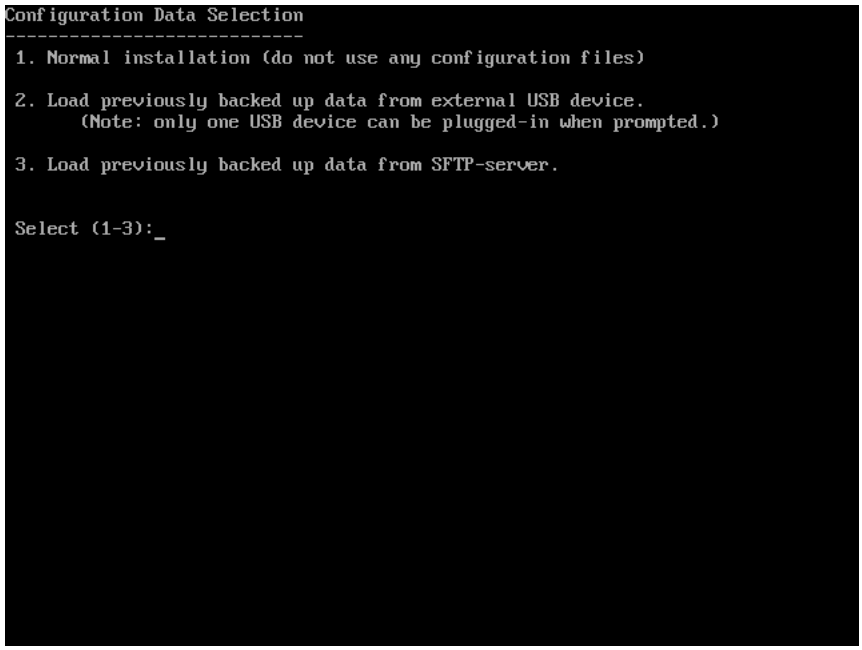
If you selected **N** , the partitions are configured as shown in Figure 5 "Existing partition not formatted" (page 17). Press **Enter** to continue.

Figure 5
Existing partition not formatted



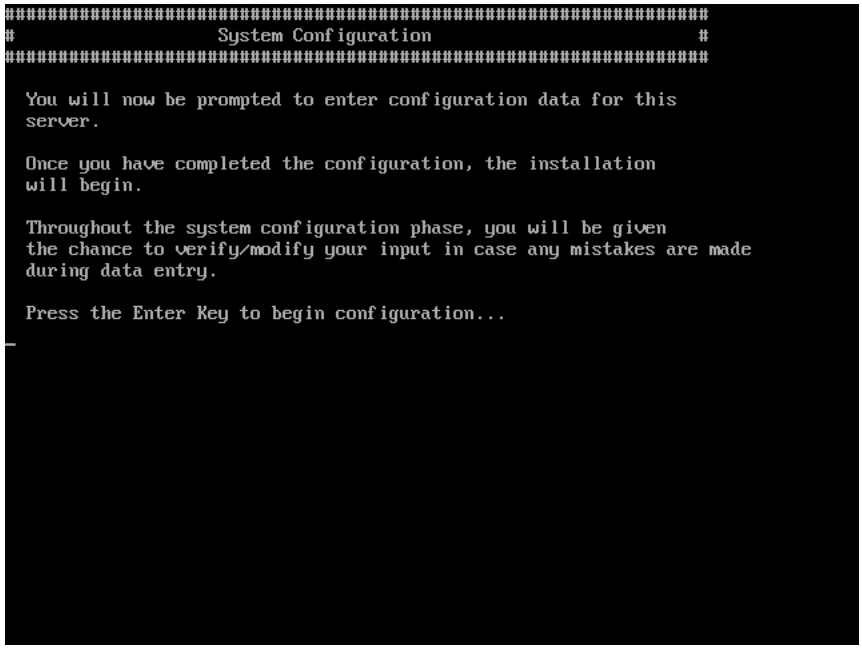
7 At the prompt, select the type of configuration data you wish to use. Type **1** for Normal installation and press **Enter**, and then press **Enter** again when prompted, as shown in Configuration data selection window.

Figure 6
Configuration data selection window



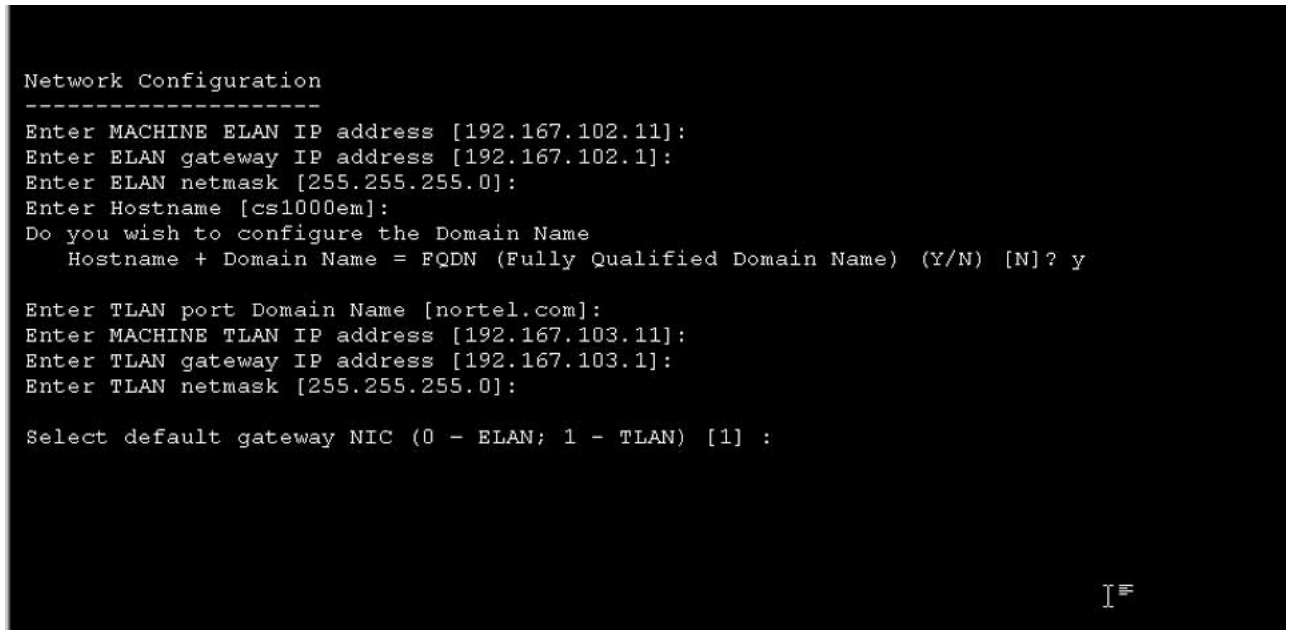
8 The **System Configuration** screen appears as shown in Figure 7 "System configuration window" (page 18). Press **Enter** to continue.

Figure 7
System configuration window



9 When prompted, in the **Network Configuration** screen, enter the customer information for **ELAN IP address**, **ELAN gateway**, **ELAN Netmask**, **Hostname**, **Fully Qualified Domain Name (FQDN)**, **Machine TLAN IP address**, **TLAN gateway**, **default gateway**, and **TLAN Netmask** , as shown in Figure 8 "Network configuration window" (page 19).

Figure 8
Network configuration window



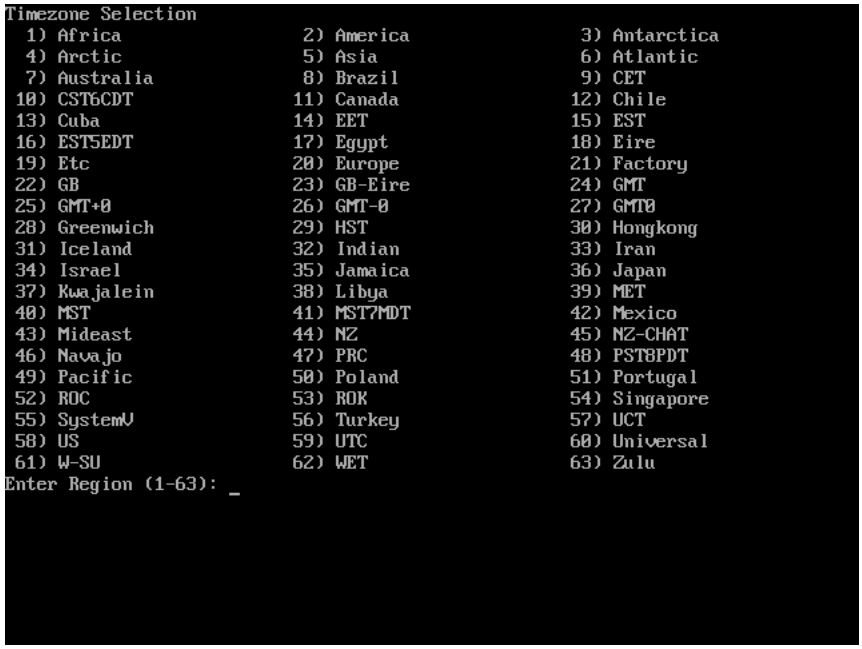
Note 1: The ELAN and TLAN network interfaces for the HP DL320 G4 server can be seen at Figure 59 "HP DL320 rear view" (page 74). The ELAN and TLAN network interfaces for the IBM x306m server can be seen at Figure 66 "IBM X306m rear view" (page 80).

Note 2: 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. Refer to the appropriate application NTP for more information.

Press **Enter** to continue. The **Time zone selection** screen appears as shown in Figure 9 "Time zone selection window" (page 20).

10 In the **Timezone Selection** screen type the appropriate region number at the prompt and then press **Enter**.

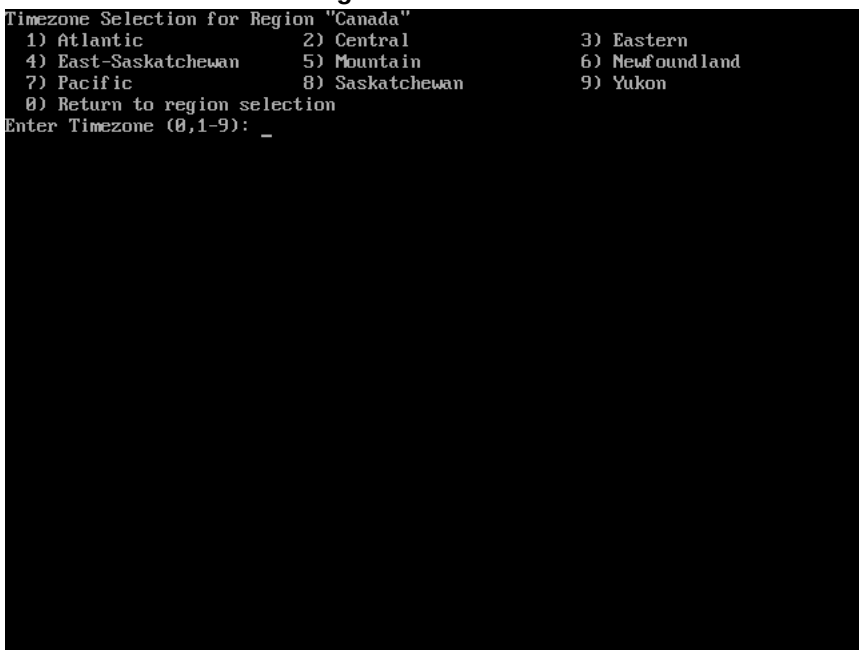
Figure 9
Time zone selection window



The **Time zone selection for region**screen appears as shown in Figure 10 "Time zone selection for region window" (page 21).

11 At the prompt, in the **Timezone Selection for Region** screen, type the appropriate time zone number and then press **Enter**.

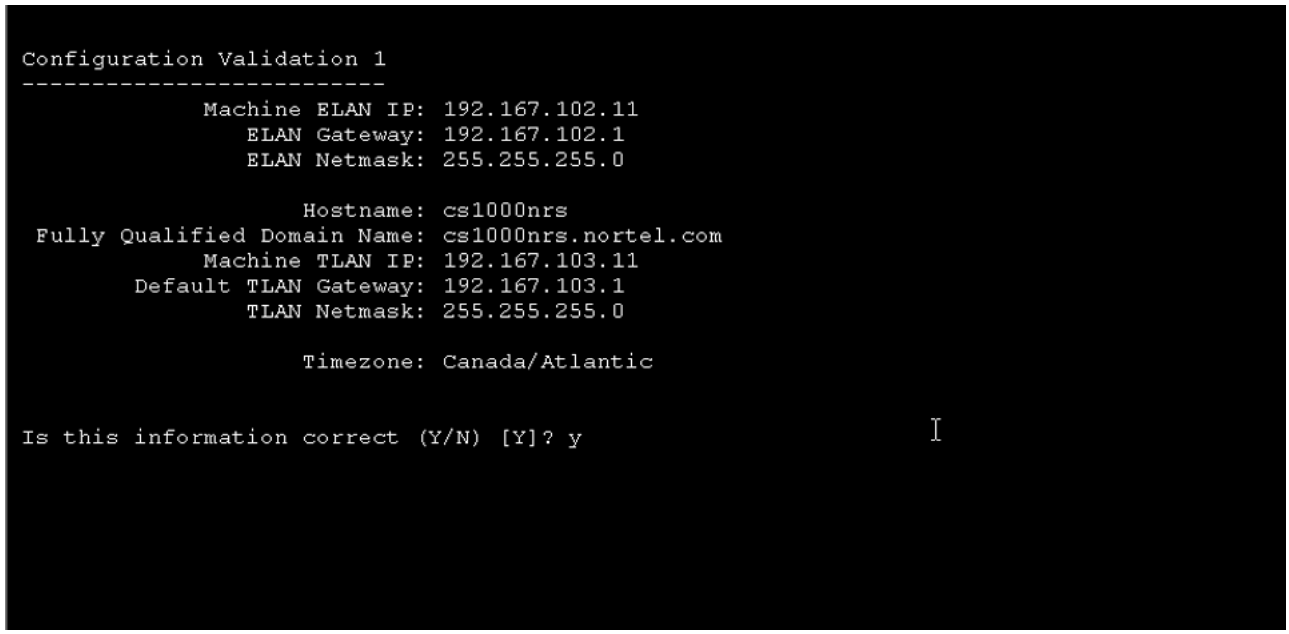
Figure 10
Time zone selection for region window



12 In the **Configuration Validation 1** screen, type **Y** for yes or **N** for no, and then press **Enter** to confirm the customer information for **Machine ELAN IP**, **ELAN Gateway**, **ELAN Netmask**, **Hostname**, **FQDN, Machine TLAN IP**, **Default TLAN Gateway**, **TLAN Netmask** and **Timezone**, as shown in Figure 11 "Configuration validation 1 window" (page 22).

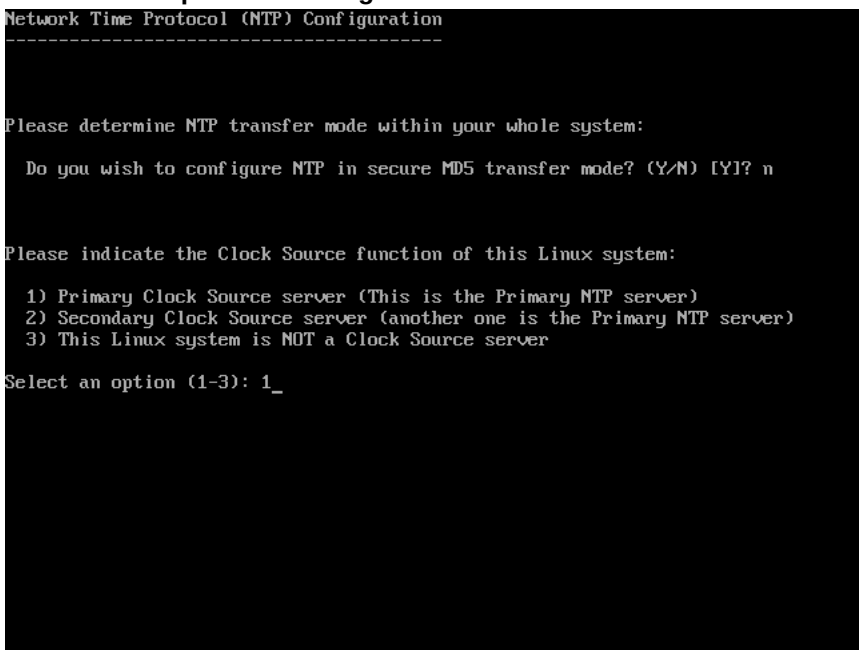
If you select **N**, edit the information as required and repeat step 10.

Figure 11
Configuration validation 1 window



13 In the **Network Time Protocol (NTP) Configuration** screen, type **Y** or **N** to choose the **NTP** transfer mode for the system. Type **1**, **2**, or **3** and then press **Enter** to indicate the clock source function of the Linux system, as shown in Figure 12 "Network time protocol configuration window" (page 23).

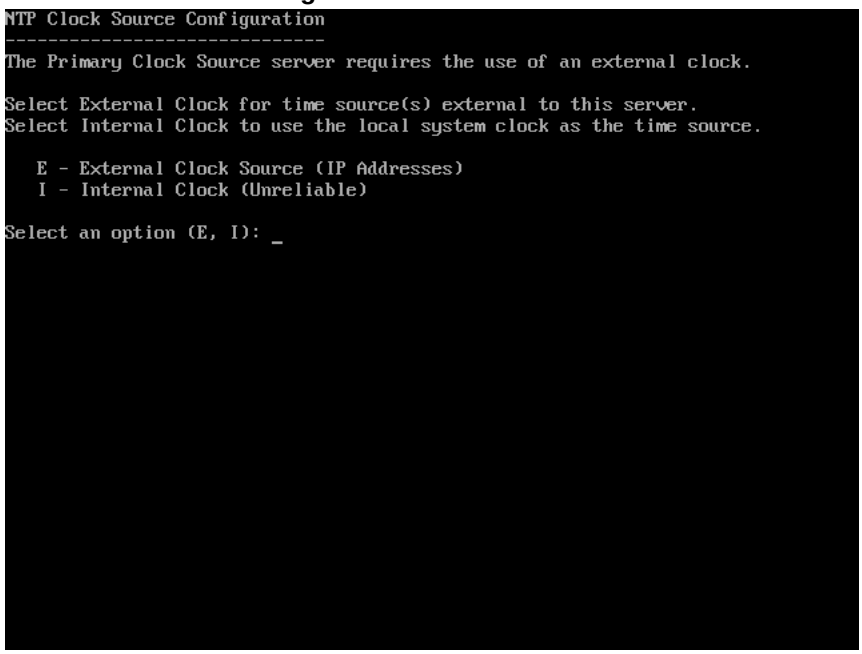
Figure 12
Network time protocol configuration window



14 In the **NTP clock source configuration**screen type **E** for an external clock source, or **I** for an internal clock source, as shown in Figure 13 "NTP clock source configuration window" (page 24).

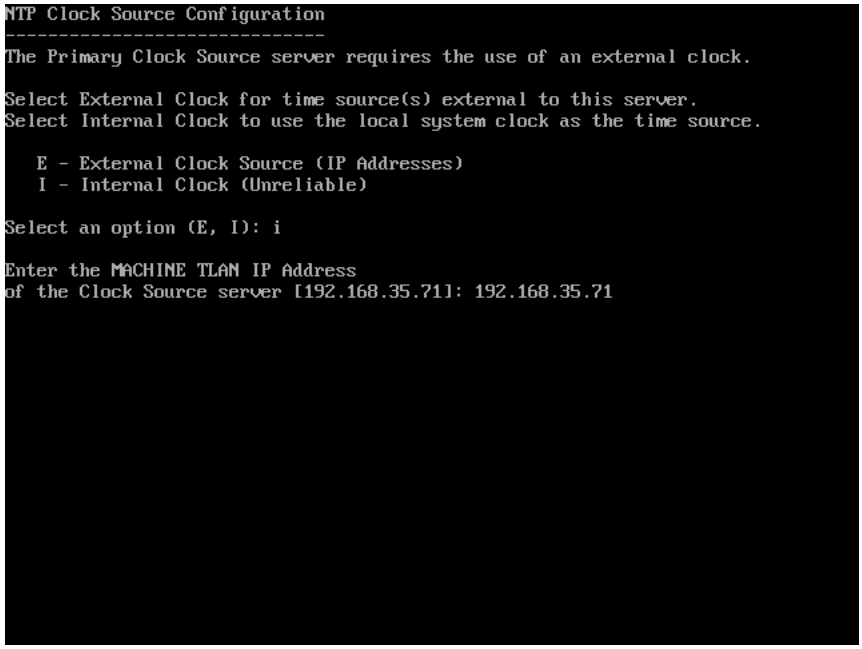
Press **Enter** to continue.

Figure 13
NTP clock source configuration window



15 At the prompt, type the machine TLAN IP address of the clock source server as shown in Figure 14 "NTP clock source configuration window" (page 24).

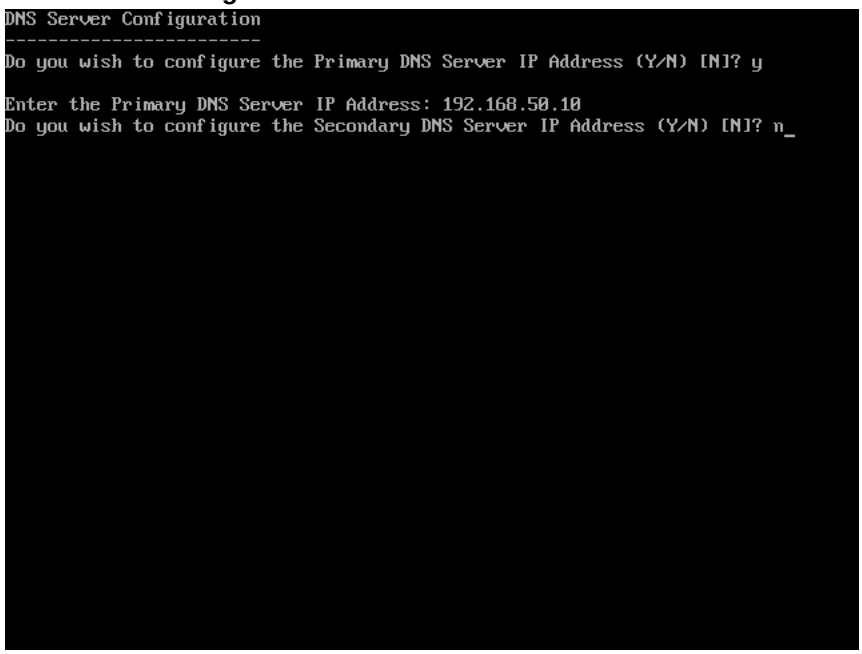
Figure 14
NTP clock source configuration window



Press **Enter** to continue.

16 At the prompt, configure the primary DNS server IP address as shown in Figure 15 "DNS server configuration window" (page 25).

Figure 15
DNS server configuration window

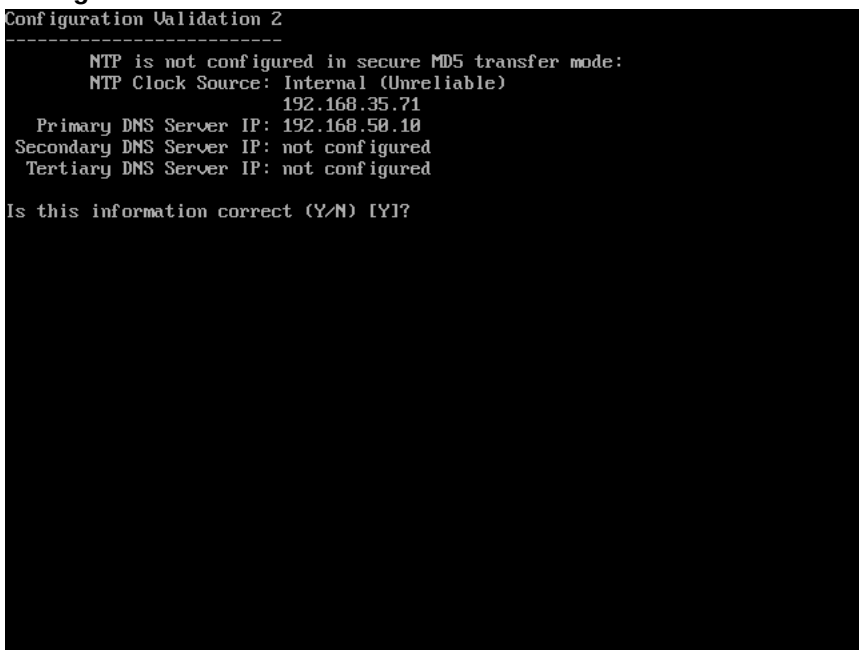


Type **Y** to configure and **N** if you do not wish to configure and then press **Enter**. If you selected **Y** , enter the IP address for the Primary DNS server at the prompt. The default for the Primary DNS server is **N**.

17 In the **Configuration Validation 2** screen, type **Y** if the information is correct and press **Enter**, as shown in n the Figure 16 "Configuration Validation 2 window" (page 26). If the information is incorrect, type **N**, make the required changes, and then press **Enter**.

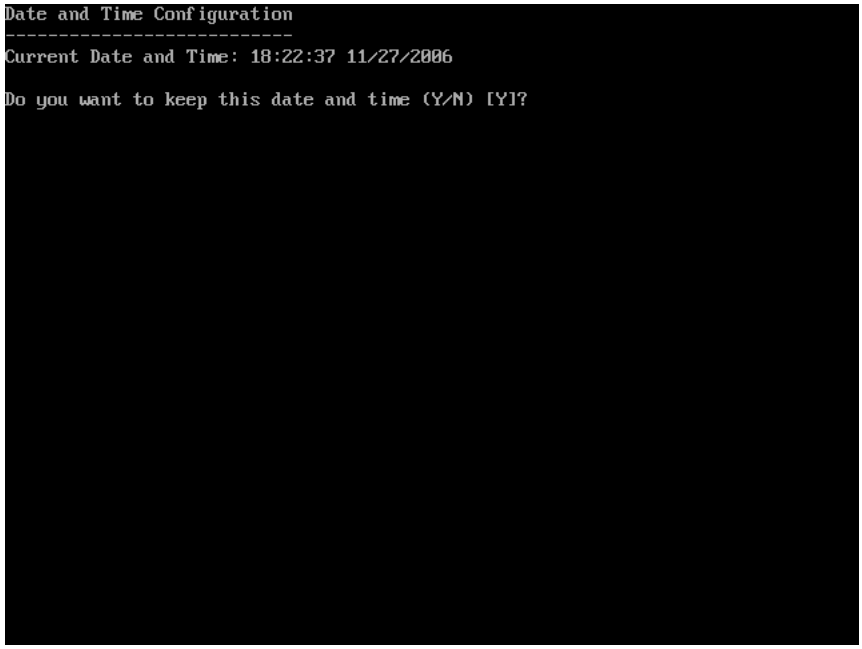
The Configuration Validation 2 screen appears with the correct information. Press **Enter** to continue.

Figure 16
Configuration Validation 2 window



18 In the **Date and Time Configuration** screen, configure the date and time, as shown in Figure 17 "Date and Time Configuration window" (page 26).

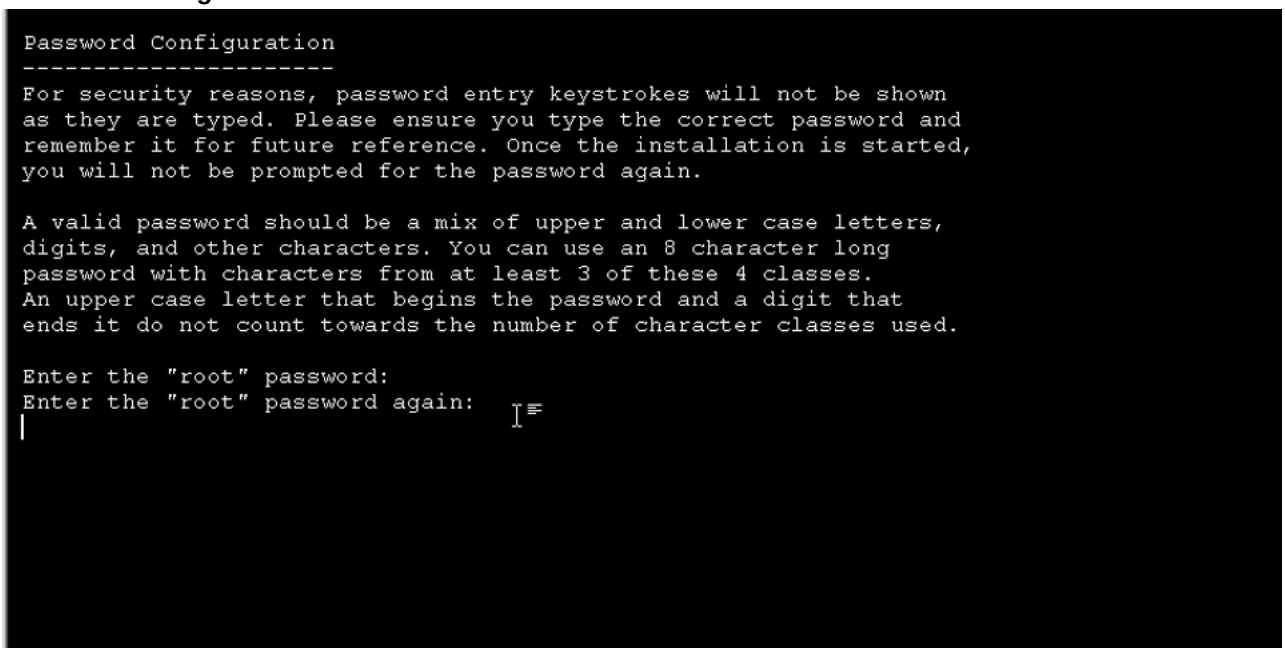
Figure 17
Date and Time Configuration window



Type **Y** to keep the date and time, and then press **Enter**. To change the date and time, press **N**, make the required changes, and press **Enter**. The Date and Time Configuration screen appears with the new date and time; press **Enter** to continue.

19 In the **Password Configuration** screen, at the prompt, enter the root password, as shown inFigure 18 "Password configuration window" (page 27). The prompt reappears.

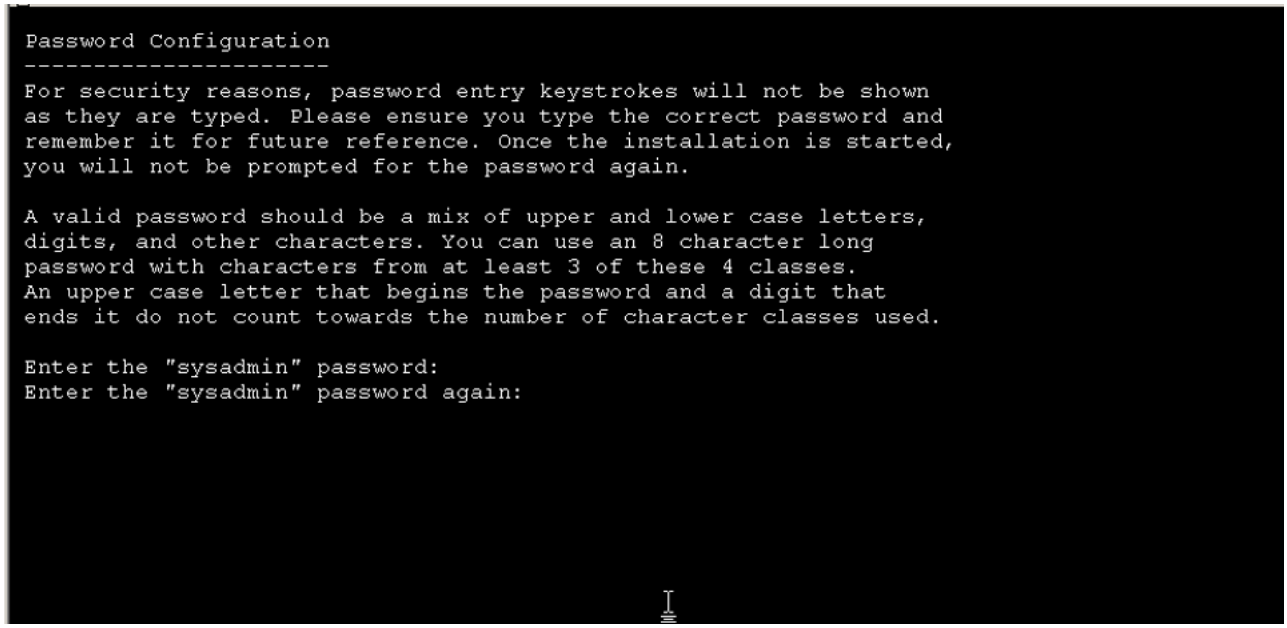
Figure 18
Password configuration window



Note: Guidelines for the creation and use of passwords are shown at "Passwords" (page 66).

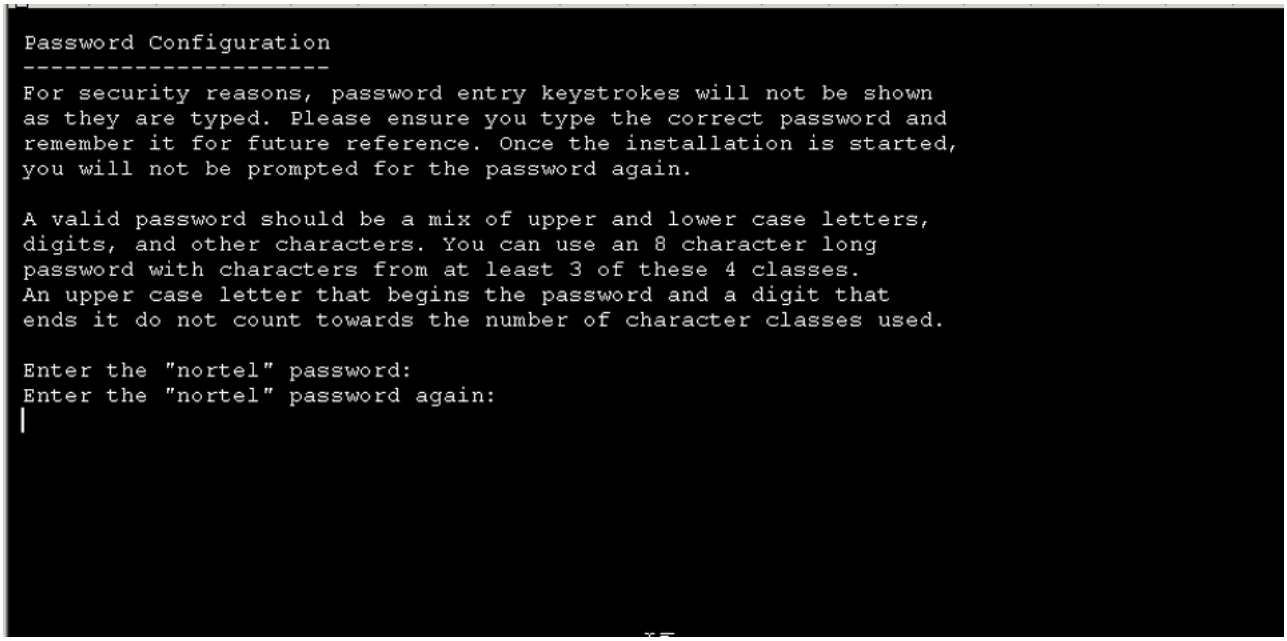
20 Enter the sysadmin password as shown in .Figure 19 "Password configuration window" (page 28). The prompt appears a third time.

Figure 19
Password configuration window



21 Enter the nortel password as shown in Figure 20 "Password configuration window" (page 28). Password policies and creation guidelines can be viewed at "Passwords" (page 66)

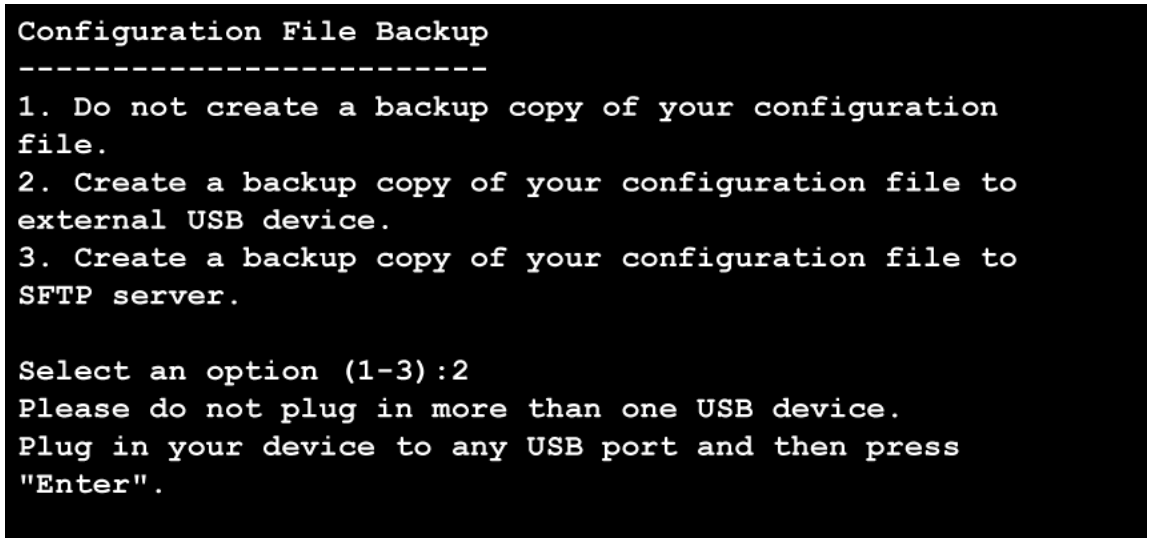
Figure 20
Password configuration window



The prompt appears until you enter all the required passwords. Press **Enter** to continue. The **Configuration File Backup** appears as shown in Figure 21 "Configuration File Backup window" (page 29).

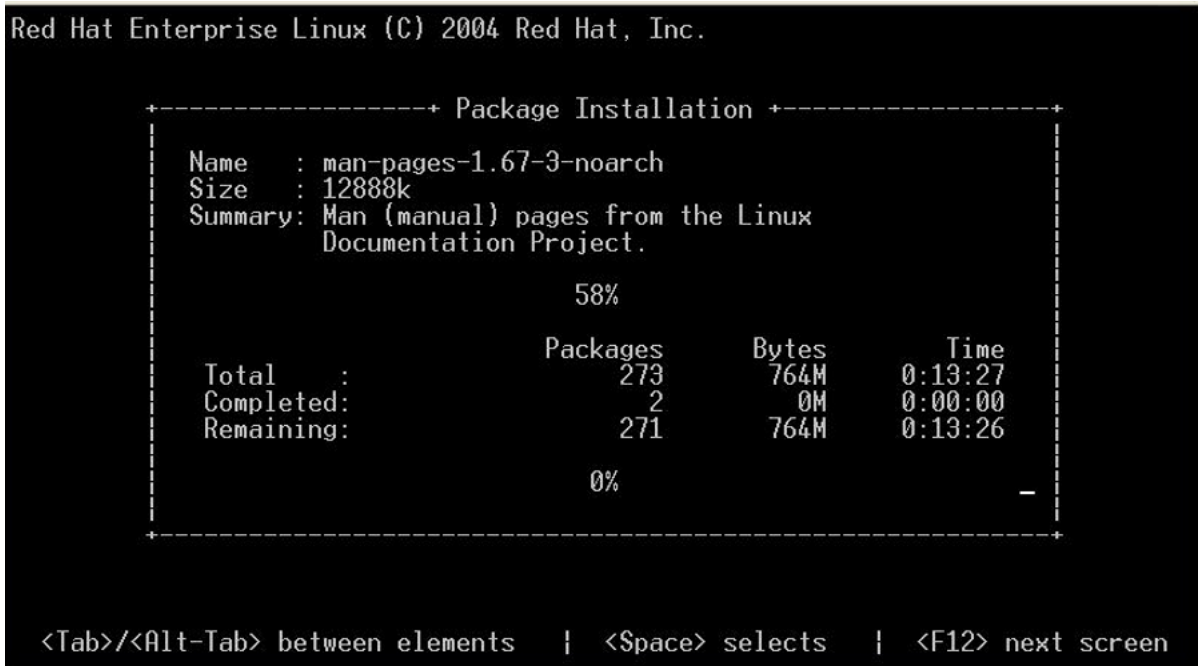
22 From the **Configuration File Backup** screen, select an option to back up the configuration data.

Figure 21
Configuration File Backup window



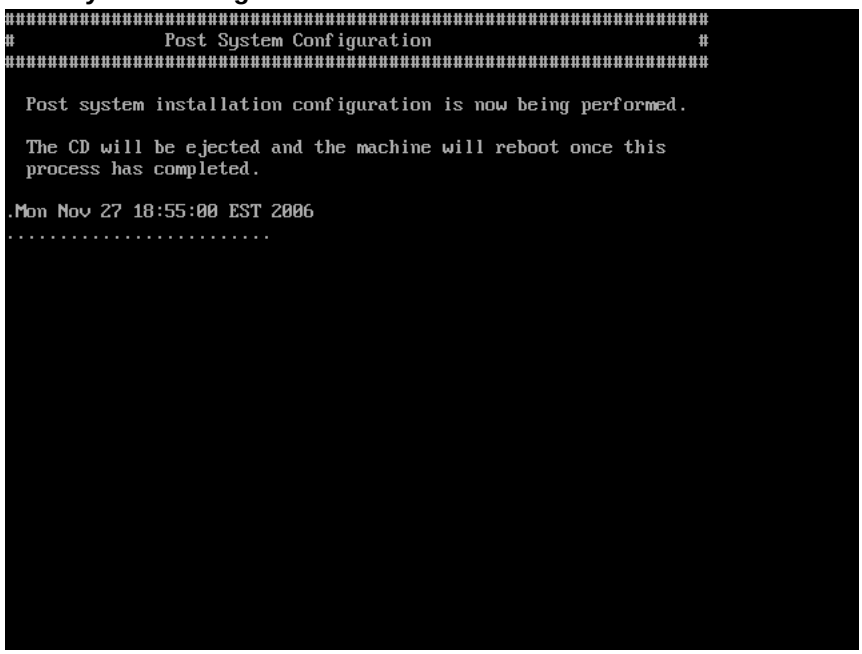
After you back up the configuration data, the **Package Installation** screen appears, as shown in Figure 22 "Package Installation window" (page 30).

Figure 22
Package Installation window



The **Post System Configuration** screen appears, as shown in Figure 23 "Post system configuration window" (page 31). The system automatically reboots as a Linux server.

Figure 23
Post system configuration window



—End—

Installation and configuration of applications on Linux base

This section provides information about the following tasks that you must complete to install and configure applications after you install the Linux base.

- configure the Primary Security Service (PSS) and Backup Security Service (BSS)
- configure the Network Routing Service (NRS) and the Element Manager (EM) applications
- configure the system account passwords for the Primary Security Service and member server, and the Backup Security Services and member server

Prerequisites to install and configure applications

Users must install the Communication Server 1000 (CS 1000) Linux base software on the HP DL320 G4 or the IBM x306m servers before they can install the applications. The Linux base software contains the Linux operating system, the framework software, and the required third-party software such as the Web server and Java runtime environment (JRE).

WARNING
Nortel Linux applications are supported only on Nortel CS 1000 Linux base. Nortel Linux applications will not function on other versions of Linux.

Install the CS 1000 applications

Use the following procedures to run the application CD-ROMs and install the applications. There is a CD for NRS applications that contains 3 application configurations and a CD for Element Manager applications (MGMT CD) that contains three application configurations.

The NRS CD contains the following configuration options:

- Primary Security Service and Network Routing Service
- Backup Security Service and Network Routing Service
- Network Routing Service

The MGMT CD contains the following configuration options:

- Primary Security Service and CS 1000 Element Manager
- Backup Security Service and CS 1000 Element Manager
- CS 1000 Element Manager

Note: The Primary and Backup Security Service can be installed with either NRS or EM. The NRS server will usually have a heavier load than the EM server. To optimize the servers' load balance, Nortel recommends that, if both EM on Linux and NRS Manager on Linux are installed, the Primary Security Service be installed with EM and the Backup Security Service be installed with the Primary NRS server. In this case the Secondary NRS will be a security client of the Primary and Backup Security servers.
If EM on Linux is not being installed, Nortel recommends that the Primary Security Service be installed with the Primary NRS server and the Backup Security Service be installed with the Secondary NRS server.

At first logon to the Enterprise Common Manager (ECM) framework, change the password. Refer to Network Routing Service Installation and Commissioning (NN43001-564) for NRS password guidelines; for EM guidelines refer to Element Manager System Reference - Administration (NN43001-632).

If a password does not meet the policy requirements, the system rejects it.

For the following procedures, installation initiates configuration of the solid data base.

Install the NRS applications

Use this procedure to run the application CD-ROM when the reboot is complete for the Linux base install.

Install the Primary Security Service and Network Routing Service

Step	Action
1	Log on to the server using the nortel account.
2	Insert the NRS CD-ROM in the CD-ROM tray.

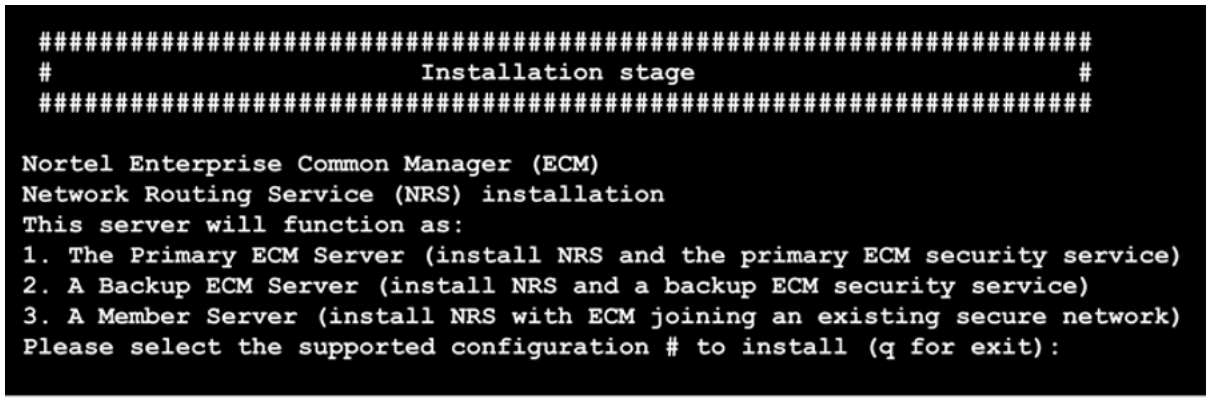
3 Enter the command **appinstall**

4 At the prompt, enter the root account password.
The system then prompts you to check the media.

5 Enter **Y** to check the media, or **N** to proceed without checking the media, and press **Enter**.

6 The **Application installation** screen appears, as shown in Figure 24 "Application Installation window" (page 35). From the **Application installation** window select 1 to install the Primary Security Service with NRS. The appropriate packages will be installed to the hard drive.

Figure 24
Application Installation window

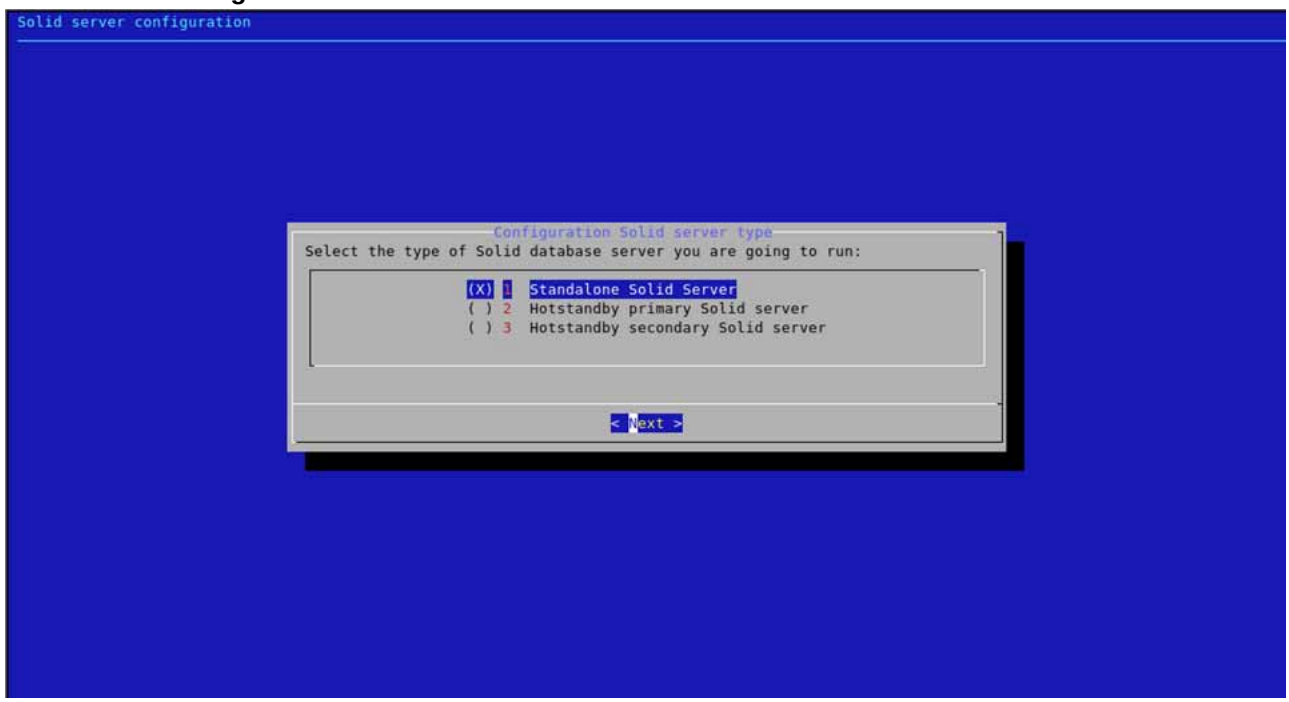


7 The Solid server window appears, as shown in Figure 25 "Solid server configuration window" (page 36). Press **Enter** to continue.

Figure 25
Solid server configuration window

8 In the Solid server configuration screen, use the arrow keys to navigate. Press the space bar to select the Solid server to install, as shown in Figure 26 "Solid server configuration window" (page 37).

Figure 26
Solid server configuration window

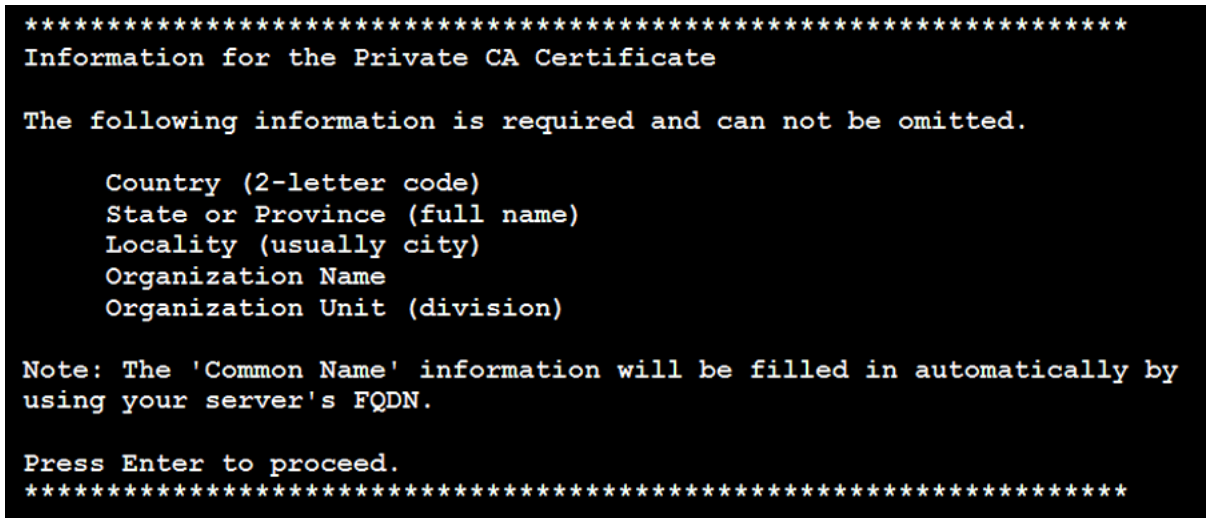


Press **Enter** to continue.

9 The Solid server configuration confirmation screen appears. Use the arrow keys to confirm the server selection by selecting **Yes**, or return to the Solid server configuration window by selecting **No**. Press **Enter** to continue.

10 The Private CA certificate window appears as shown in Figure 27 "Private CA certificate window" (page 38). At the prompts, enter the **Country**, **State or Province**, **Location**, **Organization Name** and **Organization Unit** and press **Enter** to continue.

Figure 27
Private CA certificate window



11 The **Private CA Certificate confirmation window** appears as shown in Figure 28 "Private CA Certificate confirmation window" (page 38). Verify that the common name information is correct. Type **yes** if correct or **no** if incorrect, and then press **Enter**. If you entered yes, the installation finishes and the system creates the CA certificate, as shown in Figure 29 "Making a Private CA certificate window" (page 39). If you selected no, edit the information as required and repeat the step.

Figure 28
Private CA Certificate confirmation window

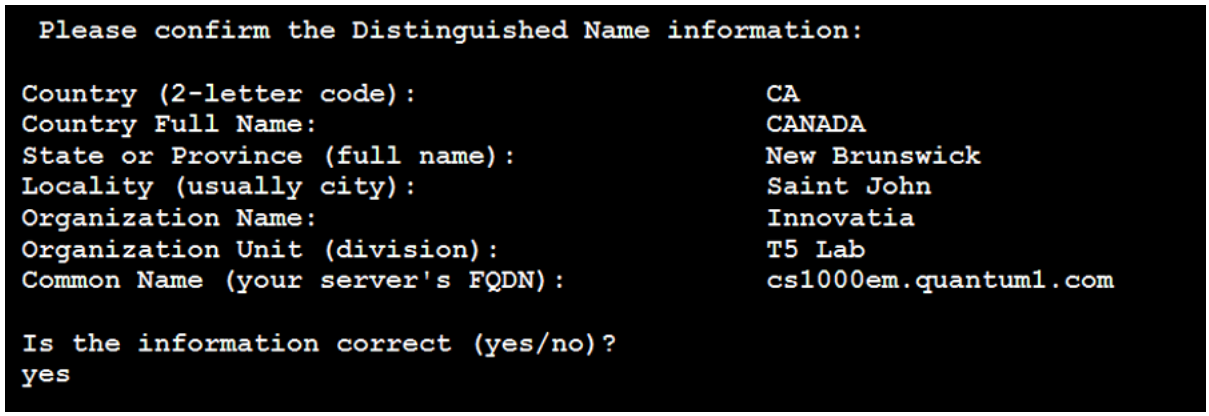
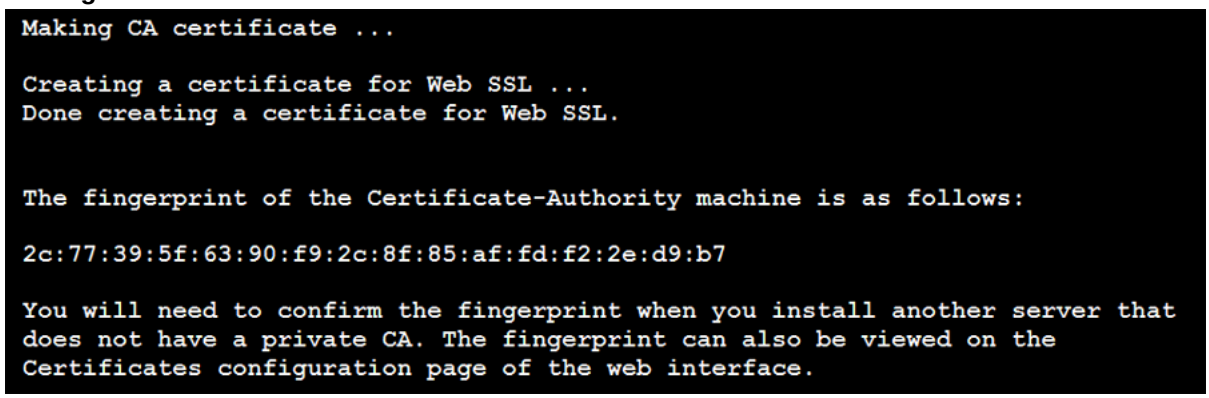


Figure 29
Making a Private CA certificate window



The installation will then complete. This will take approximately 30 minutes. When completed the disk will be ejected automatically from the drive and a summary of the installation will be shown.

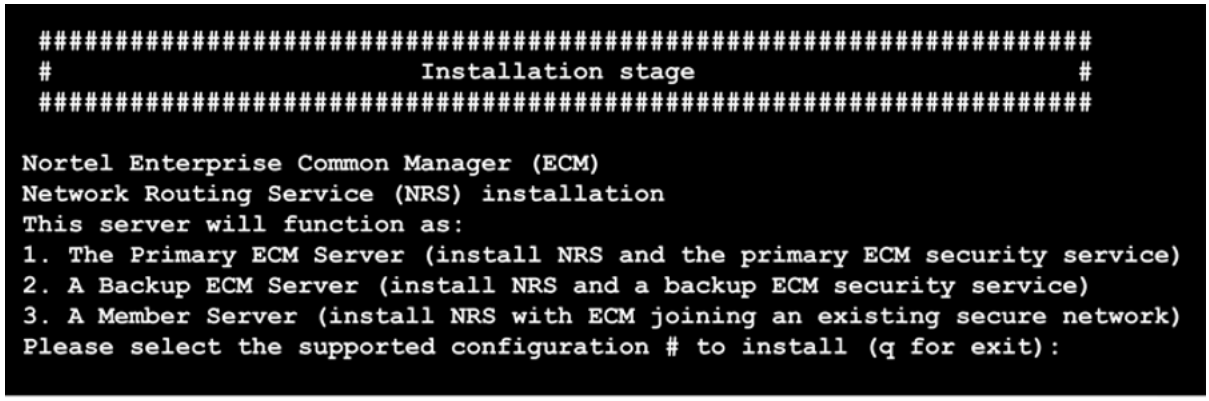
For detailed information on NRS, refer to *Network Routing Service Installation and Commissioning (NN43001-564)*.

—End—

Install the Backup Security Service and Network Routing Service

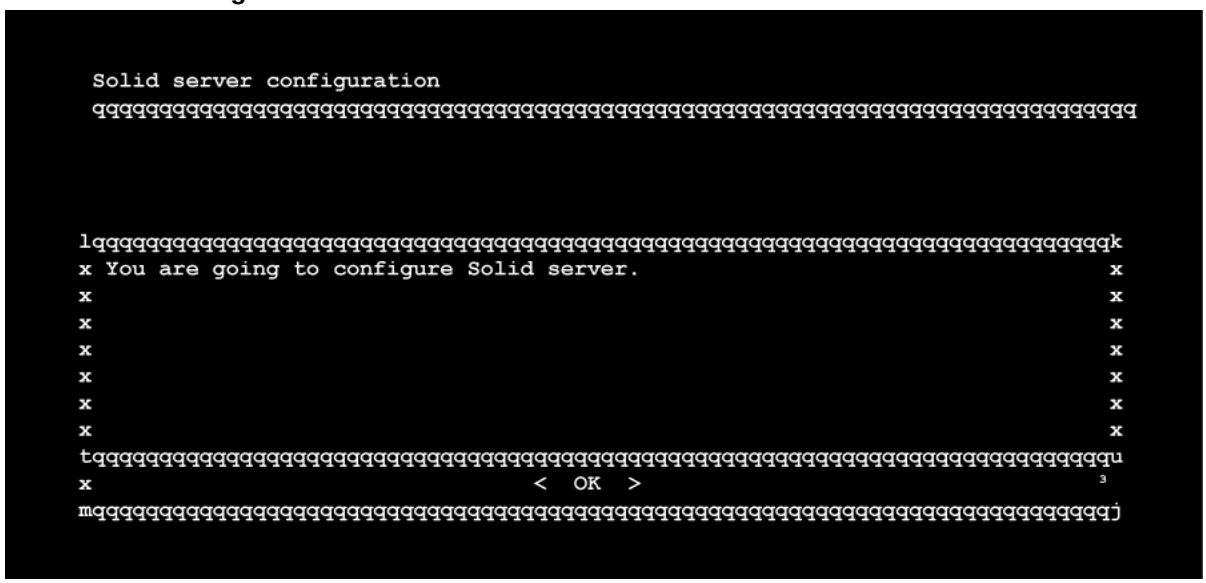
Step	Action
1	Log on to the server using the nortel account.
2	Insert the NRS CD-ROM in the CD-ROM tray.
3	Enter the command **`appinstall`**
4	At the prompt, enter the root account password. The system then prompts you to check the media.
5	Enter **Y** to check the media, or **N** to proceed without checking the media, and press **Enter**.
6	The **Application installation** screen appears, as shown in Figure 30 "Application Installation window" (page 40). From the **Application installation** window select 2 to install the Backup Security Service with NRS. The appropriate packages will be installed to the hard drive.

Figure 30
Application Installation window



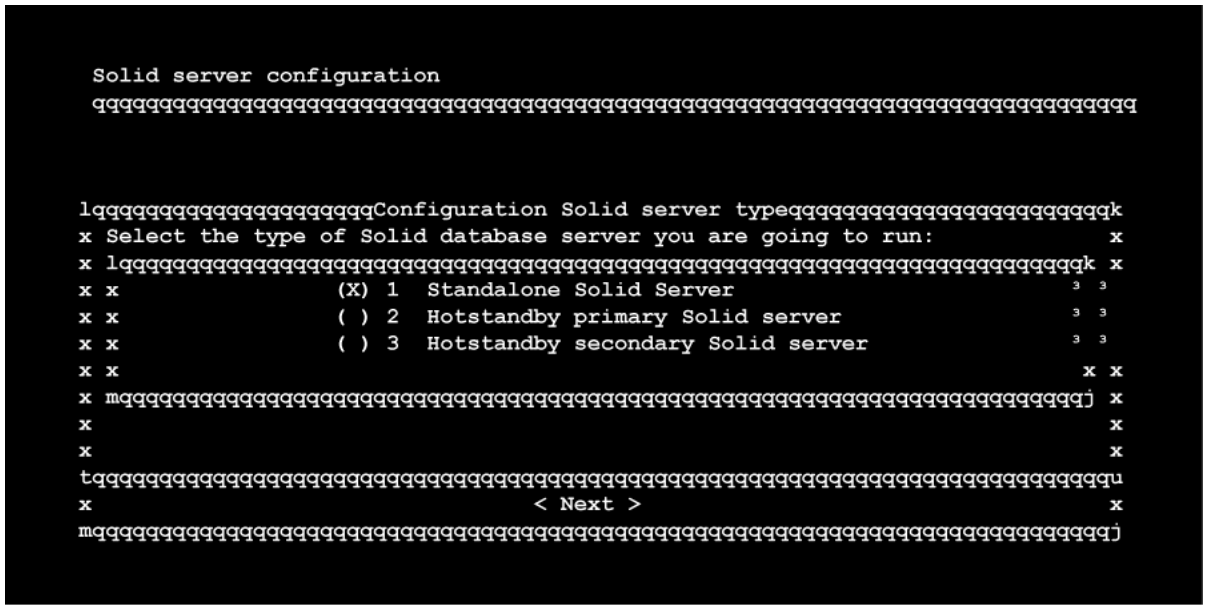
7 The Solid server window appears, as shown in Figure 31 "Solid server configuration window" (page 40). Press **Enter** to continue.

Figure 31
Solid server configuration window



8 In the Solid server configuration screen, use the arrow keys to navigate. Press the space bar to select the Solid server to install, as shown in Figure 32 "Solid server configuration window" (page 41).

Figure 32
Solid server configuration window

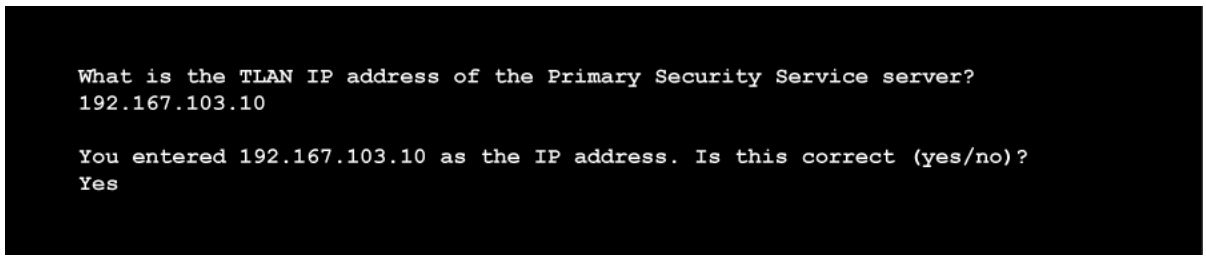


Press **Enter** to continue.

9 The Solid server configuration confirmation screen appears. Use the arrow keys to confirm the server selection by selecting **Yes**, or return to the Solid server configuration window by selecting **No**. Press **Enter** to continue.

10 The **Primary Security Service server TLAN IP address** screen appears as shown in Figure 33 "Primary Security Service server TLAN IP address window" (page 41). Enter the IP address of the TLAN network interface Primary Security Service server. Type **yes** to confirm the TLAN IP address is correct.

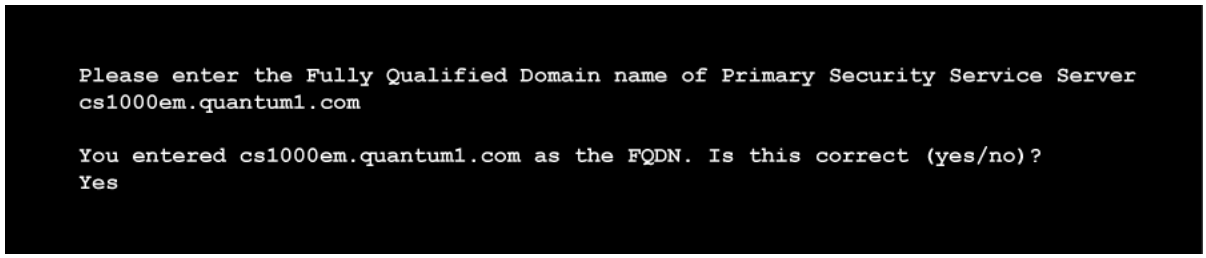
Figure 33
Primary Security Service server TLAN IP address window



11 The **Primary Security Service server Fully Qualified Domain Name (FQDN)** appears as shown in Figure 34 "Primary Security Service server Fully Qualified Domain name window" (page 42).

Enter the Fully Qualified Domain name of the Primary Security Service server. Type **Yes** to confirm the FQDN is correct.

Figure 34
Primary Security Service server Fully Qualified Domain name window



Note:

- The Primary Security Service must be up and running at this point.
- You need to know the password for the "nortel" account on the Primary Security Service server. Installation will fail if you do not know this password.

12 The **Primary Security Service fingerprint** screen appears as shown in Figure 35 "Primary Security Service fingerprint window" (page 42). Type **Yes** to verify the Primary Security Service fingerprint.

Figure 35
Primary Security Service fingerprint window

13 The "nortel" password screen appears. Type the password of the "nortel" account and press enter. The connection to the Primary Security Service server is complete.

The installation will then complete. This will take approximately 30 minutes. When completed the disk will be ejected automatically from the drive and a summary of the installation will be shown.

For detailed information on NRS, refer to *Network Routing Service Installation and Commissioning (NN43001-564)*.

—End—

Install the Network Routing Service

Step	Action
1	Log on to the server using the nortel account.
2	Insert the NRS CD-ROM in the CD-ROM tray.
3	Enter the command **appinstall**
4	At the prompt, enter the root account password. The system then prompts you to check the media.
5	Enter **Y** to check the media, or **N** to proceed without checking the media, and press **Enter**.
6	The **Application installation** screen appears, as shown in "Application Installation window" (page 43). From the **Application installation** window, select 3 to install the Network Routing Service. The appropriate packages will be installed to the hard drive.

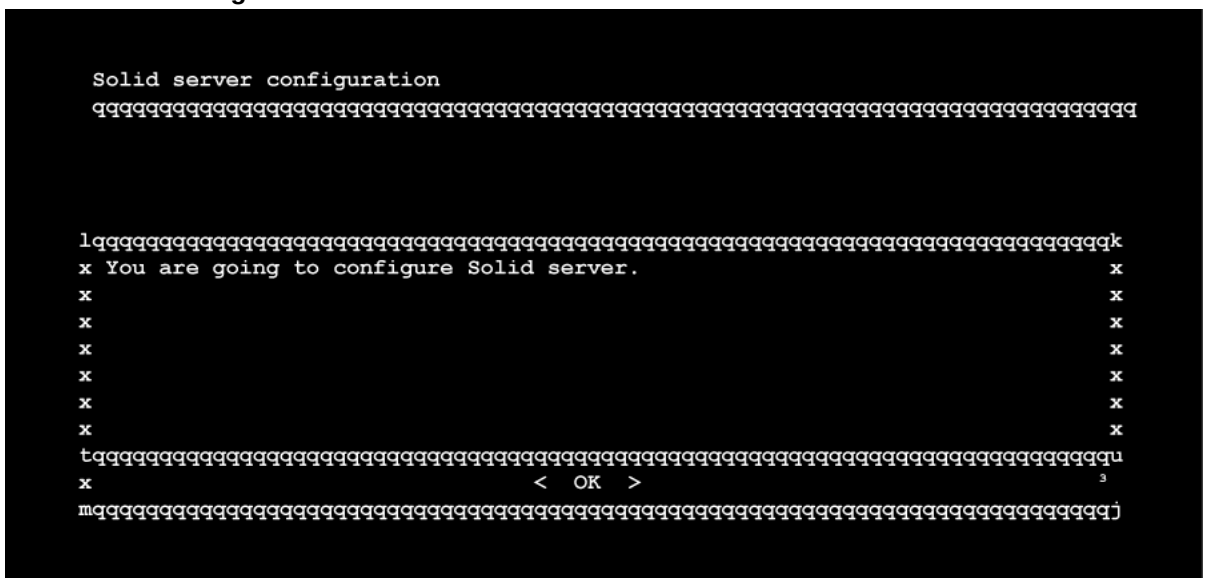
Application Installation window

```
 ##########################################################################
 #                        Installation stage                              #
 ##########################################################################

Nortel Enterprise Common Manager (ECM)
Network Routing Service (NRS) installation
This server will function as:
1. The Primary ECM Server (install NRS and the primary ECM security service)
2. A Backup ECM Server (install NRS and a backup ECM security service)
3. A Member Server (install NRS with ECM joining an existing secure network)
Please select the supported configuration # to install (q for exit):
```

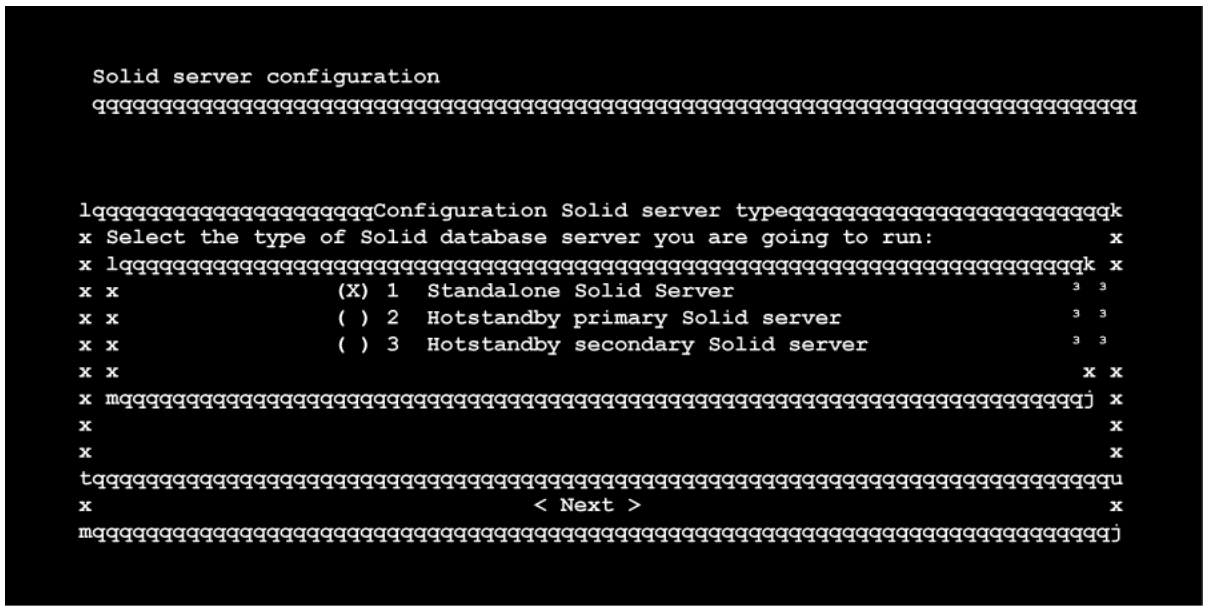
7	The Solid server window appears, as shown in Figure 36 "Solid server configuration window" (page 44). Press **Enter** to continue.

Figure 36
Solid server configuration window



8 In the Solid server configuration screen, use the arrow keys to navigate. Press the space bar to select the Solid server to install, as shown in Figure 37 "Solid server configuration window" (page 44).

Figure 37
Solid server configuration window



Press **Enter** to continue.

9 The Solid server configuration confirmation screen appears. Use the arrow keys to confirm the server selection by selecting **Yes**, or return to the Solid server configuration window by selecting **No**. Press **Enter** to continue.

10 The **Primary Security Service server TLAN IP address** screen appears as shown in Figure 38 "Primary Security Service server TLAN IP address window" (page 45). Enter the IP address of the TLAN network interface Primary Security Service server. Type **yes** to confirm the TLAN IP address is correct.

Figure 38
Primary Security Service server TLAN IP address window

```
What is the TLAN IP address of the Primary Security Service server?
192.167.103.10

You entered 192.167.103.10 as the IP address. Is this correct (yes/no)?
Yes
```

11 The **Primary Security Service server Fully Qualified Domain Name (FQDN)** appears as shown in Figure 39 "Primary Security Service server Fully Qualified Domain name window" (page 45). Enter the Fully Qualified Domain name of the Primary Security Service server. Type **Yes** to confirm the FQDN is correct.

Figure 39
Primary Security Service server Fully Qualified Domain name window

```
Please enter the Fully Qualified Domain name of Primary Security Service Server
cs1000em.quantum1.com

You entered cs1000em.quantum1.com as the FQDN. Is this correct (yes/no)?
Yes
```

Note:

- The Primary Security Service must be up and running at this point.
- You need to know the password for the "nortel" account on the Primary Security Service server. Installation will fail if you do not know this password.

12 The **Primary Security Service fingerprint** screen appears as shown in Figure 40 "Primary Security Service fingerprint window"

(page 46). Type **Yes** to verify the Primary Security Service fingerprint.

Figure 40
Primary Security Service fingerprint window

13 The "nortel" password screen appears. Type the password of the "nortel" account and press enter. The connection to the Primary Security Service server is complete.

The installation will then complete. This will take approximately 30 minutes. When completed the disk will be ejected automatically from the drive and a summary of the installation will be shown.

For detailed information on NRS, refer to *Network Routing Service Installation and Commissioning (NN43001-564)*.

—End—

Install the Element Manager applications

Use this procedure to run the application CD-ROM when the reboot is complete for the Linux base install.

Install the Primary Security Service and Element Manager

Step	Action
1	Log on to the server using the nortel account.
2	Insert the MGMT CD-ROM in the CD-ROM tray.
3	Enter the command **`appinstall`**
4	At the prompt, enter the root account password. The system then prompts you to check the media.
5	Enter **Y** to check the media, or **N** to proceed without checking the media, and press **Enter**.

6 The **Application Installation** screen appears, as shown in "Application Installation window" (page 47). From the **Application installation** window select 1 to install the Primary Security Service with Element Manager. The appropriate packages will be installed to the hard drive.

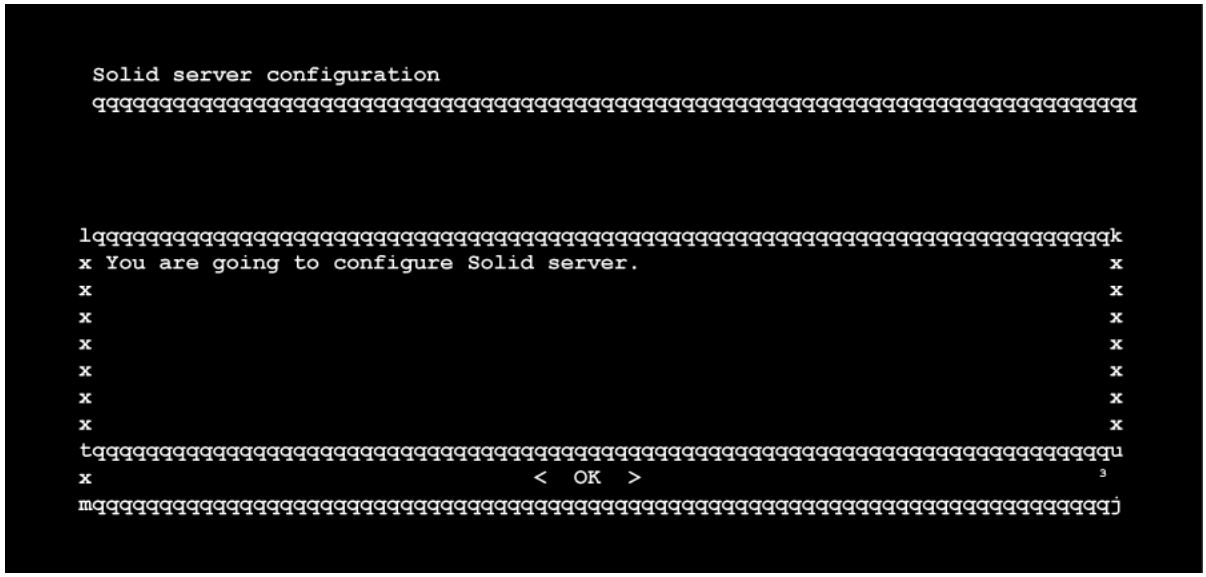
Application Installation window

```
 ##############################################################################
 #                          Installation stage                                #
 ##############################################################################

Nortel Enterprise Common Manager (ECM)
CS1000 Element Manager (EM) installation
This server will function as:
1. The Primary ECM Server (install EM and the primary ECM security service)
2. A Backup ECM Server (install EM and a backup ECM security service)
3. A Member Server (install EM with ECM joining an existing secure network)
Please select the supported configuration # to install (q for exit):
```

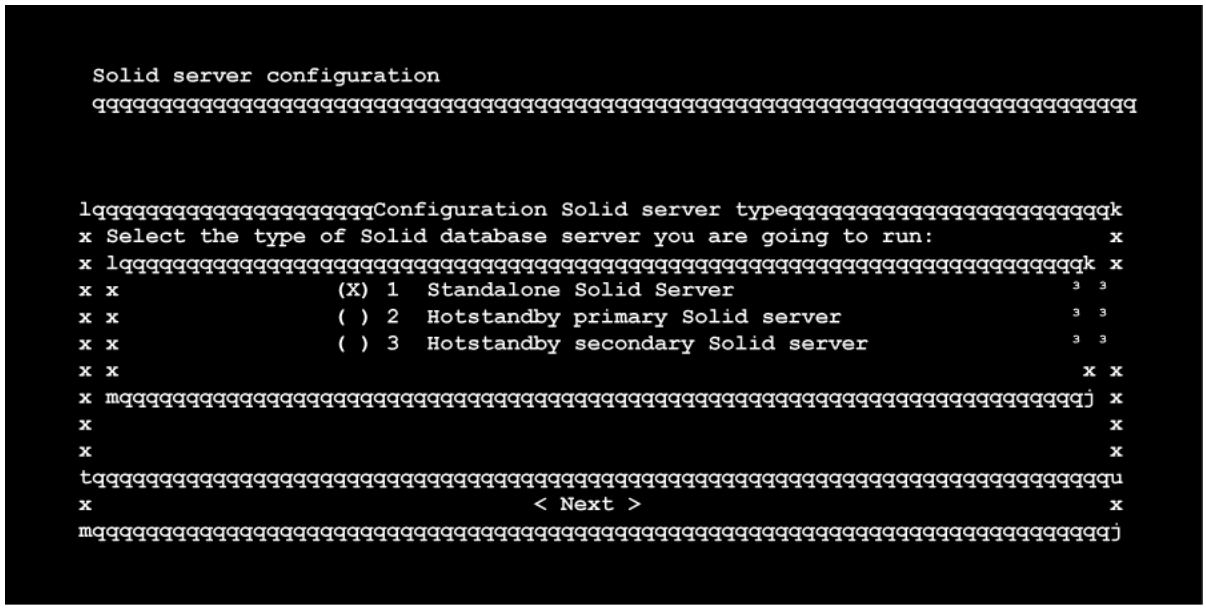
7 The Solid server window appears, as shown in Figure 41 "Solid server configuration window" (page 47). Press **Enter** to continue.

Figure 41
Solid server configuration window



8 In the Solid server configuration screen, use the arrow keys to navigate. Press the space bar to select the Solid server to install, as shown in Figure 42 "Solid server configuration window" (page 48).

Figure 42
Solid server configuration window



Press **Enter** to continue.

9 The Solid server configuration confirmation screen appears. Use the arrow keys to confirm the server selection by selecting **Yes**, or return to the Solid server configuration window by selecting **No**. Press **Enter** to continue.

10 The Private CA certificate window appears as shown in Figure 43 "Private CA certificate window" (page 49). At the prompts, enter the **Country**, **State or Province**, **Location**, **Organization Name** and **Organization Unit** and press **Enter** to continue.

Figure 43
Private CA certificate window

```
**********************************************************************
Information for the Private CA Certificate

The following information is required and can not be omitted.

     Country (2-letter code)
     State or Province (full name)
     Locality (usually city)
     Organization Name
     Organization Unit (division)

Note: The 'Common Name' information will be filled in automatically by
using your server's FQDN.

Press Enter to proceed.
**********************************************************************
```

11 The **Private CA Certificate confirmation window** appears as shown in Private CA Certificate confirmation window. Verify that the common name information is correct. Type **yes** if correct or **no** if incorrect, and then press **Enter**. If you entered yes, the installation finishes and the system creates the CA certificate, as shown in Figure 45 "Making a Private CA certificate window" (page 50). If you selected no, edit the information as required and repeat the step.

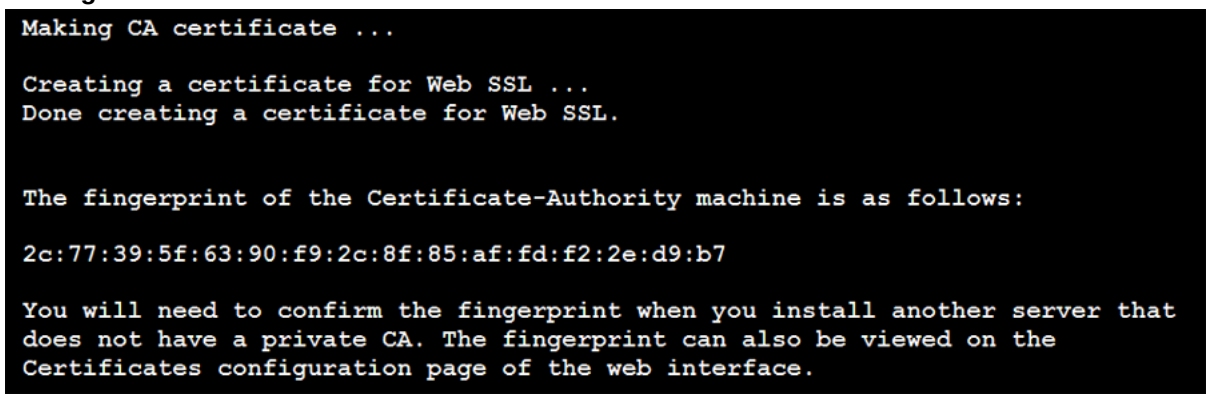
Figure 44
Private CA Certificate confirmation window

```
 Please confirm the Distinguished Name information:

Country (2-letter code):                    CA
Country Full Name:                          CANADA
State or Province (full name):              New Brunswick
Locality (usually city):                    Saint John
Organization Name:                          Innovatia
Organization Unit (division):               T5 Lab
Common Name (your server's FQDN):           cs1000em.quantum1.com

Is the information correct (yes/no)?
yes
```

Figure 45
Making a Private CA certificate window



The installation will then complete. This will take approximately 30 minutes. When completed the disk will be ejected automatically from the drive and a summary of the installation will be shown.

For detailed information on Element Manager, refer to *Element Manager System Reference - Administration (NN43001-632)*.

—End—

Install the Backup Security Service and Element Manager

Step	Action
1	Log on to the server using the nortel account.
2	Insert the MGMT CD-ROM in the CD-ROM tray.
3	Enter the command **`appinstall`**
4	At the prompt, enter the root account password. The system then prompts you to check the media.
5	Enter **Y** to check the media, or **N** to proceed without checking the media, and press **Enter**.
6	The **Application Install** screen appears, as shown in "Application Installation window" (page 51). From the **Application installation** window select 2 to install the Backup Security Service with Element Manager. The appropriate packages will be installed to the hard drive.

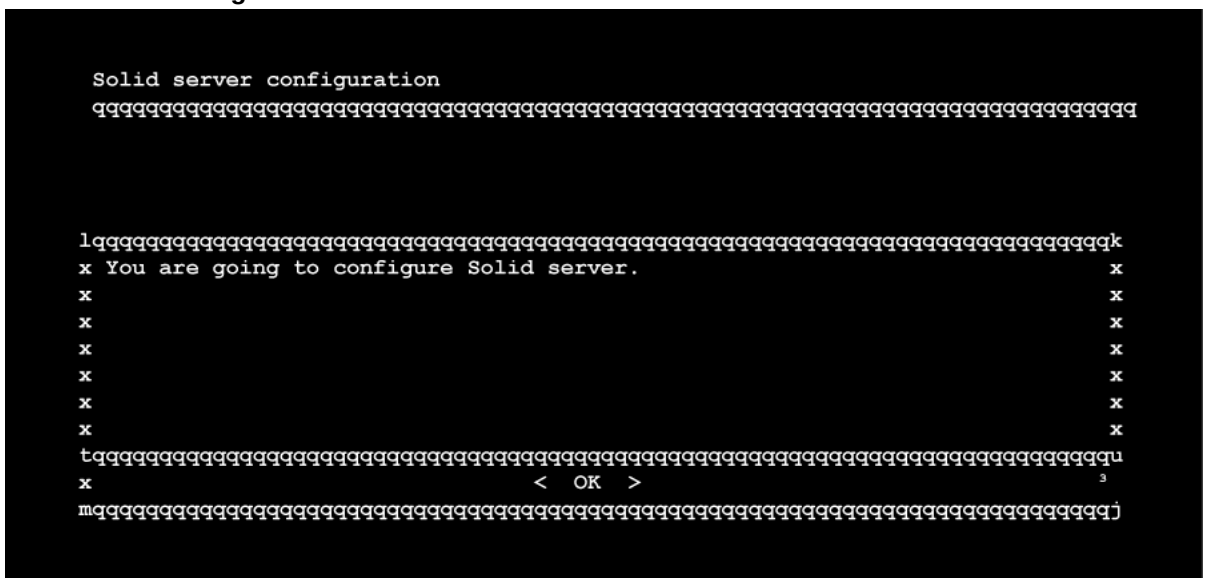
Application Installation window

```
 ########################################################################
 #                          Installation stage                          #
 ########################################################################

Nortel Enterprise Common Manager (ECM)
CS1000 Element Manager (EM) installation
This server will function as:
1. The Primary ECM Server (install EM and the primary ECM security service)
2. A Backup ECM Server (install EM and a backup ECM security service)
3. A Member Server (install EM with ECM joining an existing secure network)
Please select the supported configuration # to install (q for exit):
```

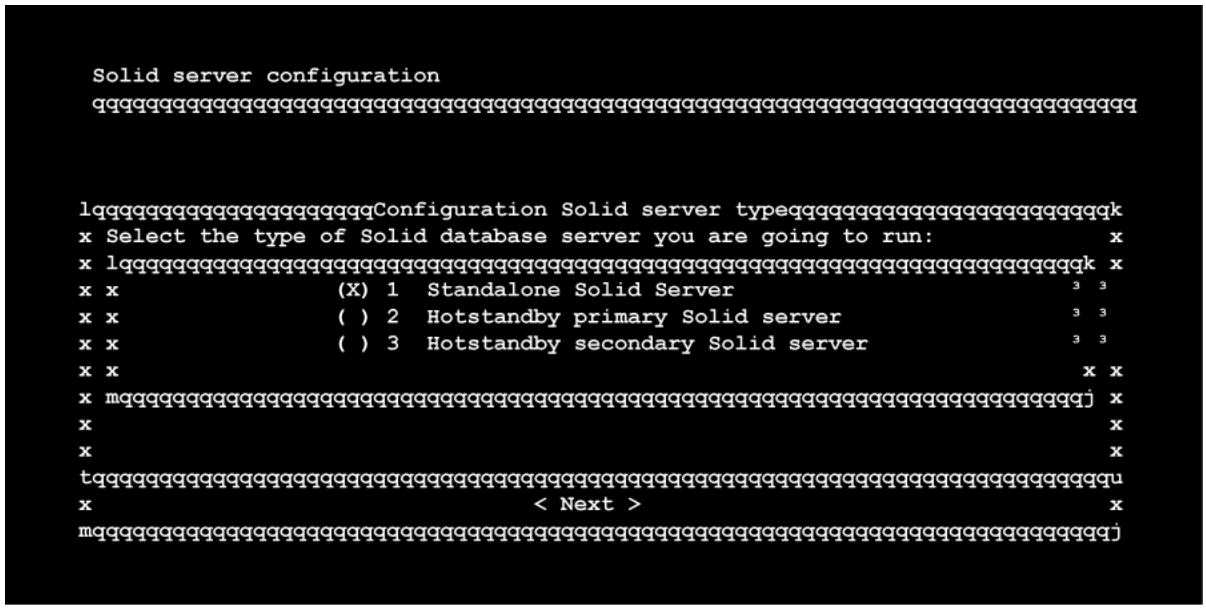
7 The Solid server window appears, as shown in Figure 46 "Solid server configuration window" (page 51). Press **Enter** to continue.

Figure 46
Solid server configuration window



8 In the Solid server configuration screen, use the arrow keys to navigate. Press the space bar to select the Solid server to install, as shown in Figure 47 "Solid server configuration window" (page 52).

Figure 47
Solid server configuration window

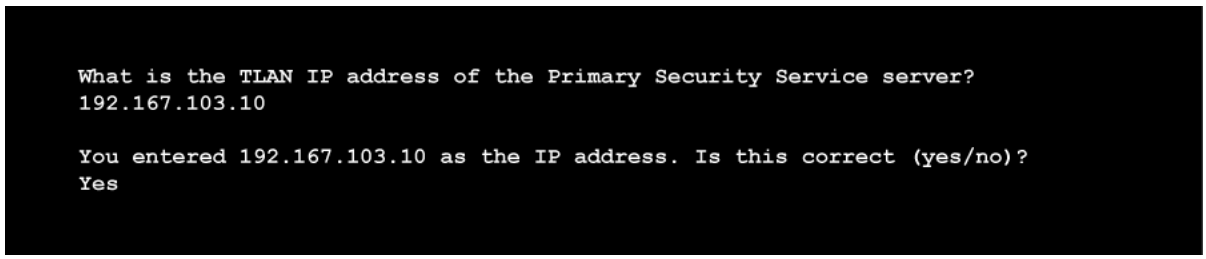


Press **Enter** to continue.

9 The Solid server configuration confirmation screen appears. Use the arrow keys to confirm the server selection by selecting **Yes**, or return to the Solid server configuration window by selecting **No**. Press **Enter** to continue.

10 The **Primary Security Service server TLAN IP address** screen appears as shown in Figure 48 "Primary Security Service server TLAN IP address window" (page 52). Enter the IP address of the TLAN network interface Primary Security Service server. Type **yes** to confirm the TLAN IP address is correct.

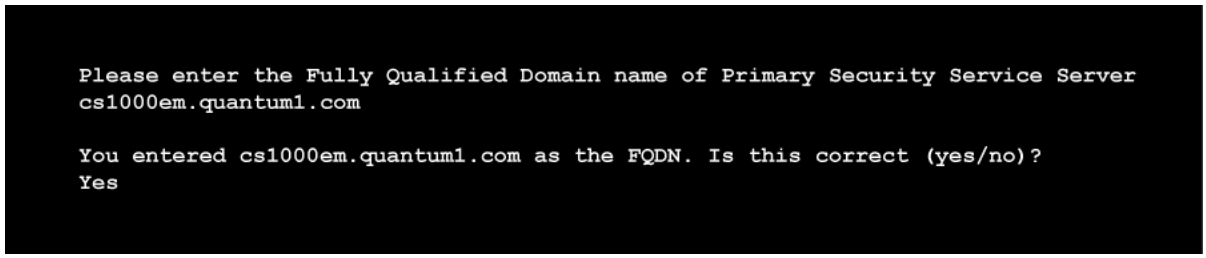
Figure 48
Primary Security Service server TLAN IP address window



11 The **Primary Security Service server Fully Qualified Domain Name (FQDN)** appears as shown in Figure 49 "Primary Security Service server Fully Qualified Domain name window" (page 53).

Enter the Fully Qualified Domain name of the Primary Security Service server. Type **Yes** to confirm the FQDN is correct.

Figure 49
Primary Security Service server Fully Qualified Domain name window



Note:

- The Primary Security Service must be up and running at this point.
- You need to know the password for the "nortel" account on the Primary Security Service server. Installation will fail if you do not know this password.

12 The **Primary Security Service fingerprint** screen appears as shown in Figure 50 "Primary Security Service fingerprint window" (page 53). Type **Yes** to verify the Primary Security Service fingerprint.

Figure 50
Primary Security Service fingerprint window

13 The "nortel" password screen appears. Type the password of the "nortel" account and press enter. The connection to the Primary Security Service server is complete and the installation finishes.

The installation will then complete. This will take approximately 30 minutes. When completed the disk will be ejected automatically from the drive and a summary of the installation will be shown.

For detailed information on Element Manager, refer to *Element Manager System Reference - Administration (NN43001-632)*.

—End—

Install the Element Manager

Step	Action
1	Log on to the server using the nortel account.
2	Insert the MGMT CD-ROM in the CD-ROM tray.
3	Enter the command **appinstall**
4	At the prompt, enter the root account password. The system then prompts you to check the media.
5	Enter **Y** to check the media, or **N** to proceed without checking the media, and press **Enter**.
6	The **Application installation** screen appears, as shown in "Application Installation window" (page 54). From the **Application installation** window, select 3 to install the Element Manager. The appropriate packages will be installed to the hard drive.

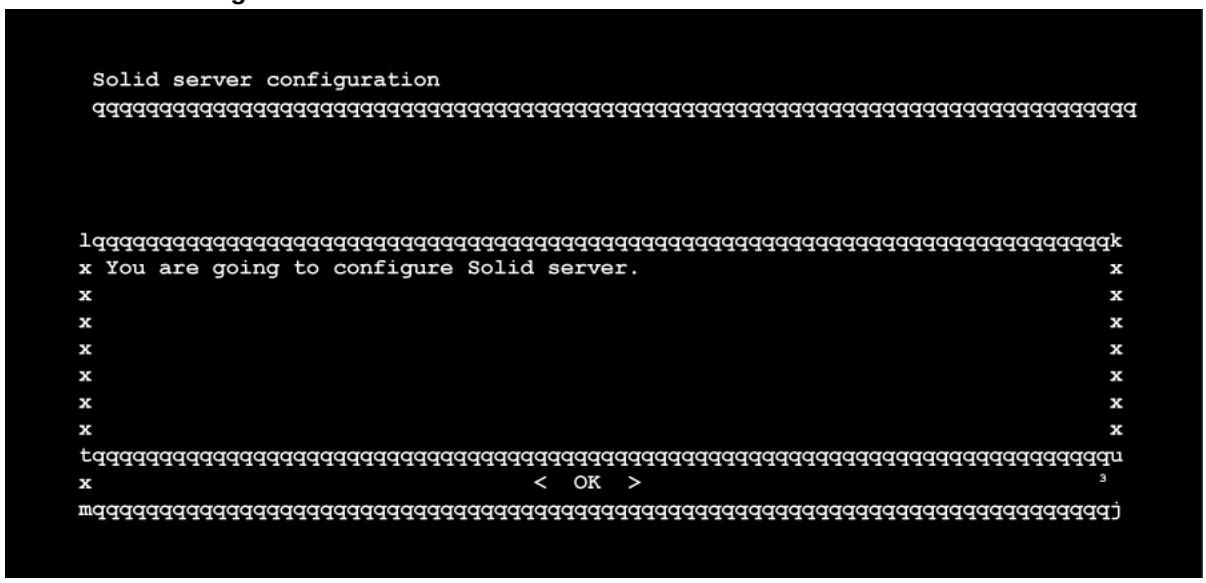
Application Installation window

```
 ########################################################################
 #                        Installation stage                            #
 ########################################################################

Nortel Enterprise Common Manager (ECM)
CS1000 Element Manager (EM) installation
This server will function as:
1. The Primary ECM Server (install EM and the primary ECM security service)
2. A Backup ECM Server (install EM and a backup ECM security service)
3. A Member Server (install EM with ECM joining an existing secure network)
Please select the supported configuration # to install (q for exit):
```

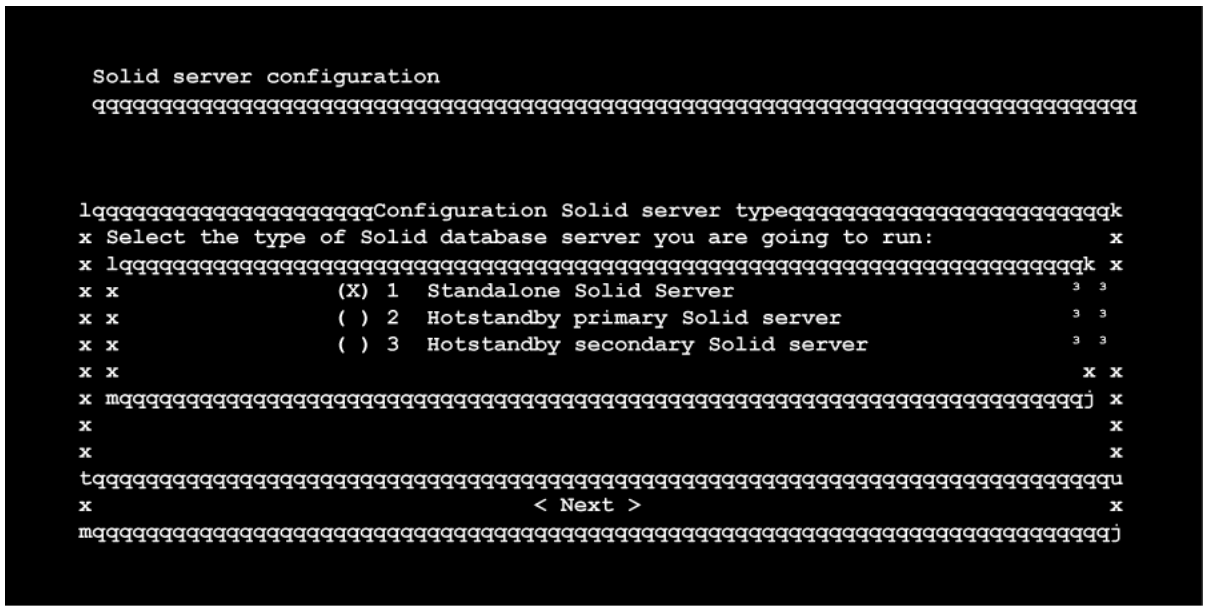
7	The Solid server window appears, as shown in Figure 51 "Solid server configuration window" (page 55). Press **Enter** to continue.

Figure 51
Solid server configuration window



8 In the Solid server configuration screen, use the arrow keys to navigate. Press the space bar to select the Solid server to install, as shown in Figure 52 "Solid server configuration window" (page 55).

Figure 52
Solid server configuration window

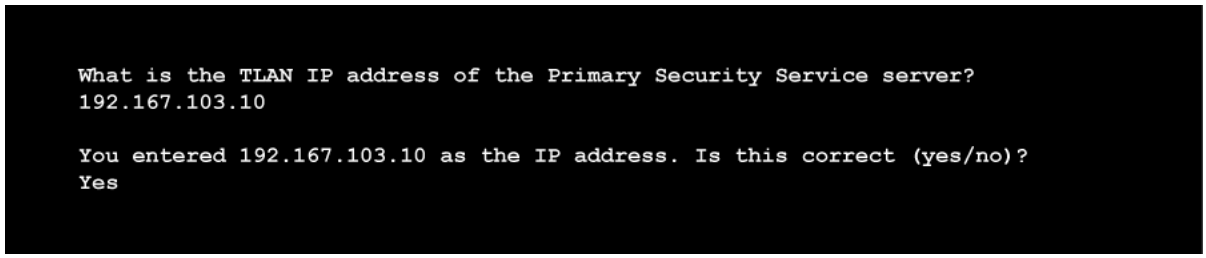


Press **Enter** to continue.

9 The Solid server configuration confirmation screen appears. Use the arrow keys to confirm the server selection by selecting **Yes**, or return to the Solid server configuration window by selecting **No**. Press **Enter** to continue.

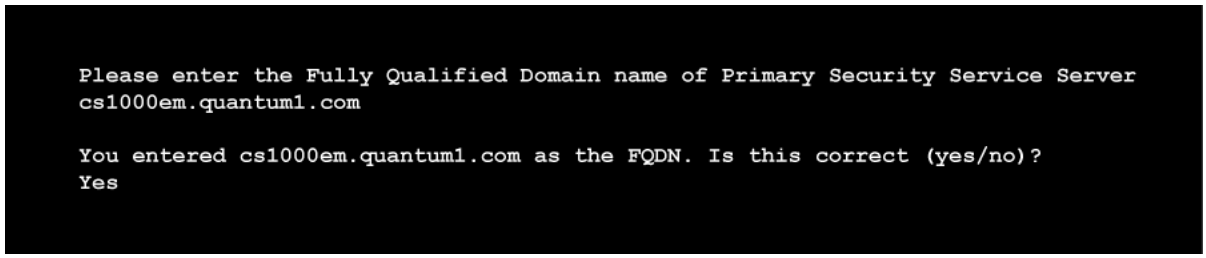
10 The **Primary Security Service server TLAN IP address** screen appears as shown in Figure 53 "Primary Security Service server TLAN IP address window" (page 56). Enter the IP address of the TLAN network interface Primary Security Service server. Type **yes** to confirm the TLAN IP address is correct.

Figure 53
Primary Security Service server TLAN IP address window



11 The **Primary Security Service server Fully Qualified Domain Name (FQDN)** appears as shown in Figure 54 "Primary Security Service server Fully Qualified Domain name window" (page 56). Enter the Fully Qualified Domain name of the Primary Security Service server. Type **Yes** to confirm the FQDN is correct.

Figure 54
Primary Security Service server Fully Qualified Domain name window



Note:

- The Primary Security Service must be up and running at this point.
- You need to know the password for the "nortel" account on the Primary Security Service server. Installation will fail if you do not know this password.

12 The **Primary Security Service fingerprint** screen appears as shown in Figure 55 "Primary Security Service fingerprint window"

(page 57). Type **Yes** to verify the Primary Security Service fingerprint.

Figure 55
Primary Security Service fingerprint window

13 The "nortel" password screen appears. Type the password of the "nortel" account and press enter. The connection to the Primary Security Service server is complete and the installation finishes.

The installation will then complete. This will take approximately 30 minutes. When completed the disk will be ejected automatically from the drive and a summary of the installation will be shown.

For detailed information on Element Manager, refer to *Element Manager System Reference - Administration (NN43001-632)*.

—End—

Configuration for Network Routing Service or Element Manager applications in ECM

The Network Routing Service or Element Manager applications must be configured in ECM after they are installed. For details on configuration and security certificate creation refer to Security Management Fundamentals (NN43001-604).

CS 1000 on Linux base

Linux Operating System and Distribution

The selected distribution is Red Hat Enterprise Linux ES 4. This distribution is built on a 2.6 kernel, and supports many Open Source Development Lab (OSDL) Carrier Grade Linux (CGL) features.

Red Hat Enterprise Linux ES 4 supports Linux kernel version 2.6 and the following for the Enterprise Common Manager (ECM) and the Network Routing Service (NRS) :

- Secure Internet Protocol (IPSec)
- Sun JVM 1.4.x
- Radvision Session Initiation Protocol (SIP) stack
- OpenSSL
- OpenSSH
- Perl
- Zlib
- (S)FTP server
- SNMPv3
- A Web application server with support for the following technologies :
  - HTTP Server (HTML, CGI)
  - Web Container (Servlet, JSP,JSF)
  - J2EE Container (EJB)
  - Portal Container (Portlet)
  - Web Services/Simple Object Access Protocol (SOAP) (for example, JBoss with appropriate optional packages)

Network and firewall

A network firewall is enabled on the server and 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 its subnet. The Linux application selects the Ethernet port to be used. The firewall protects both ports.
For a listing of Linux base open firewall ports, refer to Table 1 "Linux base open firewall ports" (page 60).

Table 1
Linux base open firewall ports

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

Note: The port numbers found in Table 1 "Linux base open firewall ports" (page 60) apply only to the Linux base. Linux applications can require different ports. Refer to the appropriate application NTP for a list of ports opened for the application.

Software reliability

Software monitoring

MONIT is an open source package used for monitoring the important daemon services automatically initiated at startup. If a malfunction occurs, MONIT provides actions such as alert, start, stop, and restart. In order to provide these actions, applications must be registered with MONIT, and the appropriate actions for each application must be specified.

Hardware watchdog

The IBM x306m, and HP DL320 G4 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 is based on current ISP1100 server, which is five minutes.

The server is reset if the watchdog timer is not reset within the allotted time. The operating system and applications are reloaded from disk and started when 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

The following features enhance Linux base security.

Virus protection

If anti Virus software is installed by the customer the following is recommended:

- Choose software that uses 100 megabytes (MB) or less of hard-drive space.
- Choose software that uses 84 MB or less of RAM.
- Always set the process priority to low.
- Perform virus scans during off-hours only.
- Choose software that is capable of removing or cleaning the viruses, as well as sending warning messages.
- Choose software that uses a maximum of 10% of CPU for a scheduled scan and 3% for an active scan.

BIOS setting and password protection

To secure the server, Nortel recommends the following:

- Disable boot from CD or DVD drive in the Basic Input Output System (BIOS).
- Add a BIOS password.
- Add a boot loader password.

Removal of the Ctrl+Atl+Del keyboard shutdown command

The Ctrl+Alt+Del shutdown command is disabled.

Single-user-text-mode booting is disabled

This booting mode is disabled to prevent the unauthorized access of the system.

Hardened communications by using secure protocols

Secure Shell (SSH) and its accompanying tools are included by default. As shown in the following table, “Security communication protocols”, these secure protocols are also a replacement for some insecure protocols.

Table 2
Security communication protocols

Insecure protocols (disabled)	Replacement secure protocols (supported)
telnet	ssh
rsh	ssh
rlogin	ssh
tftp	sftp
ftp	sftp
rcp	scp

Note: If SFTP or SCP is not available to the user, File Transfer Protocol (FTP) can be used. FTP can be accessed by invoking the CLI command **`ftpenable`**, and closed by invoking the CLI command **`ftpdisable`**. The **`ftpenable`** command opens a timed window that will close after five minutes of inactivity.

Patching

Linux base supports two patch categories:

- **Patch**: This category of patch changes program behavior for a period of time. You can use it for such things as fixing bugs or for diagnostic purposes. In some instances, you can apply this category of patch without a program restart.

- **Service Update**: A service update is a cumulative update of patches. A service update is a full application RPM package distribution that contains all patches that were applied to a specific application, and overwrites any previous service updates.

In-service patching is a CS 1000 feature that you can use to modify operating programs without restarting the program process. In-service patching has the following components:

- A target management system that supports:
  - Patch persistence.
  - Patch loading during application startup (retention).
  - Patch activation (in-service, out-service).
- Target patch mechanisms:
  - Java Archive patch (JAR) and Web Application Archive patch (WAR) file replacement.
  - Vulnerability updates.

An overview of the patching operation is provided in "Patching Operation" (page 63).

Patching Operation

Step	Action
1	Retrieve a (pxxxxxxx).el4 file from the Nortel 9.1.1 Meridian PEP Library (MPL).
2	Upload the patch file to the Linux server and save it in the /var/opt/nortel/patch directory. Secure File Transfer Protocol (SFTP) and Secure Copy (SCP) are the supported methods of patch file transfer. Patch file transfer can be initiated from within the Linux server or from an external machine. • To initiate the patch file transfer from within the Linux server: — Login to the Linux server as nortel. — Enter the **`sftp`** or **`scp`** CLI command. — Type the **`get`** command (for **`sftp`**) or the **`scopy`** command (for **`scp`**) to transfer the patch to the Linux server. • To initiate the patch file transfer from an external machine:

— Initiate an SFTP or Secure Shell (SSH) program.

— Provide the Linux server's IP address (or host name), the nortel user ID, and password as parameters.

— Type the **`put`** command (for **`sftp`**) or the **`scopy`** command (for **`scp`**) to transfer the patch to the Linux server.

Note: If SFTP or SCP is not available to the user, File Transfer Protocol (FTP) can be used. FTP can be accessed by invoking the CLI command **`ftpenable`**, and closed by invoking the CLI command **`ftpdisable`**. The **`ftpenable`** command opens a timed window that will close after five minutes of inactivity.

3 Perform one or more of the following on-target patch management CLI commands:

- **`pload`**
- **`pins`**
- **`poos`**
- **`pout`**
- **`pstat`**

—End—

Target patcher CLI commands

The on-target patch management command line interface (CLI) provides an interface command set similar to the CS 1000 patcher. The following table lists target-side patching CLI commands.

Table 3
Target-side patching CLI commands

Command	Description
pload	Load a patch from a disk file and update the on-switch database with the specific patch information.
pins	Put a patch into service; the patch will be placed into service for all processes to which it applies.
poos	Remove a patch from service. The patch is removed from service from all processes in which it was in service.
pout	Unload a patch that was loaded with the pload command.

pstat	Print a status summary of all loaded patches.
plis	Print detailed information about a specific patch.

Note: The nortel user account is the designated user account for the execution of these CLI commands.

Patch retention

A patch is always retained until the poos CLI command explicitly puts the patch out of service.

Software exceptions

Linux kernel exceptions

If the Linux kernel encounters an unrecoverable error, it prints and logs a short description of the problem, and reboots. Typical causes of such errors are unrecoverable hardware errors or bugs in the kernel software.

A nonfatal kernel exceptions is reported through a log in the kernel, captured in the syslog. Kernel logs due to invalid memory addresses do not normally result in a kernel panic (crash); instead the process that triggered the fault is terminated. These can produce a lasting negative impact on the system. It is recommended that such events be monitored in user space (using the syslog mechanism), and that a full system reboot be triggered after receipt of any kernel log report.

User Accounts and Access Control

The management of user accounts and access control methods in Linux is performed using native Linux user account management, and tools such as Radius and PAM. There is a diagnostic group and some default diagnostic users defined for debugging and maintenance purposes.

Linux base includes the following accounts:

- root (as Linux default)

  Note: Root can only log in through the COM1 console. Logging in as root from the network is prohibited.

- sysadmin: The user account designated for debugging and maintenance. This account is intended for Nortel support.
- nortel: The user account for the basic Linux base operation, including patching and application installation. For a list of CLI commands that

can be invoked by nortel, refer to Appendix " Nortel Linux base CLI commands" (page 85).

Note 1: If you log in as root or nortel and your account is inactive for 15 minutes, you will automatically be logged out.

Note 2: A nortel or sysadmin user account (except root) that makes three successive incorrect login attempts will be locked for up to one hour.

Passwords

The following regulations govern the use of passwords:

Password Policy

- Change all system-level passwords (for example, application administration account passwords) at least once every three months.
- A new password must differ from the previous three passwords.

Password creation guidelines

Passwords must meet the following criteria:

- Passwords must contain both upper- and lower-case letters.
- In addition to letters, passwords must have numeric 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 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 is not allowed.
- You can change your password by using the **`passwd`** CLI command.

System upgrades

The platform supports upgrades for delivering new interim releases. 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.

Nortel Linux base uses the CLI upgrade command to reinstall or upgrade the base installation. The Linux base installation CD is inserted and the upgrade command is invoked. You are given the choice of backing up the data to a USB device, to an SFTP server, or to accept the default /admin partition. When reinstallation begins, you are given the option of using the data stored in the /admin partition or using data stored in a USB device or SFTP server. When the base installation is complete, applications can be installed from the application CD using the appinstall command.

Note: You must login as nortel to run the installation/upgrade process.

Logging

Linux base supports syslog as the standard event logger. Event logs are stored in application-specific folders in the /var/log/nortel directory.

SNMP

Linux base supports standard server type Management Information Base (MIB)II MIBs. Linux base does not generate SNMP alarms.

Disaster recovery

Hardware faults can occur that require disaster recovery. Recovery happens in two steps. First restore the Linux base (including operating system) and then restore the applications.

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

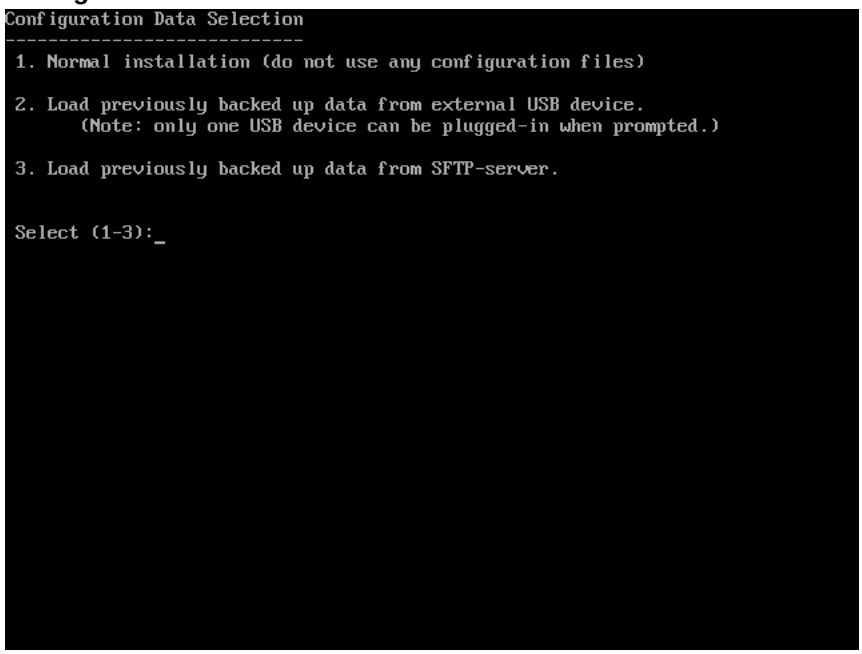
Base recovery

After a successful base installation, an operation occurs to back up pre-specified file systems (both executable binary and configuration data files) onto a USB or network Secure File Transfer Protocol (SFTP) storage device.

The installation media is also used as rescue media (CD/DVD for HP DL320 G4 and IBM x306m servers), which supports the recovery of the base system.

The following figure shows the base system recovery options:

Figure 56
Configuration Data Selection window



When a server boot-up with bootable installation media occurs, you can choose from the following options:

- Normal installation.
- Load recovery data from an external USB device.
- Load recovery data from a secure SFTP server that is accessible by ELAN.

Appendix A Passthrough end user license agreement

WARNING
Do not contact Red Hat for technical support on your Nortel version of the Linux base operating system. If technical support is required for the Nortel version of the Linux base operating system, 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 B
COTS Servers

The Linux base is installed on one of two commercial off-the-shelf (COTS) servers; the Hewlett Packard (HP) DL320-G4 1U server or the International Business Machines (IBM) X306m 1U server.

This appendix provides a brief description of each server,

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)
- 4 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 57
HP DL320 front view

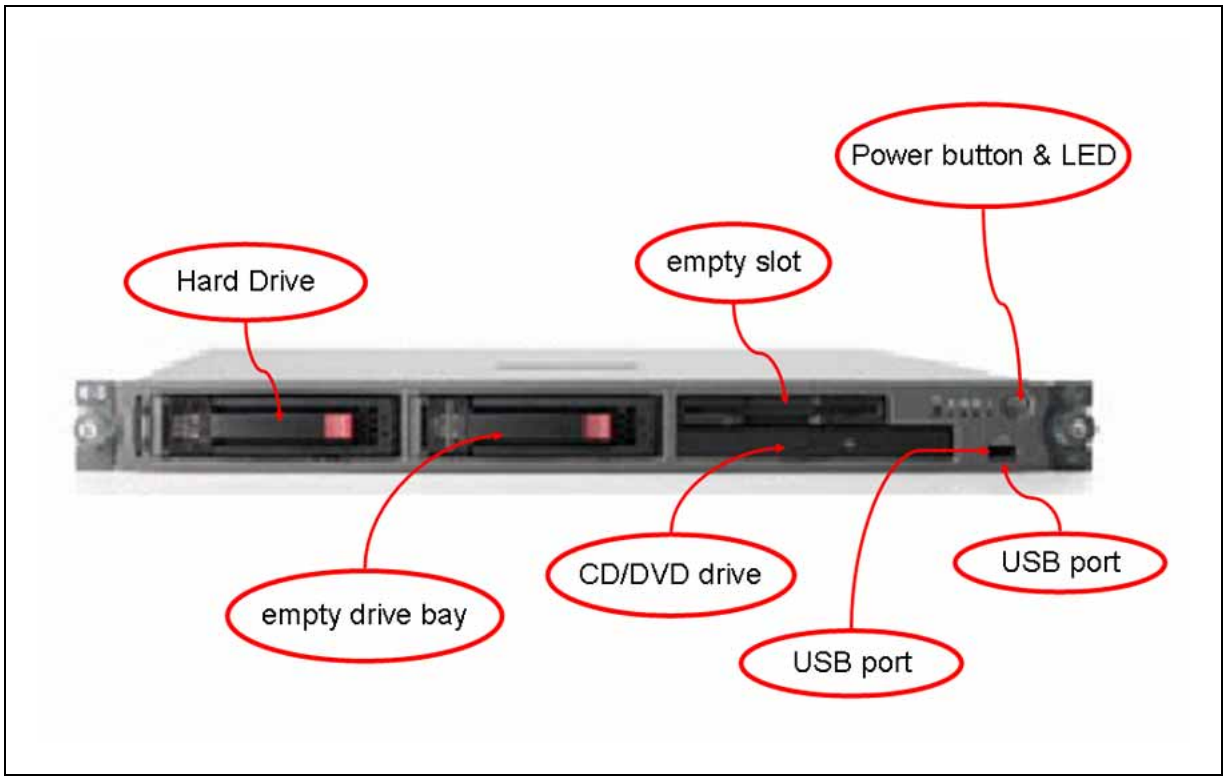
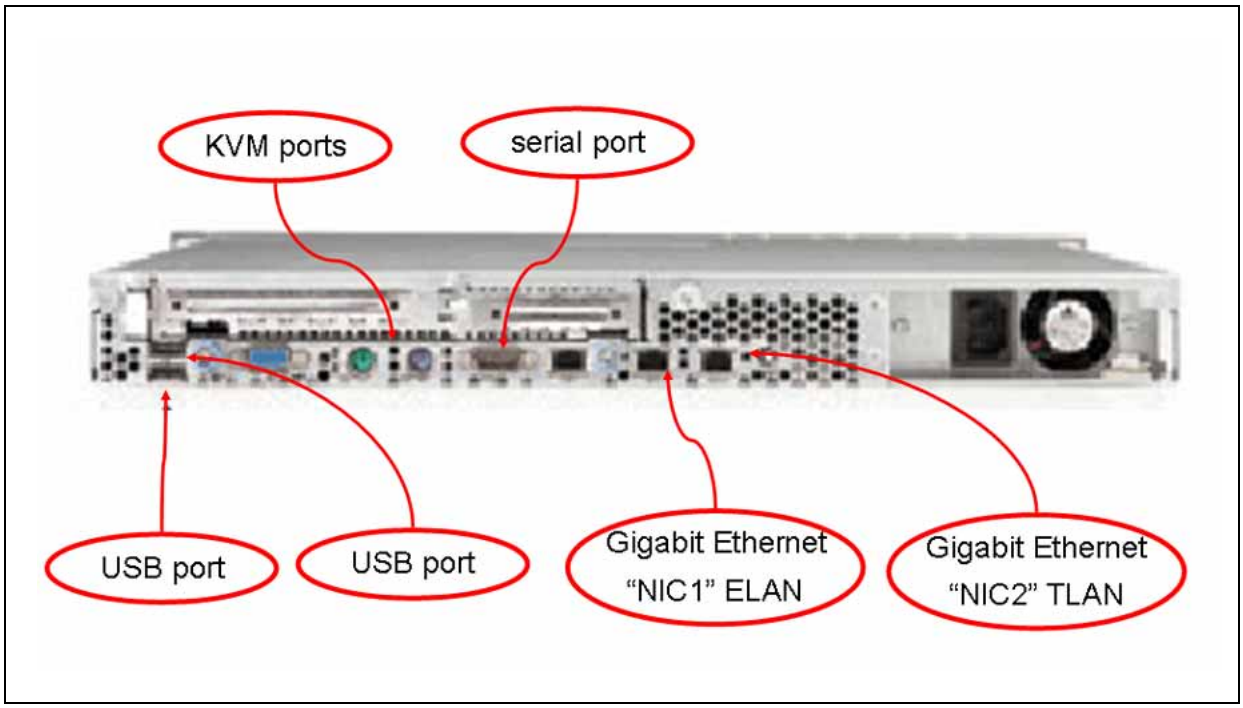


Figure 58
HP DL320 front view: LEDs

Table 4
HP DL320 LED item description and status

Item	Description	Status
1	UID button/LED (Unit Identification)	**Blue** - Identification is activated. **Flashing blue** - System is being remotely managed. **Off** - Identification is deactivated.
2	Internal health LED	**Green** - System health is normal. **Amber** - System is degraded. To identify the component, refer to system board LEDs. **Red** - Critical. To identify the component in a critical state, refer to 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 59
HP DL320 rear view



WARNING
The TLAN & ELAN port positions are reversed (L and R, 1 and 2) compared to the IBM X306m server.

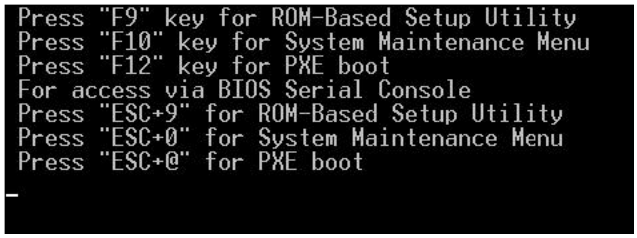
HP DL320 G4 BIOS settings

The HP DL320 G server shipped through Nortel has the correct BIOS settings. 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 servers have 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 Procedure 1 "Configure the COM1 serial port on an HP DL320-G4 server" (page 75) for instructions.
The HP DL320 G 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 2 "Change the baud rate on an HP DL320-G4 Signaling Server" (page 76) for instructions.

Procedure 1
Configure the COM1 serial port on an HP DL320-G4 server

Step	Action
1	Press the Power switch to boot the server. The server boots and the HP DL320-G4 boot screen appears.

Figure 60
HP DL320-G4 server boot screen

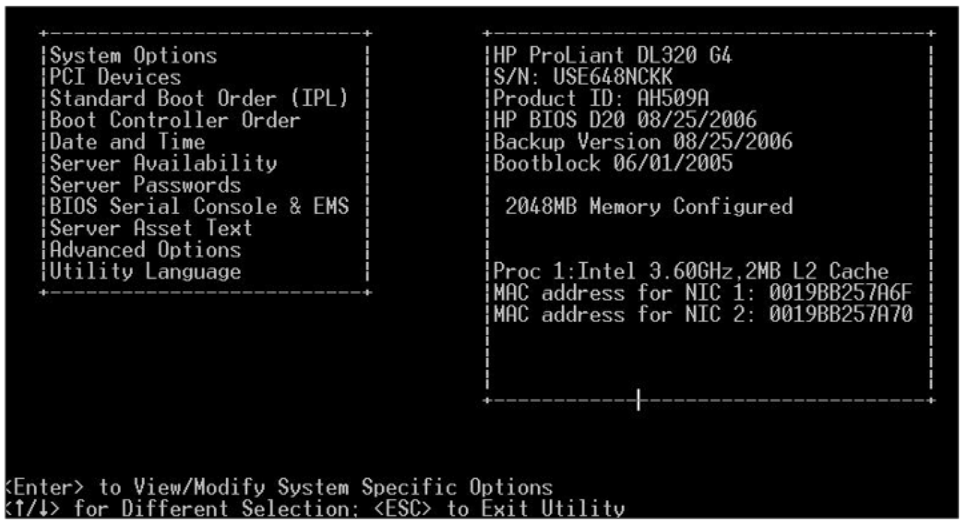


Note: If the server is already up and running, power the server off and on to reboot and receive the HP DL320-G4 boot screen.

2 Press **F9** to invoke the ROM-based Setup Utility (RBSU) menu screen.

The RBSU menu screen appears.

Figure 61
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 the user with four options:

- 1 | Auto
- 2 | Disabled
- 3 | COM 1
- 4 | COM 2

5 Navigate to the **COM 1** option and press **Enter**.

This configures the COM 1 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—

Procedure 2
Change the baud rate on an HP DL320-G4 Signaling Server

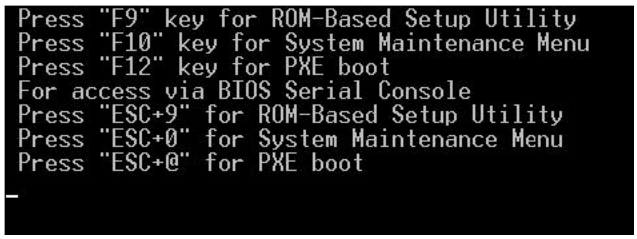
Step	Action

ATTENTION
The HP DL320 G 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 has been reset due to an error.

1 Press the Power switch to boot the server.

The server boots and the HP DL320-G4 boot screen appears.

Figure 62
HP DL320-G4 server boot screen



Note: If the server is already up and running, power the server off and on to reboot 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 63
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—

Refer to the Server Product Guide on the resource CD-ROM shipped with the HP DL320-G4 server for additional operating information.

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
  - — used 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 (Reset) button

Figure 64
IBM X306m front view

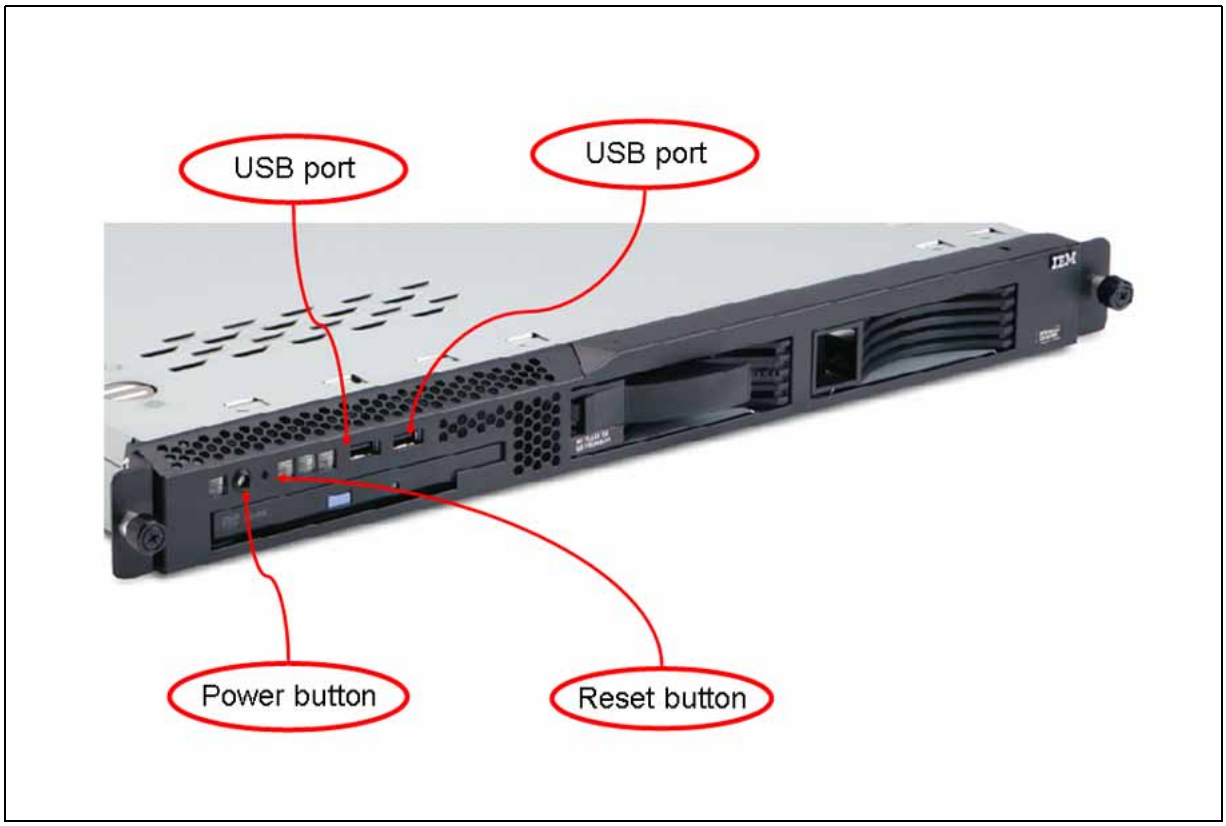


Figure 65
IBM X306m front view: LEDs

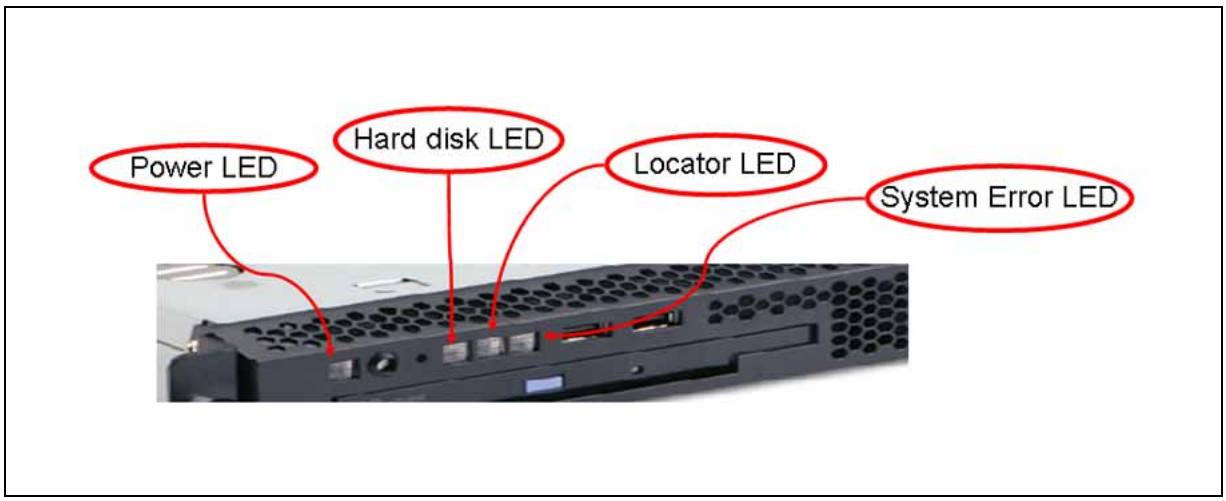
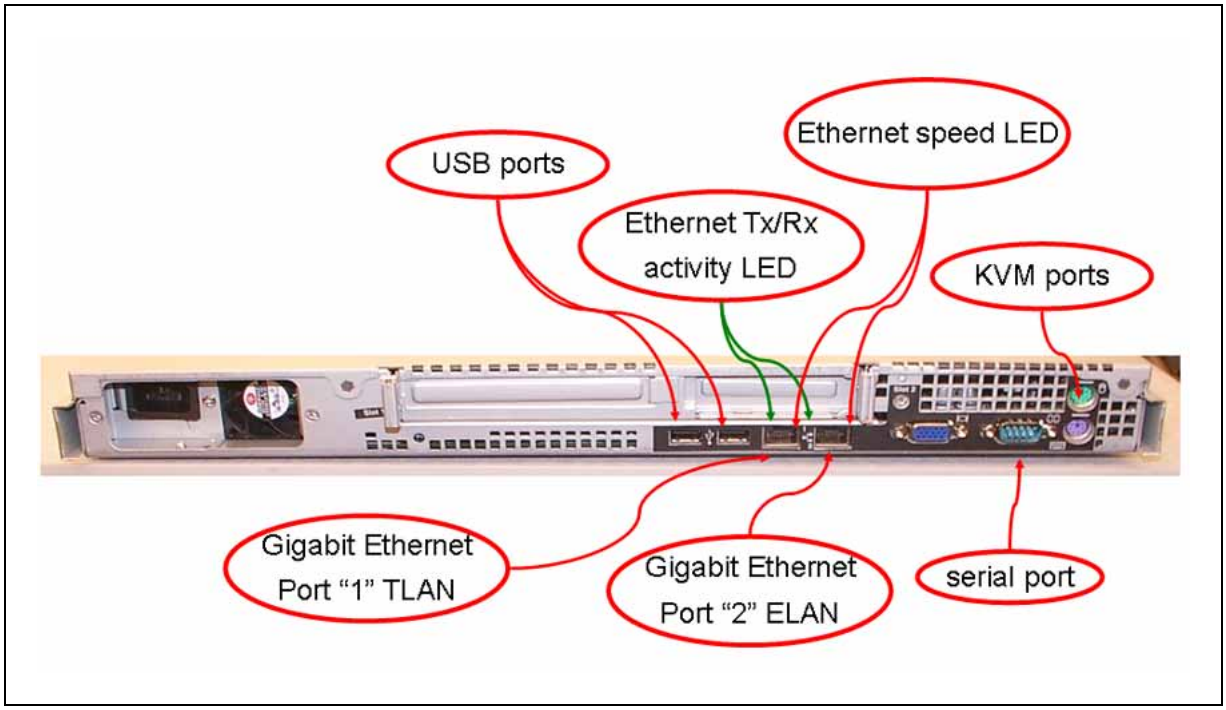


Table 5
IBM X306m LED description and status

Description	Status
Power LED	When this LED is lit, it indicates that the server is turned on. When this LED is off, it indicates that AC power is not present, or the power supply or the LED itself has failed.
Hard disk LED	When this LED is lit, it indicates that a hard disk drive is in use.
Locator LED	When this LED is lit, it has been lit remotely by the system administrator to aid in visually locating the server.
System Error LED	When this LED is lit, it indicates that a system error has occurred.

Figure 66
IBM X306m rear view



WARNING
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 IBM X306m server shipped through Nortel has the correct BIOS default settings. These settings can be viewed at Table 6 "IBM X306m default BIOS settings" (page 81).

Table 6
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
Start options - legacy USB support	Disabled

The IBM X306m server can have the default BIOS settings changed by a BIOS reset or other maintenance activity. To return the BIOS settings to the appropriate values, see Procedure 3 "Change the BIOS settings on an IBM X306m server" (page 81) for instructions.

Procedure 3
Change the BIOS settings on an IBM X306m server

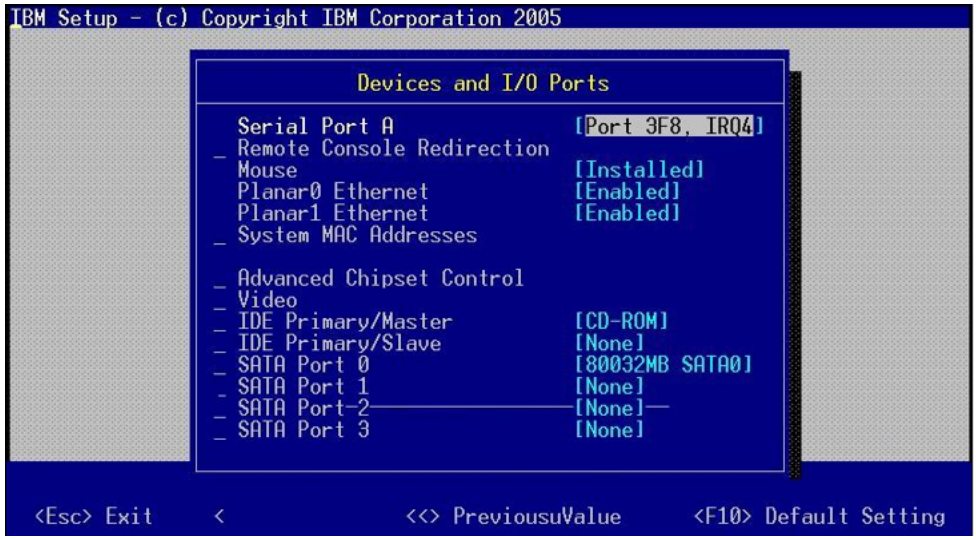
Step	Action
1	Press the Power switch to boot the server. The server boots and a **Press F1 for Configuration/Setup** message appears on the maintenance terminal. ***Note:*** If the server is already up and running, power the server off and on or press the reset button to reboot and receive the **Press 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 67
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.

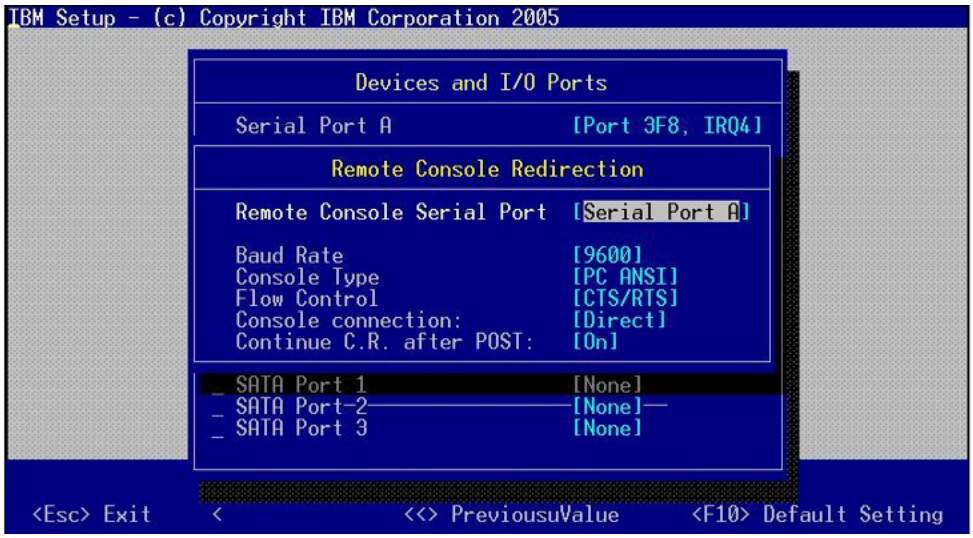
Figure 68
Devices and I/O Ports menu



4 Navigate to the **Remote Console Redirection** option and press **Enter**.

The Remote Console Redirection screen appears.

Figure 69
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 reboot automatically.

—End—

Refer to the Server Product Guide on the resource CD-ROM shipped with the IBM X306m server for additional operating information.

Appendix C
Nortel Linux base CLI commands

Nortel Linux Base uses the following Command Line Interface (CLI) commands.

Table 7
Nortel Linux base CLI commands

Command	Description
appinstall	Install Nortel applications.
appstart	Stop, start, or restart Nortel applications.
appVersionShow	Print the server's application software version.
baseparamsconfig	Configure base parameters.
baseVersionShow	Print the server's base software version.
datetimeconfig	Configure the date and time.
dnsconfig	Configure DNS values.
ftpdisable	Disable FTP.
ftpenable	Enable FTP.
ftpstatus	Show the current FTP status.
networkconfig	Configure network settings.
ntpconfig	Configure Network Time Protocol settings.
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.
swVersionShow	Print the server's software version.
sysbackup	Perform a system backup (both base and applications).

Command	Description
sysrestore	Perform a restore of the application data (backed up by sysbackup).
upgrade	Select the backup data source and reinstall Linux base.
reboot	Reboot the entire system.
passwd	Change the user's password.

Index

Nortel Communication Server 1000

Linux Platform Base and Applications Installation and Commissioning

Publication: NN43001-315
Document status: Standard
Document version: 01.01
Document date: 30 May 2007

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

Sourced in Canada.